INCIDENT PRIORITISATION FOR INTRUSION RESPONSE SYSTEMS

by

NOR BADRUL ANUAR JUMAAT

A thesis submitted to Plymouth University
in partial fulfilment for the degree of

DOCTOR OF PHILOSOPHY

School of Computing and Mathematics
Faculty of Science and Technology

February 2012

Abstract

Incident Prioritisation for Intrusion Response Systems

Nor Badrul Anuar Jumaat (B.Comp.Sc (Malaya), M.Comp.Sc (Malaya))

The landscape of security threats continues to evolve, with attacks becoming more serious and the number of vulnerabilities rising. To manage these threats, many security studies have been undertaken in recent years, mainly focusing on improving detection, prevention and response efficiency. Although there are security tools such as antivirus software and firewalls available to counter them, Intrusion Detection Systems and similar tools such as Intrusion Prevention Systems are still one of the most popular approaches. There are hundreds of published works related to intrusion detection that aim to increase the efficiency and reliability of detection, prevention and response systems. Whilst intrusion detection system technologies have advanced, there are still areas available to explore, particularly with respect to the process of selecting appropriate responses.

Supporting a variety of response options, such as proactive, reactive and passive responses, enables security analysts to select the most appropriate response in different contexts. In view of that, a methodical approach that identifies important incidents as opposed to trivial ones is first needed. However, with thousands of incidents identified every day, relying upon manual processes to identify their importance and urgency is complicated, difficult, error-prone and time-consuming, and so prioritising them automatically would help security analysts to focus only on the most critical ones. The existing approaches to incident prioritisation provide various ways to prioritise incidents, but less attention has been given to adopting them into an automated response system. Although some studies have realised the advantages of prioritisation, they released no further studies showing they had continued to investigate the effectiveness of the process.

This study concerns enhancing the incident prioritisation scheme to identify critical incidents based upon their criticality and urgency, in order to facilitate an autonomous mode for the response selection process in Intrusion Response Systems. To achieve this aim, this study proposed a novel framework which combines models and strategies identified from the comprehensive literature review. A model to estimate the level of risks of incidents is established, named the Risk Index Model (RIM). With different levels of risk, the Response Strategy Model (RSM) dynamically maps incidents into different types of response, with serious incidents being mapped to active responses in order to minimise their impact, while incidents with less impact have passive responses. The combination of these models provides a seamless way to map incidents automatically; however, it needs to be evaluated in terms of its effectiveness and performances. To demonstrate the results, an evaluation study with four stages was undertaken; these stages were a feasibility study of the RIM, comparison studies with industrial standards such as Common Vulnerabilities Scoring System (CVSS) and Snort, an examination of the effect of different strategies in the rating and ranking process, and a test of the effectiveness and performance of the Response Strategy Model (RSM). With promising results being gathered, a proof-of-concept study was conducted to demonstrate the framework using a live traffic network simulation with online assessment mode via the Security Incident Prioritisation Module (SIPM); this study was used to investigate its effectiveness and practicality.

Through the results gathered, this study has demonstrated that the prioritisation process can feasibly be used to facilitate the response selection process in Intrusion Response Systems. The main contribution of this study is to have proposed, designed, evaluated and simulated a framework to support the incident prioritisation process for Intrusion Response Systems.

This page intentionally left blank

Table of Contents

This page intentionally left blank

List of Figures

List of Tables

Abbreviations

AHP	Analytic Hierarchical Process
ALE	Annualized Loss Expectancy
API	Application System Interfaces
ARO	Annualized Rate of Occurrence
BST	Binary Search Tree
CSM	Cooperating Security Managers
CVE	Common Vulnerabilities Exposures
CVSS	Common Vulnerability Scoring System 2.0
DDoS	Distributed Denial of Service
DMZ	De Militarized Zone
DoS	Denial of Service
EF	Exposure Factor
ELECTRE	Elimination and Choice Expressing Reality
EM	Eigen Value Method
FMEA	Failure Mode and Effects Analysis
GRA	Grey Relational Analysis
HCI	Human-Computer Interaction
HIDS	Host Intrusion Detection Systems
HMM	Hidden Markov Model
HTML	Hypertext Markup Language
HTN	Hierarchical Task Network
HTTP	Hypertext Transfer Protocol
IDSs	Intrusion Detection Systems
IPSs	Intrusion Prevention Systems
IRSs	Intrusion Response Systems
IT	Information Technology
MCDA	Multicriteria Decision Analysis
MyCERT	Malaysian Computer Emergency Response Team
NIDS	Network Intrusion Detection Systems
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OCTAVE	Operationally Critical Threat, Asset, And Vulnerability Evaluation
OICM	Organization Information Criticality Matrix
OS	Operating System

OSVDB	Open-Source Vulnerability Database
RGMM	Row Geometric Mean Method
RIM	Risk Index Model
RSM	Response Strategy Model
SIEM	Security Incident Event Management
SIM	Security Incident Management
SIPM	Security Incident Prioritisation Modules
SIR	Superiority and Inferiority Ranking
SLE	Single Loss Expectancy
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

Acknowledgements

This study was financed with the aid of scholarships from the Ministry of Higher Education in Malaysia and the University of Malaya and I would like to thank to them for those scholarships.

The past three years have thus far been the most challenging, interesting, and rewarding part of my life. I am very thankful and grateful to have crossed paths with many wonderful people who have helped me in many ways in my pursuit of a PhD at the Centre for Security, Communications and Network Research (CSCAN) at Plymouth University, UK.

First and foremost, I would like to express my sincere gratitude to Prof. Steven M. Furnell, my Director of Studies and Research Director of the CSCAN group, for his supervision and advice from the very early stages of this study through to the completion of this thesis. His wide knowledge, logical way of thinking, understanding and support have been invaluable to me.

Secondly, I would like to thank Dr Maria Papadaki, my second supervisor, who was an important person in terms of giving very constructive comments and excellent advice throughout this study. Her supervision, personal guidance and support have been of great value on both an academic and a personal level, for which I am extremely grateful.

I would also like to thank my third supervisor, Dr Nathan L. Clarke, for his excellent advice and constructive comments which have also been very valuable to this study.

Special thanks go to my family, friends and all the CSCAN members in the group, who have helped and supported me over these years.

Above all, I want to thank God for it is His grace that has made it possible for me to produce this study and complete my PhD.

Author's Declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award without prior agreement of the Graduate Committee.

This study was financed with the aid of scholarships from the Ministry of Higher Education in Malaysia and the University of Malaya.

Relevant seminars and conferences were regularly attended at which work was often presented. Several papers have been submitted and published in the course of this study, details of which are listed in the appendices.

Word count of main body of thesis: 50, 582 words

Signed : ………………………………………………….

Date : ………………………………………………….

1 Introduction and Overview

Although the level of investment into security is increasing (Richardson, 2011), the problem of ever evolving and persistent threats seems far from contained. As the following statistics suggest, the war against attacks is anything but over.

A quantitative telephone survey conducted between October 2007 and January 2008 by PricewaterhouseCoopers on UK businesses revealed an increased percentage of security-related activity, such as investment, training and awareness, in comparison to the previous years; for example, there was an increase of 7% in the average IT budget spent on security since 2002 (PricewaterhouseCoopers, 2008). In addition, the latest survey conducted in 2010 revealed a dramatic increase on security breaches, especially for small organisations (<50 staff), with nearly twice as many respondents being affected than in 2008. For instance, 83% of respondents had encountered at least one incident, compared to only 45% in 2008 (PricewaterhouseCoopers, 2010). Furthermore, Schouwenberg (2008) revealed how financial malware has evolved over time and indicated that the problem is consistent.

Symantec (2009) reported that there were 1,656,227 new malicious code samples detected in 2008, an increase of more than 165% on the previous year. They also observed an average of 75,158 active bot-infected computers per day, an increase of 31% in comparison to 2007. In addition, the published incident statistics for the first half of 2011 indicate a 147% increase in the number of cases reported to MyCERT in comparison to the same period in 2010, with an additional 4,413 cases compared to 2,991 cases in 2010 (MyCERT, 2011).

The number of vulnerabilities is also rising. Based upon daily statistics published by the National Vulnerability Database, in the third quarter of 2011 the number of registered vulnerabilities is approximately 50,000[1]. This statistic is an identification of known vulnerabilities which have been identified, assigned and published under the Common Vulnerabilities Exposures (CVE) scheme (NIST, 2011). In 2010, Symantec (2011) encountered more than 286 million unique variants of malware; giving further evidence that the numbers are rising. The infographic in *Figure 1* gives a summary of the landscape of security threats, with a combination of new threats, current situations and challenges to the security communities; threats are evolving and numbers are rising, which means better ways are needed to manage them.

[1] 1st December 2011 – 48, 705 vulnerabilities identified, assigned and published with CVE-ID.

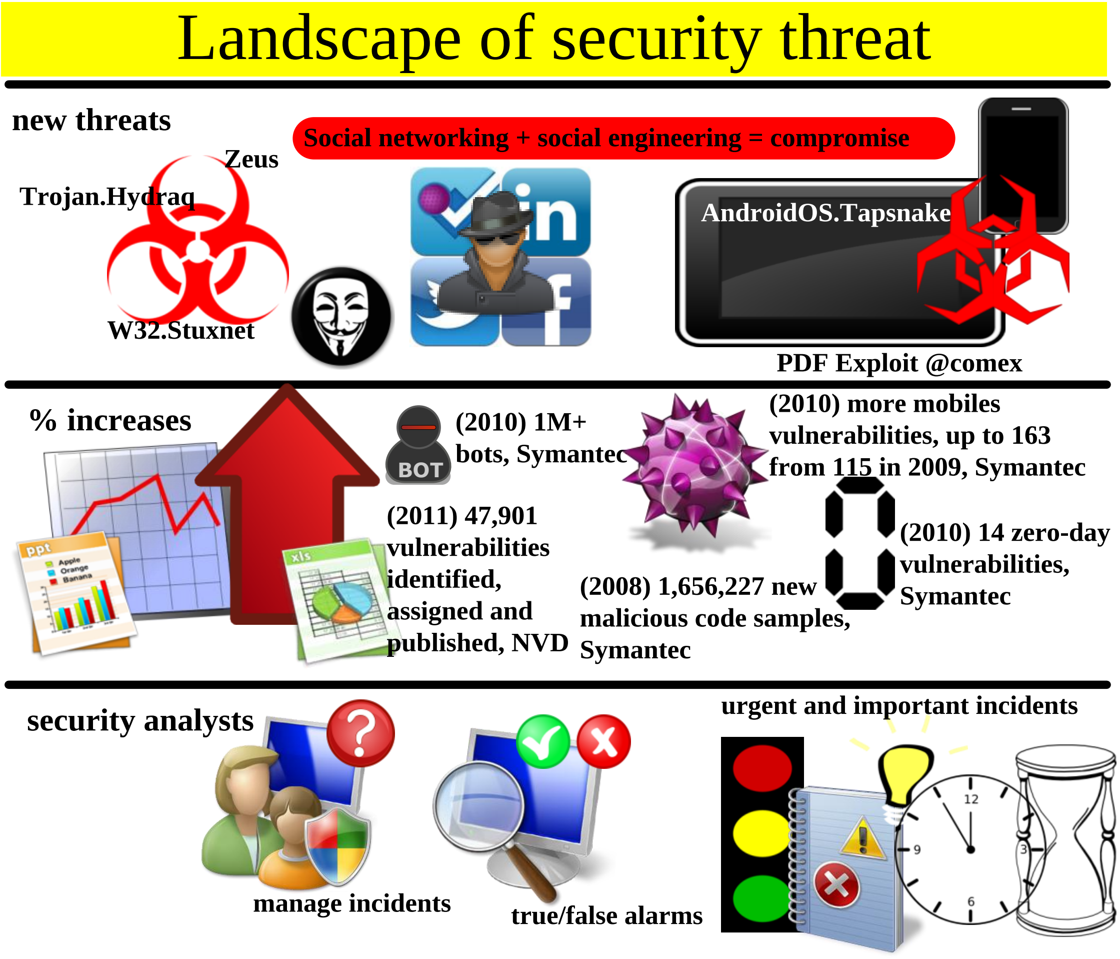

Landscape of security threat
new threats
Zeus
Trojan.Hydraq
W32.Stuxnet
Social networking + social engineering = compromise
AndroidOS.Tapsnake
PDF Exploit @comex
% increases
(2010) 1M+ bots, Symantec
BOT
(2010) more mobiles vulnerabilities, up to 163 from 115 in 2009, Symantec
(2011) 47,901 vulnerabilities identified, assigned and published, NVD
(2008) 1,656,227 new malicious code samples, Symantec
(2010) 14 zero-day vulnerabilities, Symantec
security analysts
manage incidents
true/false alarms
urgent and important incidents

Figure 1. The landscape of security threats

1.1 Intrusion Detection Studies

In order to counter threats, different approaches are available for security analysts, such as antivirus software, firewalls, access control and other security systems, like Intrusion Detection Systems (IDSs). The use of an IDS or similar system, such as an Intrusion Prevention System, is one of the most popular options in business due to their operation, openness and wide-acceptance as security devices (Nicolett and Kavanagh, 2009). In addition, security techniques such as authentication and access controls act as a first line of defence to prevent systems being compromised. An intrusion detection system (IDS) acts as the second line of defence and operates to detect suspicious activities and respond to them.

There are hundreds of published works related to intrusion detection (Sherif and Dearmond, 2002; Sherif *et al.*, 2003), which all aim to improve the efficiency and reliability of detection, prevention and response systems. There are still areas to explore, particularly with respect to the process of selecting appropriate responses. Existing studies have so far focused on reducing alerts, identifying critical attacks, prioritising incidents (Alsubhi *et al.*, 2008), eliminating and reducing false alarms

(Tian *et al.*, 2008), and increasing the confidence level of incident responses (Yu and Fríncke, 2005). Alsubhi *et al.* (2008) categorise the research studies into two types: low-level and high-level alert operations. High-level operations apply aggregation, clustering, correlation, and/or fusion to sets of alerts in order to identify trends and abstractions within them, while low-level operations aim to identify the contextual information of each alert individually, and rate it based on its potential risk. As such, high-level operations aim to reduce alerts and improve detection efficiency, whereas low-level operations aim to enable a response mechanism by informing decisions with contextual information and information on the risk of each incident. Examples of some relevant studies are listed below:

(a) *Alarm reduction*. High-level operations aim to improve detection efficiency and include aggregation (Debar and Wespi, 2001; Yu and Rubo, 2008), clustering (Xiao *et al.*, 2008; Al-Mamory and Zhang, 2009), correlation (Ning *et al.*, 2002; Kruegel *et al.*, 2004; Alserhani *et al.*, 2010) and fusion (Ning *et al.*, 2001; Valdes and Skinner, 2001), which all aim to reduce the number of alerts and false alarms.

(b) *Incident management*. Low-level operations aim to improve the process of managing incidents and selecting appropriate responses. They can be used to examine a large number of incidents and prioritise them by identifying which incidents are important, which are urgent and which are critical based on the potential risk. For example, alert or incident prioritisation (Porras *et al.*, 2002; Lee and Qin, 2003; Alsubhi *et al.*, 2008; Dondo, 2008), risk assessment of incidents (Mu *et al.*, 2008) and security incident management (SIM) (Alberts and Dorofee, 2004; Libeau, 2008) (also known as Security Information and Event Management, SIEM).

Thus, to increase the manageability of incidents and facilitate an autonomous mode in the response selection process in Intrusion Response Systems (IRSs), this study focuses upon low-level operations and specifically on the incident prioritisation process. The process examines incidents[2], manages them, identifies urgent and important incidents, and maps them with appropriate responses based upon their priorities.

1.1.1 Incident Prioritisation

When this study began in late 2008, only a few studies had been conducted on incident prioritisation. Early work on incident prioritisation had been proposed by Porras *et al.* (2002) in M-Correlator. A recent work by Alsubhi *et al.* (2008) proposed a fuzzy system based on metrics such as the applicability of attacks, the importance of victims, the relationship between the alert under evaluation and previous alerts, and the social activities between attackers and victims. Also, there are other

[2] In this particular context, an incident is referring to an event detected by security systems, which it may cause a violation or imminent threat of violation to systems.

studies that can help incident prioritisation; for example, the Common Vulnerability Scoring System (CVSS) (Mell *et al.*, 2009) was introduced in 2007 as an alternative to rating vulnerabilities quantitatively and it has been widely adopted as a medium through which to support the incident prioritisation process (FIRST, 2011). In addition, a practical approach introduced by Snort (1998), Snort Priority, also aims to prioritise groups of incidents.

In order to enable the autonomous mode in the response selection process, it is important to prioritise incidents as this provides a methodical way in which to identify which incidents are critical, which incidents are urgent and which incidents are less critical. Having prioritised these incidents, they can then be mapped automatically and flawlessly with an appropriate type of response based upon their characteristics, criticality and urgency. In this particular context, the incident criticality refers to a comparative state where one incident is critical to another based upon the important of a target asset; and it is measured based upon the impact on the asset as a result of an attack. The incident urgency refers to a state where one incident requires a speedy response compared to other incidents and it may causes a severe impact in case there is a delay; and unlike the incident criticality it is measured based upon the likelihood of threat and vulnerability. For example, a serious incident can be mapped to an active response in order to minimise its impact, while a less impactful incident can be mapped with a passive response.

The aforementioned approaches all have the ability to prioritise incidents, but they also have limitations. For example, Snort Priority groups similar critical incidents into similar groups of priorities (e.g. high, medium and low priority), with the consequence that security analysts face a challenge in analysing and differentiating which incidents are urgent and important. In addition, CVSS does not provide full coverage of new incidents, instead limiting itself to incidents with CVE-IDs; this consequently produces incomplete results that security analysts have little confidence in. Furthermore, other studies, such as Alsubhi *et al.* (2008) and Porras *et al.* (2002), have other limitations, particularly in the technical aspects of the methods adopted in their proposal. For example, although existing approaches consider multiple decision factors, they do not consider different weightings based upon the importance of different decision factors. The use of different weightings could provide more flexibility and allow the incident prioritisation process to reflect different organisational policies.

The aforementioned approaches provide various ways to prioritise incidents, but less attention has been given to adopt them in an automated response system. Porras *et al.* (2002) and Alsubhi *et al.* (2008) realised the advantages of the prioritisation process, but released no further studies showing their continuing investigating of the process’s effectiveness. Thus, this gap has opened an opportunity for this study to evaluate the feasibility and suitability of the incident prioritisation process in facilitating an autonomous mode in the response selection process.

1.2 Aims and Objectives

The aim of this study is to propose a novel framework to address the incident prioritisation process and to facilitate the autonomous mode in the response selection process in IRSs. In order to achieve this aim, several issues need to be thoroughly understood, analysed and evaluated, as follows:

(a) To comprehensively understand the domain of intrusion detection and incident response and identify the key issues with respect to the effective management of incidents.

(b) To establish the need for an incident prioritisation process as well as rating, ranking and response procedures when responding to critical incidents.

(c) To design and propose a novel framework and a new approach to more effectively rate, rank, prioritise and respond to incidents.

(d) To evaluate the performance of a proposed framework by validating it using evaluation studies at different stages in order to demonstrate the progress of results.

(e) To design and implement a novel prototype of the proposed framework to facilitate a practical evaluation using live traffic within an on-line assessment environment.

The objectives presented above relate to the general sequence of the material presented in this study, the structure of which is discussed in the next section.

1.3 Thesis Structure

Chapter 2 introduces Intrusion Detection Systems, Intrusion Prevention Systems and Intrusion Response Systems, and specifically reviews their response capabilities. A response model, based on the attack time frame is also introduced to define the different response options. The intention of this is to link priorities with responses in an Intrusion Response System. Based upon the response model, the chapter presents an investigation and survey of the current response options available in commercial and research products. The chapter also aims to underline what are the different response options for use with different priorities of incident.

Chapter 3 focuses upon existing incident prioritisation studies and presents a critical appraisal of them; identifying their similarities and limitations. It then continues with a review of relevant theories that could be used in rating, ranking and response, such as risk assessment, decision theories and measuring the risk level of incidents using several factors including threats, vulnerabilities and assets. This chapter highlights the advantages of such studies and discusses how they can be combined to produce a more effective means of rating, ranking and prioritising incidents, as well as responding more appropriately to them.

Chapter 4 presents the main contribution of this study: a novel framework and an alternative approach to rate, rank, prioritise, and respond to incidents. In presenting the framework, this chapter begins by introducing the main rationale behind the framework as well as its operational characteristics. It also introduces two integral parts of the framework itself, namely the Risk Index Model (RIM) and the Response Strategy Model (RSM).

Chapter 5 extends the study by conducting multiple experiments to validate and evaluate the proposed framework. In order to demonstrate the progress of the results, the evaluation study presents the experimental results in four stages. The first stage aims to validate the Risk Index Model (RIM) by comparing its results to the Common Vulnerability Scoring System (CVSS v2) and Snort Priority approaches. Based upon the preliminary results of the first experiment, the second stage aims to enhance RIM by analysing the effect of using different strategies in the proposed framework; the evaluation is performed using a similar methodology to the first stage. The third stage investigates the effectiveness of the proposed RIM and RSM in achieving two different goals: first it investigates the distribution of incidents in comparison with other approaches, such as CVSS v2 and Snort Priority; and secondly it investigates the relationship between response strategies and its ability to classify incidents between true and false incidents. The fourth stage investigates the performance of the proposed framework by measuring the processing time of the rating and ranking process. This chapter also gives an in-depth discussion of the implications of applying the proposed framework in practice, underlining the advantages as well as the limitations.

Chapter 6 presents the implementation of a prototype system which embodies a full set of the key elements of the proposed framework, and described the interactions and relationships among them; namely the Security Incident Prioritisation Module (SIPM). Initially, it begins with an overview of the system development process, the system design and other modules, such as the application daemon and the web modules. In addition, example scenarios are provided to demonstrate how the proposed framework operates, and how the web interfaces can be used to assist security analysts in making a decision.

Finally, Chapter 7 presents the main conclusions drawn from this study, highlights the principle achievements and limitations of the work, and makes suggestions for potential further enhancements.

The thesis also includes a number of appendices, which contain a variety of additional information in support of the main discussion, including several sets of source code and a number of peer-reviewed publications from this study.

This page intentionally left blank

2 Overview of Intrusion Response Systems

The trends in security studies related to attacks, threats and vulnerabilities have changed in recent decades so that it now mainly focuses upon studies related to detection, prevention and response strategy. Over the years of research in this area, this trend has changed the direction of studies leading to multiple areas of interest being explored. To understand the incident prioritisation studies, this chapter presents an introduction to security systems and response taxonomies, which are closely linked to intrusion studies. This chapter starts by giving an introduction to intrusion detection systems and discussing their different types which offer different modes of detection and prevention, as well as different ways of responding to incidents. It continues by establishing the relationships between the response taxonomies and response options, and showing how these relate back to the incident prioritisation research. This chapter also introduces a model to define different types of response option using an attack time frame. It strengthens these findings by highlighting the results of an investigation and survey previously conducted. Having presented the concept of the response model, this study will extend its usage to map between different priorities of incidents with different types of response options.

2.1 Detection, Prevention and Response Study

The preliminary concept of an IDS was devised by Anderson (1980) and then strengthened by the models created by Denning (1985; 1987b) and other subsequent researchers. Studies related to intrusion and their impacts have become one of the main branches in the network security research area.

Denning’s papers (Denning and Neumann, 1985; Denning, 1987b; Denning, 1987a) described the components of modern Intrusion Detection Systems (IDSs), while the extension made by Verwoerd and Hunt (2002) introduced four basic fundamental components: the sensor, monitor, resolver and controller. In extension to the basic components, the general classifications of IDSs are as follows.

(a) *Detection approach*. There are two types of detection approach, namely anomaly detection (Smaha, 1988; Lazarevic *et al.*, 2003) and misuse detection (Neumann and Parker, 1989; Kumar and Spafford, 1994).

(b) *Protection approach*. This type of system can be used to protect either hosts (Wagner and Soto, 2002) or networks (Mukherjee *et al.*, 1994), or a combination of both .

(c) *System architecture*. This type of system can be implemented either as a stand-alone system (Vigna and Kemmerer, 1998) or distributed by using an agent-based system (White *et al.*, 1996; Aussibal and Gallon, 2008)

(d) *Data source*. The data source can be gathered from a combination of audit logs (Dunlap *et al.*, 2002), network traffic (Mukherjee *et al.*, 1994) or system status events (Forrest *et al.*, 1996; Hofmeyr *et al.*, 1998).

(e) *Detection and response approach*. The detection and response approach can use either an active (Wang *et al.*, 2001a) or a passive mode.

(f) *Analysis timing.* Analysis can be done either in real time, such as in a live traffic network (Lunt *et al.*, 1989), or offline using other tools such as data mining (Cuppens and Miege, 2002).

Research initially focused upon enhancing the detection processes rather than on responses (Sherif *et al.*, 2003). Intrusion Detection Systems (IDSs) are used to detect signs of malicious activities, and they have been an area of active research for more than 30 years, ever since Anderson's paper (Anderson, 1980). However, since the beginning of the 21st century, more attention has been given to intrusion response studies, particularly when used in combination with other approaches, such as decision-making (Mu and Li, 2010). It appears that the first usage of the term "*intrusion response systems*" in the computer community appeared in the seminal works by a research group at Texas A&M University (Carver *et al.*, 2000; Carver, 2000; Ragsdale *et al.*, 2000). However, even more than 15 years later the opinion of Mukherjee *et al.* (1994) remains valid as it gives a broad overview of why prevention systems like Intrusion Prevention Systems (IPSs) are not feasible, and suggests the requirement for an alternative to this, which is an Intrusion Response System (IRS).

Before discussing the multiple types of response options, it is important to distinguish between the different modes in which Intrusion Detection, Prevention and Response Systems can operate; the following descriptions describe these modes:

(a) *Intrusion Detection System (IDS) mode*. A system running in an Intrusion Detection System (IDS) mode is able to detect intrusions; traditionally, when such an intrusion is detected, it may produce a simple warning or alarm. An IDS might be a piece of software or hardware, or a combination of both used to detect intrusions through various techniques and algorithms (McHugh *et al.*, 2000). Ultimately, the main goal of this mode is to detect the unauthorized use, misuse and abuse of computer systems by both system insiders and external intruders (Aickelin *et al.*, 2003). The main goal of this mode is to assist system administrators in determining the security state of the system and suggesting an appropriate response (Zhang *et al.*, 2009). Early types of intrusion detection system would only produce passive responses, such as producing a log or notifying an administrator about suspicious activities.

(b) *Intrusion Prevention System (IPS) mode*. Systems running in an Intrusion Prevention System (IPS) mode share similarities with the IDS mode in terms of system deployment and detection method, but perform an additional response by blocking potential intrusions or terminating the network traffic for the current intrusion. It can therefore be considered an extension to the traditional IDS mode. Normally, in order to block malicious traffic an IPS is positioned in-line with the network and is deployed together with firewalls or access control appliances (Papadaki and Furnell, 2004; Fuchsberger, 2005). In order to provide protection at a host level, a host-based IPS utilises an intelligent system, which has the ability to intercept and evaluate system calls (Paulson, 2002). For example, Kwon *et al.* (2008) introduced a host-based IPS called PROBE which monitors processes running on a host to identify abnormal process behaviour. Furthermore, in order to provide host level protection on servers and workstations, a host-based IPS also secures and controls software communication channels between a system’s applications and its operating system kernel (Patel *et al*., 2010).

(c) *Intrusion Response System (IRS) mode*. Systems running in an IRS mode perform a similar function to those in IDS and IPS modes by maintaining several approaches to detect and respond, but use multiple types of response after further analysis to minimise the impact of any incidents. The IRS mode is clearly tightly coupled with the IDS mode and takes over after signs of any intrusion, to either record the attack passively or to attempt to minimise the impact actively (Toth and Kruegel, 2002). Existing studies have aimed to create IRSs which are able to run automatically as well as reconfiguring, regenerating and rejuvenating systems once an intrusion occurs (Wu *et al.*, 2007). Unlike the IDS and IPS modes, the IRS mode offers additional functions and exhibits multiple characteristics of response to mitigate the impacts of any intrusion. Therefore, it does not just offer a passive response; instead, it also concentrates on responding with active responses in order to reduce the impact of incidents actively. In addition, within the variety of responses available, this mode is also able to initiate collaboration with other security appliances, such as working with firewalls to block and terminate suspicious traffic, working with honeypots to collect attackers’ information and trace attackers sources (Wang *et al.*, 2001b), and redirecting connections for other additional precautions (Yue and Cakanyildirim, 2007).

The discussion in this section has presented an introduction to the IDS, IPS and IRS mode used in detecting, preventing and responding to incidents. It can be seen that all three modes share similarities, particularly in the methods of system detection. From the traditional IDS mode, the other two modes inherit the system detection techniques and response methods. In terms of responses to incidents, none of the three modes are limited only to the passive responses, but can actively use multiple techniques and approaches to reduce the impact of an incident.

2.2 Response Taxonomies

This research focuses upon responding to intrusions, so this section explains the different response taxonomies and how they influence the categorisation of responses in the response model proposed.

To improve the understanding of the intrusion response studies, this section makes a critical appraisal of several response taxonomies (Fisch, 1996; Debar *et al.*, 1999; Carver, 2001; Wang *et al.*, 2006; Stakhanova *et al.*, 2007b).

The earliest taxonomy for response systems is known as the Fisch DC&A taxonomy (Fisch, 1996),which separates responses into two main classifications:

(i) Detection time - when the suspicious activities are detected. For example, the Fisch DC&A taxonomy defines that the detection time can be "after the attack" or "during the attack".

(ii) Response goal - the Fisch DC&A taxonomy defines a specific goal for a response; the available response goals are: active damage control, passive damage control, damage assessment, or damage recovery.

The classification of a response can be summarised under two main categories: active and passive. "During the attack" and "active damage control" are active responses, whereas "after the attack", "passive damage control", "damage assessment" and "damage recovery" can be classed as passive responses. To strengthen these two main categories, Debar *et al.* (1999) also described two main types of response which are also referred to as active and passive response. It appears that they followed the Fisch DC&A taxonomy, but went further by dividing the active reaction into two: either a corrective mode involving closing the vulnerability holes, or a proactive mode, involving logging out possible attackers or closing down servers. They also mentioned that the passive response can be improved by giving a simple notification system in order to respond to incidents.

In addition to the Fisch DC&A and Debar *et al.* (1999) taxonomy, two more recent taxonomies have been established by Stakhanova *et al.* (2007b) and Wang *et al.* (2006). As depicted in *Figure 2,* Stakhanova *et al.* (2007b) introduced a complex taxonomy by categorising systems from multiple views based upon different angles of characteristics and perspectives.

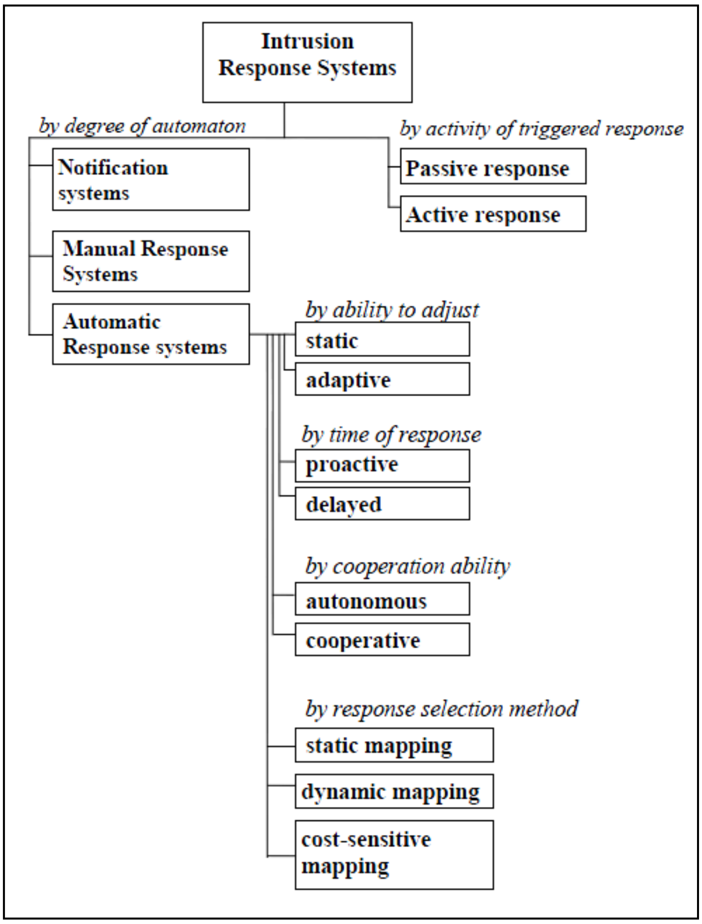


Figure 2. Intrusion Response System Taxonomy (Stakhanova *et al.*, 2007b)

The Stakhanova taxonomy categorises and measures IRSs using two main characteristics, namely '*a degree of automation*' and '*the activity of a triggered response*'. Instead of having different categories, passive and active responses are categorised together according to their characteristic of being '*the activity of a triggered response*' category. In addition to that, to enhance and strengthen the taxonomy, they proposed another characteristic called '*a degree of automation*'; under this category, depending upon the response mode, there are a few other responses including notification systems, manual response systems and automatic response systems.

The complexity of the taxonomy proposed by Stakhanova *et al.* (2007b) can be seen because it then proposes additional categories according to other characteristics under the automatic response systems. There are four other categories under the automatic system response category, including an ability to adjust, speed of response, cooperative ability and response selection method. They highlighted several requirements for an ideal IRS that future systems should aim for; these requirements include being automatic, proactive, adaptable and cost-sensitive.

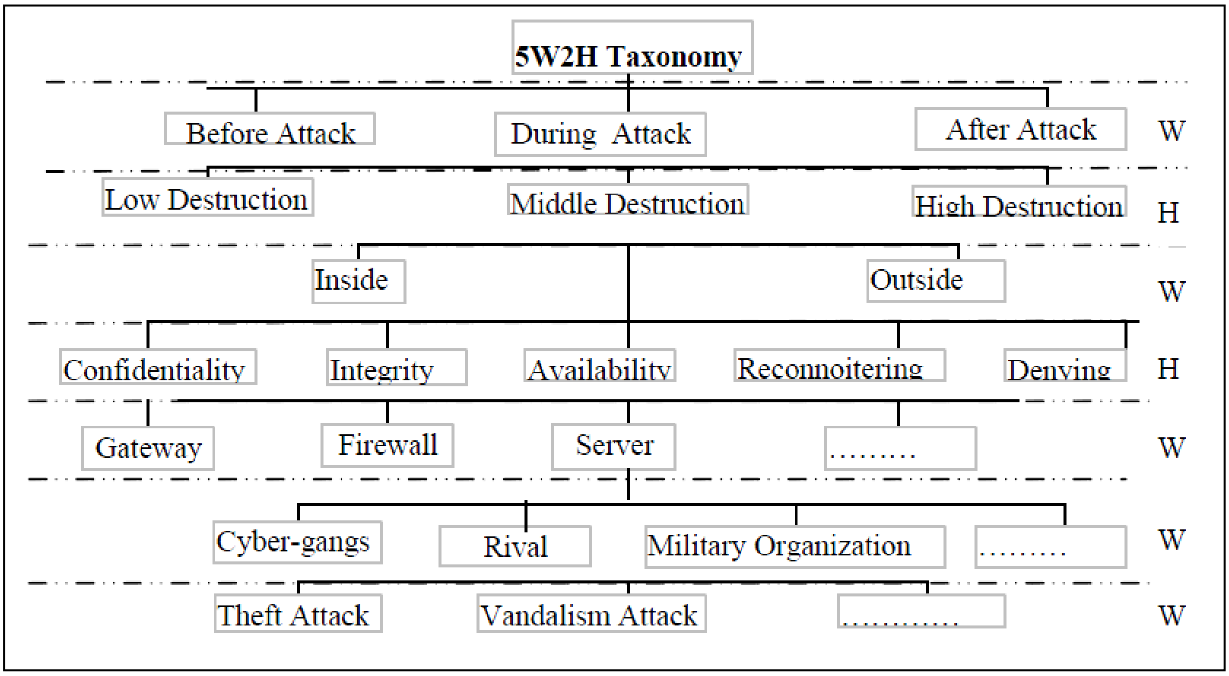


Figure 3. 5W2H Intrusion Response Taxonomy (Wang *et al.*, 2006)

In contrast to Stakhanova *et al.* (2007b), Wang *et al.* (2006) developed the 5W2H taxonomy as depicted in *Figure 3.* As can be seen, the taxonomy describes seven dimensions: when (as a dimension of time), how serious (potential of destruction), where (location of attacker), how (type of attack), what (a target or victim), what (type of attacker), and last dimension is why (plan of attack).

The 5W2H taxonomy seems very complex compared with the previous taxonomy because it has many redundant dimensions. For example, the third dimension, which is where (location of attacker), the fourth dimension, the type of attack, and the sixth dimension type of attacker, all refer to one entity, which is the attacker. In addition, the final dimension defined is unclear and vague. For example, the last dimension uses ‘why’ as a keyword to describe the plan of attacks, which it could be argued is impractical to classify, and they have not provided any clear classifications for this. Unclear and vague explanations with additional redundant terminology make the 5W2H taxonomy less useful for differentiating between responses.

Although the 5W2H taxonomy is the most recent taxonomy published by Wang *et al.* (2006), it is not widely used as it is quite similar to the Carver Taxonomy introduced by a group of researchers from Texas A&M University (Carver *et al.*, 2000; Carver, 2000, 2001). With Carver Taxonomy, in order to have a response decision process, some additional factors need to be considered, including the timing of an attack, the type of the attack and attackers, the degree of suspicion, the implications of the attack and any environmental constraints. Using these factors, Carver *et al.* (2000) identified and classified responses into three main response systems: notification systems, manual response systems and automatic response systems; these response classifications are the ones that have been adopted by Stakhanova *et al.* (2007b) in their taxonomy.

These taxonomies provided a collection of different approaches and perspectives to facilitating an autonomous mode in the response selection process in IRSs. Specifically, they provided response categorisation, assessment of response selection and response mapping. The main interest of this study is to summarise the response categorisation in those taxonomies as they facilitate the establishment of a model classifying different types of response option.

2.2.1 Response Options: Active vs. Passive

Based upon the various aforementioned taxonomies, the response options can be divided into two main types: active and passive.

(a) *Active response*. An active response is used to counter an incident in order to minimise its impact on victims.

(b) *Passive response*. A passive response normally aims to notify other parties about the occurrence of an incident and relies upon them to take further action.

Yue and Cakanyildirim (2007) described proactive responses and reactive responses as an extension to an active response. In order to provide an active response, a system needs to have an autonomous mode in its operation, since humans are not fast enough to react to high speed or broad scale attacks in an effective manner (Lewandowski *et al*., 2001).

Although an active response gives the advantage of limiting intrusion activities, it sometimes produces negative results if the response systems are not configured correctly. For example, an active response is capable of generating Denial of Service (DoS) attacks in live networks by denying legitimate connections from authorised users by blocking and terminating their connections. Thus, in order to minimise this disadvantage, a system must be configured properly so it can respond with confidence in minimising errors. In addition, an active response must have the capacity to engage in corrective action, such as updating system patches automatically, logging off a user, reconfiguring the firewall or disconnecting a port (Jackson, 1999).

Responses can therefore be described according to a number of different factors, such as the level of operation, the speed and time of response, the ability to learn and the ability to cooperate with other devices; the following descriptions are therefore useful:

(a) *Proactive response*. A proactive response is an approach that controls a potential incident activity before it happens rather than waiting to respond after it has happened.

(b) *Reactive response*. A reactive response reports any incidents detected directly to security analysts or takes action immediately in real-time, in order to minimise their impacts. Unlike the proactive response, the reactive response reacts only after an intrusion is detected.

A proactive response refers to an action that can only be taken if there is a trusted decision made by the IDS itself, and in certain cases the action can be taken immediately. It is also referred to as an immediate response (Yue and Cakanyildirim, 2007). The proactive response approach prevents a predicted incident based upon analysis, investigation, reasoning and scientific methods. For example, a probability measurement is used to give a value to the possibility of an attack happening (Stakhanova *et al.*, 2007a). In addition, a proactive response approach can predict a new intrusion and confidently know the best method to use to prevent the intrusion from spreading quickly. These proactive responses can be categorised into two further different approaches:

(a) *Prediction method*s. A prediction method gives an early response to security analysts or intelligent agent systems, while at the same time minimising the potential impacts of predicted incidents for future protection. This approach can use any machine learning approach, and the solutions proposed by Teng *et al.* (1990) and Schultz (2002) showed the capabilities of predicting a new attack and demonstrated that this technique has great potential for future response models.

(b) *Case-based reasoning method*s. This involves using a case-based reasoning method to pre-empt incidents based on historical data. For example, any incident detected in real time is stored and can later be used as an input for future responses. This is similar to the case-based reasoning approach used in an IDS (Esmaili *et al.*, 1996), but in proactive responses, any previous incident response will be used as a reference point in order to prevent future incidents with similar characteristics. For example, COBRA (Gangadharan and Kai, 2001), RedAlert (Anuar *et al.*, 2004) and ADEPTS (Foo *et al.*, 2005; Wu *et al.*, 2007) all provide proactive responses in order to minimise an intrusion’s impact on other neighbouring systems. Similar to COBRA and RedAlert, a recent study by Thames *et al.* (2008b; 2008a) used a proactive response by updating and reconfiguring a firewall dynamically and periodically.

The second category of active response is the reactive response. There is no clear definition of this, but it accepted as an approach where security systems are maintained in a real-time interactive environment or by using human experts with automated tools to assist in finding the best responses

(Fessi *et al.*, 2007). As mentioned earlier, a reactive response occurs only after an intrusion is detected. Therefore, it is suggested that there are two stages of responding in this situation;

(a) The first stage of a reactive response is to issue a confident response immediately after an incident is detected.

(b) The second stage of the reactive response involves investigating incidents and learning about them so future responses can be refined.

The first stage of the response acts only after incidents are detected and aims to reduce their impact. For example, an automated response system with automated system capabilities, such as Cooperating Security Managers (CSM), can be considered to be a reactive response. CSM, which was proposed by White *et al.* (1996), proactively detects suspicious activities but reactively responds to them (Wu *et al.*, 2007). In addition, in order to reduce the impact of incidents, responses at this stage have the ability to collaborate with other security appliances, such as a firewall; this can be seen in the Taichi system (Han *et al.*, 2006), which combines heterogeneous IDSs with improved distributed firewall systems and is able to detect and prevent intrusion automatically.

The second stage of a reactive response applies to incidents with high uncertainty that need to have their behaviour investigated and understood before a further response can be applied. This category is fundamentally based upon a study by Yue and Cakanyildirim (2007), who suggest that a reactive response is defined as a response involving sending alarms to security analysts. At this stage, unlike the first stage, to reduce uncertainty in the incident, no response is made immediately and instead the system waits for the incident to be investigated, such as, tracing the incident (Chen *et al.*, 2006) or using a honeypot (Feng *et al.*, 2003) to collect additional incident data for investigation purposes. This stage is similar to a passive stage, as there is no action being taken to minimise the incident’s impact, and it merely provides feedback. However, the literature generally claims that responses in this stage are still categorised as an active response (Wang *et al.*, 2001a; Wang *et al.*, 2001b; Jang and Kim, 2002; Feng *et al.*, 2003; Chen *et al.*, 2006; Stakhanova *et al.*, 2007a).

Finally, a passive response does not react in any way to minimise the impact, and only notifies and collects information about the intrusion. A passive response is one of the earliest responses that was used in IDSs, and is therefore vulnerable and may give an advantage to the attackers. A case study which explains the disadvantages of this approach is clearly given by Cohen (1999). In certain cases, ignoring an incident can also be seen as a passive response (Yu and Rubo, 2008).

2.2.2 Response Model for Intrusion Response Systems

Based on earlier discussion, it can be seen that the response can be divided into several different categories and stages. Therefore, in order to show the relationship between them, this study uses an attack time frame, as illustrated in *Figure 4*, to show a common time frame when attacks or intrusions are detected and responded to by any security appliance. In differentiating the type of response and describing the response model, the attack time frame clearly depicts the stages of the response. In the figure, the relationship between the responses is formed based upon the attack time frame and contains three main lines t_0, t_1 and t_2, where t_1 denotes the time of the intrusion alarm. Based on t_1, the following two stages appear;

(a) Before intrusion alarm, between t_0 and t_1,

(b) After intrusion alarm, between t_1 and t_2.

In addition to these two stages, there is another stage in the attack time frame which comes after t_2, which refers to the stage after a reactive response. In the stage before t_0, the system is assumed to be in a normal state in which no intrusions have been detected. With a total of three main stages, the attack time frame in *Figure 4* is considered appropriate to describe the variety of responses explained in the previous section. Therefore this will be used as the response model for IRSs.

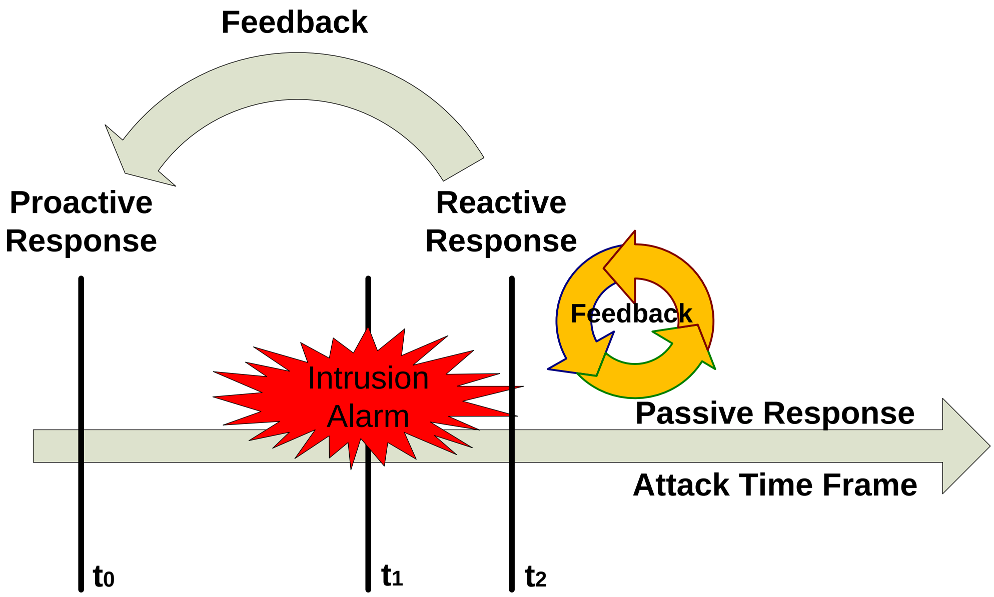


Figure 4. Relationship between passive, proactive and reactive response using attack time frame

The attack time frame for the response model starts at stage t_0, which is the stage before any incidents are detected by the IDSs, which occurs at t_1. In this stage, proactive responses play a big role in defending hosts and networks from being attacked. For example, precautionary actions such as blocking any predicted potential incident and adjusting system configurations can be taken. Based upon the two aforementioned scenarios for proactive responses, this stage provides two critical response actions; (i) prevent any future potential incident based on prediction analysis, and (ii) prevent current and future potential incidents based on feedback from the passive and active responses.

Between t_1 and t_2, the reactive response is most involved in minimising the incident's impact. In this stage, countermeasures like terminating users, processes or network traffic that have direct influence on attackers are taken against for activities identified as suspicious with high levels of confidence. At this stage, in order to respond to these countermeasures, significant collaboration between security appliances such as access control systems and firewalls would be a great benefit. Since this is a critical stage, the response measures should be taken only if the confidence level of the related incidents is considered very high, as it is important in order to minimise the response errors. This stage ends immediately at t_2, and for any incident that cannot be resolved within this time an escalation process occur to take it to the second stage of the reactive response.

Unlike the previous stages, the stage after t_2 is an investigation phase. The stage is continuous with no specific end point; therefore, this stage is suitable for non-critical systems. This stage ends once the incident has been investigated and appropriate actions have been taken against them. This stage is the second stage of reactive response which involves waiting, investigating and learning about the incident before any further response can be applied.

At stage t_2, some incident feedback can also be collected from passive responses. This can be combined with feedback on the current stage and act as an input for reactive and proactive responses. Furthermore, the feedback cycle between reactive and passive responses provide bidirectional feedback; both responses communicate continuously in order to provide better investigation and analysis of any incident.

The discussion above clearly indicates that the response model for IRSs can be divided into two main response zones: the passive and active zones, where the active zone involves proactive and reactive responses.

It is important to differentiate the different types of response option. In particular, the different capabilities they have should be mapped with different types of incident according to their priority.

2.2.3 An investigation and survey of response options for IRSs

This section presents an investigation and survey of the different types of the response option available. It helps to investigate the level of response applied in commercial and research products, looking at IDS, IPS and IRS technologies, as well as Security Information and Event Management (SIEM) products.

SIEM products are being considered due to their characteristics; although the product is considered as a new tool in the security industries, the objectives for deploying it are to monitor, identify, document and respond to security threats and to reduce false positive incidents (Miller *et al*., 2010).

SIEM is a technology which provides real-time monitoring of multiple security appliances and historical reporting of security events from networks, systems and/or applications (Nicolett and Kavanagh, 2009). It can be seen as a new approach for enhancing the IDS, IPS and IRS technologies. SIEM technology does not only collect hundreds of incident events from various types of appliances, but can also respond to them. Given their relevance to responses, it is proper that SIEM technologies be included in this investigation.

A total of 34 systems were compared, including both commercial and non-commercial products. The commercial products were selected based on two reports from Gartner, namely the Magic Quadrant for Network Intrusion Prevention System Appliances (Young and Pescatore, 2009) and Magic Quadrant for Security Information and Event Management (Nicolett and Kavanagh, 2009). As a guideline, the non-commercial products were selected based upon the online ratings of open source products published by several experts in the area (Bejtlich, 2004; Wotring, 2005; SECTOOLS, 2010).

Using the categorisation in the response model presented the previous section; *Table 1* shows the results of the survey. In comparing the products, the study tabulates the survey results for the 1st stage of reactive response into two categories: collaboration and termination. The first category covers any responses that involve collaboration between the product and other products, while the second category refers to the ability of the product to terminate users, processes and/or network traffic. In addition, the table contains the survey results for the 2nd stage of reactive response in the “collects information” column. Finally, the study covers six categories of passive response, namely syslog and console, email, pager, SNMP, HTML and PDA/Mobile.

Product literature and documentation, white papers, and online articles were then investigated in order to determine the response options offered by the selected products. The potential for misclassification of responses is considered low, but there is some minor potential for error.

Table 1. Comparison on IDSs/IPSs/SIEM products

						Proactive			Reactive			Passive					
No.	**Name of Product**	**Company /Organization**	**Commercial (C)**	**HIDS/NIDS/SIEM**	**With SIEM**	**predicts a new attack**	**blocks future attack**	**adjust regularly**	**collaboration**	**termination**	**collects information**	**syslog and console**	**email**	**pager**	**SNMP**	**HTML**	**PDA/Mobile**
1	AlienVault	AlienVault	Both	SIEM			X	X	X	X	X	X	X		X	X	
2	ArcSight Enterprise Security Manager	ArcSight	C	SIEM			X	X	X	X	X	X	X		X	X	
3	Bro IDS with Plugin	Lawrence Berkeley National Laboratory	NC	NIDS			X		X	X	X	X	X	X	X	X	X
4	CA-Host Based IPS	CA Inc	C	HIDS	SIEM		X		X	X	X	X					
5	Checkpoint IPS-1	Checkpoint Inc	C	NIDS			X		X	X	X	X	X				
6	Cisco IDS	Cisco Systems Inc	C	NIDS	SIEM		X		X	X	X	X					
7	Cisco Security Monitoring, Analysis and Response System (MARS)	Cisco Systems Inc	C	SIEM			X	X	X	X	X	X	X	X	X	X	
8	DeepNines IPS	DeepNines Technologies Inc	C	NIDS			X	X	X	X	X	X					
9	Enterasys Intrusion Prevention System	Enterasys Networks, Inc.	C	NIDS HIDS	SIEM		X	X	X	X	X	X	X		X	X	
10	FlowMatrix	AKMA Labs	NC	NIDS							X	X				X	
11	IBM Proventia Desktop	IBM	C	HIDS	SIEM		X		X	X	X	X					
12	IBM Proventia Network IPS Series	IBM	C	NIDS	SIEM		X		X	X	X	X			X	X	
13	IBM Tivoli Security Operation Manager	IBM	C	SIEM			X			X	X		X		X	X	
14	iPolicy Intrusion Detection/Prevention	iPolicy Networks	C	NIDS			X	X	X	X	X	X	X			X	
15	Juniper IDP	Juniper Networks, Inc	C	NIDS			X	X	X	X	X	X			X		
16	Loglogic Exaprotect	Loglogic	C	SIEM			X	X	X	X	X					X	
17	McAfee Host Intrusion Prevention for	McAfee, Inc.	C	HIDS			X	X	X		X					X	
18	McAfee IntruShield	McAfee, Inc.	C	NIDS	SIEM		X	X	X	X	X	X			X	X	
19	McAfee IntruShield® Security Manager (ISM)	McAfee, Inc.	C	SIEM		X	X	X	X	X	X	X	X	X	X	X	X
20	netfence gateways	phion AG	C	NIDS			X		X	X	X	X	X		X		
21	NetIQ Security Manager SIEM	NetIQ	C	SIEM					X		X	X	X	X			X
22	NitroSecurity Guard IPS	NitroSecurity	C	NIDS	SIEM		X	X	X	X	X	X	X	X	X		
23	Osiris	Brian Wotring	NC	HIDS					X		X	X	X			X	
24	OSSEC	Trend Micro, Inc.	NC	NIDS HIDS SIEM			X		X	X	X	X	X	X			X
25	PHPIDS	PHPIDS Team	NC	HIDS						X	X		X			X	
26	Radware's DefensePro (APSolute Immunity)	Radware Ltd.	C	NIDS		X	X	X		X	X	X					
27	SAMHAIN	samhain design labs	NC	HIDS			X		X	X	X	X	X			X	
28	SecureNet IDS/IPS	Intrusion, Inc.	C	NIDS			X			X	X	X				X	
29	Snort IDS (Sourcefire IPS)	Sourcefire, Inc.	NC	NIDS			X		X	X	X	X	X	X	X	X	X
30	StoneGate IPS	Stonesoft Inc.	C	NIDS			X		X	X	X	X	X		X		X
31	Strata Guard	StillSecure	C	NIDS			X			X	X	X	X		X	X	
32	Symantec Critical System Protection	Symantec	C	HIDS			X		X	X	X	X			X	X	
33	TippingPoint IDS/IPS	3Com	C	NIDS			X	X	X	X	X	X	X	X	X		
34	Top Layer Security : IPS	Top Layer Networks	C	NIDS			X	X	X	X	X	X	X		X	X	

From the table, it can be seen that the Network Intrusion Detection Systems (NIDS) category is dominated by commercial products, and only 4 out of those 19 products are non-commercial. Apart from those, the survey results show that 26 products are classed as stand-alone IDS or IPS product while the rest are SIEM products or a combination of SIEM and IDSs/IPSs products. This report highlights that at least seven IDS/IPS products use an SIEM from same company, namely Trend Micro, McAfee, IBM, Enterasys Networks, NitroSecurity, Cisco Systems and CA Inc.

Interestingly, the survey highlights the following;

- Only two products used the first type of proactive response: McAfee IntruShield® Security Manager (ISM) and Radware's DefensePro (APSolute Immunity).

- Most of the products apply the second stage of the proactive response; 80% of the products apply blocking mechanism techniques as a proactive response, but only 44% of products had the ability to automatically adjust the configuration regularly.

- Not all the products have the ability to establish a collaboration with other security appliances, and only 82% of the products surveyed use first stage of the reactive response

- 30 products, or 88% of the products surveyed, are able to terminate incident traffic sessions actively.

- All the products have an ability to collect information about incidents, which is the second stage of the reactive response.

- All the products support passive responses, with 88% of the survey products using either console or syslog as the main notification method.

- Email, HTML and SNMP are supported by the majority of products to notify security analysts.

- Pager and mobile notification are relatively rare, with less than 10% using these types of notification.

In conclusion, the survey results have demonstrated that there are a wide range of types of response option in the latest security tools; it also showed the categorisation of the response model used was satisfactory.

Although this survey has provided an analysis of the response options available in IDSs and other security tools, the results cannot be used as an evidence to demonstrate the best product for mitigating intrusions. For instance, if one of the products listed in the table has more than one type of response, or even if it has all of them, that does not necessarily mean it is the best product.

2.3 Summary

This chapter has underlined the current state-of-the-art types of response by investigating and comparing their unique characteristics and operations through the different modes of IDSs, response taxonomies and response models. The response model used divides responses into several categories, include proactive, reactive and passive responses.

Strengthened by the result of an investigative survey, the categorisation allows the strategy used to respond to incidents to be modelled. The objective of the strategy is to map incidents with appropriate type of responses flawlessly based upon their characteristics, criticality and urgency. For example, a serious incident can be mapped to a proactive response or reactive response in order to minimise its impact, as opposed to incidents with less impact which can be mapped to passive ones.

In order to propose a framework to satisfy the latter example, there are many other aspects that need to be discussed. Although the mapping process can be achieved manually, it is not as easy as its sounds because there are different types of incident that must be dealt with. Several issues therefore need to be considered before the selection process can be done, such as the decision factors and their assessment. In the next chapter, a review of the relevant theories that could be used in facilitating the response selection process will be presented. The review examines the state-of-the-art incident prioritisation processes, risk assessments and decision theories.

3 Incident Prioritisation and Issues

A response to an incident can be achieved by initiating one or more response options, as detailed in the previous chapters. The response selection process can be done manually, where security analysts select an appropriate response based upon their experience, in order to minimise the impact of the incident. In view of that, a methodical approach that identifies the importance of incidents is essential. However, with thousands of incidents being identified every day, relying upon manual processes to identify their importance and urgency is tedious, difficult, complicated and error-prone, as well as time-consuming, and so an automated operation is needed.

To enable an autonomous mode, two types of assessment can be used: a qualitative or a quantitative assessment. After reviewing earlier works on response selection (Carver, 2001; Lee *et al.*, 2002; Papadaki, 2004), the consensus is that quantitative assessments are preferable to qualitative assessments due to certain characteristics, such as the decision factors (objective data and numerical value), the adoptability of the assessment, and the usability of the results. There have been two seminal works on the response selection process: the adaptive approaches (Carver *et al.*, 2000; Ragsdale *et al.*, 2000; Carver, 2001) and cost-sensitive approaches (Lee *et al.*, 2002; Stakhanova *et al.*, 2007a). In addition, several studies have been published more recently, in 2009 and 2010, which look at areas such as using decision theories with hierarchical task network planning (Mu and Li, 2010), decision models using genetic algorithms (Fessi *et al*., 2009), and the adaptation of game theory to give a cost-sensitive approach (Lye and Wing, 2005; Zonouz *et al.*, 2009).

Compared to the amount of work published on the response selection assessment, there has been less study of incident prioritisation as part of the response selection process, mainly because the quantitative assessment has been dominated by the cost-sensitive approach and its varieties. Fundamentally, incident prioritisation is normally used to rate and rank incidents (Porras *et al.*, 2002; Lee and Qin, 2003), and based upon some studies (Årnes *et al.*, 2005; Mu *et al.*, 2008; Zhang *et al.*, 2009), the process of determining the incident priority has huge potential in selecting an appropriate response according to the different characteristics of incidents, such as asset criticality and threat severity. Although the incident prioritisation process is a quantitative assessment, its characteristics are dissimilar to the adaptive and cost-sensitive approaches due to the decision factors and estimation models used to facilitate the response selection process. Porras *et al.* (2002) and Alsubhi *et al.* (2008) realised the advantages of incident prioritisation, but less attention has been given to adapting this approach in automated response technologies. Due to these factors, this study explored the feasibility of adapting the incident prioritisation process into the response selection process in order to facilitate an autonomous mode in IRSs.

Prior to presenting the proposed new framework for incident prioritisation, it is important to analyse the existing work in the area. This chapter begins by reviewing the research on incident prioritisation, as well as the work that has influenced and informed the proposed framework. The chapter concludes by identifying all the important issues that surround and support the incident prioritisation and response selection process.

3.1 Incident Prioritisation

An early study in incident prioritisation was conducted by Porras *et al.* (2002), who focused on alert ranking and introduced a system called the M-Correlator. Since then, several other studies have been published (Lee and Qin, 2003; Alsubhi *et al.*, 2008; Dondo, 2008), each adopting a different approach to the prioritisation of incidents. The common approaches in prioritising incidents include *static prioritisation*, *vulnerability pre-prioritisation* and *post-incident prioritisation*.

3.1.1 Static Prioritisation

The static prioritisation approach uses tagging and tuning of signatures based upon the characteristics of the vulnerabilities and experts' experiences in order to prioritise incidents. For example, Snort 2.1 provides the *Severity Identifier* option which can be used to set a priority tag for some signatures which overrides the default priority (Caswell and Beale, 2004). The process of tagging priorities in the Snort IDS involves two different approaches: a manual tagging process for the signatures and a typical customisable configuration file named *classification.config.* Some commercial products have adopted a similar approach to the Snort IDS; for example, Cisco Systems Inc (2009) provides an alert-severity as one of the parameters in its signature engines. The advantage of this approach is that it offers a pre-prioritisation process that assists proactive responses, and it estimates the potential impact and severity of each specific vulnerability based upon the characteristics of the vulnerability itself. On the other hand, there are a number of drawbacks to this approach, such as:

(a) *Manual Processes*. The manual processes involved in tagging and tuning signatures are time-consuming and hence impractical. In addition, the signature tuning process needs knowledgeable experts, otherwise the it could actually increase the risk of missing real attacks (Tjhai *et al.*, 2008b).

(b) *Static Rules*. Since signatures are static, only incidents with particular known vulnerabilities can be prioritised. A new and unknown signature needs to be analysed later and, as such, new incidents cannot be prioritised.

(c) *Different tags in different contexts*. Based upon where or when the signature is triggered, its priority might need to change accordingly. However, this is not possible with static prioritisation. For example, an incident detected in a critical asset, such as a server, might be considered to be a high priority incident as opposed to if a similar incident affected a non-critical asset such as a personal computer.

(d) *Time*. Although the process of tagging can be minimised using groups of attack classifications, an additional process is still needed to classify new attacks, and so, again, extra time is needed.

(e) *No clear guidelines*. Determining the value of the priority is largely subjective. Since there is no systematic approach, its effectiveness could be influenced by the expertise of the people tagging and tuning the signature.

Static prioritisation still has merits as a way to roughly differentiate groups of attacks based on their type and severity. However, it is still far from being able to offer a flexible and adaptable prioritisation solution to suit different contexts.

3.1.2 Vulnerability Pre-prioritisation

Vulnerability pre-prioritisation offers a similar approach to static prioritisation but uses more systematic methods such as risk assessment or expert systems to determine the priority of vulnerabilities. Dondo (2008) applied a fuzzy system approach in assessing the potential for risk in order to rank vulnerabilities. Perhaps the most widely-used approach is the Common Vulnerability Scoring System (CVSS) (Mell *et al.*, 2009), which provides severity impact scores for known vulnerabilities. The advantages of the vulnerabilities pre-prioritisation approach are similar to those of the static prioritisation approach, and include:

(a) *More systematic approach*. This approach applies clear indicators in estimating the risk of potential incidents. For example, the Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of vulnerabilities, which it places into three main groups: Base, Temporal and Environmental (Mell *et al.*, 2009).

(b) *Increased automation*. This approach is more systematic and therefore reduces the need for manual prioritisation by using semi-automatic or fully-automatic processes.

(c) *Proactive responses*. This approach offers a pre-prioritisation process which benefits proactive responses. For instance, a manual proactive response, such as blocking specific events using firewall rules, can be done for potential incidents with a high severity impact.

However, it also has some drawbacks:

(a) *Increased complexity*. The method of calculating the vulnerability risk can be complex, and the number of indicators that need to be estimated can be considerable. This could be even more significant when the process is completed manually.

(b) *Applies only to known vulnerabilities*. A vulnerability score needs to be given before incidents can be prioritised. Therefore, unknown and new vulnerabilities cannot be considered in the first instance. Given the increasing number of vulnerabilities discovered every day (Symantec, 2011), this poses a significant disadvantage.

(c) *Does not consider the asset characteristics*. The estimation of risk is solely based upon the risk of the vulnerability and not on the characteristics of the target.

(d) *Limited flexibility.* Another limitation is that the estimation of risk is static and does not take into account changes in the environment over time. For example, a risk cannot change automatically if new patches or solutions are discovered.

The two aforementioned approaches allow incidents to be prioritised based upon pre-determined vulnerability tags, the priority of those vulnerabilities and signature tuning. Their main limitation is that they only prioritise incidents with known vulnerabilities.

3.1.3 Post-incident Prioritisation

Unlike the previous approaches, post-incident prioritisation focuses upon the process of investigating and evaluating incidents based on the level of potential risk after incidents occur. It has been introduced by Porras *et al.* (2002), Lee and Qin (2003), Yu *et al.* (2004), Årnes *et al.* (2006) and Alsubhi *et al.* (2008).

(a) *M-Correlator*. Porras *et al.* (2002) introduced an incident ranking computational model in a “mission-impact-based” correlation engine, known as the M-Correlator, which bases its judgements upon several factors, such as the likelihood that an attack will succeed, the importance of the targeted assets and the popularity of an attack.

(b) *Bayesian Network Model*. Lee and Qin (2003) proposed a priority computational model based upon Bayesian Networks which estimate risk by considering three criteria; computer network assets, attacks and vulnerabilities.

(c) *Collaborative Architecture*. Yu *et al.* (2004) proposed a general collaborative architecture for multiple IDS products by combining intelligent agents and knowledge-based alert evaluation. They evaluated the alert priority, based on asset characteristics, and they used it as the input to their correlation system.

(d) *Risk Assessment Model*. Årnes *et al.* (2006) proposed a network risk assessment using several strategies including examining the composition of risks to the individual host and applying the Hidden Markov Model (HMM) to represent the likelihood of transitions between security states.

(e) *Fuzzy system*. Alsubhi *et al.* (2008) proposed a fuzzy system based upon several metrics, such as the applicability of attacks, the importance of victims, the relationship between the alerts under evaluation and previous alerts, and the *social activities* occurring between the attackers and the victims.

The advantages of adopting post-incident prioritisation are as follows:

(a) *It includes pre-prioritisation*. The post-incident prioritisation scheme incorporates the advantages of pre-prioritisation, and extends them by offering real-time risk assessment of incidents.

(b) *Increased automation*. Inherited from the pre-prioritisation approach, this approach increases automation by applying semi-automatic or fully-automatic processes.

(c) *Increased contextual awareness*. In order to increase contextual awareness it incorporates more decision factors, such as ones related to assets and vulnerabilities.

(d) *Evaluates new and unknown vulnerabilities*. Given that the estimation of risk does not rely solely on the risk of vulnerabilities, it is also possible to prioritise incidents that involve new and unknown vulnerabilities.

(e) *Increased flexibility*. Priorities can be changed to accommodate changes in the environment, such as the release of new patches or solutions.

However, the post-incident prioritisation also displays the following drawbacks:

(a) *Increased complexity*. The increased number of indicators could result in a lengthier and more complicated process for the collection and gathering of information. For example, the approach uses many matrices, which can arguably place practical limitations on live traffic networks and online assessment systems.

(b) *Unavailability of information*. The prioritisation process could be affected by missing or unavailable information, which is used to estimate indicators.

(c) *Lack of weighted factors*. It does not allow for different weightings based upon the importance of different factors. The use of different weightings could provide more flexibility and allow the incident prioritisation process to reflect organisational policies.

(d) *Lack of prioritisation schemes.* It does not provide any specific scheme to prioritise incidents. It only uses a high number for high priority and a low number for low priority, without specifying any detail about the priority itself.

Apart from studies focusing on incident prioritisation, there are also other approaches that are loosely related, mostly focused upon response selection. Zhang *et al.* (2009) explored the relationship between network assets and intrusion alerts in an effort to provide alert prioritisation. Incident prioritisation is often attempted indirectly by cost-sensitive response approaches in which a response is selected based on cost factors, such as the operational, damage and response costs. Lee *et al.* (2002), Stakhanova *et al.* (2007a) and Wang *et al.* (2007) all discussed the relationship between cost and responses. Incidents are often prioritised indirectly based on the relationship between the response and cost, but, again, there is not enough emphasis on incident prioritisation.

In order to facilitate the response selection process, post-incident prioritisation is the best approach. With the advantages it brings, the process could be implemented to be automatic. In addition, it also considers different contexts in initiating the response selection. As this is the first attempt to consider the feasibility of prioritisation as one of the response selection assessments, there are other key areas that need to be examined, particularly the details of the process itself.

3.2 Proposed study key focus areas

In order to establish a methodological approach to prioritising incidents and to support the response selection process, based on the limitations of existing studies, the proposed study believes the most important issues to be focussed on are rating, ranking and response.

Generally speaking, the combination of these three issues is necessary in order to provide a methodical approach to facilitating the incident prioritisation and response selection process. *Figure 5* illustrates briefly how this combination of factors can be used to determine the importance of each issue as well as the relationships between these factors.

Firstly, in order to differentiate between the most critical incidents and less critical ones, it is important to rate them. The rating procedure rates incidents and aims to produce quantitative values. Risk assessment plays a key role in achieving that by evaluating and investigating incidents. Based upon the values produced, the rating procedure aims to rank them quantitatively and then categorise them into qualitative groups. To achieve the second part, decision theories are the focal point of the study. Finally, the next step after the rating and ranking procedures is to respond to them. Thus, the key area upon which to focus is the strategy to be used to map incidents to appropriate responses based upon their priorities.

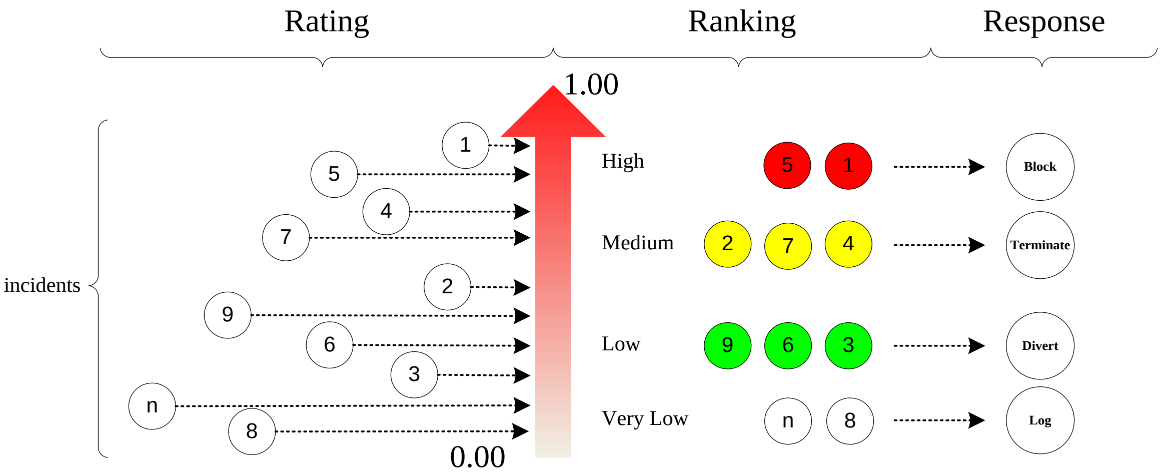


Figure 5. Rating, Ranking and Response

3.2.1 Rating incidents

This section discusses the role of risk assessment and how it can be used in incident prioritisation. Fundamentally, risk assessment is a risk estimation process based on a combination of the likelihood of an event and the consequences of that event, as well as the relationship between risk and uncertainty (Kaplan and Garrick, 1981; Kaplan, 1997). A risk assessment model has been successfully adopted in the many studies in areas such as engineering, science, manufacturing, business, management and public policy, as it not only helps analysts to evaluate risks, but also to identify, measure and quantify them and evaluate their consequences and impacts (Haimes, 2009). Its most valuable aspect is therefore in facilitating the decision-making process (Haimes, 2009). In security contexts, the assessment is done in the following stages.

(a) *Risk assessment models.* One of the earliest models, proposed by Campbell and Sands (1979),took a modular approach to managing computer security risk and its design provides a model that consists of several sub-models, including value analysis, threat analysis and identification, vulnerability analysis, risk analysis, risk assessment, management decision and control implementation (Hamdi and Boudriga, 2005).

(b) *Risk assessment adoption*. Gehani and Kedem (2004) and Mu *et al.* (2008) introduced an online risk assessment model and Zhang *et al.* (2008) presented a model-based semi-quantitative approach to evaluate security in enterprise networks. These projects offer only general risk assessment and have not been designed with incident prioritisation in mind.

(c) *Risk assessment standards.* Risk assessment is the core competence of information security management and has been adopted in many standards, such as the National Institute of Standards and Technology (NIST) (Stoneburner *et al.*, 2002; NIST, 2009) and the ISO/IEC 27000 family (Calder and Watkins, 2010). In general, these standards provide a foundation for the development of an effective risk management programme.

(d) *Risk assessment frameworks*. The risk assessment framework is not a new concept (for examples see FMEA (IEC, 2006), OCTAVE (CERT, 2009), CRAMM (1987) and CORAS (2001)); they generally provide comprehensive tools to evaluate risk.

Risk assessment is a methodical approach used to aid security analysts in evaluating an incidents' risk using threats, vulnerabilities and assets. In managing the risk assessment, risk management is used to express the entire management process of risk assessment (Haimes, 2009). In computer security contexts, risk management is defined as a systematic process used to identify, mitigate and control risks. It consists of several sub-processes, including risk assessment, risk identification, risk mitigation, risk monitoring and risk evaluation (Stoneburner *et al.*, 2002; Hamdi and Boudriga, 2005). Risk assessment offers several advantages to the incident prioritisation process, such as:

(a) *Systematic procedures*. Risk assessment combines systematic processes in identifying incidents' risk, and in determining their consequences and how to deal with them. In addition, it gives a wide definition of risk by focusing upon the relationships between incidents, threats, vulnerabilities and assets, which benefits the incident prioritisation process.

(b) *Covers various factors*. Risk assessment covers various factors to facilitate decision making such as an analysis of assets and values, an identification of threats and vulnerabilities, management control, and cost-benefit evaluation.

(c) *Easy to adopt.* Risk assessment is not a new concept and so is easy to adopt in organisations. In addition, risk assessment supports various standards, frameworks and tools that allow the incident prioritisation process to be understood easily by different levels of management.

(d) *Appropriate responses to risks.* Risk assessment facilitates decision makers in identifying the risk of incidents using a variety of approaches, such as qualitative or quantitative approaches (Kaplan and Garrick, 1981), and it allows the identification of high-risk incidents based upon their priority, urgency and importance. As a result, an appropriate response could be arranged to counter those incidents.

(e) *Usability of results.* Risk assessment always uses the same decision factors to evaluate an incident's risk and so produces consistent results. This allows information sharing between networks and organisations and allows the incident prioritisation process to cover a wide range of networks.

(f) *Easy to understand results.* Although the incident prioritisation process can be done systematically, sometimes the assessment results are not user friendly and can be hard to understand. However, the use of risk assessment allows assessment results to be shared with other third parties, such as employees, board members, and shareholders, because the results can be represented in many ways (such as using qualitative or quantitative results). Furthermore, the diversity in the presentation of results offers a simple and practical way to aid different levels of management in their decision making.

Apart from the aforementioned general advantages, there are also more specific advantages to be gained depending upon the specific approach taken towards risk assessment. There are two approaches to risk assessment: qualitative and quantitative (Kaplan and Garrick, 1981). *Figure 6* briefly illustrates the common objective of both approaches, despite their dissimilarities in terms of their processes.

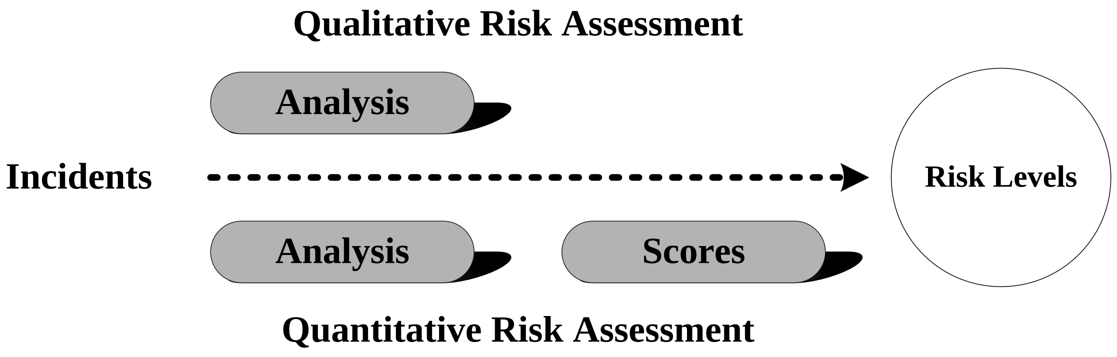


Figure 6. Qualitative and Quantitative Risk Assessment

A quantitative risk assessment is a methodical, step-by-step calculation of asset valuation, exposure to threat and the financial impact or loss of an event (Gregg and Kim, 2005). Quantitative assessment uses monetary values and applies it to the components used in the estimation process (Munteanu, 2006). Using quantifiable data and results, quantitative risk assessment applies mathematical models, functions and theories. Therefore, quantitative assessment produces a lot of numerical relationships, mathematical equations and utilises statistical techniques in the analysis procedures, which include the Single Loss Expectancy (SLE), Exposure Factor (EF), Annualized Rate of Occurrence (ARO), Annualized Loss Expectancy (ALE), and the safeguard cost or benefit analysis (Blakley *et al.*, 2001; Munteanu, 2006). Furthermore, Butler (2002) and Ekelhart *et al.* (2007) discussed the relationship between the results of a quantitative risk assessment and a cost-sensitive or cost-benefit analysis. Interestingly, the cost-benefit ratio of individual safeguards discussed there is similar to a study involving the cost-sensitive modelling of intrusion responses conducted by Lee *et al.* (2002).

Alternatively, instead of having numbers and equations like the quantitative risk assessment, the qualitative risk assessment takes a scenario-based approach (Munteanu, 2006), where the scenario is examined and assessed for each critical or major threat to an asset (Gregg and Kim, 2005). The qualitative risk assessment requires the calculation of intangible factors (i.e. factor that does not having a physical substance or an intrinsic productive value), such as impact (i.e. asset criticality) and subjective attack probability (whether there is a high, medium or low level of threat and vulnerability). In this approach, intangible factors and subjective probability need to be measured so that the value is quantifiable and easy to evaluate and compute. The purpose of a qualitative risk assessment is to provide a consistent and subjective assessment of the risk (Gregg and Kim, 2005). In order to estimate risk, the qualitative risk assessment uses some transition tables such as *a qualitative scale*, *the probability and impact matrix*, and *risk matrix summary table*. These tables and scales are important to the qualitative risk assessment as they can be used to transform numerical values such as 1, 2 and 3 into verbal values such as low, medium and high, and vice-versa.

Both approaches offer promising results in valuing threats, assets and vulnerabilities. However, both approaches also give similar degrees in terms of the advantages and disadvantages. It is thus important to address these strengths and limitations.

The adoption of risk assessment in the incident prioritisation process has both advantages and disadvantages. Therefore, in order to reduce the disadvantages while at the same time promoting the advantages, the following suggestions should be considered when combining the use of both types of assessment.

(a) *Input to the decision factors*. In order to support the decision factors of the incident prioritisation process, different types of input should be properly considered in order to obtain the best input, whether qualitative or quantitative, to support the assessment. The use of quantitative data is always better than qualitative data (Munteanu, 2006). Additionally, quantitative data is more precise than qualitative data (Houmb *et al.*, 2009). Unlike qualitative data, quantitative data is objectively measurable because it uses numbers for values. As there is no translation from a numerical value to a different qualitative scale (such as high, low or medium), it represents a more accurate value.

However, the process of obtaining quantitative data is not an easy process. The collection of quantitative data requires many procedures; therefore, it needs an appropriate tool to synchronise the data or else the final results will not be reliable enough. However this limitation can be reduced by using automatic tools to collect the data.

As the use of quantitative data gives advantages in terms of its usability and results, this type of information is preferable. However, if there are difficulties in obtaining quantitative data, qualitative data should be considered. The use of qualitative data should involve their transformation to numerical values to facilitate the estimation process. However, the process of transforming or rescaling subjective data is not easy to be achieved.

(b) *Risk estimation process*. Both approaches use mathematical functions to estimate risk, but the qualitative assessment uses less complex functions compared to the quantitative assessment due to its characteristics, such as having less numerical values and adopting matrix tables such as the raw risk ratings matrix and the impact and probability matrix. The adoption of sophisticated mathematical formulae in the quantitative assessment increases the use of numerical values, and often requires more processing power and this overhead for the processing power might be a disadvantage for real-time systems. Therefore, reducing the overhead should be one of the considerations. In addition, arithmetic operations could be reduced by applying simple mathematical functions, as one of the advantages of adopting a quantitative assessment is that it provides a measurement of the magnitude of the impact, which can then be used in the cost-benefit analysis (Stoneburner *et al.,* 2002). In previous works on response selection (Carver, 2001; Lee *et al.*, 2002; Papadaki, 2004), quantitative assessment is generally preferred to qualitative assessment due to its characteristics such as decision factors (e.g. objective data and numerical values), the adoptability of the assessment and the usability of results.

(c) *Output – result representations*. As both types of assessments have many advantages in terms of their representation of results, it is suggested that both should be considered. The combination of both qualitative and quantitative results benefits the interpretation of the incident prioritisation results, as the variety of result representations helps improve understanding at different levels of management. However, using a suitable scale to transform numerical results to verbal results is another challenge. In terms of the level of efficiency, the adoption of quantitative assessment provides more efficient results than qualitative due to the implementation of mathematical functions and statistical models. As such, it provides a credible set of results which remain the same even if the process is run in different environments and at different times. The usability of results in a quantitative assessment is better than in a qualitative assessment, and in most cases they can also be used again in different environments. Although the usability of results is better in the quantitative assessment, high-level management who are not directly engaged with the assessment process may have different understandings of certain types of mathematical functions and graphs. Sometimes, therefore, the numerical results need to be interpreted in a qualitative manner (Stoneburner *et al.*, 2002). Some results might need to be expressed in a management language in order to increase the level of understanding. However, the process of changing the original expression reduces the precision of the result and may differ from the original objectives. Furthermore, qualitative assessments often produce hypotheses and provide a broad view of understanding that can be linguistically understood by most non-technical people. However, in such a subjective representation, this can be hard to measure. In addition, the results of a qualitative assessment process cannot be easily tracked because of their subjective nature and the difficulty in evaluating them (Hamdi and Boudriga, 2005).

3.2.2 Ranking incidents

Although the prioritisation process can be achieved strategically using risk assessment, understanding the risk itself is not sufficient to allow incidents to be prioritised. There are other issues inherent in the rating procedures, such as the selection of a suitable approach to facilitate the assessment process and how to represent the final result; particularly whether the results are ranked in qualitative or quantitative manners. Thus, this section will establish the general issues pertaining to the process, including the decision theory and the theory of measurement.

In addressing some of the limitations of the previous approaches, this section will focus upon the rating and ranking issues by looking at the most suitable method for making a systematic decision. When selecting a methodical approach for prioritising incidents, there are many approaches that can be used. On top of risk assessment, this study explores the possibility of using other methods, particularly common and well-known approaches from the decision making studies but which are not currently being adopted and applied in the incident prioritisation process.

Since many approaches can be used in prioritisation, there is confusion amongst decision makers on selecting which method is the best. Therefore, to reduce the confusion, the specific type of the prioritisation method can be explained by giving the scale used in the result representation. For example, Forman and Gass (2001) discussed the importance of the scale in relation to the result of the decision-making process. With appropriate scales, the results from the prioritisation process can be arranged either as *a list* or as *a group* of incidents, based upon their numerical (e.g. 1, 2 and 3) or verbal (e.g. low, medium and high) values. Therefore, it is important to explain the scale first.

In the theory of scales, Stevens (1946) introduces four different types of scales that can be used for measurement: nominal, ordinal, interval and ratio. However, in the prioritisation process, only two main scales are widely adopted, a ratio scale and an ordinal scale.

(a) *Ratio scale.* This not only provides ordering of results and relative distance between them, but also considers their importance (Karlsson *et al.*, 2006). Using a ratio scale, the differences between results can be measured statistically where the distance is clearly defined. For example, if the scale uses 1, 2, 3 and 4 to differentiate between results, the scale value of two means the value 2 is twice that of one, while if a scale value of four is used, then the result is four times better to the scale of 1 and two times better than scale of 2. For example, Hierarchical Cumulative Voting (Berander and Jönsson, 2006), Analytic Hierarchical Process (AHP) (Saaty, 2008a, 2008b), Paired Comparison Analysis (Thurstone, 1927) and Grid Analysis (Manktelow, 2003) use this type of scale.

(b) *Ordinal scale*. Alternatively, an ordinal scale uses a scale either using numbers like 1, 2, 3, and 4 or qualitative groups, like high, medium and low, which denote whether one result is higher or lower than another. For example, to illustrate the use of this scale, unlike in the ratio scale, a result with a scale of '4' does not imply a value that is double that of '2', and a result with a scale of '2' does not indicate a value worth twice that scale of '1'. The ordinal scale illustrates the rank of qualitative and uncertain value by indicating that '2' is 'more' than '1', and that '3' is 'more' than '1' and '2', and so on. Originally, an ordinal scale arose from the operation of rank-ordering, and this scale is widely and effectively used by psychologists (Stevens, 1946). Some well-known methods use this type of scale, such as Cumulative Voting (Bhagat and Brickley, 1984), Multi-Voting, Binary Search Tree (BST), Covey's Quadrants (Covey, 2004), Planning Game Partitioning (Karlsson *et al.*, 2007), and ABC Analysis (Chu *et al.*, 2008).

Thus, in order to facilitate the result representation and the risk assessment approaches, it is important to consider an appropriate scale for the proposed framework. As one of the important characteristics of the proposed framework is to have a relative distance between incidents' priorities, the ratio scale is most applicable.

To extend the incident prioritisation approached considered for adoption and to overcome some of the limitations of the existing approaches, this study will now explore the Analytic Hierarchy Process (AHP).

One popular prioritisation method is the Analytic Hierarchy Process (AHP) which has already been successfully applied in several non-security contexts (Zahedi, 1986; Forman and Gass, 2001; Saaty, 2008a). AHP is a theory of measurement through pair-wise comparisons and relies upon the judgement of experts to derive priority scales (Saaty, 2008a). Over the last decade, AHP has been used as a method for decision makers in solving complicated problems and also as a methodology for structuring complexity (Forman and Gass, 2001). AHP uses a ratio scale and it has the ability to facilitate a synthesised process as well (Forman and Gass, 2001). In addition to prioritisation, AHP also has been applied in many decision situations in both research and the real-world, including making a choice, resource allocation, benchmarking, quality management and strategic planning. According to Karlsson *et al.* (1998), in an evaluation of six different prioritisation approaches (i.e. analytic hierarchy process (AHP), hierarchy AHP, spanning tree matrix, bubble sort, binary search tree and priority groups), they found AHP to be the most promising method, although it may be problematic to scale up.

AHP is a practical methodical approach to making decisions and the use of the method could help security analysts to identify which incidents are important and which are trivial. It consists of three main basic principles: *decomposition*, *comparative judgement* and *hierarchic composition* or *synthesis of priorities*. Compared with other methods, AHP has several advantages in the incident prioritisation process; for example, it:

(a) *Allows for a multiple-criteria environment and multi decision factors*. The primary use of AHP is to make a choice in a multiple-criteria environment; it also allows multiple factors to support the decision-making process. Its decomposition principle allows a complex problem to be structured into a hierarchy of clusters or sub-clusters.

(b) *Uses different weightings of criteria*. AHP uses different weightings of criteria and sub-criteria in prioritising options. For instance, in this study, the term 'options' is similar to incidents.

(c) *Homogeneous clusters*. AHP provides a simple way to deal with complexity by allowing homogeneous clusters of factors (Forman and Gass, 2001).

(d) *Simple and improved way*. AHP allows a simple and improved way to measure objective and subjective factors (Forman and Gass, 2001).

(e) *Ratio scale as a result*. AHP produces a ratio scale as a result of the estimation process and therefore allows decision makers to differentiate between results in a statistical manner as well as consistent between them. In addition, it has been shown that the ratio scale priorities produced by AHP are more powerful than other theories that rely upon ordinal or internal scales (Forman and Gass, 2001).

(f) *Synthesis process*. AHP facilitates analysis of the decision goals as well as allowing a synthesis process upon the decision process where it allows the decision factors to be combined to produce a complex result (Forman and Gass, 2001).

In addition to having these advantages, AHP has the ability to reduce some limitations of the post-incident prioritisation approach discussed in Section 3.1, specifically as follows:

(a) *Different weightings*. AHP allows different weightings based upon the importance of different decision factors. As such, the important indicator can be addressed differently than other less important indicators. The use of different weightings could provide more flexibility and also allow the incident prioritisation process to reflect different organisational policies.

(b) *Multiple decision factors*. AHP also allows multiple decision factors and, with different levels of decision-making and with the decomposition principle, the basic components in the incident prioritisation process can be determined with less complexity.

(c) *Practical, simple, flexible and systematic*. AHP provides a practical, simple, flexible and systematic approach in rating and ranking incidents. As such, it is very useful as an alternative approach to rate, rank and prioritise incidents in real-world applications.

(d) *Accurate, reliable, mathematically proven and easy to understand results*. AHP provides accurate, reliable, mathematically proven and easy to understand results; as such, this could increase their confidence, understanding and consistency level (Forman and Gass, 2001; Saaty, 2008b).

Recently, Saaty (2008a) discussed two modes of AHP in making decisions and prioritising alternatives: a relative and rating mode. Although the common relative mode is more accurate for comparison of alternatives, the rating mode has an advantage in rating a large number of alternatives. Therefore, in this particular case, since incidents involve many alternatives (e.g. more than 1,000 incidents), the rating mode can be considered as a preferred approach. In terms of the result of the priorities, although both methods do not deliver similar results, they are adequately close (Saaty, 2008a).

As an alternative to AHP, in the multicriteria decision analysis (MCDA) study, there are many well-proven and documented decision methods that can be used to prioritise alternatives. These include the elimination and choice expressing reality (ELECTRE) (Roy, 1991), superiority and inferiority ranking (SIR) (Xu, 2001) and grey relational analysis (GRA) (Chan and Tong, 2007). Although the aforementioned methods use multiple-criteria in making decisions and prioritising results, the reason behind exploring AHP with rating mode is simply because it *performs faster at rating a large number of alternatives* (Saaty, 2008a) and has a huge potential to prioritise incidents. Similarly, there are also other prioritisation methods, such as Weiger's Method (Wiegers, 1999), Grounded Theory (Herrmann and Daneva, 2008), Binary Search Tree (BST) (Karlsson *et al.*, 1998), Priority Group (Karlsson *et al.*, 1998; Karlsson *et al.*, 2007), Theory-W (Boehm and Ross, 1989), voting schemes (e.g. Cumulative Voting or Weighted Voting (Ayad and Kamel, 2008), and 100-Point Method (Leffingwell and Widrig, 2003). These are also *limited to a small number of criteria and alternatives* and hence they are not suitable for rating and ranking incidents. Furthermore, AHP is the most popular, approachable, and practical, as well as being a well-proven method used in decision-making, and it has been validated in many real and hypothetical examples (Saaty, 2008b).

Although there are some criticisms of AHP, Zahedi (1986), Forman and Gass (2001) and Saaty (2008a) reported that many applications apply AHP in making decisions. The criticisms that exist are mainly focused upon the theoretical and technical aspects of AHP, such as rank reversal, inconsistent judgement on priorities, fundamental scales used in AHP and the pair-wise comparison method. However, these issues are not a big problem because AHP provides a way to make a complex decision and has been used in many studies and has also been validated in many examples, both real and hypothetical (Saaty, 2008b). In detail, some of the interesting criticisms are as follows:

(a) *Rank reversal*. Risk reversal is concerned with the illegitimate changes in the rank of results (e.g. alternatives) upon changing the structure of the decision, such as i) add or delete new input (e.g. alternatives) and ii) add and delete new decision factors (e.g. criteria). This, however, has been addressed by other studies (Forman and Gass, 2001; Saaty, 2008b) and it is important to know that it can be reduced in some specific cases, such as i) only in an ideal mode can the rating be made where the decision factors or input (e.g. alternatives) have been decided first before it can be used (i.e. known as a closed system). Other detailed explanation can be found in Forman and Gass (2001).

(b) *Inconsistent judgement on priorities*. The second problem is related to inconsistent verbal judgments (e.g. low, medium and high) and their effect on aggregating such judgments or on deriving priorities from them. This, however, has been proven by other empirical studies and as a result the judgement priorities can be tested using Random Index (RI), consistency index (CI) and consistency ratio (CR) formulas (Saaty, 2008b).

(c) *Fundamental scales used in AHP*. The third criticism is related to the fundamental scales used in AHP. Fundamentally, the scales are originally proposed in the earlier studies of AHP using verbal judgements (e.g. equal, weak, strong, etc). However, the modern trend of AHP has adopted a numerical scale where an ordinal scale is transformed into a ratio scale, and this scenario has created scientific arguments amongst analysts. This criticism has been addressed using a similar answer to the previous one. In addition, the fundamental scales have been proven acceptable and are widely used by other studies.

(d) *Pair-wise comparison method*. The last criticism is concerned with the limitation upon the pair-wise comparison method used in determining the priorities in AHP. This limitation addressed the theoretical and technical aspects of the method and it has been discussed in many studies (Harker, 1987; Forman and Gass, 2001; Saaty, 2008b).

Furthermore, one such example, where AHP has been used in a security context, was proposed by Wu *et al.* (2008). AHP was used to generate weights for factors in the response selection process of an automated IRS. They utilised factors such as attack restraint, service maintenance, time spending and resource consumption. More recently, Xi *et al.* (2009) used AHP to evaluate computer network information security, based upon several decision factors such as environment safety, hardware and software safety, and data security. In addition, following a similar approach, Wu *et al.* (2009) improved information system security risk assessment using fuzzy AHP. Although these studies have adopted AHP, little attention has been given to focusing upon the incident prioritisation and response selection process. In addition, there is no evidence to demonstrate an investigation upon any dataset to support such a claim.

3.2.3 Measuring Incidents with Threats, Vulnerabilities and Impacts

From several seminal works in the response selection studies (Carver, 2001; Foo *et al.*, 2005; Papadaki and Furnell, 2005; Stakhanova *et al.*, 2007a; Mu and Li, 2010), the key decision factors are mainly focused upon threats, vulnerabilities and asset characteristics which are not limited to workstations and personal computers but also include network assets (e.g. routers and servers) as well as security appliances (e.g. firewalls). As these factors are similar to the general decision factors in risk assessment, the main question is *how to measure these* and secondly, *how to make the result quantifiable so that it can be sorted according to its priority*.

Since an incident is associated with an event, particularly in an intrusion scenario, this study establishes indicators that support the decision making upon the two aforementioned decision factors (i.e. impact on asset and likelihood of threat and vulnerability). These indicators were determined by reviewing the existing literature. In order to reduce the uncertainty within the factors, this study uses a decomposition approach which has been applied in other security metrics studies (Wang and Wulf, 1997; Heyman *et al.*, 2008) and has proven useful in identifying basic components from higher level requirements (Savola and Abie, 2009); it is also one of the main principles in AHP. For instance, the basic components in the model refer to the elements that contribute input into the decision factors, also called indicators, such as type of incidents, time of incidents, cost of maintenance, replacement and other related data.

There are two well-known methods to measure the impact upon a specific asset, namely the qualitative and quantitative approaches (Hamdi and Boudriga, 2005). Fundamentally, the impact is measured using the value of the asset (Dondo, 2008). The usage of both types of data, either qualitative or quantitative, has been discussed in the previous section (see *Section 3.2.1*). The quantitative data is preferable. However, there is a limitation in making a precise and quantified value of the relevant factors that influence the assets, such as misleading results in identifying the monetary costs. Thus, in order to measure the relative magnitude of cost factors, an informal or incomplete qualitative approach has been considered in the cost-sensitive studies (Lee *et al.,* 2002; Stakhanova *et al.*, 2007a).

To determine the precise state of assets is often impossible, but it can be characterised using unique qualitative costs, in order to establish a state where one factor is independent of the others. Furthermore, the process of gathering the values that influence the decision factors is often impossible to obtain and hard to measure. Therefore, these limitations have to be considered first.

Extrapolating from the response selection studies (Lee *et al.*, 2002; Porras *et al.*, 2002; Lee and Qin, 2003; Munteanu, 2006; Stakhanova *et al.*, 2007a; Zhang *et al.*, 2007; Dondo, 2008; Mu *et al.*, 2008; Pak and Cannady, 2009; Strasburg *et al.*, 2009b; Zhang *et al.*, 2009; Kheir *et al.*, 2010), several terms have been used to draw the uniqueness of those factors, such as maintainability, criticality (i.e. confidentiality, availability and integrity), replaceability, response, failure, control and dependability cost. Since the risk assessments are done on site based (i.e. based upon organisations), there is no specific guideline or best selection because they are often selected to fit with an organisation's policies. However, to assist the selection of the best decision factors there are two considerations. Firstly, by identifying the decision factors that were actively used by the previous response selection studies, and secondly by considering the most recently used and flagged by more recent studies.

Besides the asset characteristic factors in risk assessment, the decision factors that influence the incident characteristics are important too. Extrapolating from similar studies with asset related factors, in order to measure incidents, there are several attributes which are directly carried by the detected events, including their severity, targets or victim, sources or attacker, and the time of the incident. On top of that, there are other decision factors which are indirectly carried by incidents, such as their frequency and similarity, as well as where they are detected (e.g. the placement or sensitivity of sensors). These factors are important too and they could be used to show the levels of confidence or suspicious of attacks; a higher degree contributes more value to the decision factors.

By extension, with a new exploration in security metrics in industries such as Common Vulnerability Scoring System (CVSS) (Mell *et al.*, 2006; Mell *et al.*, 2009), Cisco Risk Rating (Cisco Systems Inc, 2011) and CIS Consensus Security Metrics (CIS, 2010), where quantified values like vulnerabilities' severity could be gathered practically using an industrial standard, these could be useful as decision factors.

Furthermore, there is a dominant factor in many response selection assessments that enables the cost-sensitive approach – the effect of implementing a certain type of response as one of the decision factors. This factor has been used to measure the effectiveness of the previous response and its negative impacts. In order to define an accurate measurement of this factor, this factor has emerged with a combination of various factors, such as asset or service dependencies (Toth and Kruegel, 2002; Balepin *et al.*, 2003; Kheir *et al.*, 2010) and the importance of system resources (Stakhanova *et al.*, 2008; Strasburg *et al.*, 2009a).

It is important to understand that the process of obtaining the aforementioned information is not an easy task. *Table 2* and *Table 3* show the unique indicators to support the risk estimation process, and to indirectly facilitate the incident prioritisation and response selection processes as well. The decision factors are separated into two tables. The first table tabulates the related indicators that support the *impact on asset* decision factors or related to asset values, and the other one tabulates indicators that support the *likelihood of threat and vulnerability* decision factors. There are four columns in each table and the first column presents the indicator followed by its type in the second column. The third column describes the indicator and the last column lists the most significant references on which each indicator is based.

There are two main categories in differentiating the indicators: essential and desirable. An essential indicator (labelled ‘E’ in the tables) is a main indicator and it has been applied in many previous frameworks and is actively flagged by more recent studies. On the other hand, desirable indicators (labelled ‘D’ in the tables) are categorised as secondary indicators, only previously used by a few studies. In order to reflect this difference, essential indicators are given a higher priority in terms of their value, whereas desirable indicators receive a lower priority.

Table 2. Indicators for Impact on asset

Indicator	Type	Description	References
Criticality	E	Criticality estimates the importance and value of the asset. Criticality is based on three main and common attributes in security, such as confidentiality, integrity and availability. Criticality also uses an asset value in estimating the final rating. Generally, the higher the criticality, the higher the impact on the asset.	Lee *et al.* (2002) Porras *et al.* (2002) Gregg and Kim (2005) Rogers *et al.* (2005) Davis *et al.* (2007) Zhang *et al.* (2007) Dondo (2008) Fenz and Neubauer (2009) Mu *et al.* (2008) Zhang *et al.* (2009)
Maintainability	D	Maintainability measures the cost of maintaining assets and is based on monetary value. Maintainability is similar to operational costs where it is used in maintaining the operation of the assets as well as the setup cost to protect them. For example, the cost of maintenance is measured by calculating the average cost in maintaining and protecting assets annually. Generally, the higher the maintainability, the higher the impact on the asset.	Lee *et al.* (2002) Munteanu (2006) Zhang *et al.* (2009) Strasburg *et al.* (2009b)
Replaceability	D	Replaceability refers to the ability to replace an asset in terms of cost and time. There is a trade-off between replaceability and asset criticality. Unlike the asset criticality, the higher the asset replaceability, the lower the impact on the asset. For example, the rating of the replaceability can be estimated using the cost of replacement and mean time to replace. By extension, cost of replacement can be estimated using the total of replacement cost for a specific asset within a year. Furthermore, the mean time to replace measures the effectiveness of the asset to be replaced from any incidents' impact. The sooner the replacement is placed, the less impact on the asset.	Lee *et al.* (2002) Munteanu (2006) Haslum *et al.* (2007) Pak and Cannady (2009) Zhang *et al.* (2009) Strasburg *et al.* (2009b)
Dependability	D	Dependability determines whether the asset is operated alone or if it depends on other assets or applications or services. The more connections an asset has with other assets, the higher its dependability is. In other words, the more connections between assets and applications, the higher the impact on the asset.	Porras *et al.* (2002) Toth and Kruegel (2002) Lee and Qin (2003) Nicole *et al.* (2004) Kheir *et al.* (2010)
Control	D	This measures the control factors that are implemented by an asset or application. Controls are used to mitigate potential vulnerability and threat. For example, the Center for Internet Security proposed three metrics to measure	Lee *et al.*(2002) Lee and Qin (2003) Dondo (2008) Ekelhart *et al.* (2009)

security metric related to control, such as Percent of Changes with Security Review, Percent of Changes with Security Exceptions and Percentage of Incident Detected by Internal Control (CIS, 2009). Generally, the higher rating of asset control, the lower the impact on the asset.

Table 3. Indicators for likelihood of threat and vulnerability

Indicator	Type	Description	References
Severity	E	Severity refers to the severity of the potential incidents and the estimation of it may relate to the extent of vulnerability. As such, the extent of vulnerability can be obtained from other sources such as the Common Vulnerability Scoring System (CVSS). Generally, the higher the likely incident severity, the higher the potential risk.	Abedin *et al.* (2006) Lai and Hsia (2007) Alsubhi *et al.* (2008) Ahmed *et al.* (2008) Ausibal and Gallon (2008) Lin *et al.* (2008) Dondo (2008) Mu *et al.* (2008) Houmb and Franqueira (2009) Subramanian *et al.* (2009) Zhang *et al.* (2009) Fenz and Neubauer (2009)
Exploitability	D	Exploitability measures the general level of exploitability of incidents at a specific time. It shows the current state of the related vulnerability and verifies the impact to a specific asset at any specific time. Generally, the higher the status of the incident's exploitability, the higher the risk.	Mell *et al.* (2006) Dondo (2008) Houmb and Franqueira (2009) Hausrath (2011) Clark and Stavrou (2011)
Sensitivity	D	Sensitivity measures the initial priority of incidents. The sensitivity shows the seriousness of the incident which is detected by certain detectors or appliances and the efficiency of detecting incidents. Sensitivity can be measured using sensor sensitivity where it indicates the current state of the incident based on the appliance and detector state. Generally, the higher the rating of the incident's sensitivity, the higher the risk.	Årnes *et al.* (2005) Årnes *et al.* (2006) Haslum and Årnes (2007) Alsubhi *et al.* (2008) Noel and Jajodia (2008) Zhang *et al.* (2009)
Similarity	D	Similarity represents the similarity between incidents' attributes within a particular period of time. The attributes are obtained from the detail between attacker and victim and they are the IP address, protocol, services and time of occurrence. In some cases, an attacker creates a scenario of incident where the process of attacking starts with scanning or reconnaissance before the real attack is done. Therefore, the similarity between incidents' attributes can be used to estimate the seriousness of the incident. Generally, the higher the incident similarity, the higher the risk.	Valdes and Skinner (2001) Xu and Ning (2005) Alsubhi *et al.* (2008) Xiao *et al.* (2008) Yu and Rubo (2008)
Frequency	D	Frequency represents the frequency of the similar incidents that occurred within a particular period of time. Unlike the	Ning *et al.* (2004) Haslum and Årnes (2007) Alsubhi *et al.* (2008)

	similarity indicator, the frequency identifies the similarity between vulnerabilities in terms of number of occurrences within a particular period of time. Frequency can be measured using incident frequency scoring where it measures the percentages of similar types of vulnerability between incidents within a certain period of time. There are several attributes which can be used to measure the frequency, including the number of alerts, number of vulnerabilities, and type of vulnerability. Generally, the higher the incident frequency, the higher the risk.	Yu and Rubo (2008) Houmb *et al*. (2009)

3.2.4 Response

So far, this study has presented issues related to the key areas applied in the rating and ranking procedures. The other challenge before a novel framework can be proposed are issues related to the strategy used to respond to incidents. The response strategy is an important issue in order to establish a proper method to establish a relationship between incidents and how to respond to them (i.e. response options). As the one of the key findings in *Chapter 2,* there are different types of responses and they may need to be mapped with incidents based upon different level of priorities.

To satisfy the latter claim, there are two types of mapping approaches in the response selection process: static and dynamic mapping (Mu and Li, 2010).

(a) *Static mapping models*. To mitigate incidents, static mapping models map incidents to predefined responses. Snort (1998) uses a static notification system to react to specific types of incidents by using a simple decision and predefine table. Although the static model is easy to define, it inherits some weaknesses. Specifically, it is possible for an attacker to predict the predefined responses. Also it does not consider the context of an incident, and it cannot be deployed in large scale systems (Mu and Li, 2010).

(b) *Dynamic response mapping models*. In contrast, dynamic response mapping models use more sophisticated methods of mapping incidents with response options, by adopting a dynamic decision making approach where responses are selected dynamically based upon the context of an incident (Mu and Li, 2010), for example, the AAIRS (Carver, 2001) and EMERALD (Porras and Neumann, 1997) systems. Several factors are used to make a systematic decision and they include attack metrics (e.g. attack confidence and severity of incident), system states (e.g. existing vulnerability and service implication) and the will of security analysts such as response goals and security policy constraint (Mu and Li, 2010). This approach has been adopted in many studies (Lee *et al.*, 2002; Stakhanova *et al.*, 2007a; Wang *et al.*, 2007).

In addition to the dynamic response model, different response strategies are adopted, such as response goal strategy (Carver, 2001; Mu and Li, 2010), response stopping power (Papadaki and Furnell, 2005) and adaptive response strategy (Foo *et al.*, 2005; Stakhanova *et al.*, 2007a).

(a) *Response goal strategy*. Carver (2001) proposed a response goal strategy where a sequence of actions (also called subtasks) is arranged to achieve a specific goal. The approach uses a prototype master analysis using fuzzy rule based on making decisions upon incidents. The study has listed several possible response goals, including analysing the attack, catching the attack, masking the attack, maximising confidentiality, maximising data integrity, minimising cost, recovering gracefully, and sustaining service. One or multiple goals need to be selected from the list and normally the selection of them is done manually by security analysts. Similarly with Carver (2001), Mu and Li (2010) developed an automated intrusion response system by adopting the hierarchical task network planning approach in their response decision-making model. In addition, they addressed the importance of response time in mapping response options and suggested that in response time decision-making, an intrusion response system can apply different response strategies to achieve a different set of response goals.

(b) *Response Stopping Power*. Papadaki and Furnell (2005) used a rule based module to identify the most appropriate response characteristics based on a Response Policy. The policy aimed to determine the most appropriate Response Phases and it is similar to the response goals used by Carver (2001). In particular, one of the characteristics to determine the policy is Response Stopping Power, where the maximum level of it reflects the strength of a response. The maximum level of Stopping Power is determined by considering factors such as responder efficiency, alert status, urgency and target importance. An advantage compared to the previous strategy is that their model considers urgency (i.e. related to response time) and target importance (i.e. asset criticality) as decision factors.

(c) *Adaptive response strategy*. This cost-sensitive model proposed by Stakhanova *et al.* (2007a) applied an adaptive response strategy and updated response options based upon the status of the previous triggered response and the value of cost as a decision factor. Their approach closely follows the approach proposed by Foo *et al.* (2005) in ADEPTS.

Although they introduced different ways to respond to incidents, they inherited some limitations as follows:

(a) *Response goal strategy*. Although the response goal strategy approach improves response performances, it is insufficient to address the urgency and importance of response time because responses are launched in sequences. In addition, since the selection of the goals is made manually, several goals need to be planned first before they can be used; hence this needs security analysts' experience.

(b) *Response Stopping Power*. The strategy relies upon inflexible and complex policies. Although it applies a customisable policy, the changes and modification to it require experts and experienced security analysts. As such, in order to reduce misconfiguration and errors in the policies, more time needs to be spent on the process of configuring the policy.

(c) *Adaptive response strategy*. There are two immediate limitations. Firstly, when dealing with an immediate response, the strategy is not very robust, mainly because it needs extra time in estimating the relative difference between the cost of damage and the cost of response. Secondly, if the first response were not effective, there would be considerable delay before another effective response could be triggered again.

Although the response selection process can be achieved using a different approach of strategies, they may share some of the following objectives.

(a) *Autonomous modes*. The dynamism of the strategy in the selection process aims to map incidents and responses automatically. This means that, instead of selecting response manually, the operation is run in an autonomous mode by initiating the appropriate response to respond to incidents based upon the assessment results. Furthermore, a serious limitation of a manual selection lies in the fact that it will only be effective with human availability, meaning a large disadvantage in case of unavailability.

(b) *Response Time*. To illustrate the importance of timely response, Cohen (1999) highlights that the longer the delay between detection and response, the higher the attack success rate is. Therefore, a fast response is important. Although the autonomous mode has indirectly improved the response time, other factors need to be considered in achieving this objective, such as assessments, its formulation and calculation, and the information gathering process, which may induce an overhead in the performance of the entire process.

(c) *False responses*. In order to increase the reliability of an automated response system, a system needs to consider false incidents. Papadaki (2004) identified this as one of the challenges in establishing an automated response system. Although the case of having false incidents is hard to identify, a proper mapping approach should consider this too. For example, a false incident should be mapped with a passive response, as opposed to a true one.

(d) *Online assessment*. In order to support real time processing, there are many factors that need to be considered, such as hardware, algorithms, codes optimisation, processor utilisation and also communication between systems (Stankovic, 1988). Although providing an online assessment system may induce an overhead in terms of its processing and performance, it benefits security analysts and automated systems to respond fast. Furthermore, although this objective is hard to achieve, Stakhanova *et al.* (2007a) identified this as a direction for their future studies.

In conclusion, the proposed framework adopts the dynamic model in its response model, as this provides some flexibility in selecting an appropriate response. In addition, in order to demonstrate the feasibility of adopting the prioritisation process in facilitating the response selection process, the aforementioned objectives have also been considered in the evaluation study for the proposed framework.

3.3 Summary

The main focus of this chapter was to establish the main challenges facing the incident prioritisation process as follows.

(a) *Incident Prioritisation*. The discussion started with the comparison of the incident prioritisation process. In order to facilitate the autonomous mode in the response selection process, the post-incident prioritisation is taken into consideration as it inherits advantages from other approaches together with other new advantages. Besides, it also reduces some of the limitations of the static prioritisation and vulnerabilities pre-prioritisation.

(b) *The rating procedures*. The main challenge in the rating procedures is to determine the suitable approach to adopt in a risk assessment process, either to apply a qualitative or a quantitative approach. Several other issues have been discussed in order to reduce the complexity of the adoption of risk assessment in the incident prioritisation process. These can be seen by categorising the general issues in the input, process and output of the procedures.

(c) *The ranking procedures*. In addition to the previous challenge in the rating process, the ranking procedures have contributed some degree of solutions in the input, process and output of the incident prioritisation process. However, there are other specific challenges in the ranking procedures. To reduce the complexity of input, there are two lists of independent indicators to support the decision factors in the risk assessment. Furthermore, in order to address the limitation of the previous approaches in the incident prioritisation process, this section discussed the advantages of considering the AHP approach. Finally, to rank incidents based upon their results, this chapter discussed the usage of two different types of scale, ordinal and ratio scale.

(d) *The respond strategy.* Along with methodical procedures in the rating and ranking procedures, the need of a systematic strategy to respond to incidents is important too. In order to propose a response model to map with the incident priority, this chapter discussed the major approaches adopted in the previous response selection studies and focused upon the dynamic mapping models. In addition, in order to demonstrate the feasibility of the prioritisation process in facilitating the selection process, there are four objectives which need to be considered.

In conclusion, this chapter intensively highlighted some related and important issues as well as some strategies to reduce the limitations upon them. Thus, it is important to address the limitations and inherit their advantages so they can be used as a guideline to build a useful and dynamic framework or enhance the current approaches, or even to improve the prioritisation process in general.

This page intentionally left blank

4 Incident Prioritisation for Intrusion Response Systems: The Framework

Having identified the literature and studies on the incident prioritisation process, this chapter details the proposed framework. The aim of the framework is to prioritise incidents based upon the identified decision factors together with the selected methods and models. The prioritisation process in the proposed framework is important as it facilitates the autonomous mode in the response selection process in IRSs. To support the process, this chapter details the procedures in the rating, ranking and response process as well as the rationale behind their implementation. The discussion continues with a detailed description of the main and sub-models that support the proposed framework.

The proposed framework attempts to identify the importance and urgency of incidents, by using a priority model called *Intrinsic Importance*. This model is based on similar work by Yoo (2010), who proposed an email prioritisation study. Choosing appropriate strategies to adopt in the framework is very important, especially when dealing with the technical aspects in the selected approach.

The proposed framework is established with the combination of two main models: Risk Index Model (RIM) and Response Strategy Model (RSM). With the aid of the Analytic Hierarchy Process (AHP), decision factors and a list of unique indicators identified in the previous chapters, RIM is a model to support the procedures in the rating and ranking process, which aims to prioritise incidents. Furthermore, RSM is a model to offer a methodical approach to a strategy for responding to incidents. The model maps different types of response options with different levels of incident based upon their priority.

Finally, in order to establish the relationship between RIM and RSM, a *Multi-Strategy Incident Prioritisation Framework* is proposed. As a first attempt to directly combine the prioritisation and response selection process, the framework combines both models together with other modules, such as web modules, in order to satisfy the objectives of this study. Furthermore, in addition to the main objective to prioritise incidents and facilitate the autonomous mode, the framework also address the limitation of the prioritisation process, which was identified in previous chapters.

4.1 Risk Index Model (RIM)

To address the issues in the rating and ranking process, this study adopts an AHP approach by establishing a new risk estimation model, which has been termed the Risk Index Model (RIM). The model estimates the risk index for every single incident based upon indicators and input obtained from asset environments and other significant attributes within the incidents (e.g. IP addresses). Based upon the strengths of the post-incident prioritisation, the Risk Index Model inherits them by rating each of the incidents to produce a risk index value. Based on the value of the risk index, incidents are ranked quantitatively from the highest to the lowest index.

The model uses a combination of two decision factors, impact on asset and likelihood of threat and vulnerability. In addition, the aforementioned factors use several other indicators such as criticality, maintainability, replaceability, etc., as listed in the previous chapters (see *Table 2* and *Table 3*; pp. 49).

4.1.1 Decision Factors for Risk Index Model

Figure 7 depicts a block diagram with the indicators that are used to estimate the risk index. Although there are other indicators, which are closely related to the factors that influence an asset’s impact and the likelihood of incidents, this study limits them to only ten indicators. The rationale behind this decision was to allow the proposed framework to work flawlessly in facilitating the autonomous mode in the response selection process. This is also important in order to operate the framework to run in a live traffic network and have the ability to perform in online assessment mode; the smaller the number of indicators the easier they are to measure, obtain and process.

Figure 7 depicts three levels of decision hierarchy structure for RIM. The decision hierarchy structure contains:

(a) Level 1 is the goal of the model. In this particular context, the model aims to rate, quantify and estimate the risk index for incidents.

(b) Level 2 includes the decision attributes of the model. These are the factors that influence the goal (e.g. the consequence, in terms of the impact on the asset, and likelihood of event, based in turn upon the likelihood of associated threats and vulnerabilities).

(c) Level 3 details the decision attributes defined in the 2nd level. Five indicators influence the impact on asset and a further five inform the likelihood of threat and vulnerability. Each indicator uses quantitative values obtained from information metrics (e.g. incident information, criticality, incident severity and sensor sensitivity).

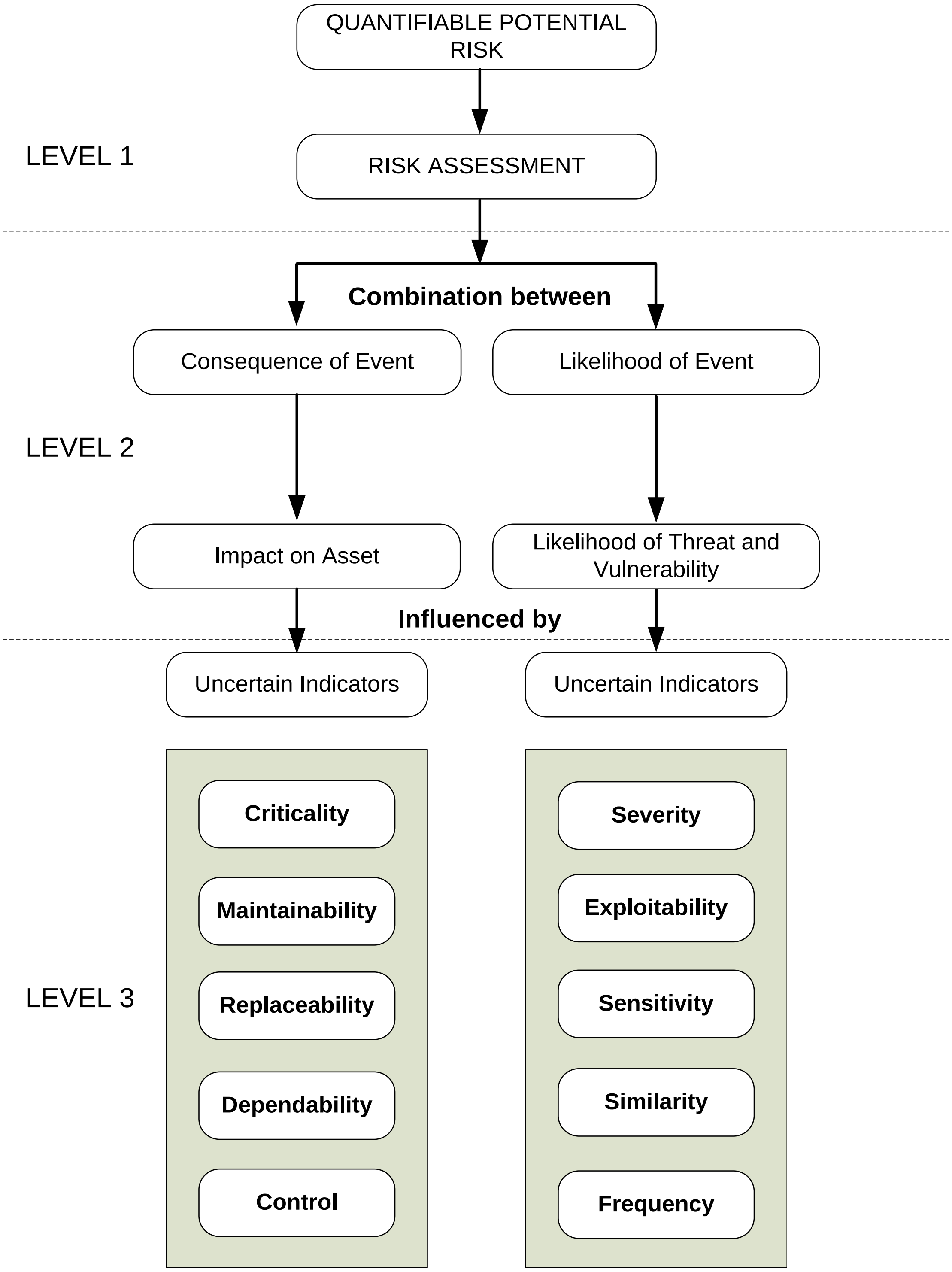
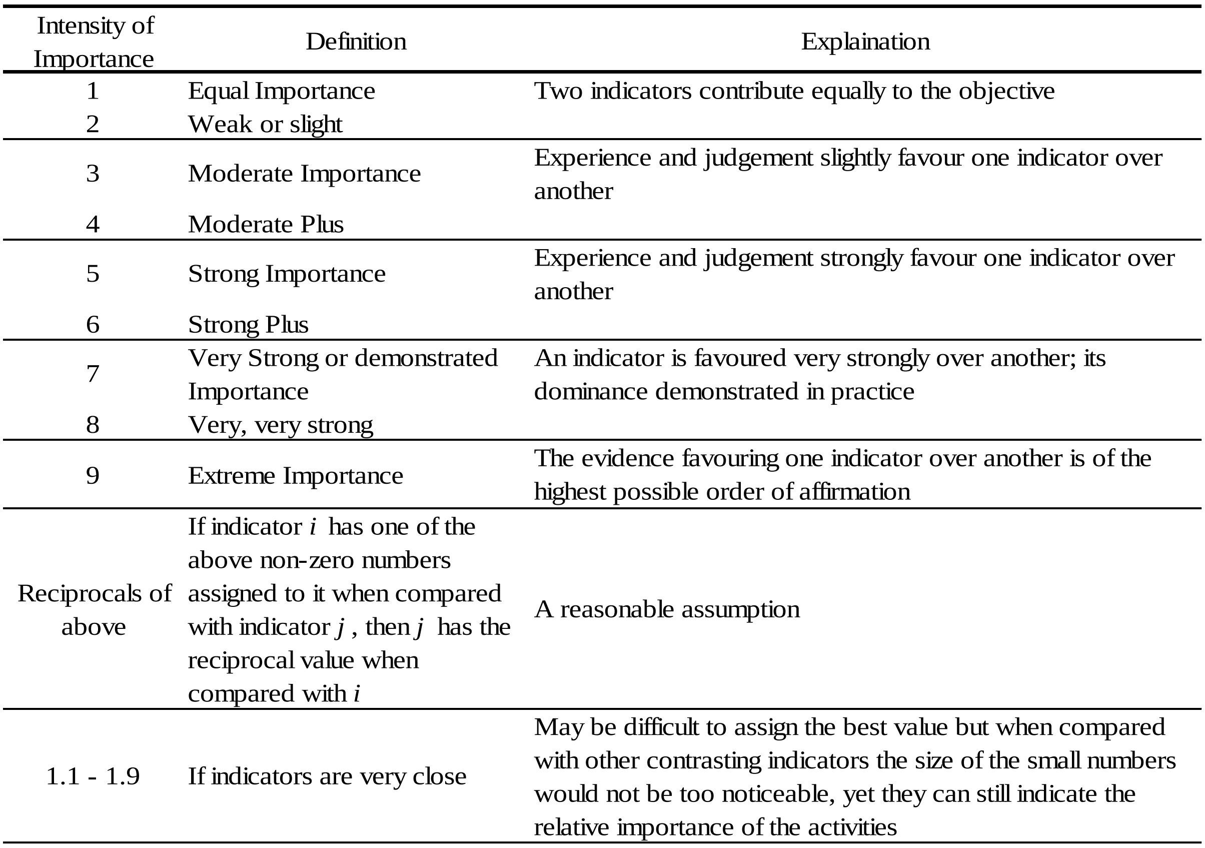


Figure 7. Decision Hierarchy for Risk Index Model

4.1.2 The aid of Analytic Hierarchy Process (AHP)

This study combines all the indicators in the model and estimates the incident risk indexes using RIM with the aid of AHP. In order to differentiate the importance of the indicators, the model adopts the fundamental scale proposed by Saaty (2008a). The scale was chosen because it provides a clear distinction between indicators and also has been used in the most recent studies relating to AHP (Barker and Zabinsky, 2011; Huang *et al.*, 2011). *Table 4* describes the fundamental scale used for the analysis in weighting the indicators. For example, if the criticality indicator is moderately important compared to maintainability, value 4 is assigned in the criticality-maintainability comparison matrix and reciprocal value (1/4) is assigned to the maintainability-criticality comparison matrix (see *Table 5*). In the process of comparing indicators, each indicator will be compared with another indicator by choosing which is the most important and which gives the greatest advantage between two pairs. The process is continued with the other two pairs until all indicators are compared.

Table 4. Fundamental Scale of absolute numbers (Saaty, 2008a)



Intensity of Importance	Definition	Explaination
1	Equal Importance	Two indicators contribute equally to the objective
2	Weak or slight	
3	Moderate Importance	Experience and judgement slightly favour one indicator over another
4	Moderate Plus	
5	Strong Importance	Experience and judgement strongly favour one indicator over another
6	Strong Plus	
7	Very Strong or demonstrated Importance	An indicator is favoured very strongly over another; its dominance demonstrated in practice
8	Very, very strong	
9	Extreme Importance	The evidence favouring one indicator over another is of the highest possible order of affirmation
Reciprocals of above	If indicator *i* has one of the above non-zero numbers assigned to it when compared with indicator *j* , then *j* has the reciprocal value when compared with *i*	A reasonable assumption
1.1 - 1.9	If indicators are very close	May be difficult to assign the best value but when compared with other contrasting indicators the size of the small numbers would not be too noticeable, yet they can still indicate the relative importance of the activities

This study satisfies the first need of AHP using the fundamental scale by producing a judgement matrix for the indicators. Consider *n* number of indicators, where *A* represents the indicators themselves; therefore, with *n* indicators, the reciprocal matrix emerges as follows:

$$\begin{array}{c|ccccc}
\mathrm{A} & \mathrm{A}_1 & \mathrm{A}_2 & \cdots & \mathrm{A}_n \\
\hline
\mathrm{A}_1 & \frac{\mathrm{A}_1}{\mathrm{A}_1} & \frac{\mathrm{A}_1}{\mathrm{A}_2} & \cdots & \frac{\mathrm{A}_1}{\mathrm{A}_n} \\
\mathrm{A}_2 & \frac{\mathrm{A}_2}{\mathrm{A}_1} & \frac{\mathrm{A}_2}{\mathrm{A}_2} & \cdots & \frac{\mathrm{A}_2}{\mathrm{A}_n} \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
\mathrm{A}_n & \frac{\mathrm{A}_n}{\mathrm{A}_1} & \frac{\mathrm{A}_n}{\mathrm{A}_2} & \cdots & \frac{\mathrm{A}_n}{\mathrm{A}_n}
\end{array}$$

Since there are two types of indicators (i.e. essential and desirable), this study controls the essential indicators by giving a slightly higher value compared to the desirable indicator values. The valuation of the indicator is easy because the essential indicator for both decision factors always becomes a higher priority. For example, *Table 5* shows the example of the judgement matrix for the indicators that influence the impact on the asset. The table is not complete because there is no priority and weight assigned for each indicator yet. The complete result is shown in the next section. In a normal case, the judgement matrix is assigned manually by security analysts and the priority can change from time to time.

Table 5. Example of the reciprocal matrix for the indicators

Impact on an Asset	Criticality	Maintainability	Replaceability	Dependability	Control
Criticality	1	5	3	2	2
Maintainability	1/5	1	1/2	1/4	1/3
Replaceability	1/3	2	1	2	2.2
Dependability	1/2	4	1/2	1	1.5
Control	1/2	3	1/2.2	1/1.5	1

In extending the weighted process, this study applies an approach similar to that used by Saaty (2008a) to calculate the indicator priorities. This study uses the Eigenvalue Method (EM) in giving an appropriate priority for each indicator. Other than EM, the Row Geometric Mean Method (RGMM) is one of the common methods in estimating priority (Crawford and Williams, 1985). According to Dong *et al.* (2008) and Herman and Koczkodaj (1996), with regard to the result, both methods (i.e. EM and RGMM) show almost the same priority results and are accurate enough to be used for practical applications. With the EM, the matrix satisfies the following formula in (1) (Saaty, 2008b).

$$A_nW = \lambda_{max}W \tag{1}$$

In making a judgement for matrix A_n with $n\ x\ n$ matrix, λ_{max} is the largest Eigenvalue of A_n and W is the right Eigenvector. With regard to the formula, λ_{max} is always greater than or equal to n. Precisely, the closer value of λ_{max} is to the n, the more consistent are the values in the judgement matrix A_n. In order to calculate λ_{max} and Eigenvector, W, this study uses a matrix calculator (e.g. a function in Matlab). The matrix calculator will produce several values for λ_{max} and Eigenvector, W. The largest λ_{max} and its Eigenvector, W will be used for the priority calculation. Furthermore, the judgement matrix of the influence factor in *Table 7* is to consider for an example. The priorities values in *Table 7* (i.e. 0.4444 and 0.5556) are calculated by normalising the Eigenvector, $W = \begin{Bmatrix} 0.6247 \\ 0.7869 \end{Bmatrix}$. To ask if $W = \begin{Bmatrix} 0.6247 \\ 0.7809 \end{Bmatrix}$ is the right Eigenvector corresponding to the Eigenvalue, λ_{max} = 2.000 for $A_2 = \begin{Bmatrix} 1.0000 & 0.8000 \\ 1.2500 & 1.0000 \end{Bmatrix}$, they are formulated as follows:

$$\begin{aligned} A_nW &= \lambda_{max}W \\ \begin{Bmatrix} 1.0000 & 0.8000 \\ 1.2500 & 1.0000 \end{Bmatrix} \begin{Bmatrix} 0.6247 \\ 0.7809 \end{Bmatrix} &= 2.000 \begin{Bmatrix} 0.6247 \\ 0.7809 \end{Bmatrix} \\ \begin{Bmatrix} 1.2494 \\ 1.5618 \end{Bmatrix} &= \begin{Bmatrix} 1.2494 \\ 1.5618 \end{Bmatrix} \end{aligned}$$

Therefore, λ_{max} = 2.000 and $W = \begin{Bmatrix} 0.6247 \\ 0.7869 \end{Bmatrix}$ are an Eigenvalue and an Eigenvector, respectively, for $A_2 = \begin{Bmatrix} 1.0000 & 0.8000 \\ 1.2500 & 1.0000 \end{Bmatrix}$.

In order to extend the different weightings upon the indicators, three judgement matrices can be established with the model: the judgement matrix of the influence factor (i.e. as can be seen in *Table 7*), judgement matrix of the main indicator for consequence of event (i.e. impact on asset - *Table 8)* and the judgement matrix of the main indicator for likelihood of event (i.e. likelihood of threat and vulnerability - *Table 9*). The judgement matrices were used to evaluate the different results of the risk index. Generally, the judgement matrices are manually configured and *Table 7*, *Table 8* and *Table 9* show examples of the judgement matrices for the decision factors and indicators used in RIM. Having identified the drawbacks of the previous study in the post-incident prioritisation, in particular with the lack of different weight in the decision factors, the consideration of adopting these judgement matrices is significant.

Although the judgement matrices were manually configured, they need to evaluate in order to maintain their consistency. To evaluate the consistency within the indicators, Random Index (RI) (Saaty, 2008b) is introduced (as tabulated in *Table 6*) with the consistency index (CI) and consistency ratio (CR) formulas.

Table 6. Random Index (RI) (Saaty, 2008b)

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
RI	0	0	0.52	0.89	1.11	1.25	1.35	1.40	1.45	1.49	1.52	1.54	1.56	1.58	1.59

$$\mathrm{CR} = \frac{\mathrm{CI}}{\mathrm{RI}} \tag{2}$$

where, $$\mathrm{CI} = \frac{\lambda_{max} - n}{\mathrm{n} - 1} \tag{3}$$

To look at them closer, on the bottom of the tables there are three variables which are λ_{max}, consistency index and consistency ratio. The λ_{max} is obtained from the largest value of the Eigen value and is used to estimate the consistency index (CI). With the consistency index (CI) formula and Random Index (RI) in *Table 6*, the consistency ratio (CR) is estimated using the given formula. According to Zahedi (1986) and Saaty (2008b), if the consistency ratio value is less than 10%, then the value can be considered as a reasonable and acceptable judgement or otherwise the judgement matrix is not consistent. Based on the value of the consistency index and consistency ratio, all the assessment and values for the indicators' weight in the judgement matrices in the tables are considered consistent.

Table 7. Judgement Matrix of the Influence Factor

	Consequence of Event	Likelihood of Event	**Priorities**
Consequence of Event	1.0000	0.8000	**0.4444**
Likelihood of Event	1.2500	1.0000	**0.5556**

λ_{max} = 2.0000; Consistency Index= 0.0000; Consistency Ratio = undefined

Table 8. Judgement Matrix of the main Indicator for Impact on Asset

	Criticality	Maintainability	Replaceability	Dependability	Control	**Priorities**
Criticality	1.0000	5.0000	3.0000	2.0000	2.0000	**0.3859**
Maintainability	0.2000	1.0000	0.5000	0.2500	0.3333	**0.0659**
Replaceability	0.3333	2.0000	1.0000	2.0000	2.2000	**0.2210**
Dependability	0.5000	4.0000	0.5000	1.0000	1.5000	**0.1834**
Control	0.5000	3.0000	0.4545	0.6667	1.0000	**0.1437**

λ_{max} = 5.2684; Consistency Index= 0.0671; Consistency Ratio = 6.05%

Table 9. Judgement Matrix of the main Indicator for Likelihood of Threat and Vulnerability

	Severity	Exploitability	Sensitivity	Similarity	Frequency	**Priorities**
Severity	1.0000	6.0000	7.0000	3.0000	4.0000	**0.4954**
Exploitability	0.1667	1.0000	2.0000	0.3333	0.3333	**0.0716**
Sensitivity	0.1429	0.5000	1.0000	0.1667	0.2000	**0.0426**
Similarity	0.3333	3.0000	6.0000	1.0000	2.0000	**0.2300**
Frequency	0.2500	3.0000	5.0000	0.5000	1.0000	**0.1604**

λ_{max} = 5.1574; Consistency Index = 0.0394; Consistency Ratio = 3.55%

As can be seen from the three tables of the judgement matrices above, the priorities of the indicator in each table refer to the weights of the indicator. These values will be used as a key to rate the incident risk indexes. As noted, the total of the priority in indicators is equal to 1 where each priority for each indicator must be equal to or greater than 0.

With the result of the weight for each indicator, this study rates an incident using the rating mode, with one modification - the rating category has been modified to a fixed rating for each incident. This consideration has been identified in the previous chapter, where the rating mode gives advantage in terms of rating a higher number of incidents. As a result, with the modification each incident has a specific value for each indicator and this value is then used to produce the rating of the overall value. The rationale behind this change is that the rating category limits the selection of criteria into several appropriate qualitative categories (e.g. high, low, medium) and using pair-wise comparison, each category has its quantitative value. Modifying the rating category allows the model to produce a clear distance value between incidents as well as results in a variance rating of the overall value.

4.1.3 Rating and Ranking Strategy in Risk Index Model

The establishment of RIM shows the general view of the model. This section discusses the detail of the algorithms and strategies used to estimate the risk index.

There are ten indicators used to rate and estimate the incident risk index and they comprise the following elements:

(a) All the indicators related to assets (i.e. *criticality*, *maintainability*, *replaceability*, *dependability* and *control*) are estimated quantitatively by giving a numerical value between 0 and 10, where 0 represents the lowest value or non-critical. The highest value gives a higher contribution to the risk index value.

(b) *Severity and Exploitability*. The rating for the severity and exploitability indicator is obtained directly from the Common Vulnerability Scoring System (CVSS) (NIST, 2011). In case the value is unavailable, then 0 will be used as the contribution value.

(c) *Sensitivity*. The sensitivity indicator is based upon the sensitivity of sensors and it is manually provided by security analysts. The sensitivity of sensor is identified quantitatively by giving a numerical value between 0 and 10. The highest value gives a higher contribution to the risk index value and 0 as the lowest value to represent a non-sensitive sensor.

(d) *Similarity*. This study adopted the similarity concept using a hierarchy-based approach and probabilistic alert correlation. Organised as a tree, the hierarchy based approach consists of a set of specific-general relations, where leaf nodes denote the most specific concepts (original attributes value) and the root represents the most general concept in the hierarchy (Xu and Ning, 2005). For example, the hierarchy based approach has been used in many alert correlation studies in correlating alerts using IP address such as Xiao *et al.* (2008) and Yu and Rubo (2008). In this study, the similarity indicator calculates its value using IP addresses and port similarity. The contribution value for port similarity was based on functions used by Xiao *et al.* (2008) (i.e. equations (6) and (7)). In addition, the value for IP address similarity was based on Yu and Rubo (2008) (i.e. equation (5)). Thus, this study combined both functions and used it as a function to rate the similarity indicator (i.e. equation (4)). The study also used the probabilistic alert correlation proposed by Valdes and Skinner (2001) where the similarity function returns a number between 0 and 1. This indicator calculates the percentage of incidents' similarity based on conditions which look into incidents' attributes and whether they use specific types of protocol (e.g. UDP or TCP). If they use a specific type of protocol like TCP, the similarity indicator calculates the average between incidents' ports similarity and IP addresses similarity. The IP address similarity is calculated based on the comparison between incidents' IP addresses (e.g. in equation (5), IP_1 is compared with IP_2; both are two different IP addresses) and uses three conditions: if they are similar then value 1 is returned, if they are not similar but with a similar subnet based on standard network classes (e.g. Class A, B and C network) then a value 0.5 is returned and if they are not under any previous conditions then a value 0 is returned. Furthermore, the ports similarity is calculated based on the comparison between incidents' ports (e.g. in equation (6) and (7), $Port_1$ is compared with $Port_2$; both are two different incidents) and it uses two conditions. If they are equal, then value 1 is returned or otherwise, the second condition in the equation will be used where the difference between them is calculated. To estimate similarity between ports, the second condition applies three hierarchies of ports and they are divided into ports below 1024 (i.e. well-known server ports), ports between 1024 and 49151 (i.e. registered ports and assigned by Internet Assigned Numbers Authority (IANA) for specific services) and ports between 49152 and 65535 (i.e. dynamic or private ports that cannot be registered with IANA). The value returned by the second condition is between 0 and 1. However, this indicator may be degraded since there are limitations in calculating the incident risk index. For example, the problem of the implementation of CIDR (i.e. Classless Inter-Domain Routing) and when there are DDoS attacks. The implementation of CIDR dismisses the need of subnet in a network and the DDoS attacks decreases the similarity values between IP addresses and ports (e.g. when attackers use random IP addresses and ports).

$$Similarity = \begin{cases} \frac{1}{2}\left(\frac{\sum Port}{\sum Incident} \times 100\right) + \frac{1}{2}\left(\frac{\sum IP\ Address}{\sum Incident} \times 100\right), & Port = \{UDP, TCP\} \\ \left(\frac{\sum IP\ Address}{\sum Incident} \times 100\right), & Port \neq \{UDP, TCP\} \end{cases} \quad (4)$$

$$IP\ Address, S\ (IP_1, IP_2) = \begin{cases} 1, & IP_1 = IP_2 \\ 0.5, & IP_1 = Subnet(IP_2) \\ 0, & IP_1 \neq IP_2 \end{cases} \quad (5)$$

$$Port, P(Port_1, Port_2) = \begin{cases} 1, & Port_1 = Port_2 \\ 1 - \frac{L(Port_1, Port_2)}{H}, & Port_1 \neq Port_2;\ L(Port_1, Port_2) = |\ Port_1 -\ Port_2| \end{cases} \quad (6)$$

$$H = \begin{cases} 1024, & 0 < L(Port_1, Port_2) \leq 1024 \\ 49151, & 1024 < L(Port_1, Port_2) \leq 49151 \\ 65535, & 49151 < L(Port_1, Port_2) \leq 65535 \end{cases} \quad (7)$$

(e) *Frequency*. This indicator calculates the similarity of incidents using signature and signature class attributes within a particular period of time. The frequency calculates the average between the percentage of the similar signature and signature class between incidents. The percentage of the similar signature is calculated by dividing the summation of incidents with similar signatures by the total of incidents. A similar calculation is applied to incidents with similar signature classes, in order to obtain the percentage of the similar signature class.

$$Frequency = \frac{1}{2}\left(\frac{\sum Similar\ Signature}{\sum Incident} \times 100\right) + \frac{1}{2}\left(\frac{\sum Similar\ Signature\ Class}{\sum Incident} \times 100\right) \quad (8)$$

In order to compile the indicators, there are other intangible factors that influence the decision in the process and they should be considered before any assessment is put in place. These factors are considered as technical factors because their involvement is only required when the assessment is performed. For example, in the cost-sensitive modelling, the changes of the information related to asset and security policies are taken into the consideration. Lee *et al.* (2002) suggested that the process to estimate the cost metric must be done periodically. To extend this consideration, the study considers three factors based upon the characteristic of input. Firstly, the characteristic of those factors, whether they are independent input or not. Secondly, the nature of the factors whether they are dynamically changed. Thirdly, the importance of factors where some factors are important and others may be less so. The main implication of considering these factors is that they are able to improve the rating process besides controlling the input of the factors. The third factor has been considered in the adoption of AHP in the prioritisation process. The other considerations are described using the following descriptions (See *Table 10*).

(a) *Type of input*. For each indicator, the input can be divided into two types: *dependent* and *independent input*. In considering the characteristic of input, an independent input is obtained directly from sources with no immediate modification made to it (e.g. CVSS v2 as the severity indicator). As opposed to the independent input, a dependent input is obtained indirectly from sources whereby it needs to be modified before it can be used by any indicator. For example, the dependent input, such as frequency and similarity, needs to go through a computing and reasoning process, using one or a combination of more input from different sources.

(b) *Update Frequency*. There are two types of update frequencies that can be considered in updating indicators namely, the *on-demand* and *delay* frequencies. An *on-demand* frequency updates the indicator when an incident is detected by IDSs or when the indicator values are needed (e.g. the similarity indicator). In contrast, a delay frequency updates indicators based on a fixed or timed schedule which is configured manually by security analysts (e.g. the criticality indicator).

Table 10. Characteristic of input for each indicator

	type of input		update frequency	
	independent	dependent	on-demand	delay
The *impact on asset* indicators				
criticality		x		x
maintainability		x		x
replaceability		x		x
dependability		x		x
control		x		x
The *likelihood of threat and vulnerability* indicators				
severity	x			x
exploitability	x			x
sensitivity	x			x
similarity		x	x	
frequency		x	x	

In extension, to estimate the incident risk indexes, the proposed framework considered the following strategies in the rating and ranking process:

(a) *Rating Strategy*. Based upon the input characteristics, there are two modes in the rating strategy used to rate and update the incident risk indexes. The first strategy in the rating process uses a *static mode* where the incident risk indexes are updated and rated once only at the time when incidents are detected. As for following the second characteristic, the second strategy in the rating process uses an *on-demand mode* which updates the incident risk indexes dynamically each time a new incident detected but limited within a certain period of time which can be configured manually by security analysts (e.g. one hour after detection). This limitation is important because the consideration of adopting the *on-demand mode* induces an overhead on the prioritisation process.

(b) *Ranking Strategy*. Based upon the strategy used in the rating process, this study establishes one important strategy which aims to reduce the number of incidents that need to be ranked. The strategy ranks incidents based upon the advantage of time interval, as it is similar to the *on-*

demand mode strategy in the rating process. In addition to reducing the number of incidents to be ranked, this is also important for security analysts to identify which incidents are really critical in a certain period of time. For example, if the strategy is configured to limit the ranking process to 1 hour, only incidents which have been detected in the last 60 minutes will be ranked and the rest will be dropped and excluded from the ranking process.

Table 11 and *Table 12* illustrate the difference between two strategies in the rating process. Although the *static* mode can be applied in the rating process in order to rate incidents, the adoption of the *on-demand mode* is significant to improve the results. However, the adoption of the *on-demand mode* influences the performance of the rating process.

In order to show a significant improvement in the adopted strategy, *Table 11* and *Table 12* tabulate the output of two indicators. The illustration in the tables uses the example of the real incidents which can later be found in the experiment conducted in this study. *Table 11* shows a partial result of the *frequency* indicator and *Table 12* shows an identical result for the *similarity* indicator. Both tables tabulate results for the first 10 incidents and *Table 11* displays the results based on event ID, signature name, timestamp, local signature ID, local class ID and values for the *frequency* indicator. The local signature ID links to a specific type of incident and local class ID refers to a group or classtype which is assigned and defined by Snort automatically. The last column shows 10 different intervals where one interval is considered as the time of the incidents detected. It contains a specific value for the *frequency* indicator and is updated dynamically using *on-demand mode* which produces a new value each time a new incident is detected.

Table 11. Example for the *frequency* indicator

					Frequency Indicator									
Event ID	**Signature name**	**Timestamp**	**Local Signature ID**	**Local Class ID**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	ATTACK-RESPONSES directory listing	09:29:20	55	19	1.0000	1.0000	1.0000	0.8750	0.8000	0.6667	0.6429	0.5625	0.5556	0.5000
2	ATTACK-RESPONSES directory listing	09:29:23	55	19	-	1.0000	1.0000	0.8750	0.8000	0.6667	0.6429	0.5625	0.5556	0.5000
3	ATTACK-RESPONSES directory listing	09:29:24	55	19	-	-	1.0000	0.8750	0.8000	0.6667	0.6429	0.5625	0.5556	0.5000
4	FTP Bad login	09:32:34	56	19	-	-	-	0.6250	0.6000	0.5000	0.5000	0.4375	0.4445	0.4000
5	TELNET login incorrect	09:32:34	57	19	-	-	-	-	0.6000	0.5000	0.5714	0.5000	0.5556	0.5000
6	ATTACK-RESPONSES Invalid URL	09:37:05	58	20	-	-	-	-	-	0.1667	0.1429	0.1875	0.1667	0.1500
7	TELNET login incorrect	09:44:51	57	19	-	-	-	-	-	-	0.5714	0.5000	0.5556	0.5000
8	ATTACK-RESPONSES 403 Forbidden	09:45:34	59	20	-	-	-	-	-	-	-	0.1875	0.1667	0.1500
9	TELNET login incorrect	09:45:36	57	19	-	-	-	-	-	-	-	-	0.5556	0.5000
10	ICMP PING	09:45:37	60	21	-	-	-	-	-	-	-	-	-	0.1000

With the *on-demand mode* strategy in the rating process, the value of the *frequency* indicator is changing from one interval to another. As opposed to the *static mode* strategy where the indicator value is marked only at the time of incidents detected, the *on-demand mode* strategy updates the value dynamically. To illustrate the improvement with the *on-demand mode* strategy, two different events, namely the 3rd and the 6th event, are compared. Using the *static mode* strategy, the value of the *frequency* indicator is computed at the time of the correspondent incident detected as tabulated as the first value of the indicator in every row in the table, which is 1.0000 for the 3rd event and 0.1667 for the 6th event. In considering the *static mode* strategy, the value is unchanged and therefore no estimation will be made again after that. However, with the *on-demand mode* strategy, the value for the 3rd event is dynamically decreased from 1.0000 to 0.5000 and the value for the 6th event is changed from 0.1667 to 0.1500. The change of the values is because one of attributes in the estimation formula has significantly changed, particularly in the total number of incidents detected. A similar result can be seen in the *similarity* indicator, as shown in *Table 12*.

The *similarity* indicator in *Table 12* shows significant improvement, particularly in updating the value of the risk index in each interval. *Table 12* tabulates the result for the *similarity* indicator. Using a similar example, like the *frequency* indicator, the table figures the *similarity* indicator value based upon source and destination IP address, as well as source and destination ports. For example, in *Table 12*, the value for the 1st event is changed from 1.0000 to 0.6862 when it reaches the last interval. The changes improve the accuracy of the *similarity* indicator because it uses a new input from the rating process. To illustrate the accuracy, in the 4th interval, the value for the 1st event was changed from 1.0000 to 0.9061 because a new incident was detected. The new value was updated because the total number of incidents detected at that time was increased from three incidents to four incidents. As opposed to that scenario, with the *static mode* strategy the value remains static where the 1st event is holding 1.0000 as the indicator value at every single interval until the end of the process. Therefore, the changes of the *similarity* indicator according to total number of incidents are more accurate compared to a static value applied in the *static mode.*

Table 12. Example for the s*imilarity* indicator

							Similarity Indicator									
Event ID	**Signature name**	**Timestamp**	**Source**	**Destination**	**Source Port**	**Destination Port**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	ATTACK-RESPONSES directory listing	09:29:20	172.16.112.100	172.16.112.194	23	25625	1.0000	1.0000	1.0000	0.9061	0.8313	0.7907	0.7849	0.7480	0.7346	0.6862
2	ATTACK-RESPONSES directory listing	09:29:23	172.16.112.100	172.16.112.194	23	25625	-	1.0000	1.0000	0.9061	0.8313	0.7907	0.7849	0.7480	0.7346	0.6862
3	ATTACK-RESPONSES directory listing	09:29:24	172.16.112.100	172.16.112.194	23	25625	-	-	1.0000	0.9061	0.8313	0.7907	0.7849	0.7480	0.7346	0.6862
4	FTP Bad login	09:32:34	172.16.115.20	172.16.113.50	21	1045	-	-	-	0.7184	0.6560	0.6237	0.6387	0.6148	0.6149	0.5785
5	TELNET login incorrect	09:32:34	172.16.113.50	195.115.218.108	23	43886	-	-	-	-	0.6006	0.5699	0.5467	0.5123	0.5009	0.4759
6	ATTACK-RESPONSES Invalid URL	09:37:05	207.200.75.201	172.16.113.148	80	30239	-	-	-	-	-	0.6069	0.5864	0.5731	0.5611	0.5050
7	TELNET login incorrect	09:44:51	172.16.114.50	172.16.112.194	23	1130	-	-	-	-	-	-	0.6929	0.6649	0.6618	0.6206
8	ATTACK-RESPONSES 403 Forbidden	09:45:34	137.245.85.134	172.16.113.204	80	1714	-	-	-	-	-	-	-	0.5169	0.5241	0.4717
9	TELNET login incorrect	09:45:36	172.16.112.50	172.16.113.84	23	1591	-	-	-	-	-	-	-	-	0.6214	0.5843
10	ICMP PING	09:45:37	172.16.113.84	135.13.216.191	-	-	-	-	-	-	-	-	-	-	-	0.2750

Although the consideration of adopting the *on-demand mode* strategy improves the value upon the indicators, it induces an overhead in the prioritisation process. Thus, in order to investigate the performance of the proposed framework, the selected strategies are evaluated in the next chapter.

4.2 Response Strategy

To address the response strategy used in the proposed framework, this section presents the Response Strategy Model (RSM) which can be applied as part of the dynamic response mapping model. As identified in the previous chapter in *Section 3.2.4*, the dynamic response mapping model gives more advantages compared to the static mapping.

The model creates a relationship between incidents and different types of response option with different levels of priority. Based upon attack metrics and system states as decision factors, this study uses an alternative approach in exclusively mapping an appropriate response option with an appropriate incident by considering risk assessments as decision factors, risk response planning as well as a time management concept in addressing the importance of response time. In addition, this study proposes the response strategy by grouping incidents into a similar group based on their priority and it also allows for a simultaneous response.

Using a simple and static policy with dynamic decision-making, the proposed model aims to reduce the delay problem upon making an appropriate decision and response; hence, it is suitable to be applied in a live traffic network in order to facilitate a fast response in a real time system.

4.2.1 Time Management Concept

The time management concept applied in RSM aims to create effective responses to critical incidents. In time management concepts, Covey (2004) presents four categories of tasks which are mapped onto four different quadrants; Q1: important and urgent, Q2: important but not urgent, Q3: not important but urgent, and Q4: not important and not urgent. Fundamentally known as the Eisenhower priority matrix, the quadrant is widely used by many studies particularly in the prioritising studies and related to time management; for example, in email prioritisation (Yoo, 2010), risk management (Haimes, 2001) and time management (Gonzalez *et al.*, 2008).

However, in order to fit with the proposed framework, this study modifies the quadrant to address the time management in responding to incidents. Instead of using “important”, this study uses “critical” to show the relationship between time and impacts; therefore, the new quadrants consider the combination between urgent and critical incidents. The quadrants for the time management concept contain four different levels and *Figure 8* shows the criticality and urgency quadrants.

The four quadrants are divided into:

(a) *1st Quadrant: Urgent incident and for a critical asset*. This quadrant is for the top and high priority incidents. This category allocates immediate response options, which aim to minimise and prevent adverse impacts from any future incidents. For example, an incident with a high severity score (e.g. 10 score in CVSS v2) detected in a very critical asset such as server or firewall can be classed with this category.

(b) *2nd Quadrant: Not an urgent incident but for a critical asset*. This quadrant is less urgent compared to the 1st quadrant but still considered as the top priority quadrant. It allocates any planned response options where a proper action is confidently taken to minimise the incident's impact. For example, an incident with a low severity score (e.g. 2 score in CVSS v2) and detected in a similar asset to the previous quadrants.

(c) *3rd Quadrant: Urgent incident but for a noncritical asset*. This quadrant is the third priority and considered a low priority quadrant and it allocates any action that needs additional time to analyse incidents in order to increase the confidence level of the planned responses. Almost the same as the 2nd quadrant in minimising incidents' impact, this quadrant slowly collects information about incidents as well as minimising the future impacts of incidents, for example a similar incident to the first quadrant, but detected in a noncritical asset such as a personal computer.

(d) *4th Quadrant: Not an urgent incident and for a noncritical asset*. This quadrant is the lowest priority and for a non-urgent incident and noncritical asset. This category includes passive responses. For example, a similar incident to the second quadrant, but detected in a similar asset to the third quadrant, such as a personal computer.

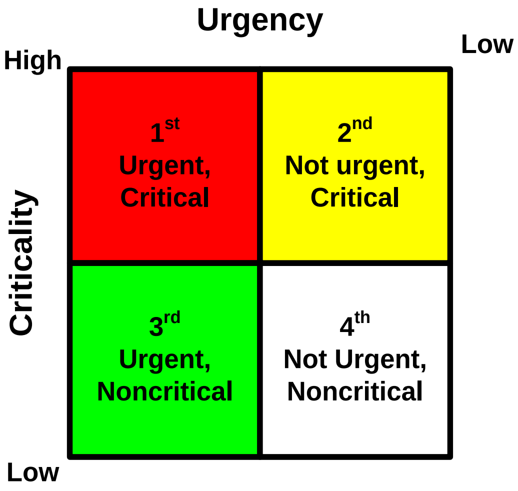


Figure 8. Urgency and Criticality Quadrants

4.2.2 Risk Response Planning

In order to establish a strategic RSM, this study uses the risk response planning concept. It contains four different strategies: avoidance, transfer, mitigation and acceptance. According to Hillson (1999), the risk response planning can be prioritised where avoidance can be the first option followed by transfer, mitigation and acceptance. This study chooses risk response planning simply because it is one of the risk assessment phases and allocates specific responses by offering an appropriate, achievable and affordable to identify risks (Hillson, 2002). Although there are other methods available to respond to risk, like the possible techniques in Baker *et al.* (1999) (i.e. risk elimination, risk transfer, risk retention and risk reduction) and other approaches summarised in Ben-David and Raz (2001) (such as risk absorption, prevention and contingency), the response planning proposed in (Hillson, 1999, 2002) is more suitable to this study because it is limited to only four strategies which literally appropriate four different levels of quadrant, besides avoiding any trade-off between achievability and complexity in having too many quadrants. Below are their descriptions.

(a) As the highest priority, a *risk avoidance response* is a strategy to eliminate uncertainties. In the model, an avoidance strategy eliminates risks by reducing factors that have direct influences on uncertainties. For example, the response options such as blocking and adjusting the related events are significant with the strategy. These options can be applied to users, processes as well as network traffic, and they aim to minimise the impact on future intrusions too. Fundamentally, there are two types of incidents which can be classed under this category. Firstly, incidents which are already predicted to be high risk and have serious impacts. Secondly, incidents which are identified as similar to previous high risk incidents historically.

(b) A *risk mitigation response* is an alternative strategy between two strategies: avoidance and transfer. Mitigation strategy deals with incidents that cannot be addressed by avoidance and transfer strategies. It deals with incidents above the transfer threshold but below the avoidance threshold and it aims to reduce the "size" of the risk exposures to the lowest risk. For example, terminating network traffic using security appliances like a firewall can be used as one of the response options. It terminates suspected traffic which related to incidents, rather than blocking all the communications.

(c) A *risk transfer response* aims to pass ownership and/or liability of any particular risk from one party (i.e. security device) to other third parties. By transferring risks to a new party, it allows victims to reduce its impact. One example of the third party appliances associated with this strategy is the honeypot and this handles any suspected network traffic by redirecting it from the original victims to a dummy system in order to collect information about the attackers.

(d) Finally, the lowest strategy is a *risk acceptance response* and this addresses an incident with a low risk and low impact upon victims or one which is considered as acceptable by most victims' systems. Considered as a very cost-effective strategy, it requires far less expense in order to repair a victim's system if anything happens. In order to respond to incidents, a passive response like system of notification is one of the response options classed under this strategy.

4.2.3 Response Strategy Model

Having presented the latter concepts, *Figure 9* shows a block diagram for RSM and contains four blocks of quadrants which come from a combination of the risk response planning and time management concepts.

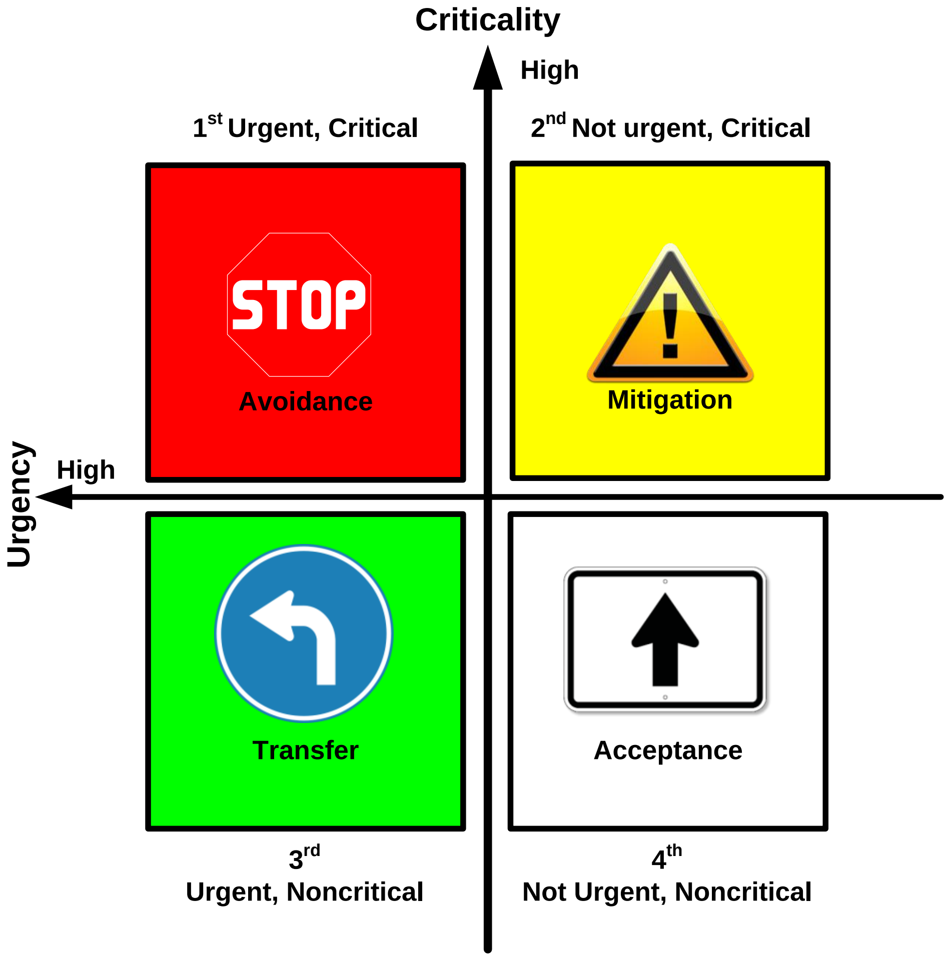


Figure 9. Risk Response Planning with time management concept in Response Strategy Planning

Table 13 shows the relationship map between them and their correspondent quadrants as well as some related examples for their response options.

With different levels of the response strategies, incidents are mapped with response options using four different levels based upon their urgency and criticality. Since there is no significant study relating to the arrangements of the quadrants, the response strategies listed in the table are considered an appropriate arrangement; however it is not definitive and is subject to other appropriate modification according to the needs of the security analysts and organisations. In particular, the 2nd and 3rd quadrants are interchangeable; for instance, in case of incidents being more important compared to critical assets, the "*urgent incident but noncritical asset*" in the 3rd quadrant can be swapped with the 2nd quadrant.

Table 13. Response Strategy Planning with Response options

Risk Response Planning	**Quadrants**	**Response options**
Avoidance	1st Quadrant: Urgent incident and for a critical asset	• Block users, processes or network traffic in preventing future attacks. • Adjust users, processes or network traffic configuration in minimising impacts but maintain system's performances.
Mitigation	2nd Quadrant: Not an urgent incident but for a critical asset	• Collaborate with other appliances by limiting users, processes or network traffic for delaying the process of attacks (Example: using access control, firewall, enabling other countermeasures or antivirus). • Terminate users, processes or network traffic in preventing continuous attacks (Example: locking OS, resetting connection, dropping user and killing process).
Transfer	3rd Quadrant: Urgent incident but for a noncritical asset	• Collect information about incidents for passive responses, proactive responses as well as forensic evidence (Example: trace connections, decoy systems, honeypots, forensic evidence, recovery, incidents' blacklisting and white listing). • Escalate to administrator for a further investigation (Example: attack verification, damage recovery and assessment).
Acceptance	4th Quadrant: Not an urgent incident and not for a critical asset	• Establish passive responses like enabling a notification via syslog, console alert, email, pager, PDA or mobile.

Furthermore, the quadrants in the table are identical with the response options described in the response model proposed in Chapter 2. In particular, the 1st quadrant is mapped with proactive responses, 2nd and 3rd quadrants with reactive responses and 4th quadrants with passive responses.

As shown in the table, the 1st quadrant is mapped with the avoidance strategy where all related response options are used to eliminate uncertainties between incidents. One of the best response options for this category is a proactive response option, such as blocking suspicious network traffic, and it is suggested there are two ways to establish the response options: either to have a prediction approach or with the case-based approach.

Furthermore, the 2nd and 3rd quadrants are mapped with the mitigation and transfer strategy and they aim to counter incidents by facing them directly or transferring them actively. Both strategies operate in an active environment and a reactive response is the best and preferable for mapping with them. There are two different stages of reactive response: a) issuing confident responses immediately after an incident is detected, and b) investigating and learning about the uncertain incident before further responses can be applied. In particular, the 2nd quadrant is suitable for the first stage of reactive responses where incidents are mitigated immediately in order to reduce their risks. Furthermore, the 3rd quadrant is appropriately mapped with the second stage of reactive responses where incidents are transferred immediately to a third party security appliance like honeypots. Similar with the 2nd quadrants, the 3rd quadrant also reduces an incident’s impacts, risks to victims, and at the same time allows third party appliances to investigate and learn about the source of incidents (i.e. attackers).

The last quadrant is suitable for the acceptance strategy where the lowest risk is mapped with a cost-effective response option which is likely to incur a very low cost in establishing responses. For example, since incidents’ risks are low and considered as not meriting the launch of a high budget response option, a passive response like system notification (e.g. email, mobile, pager, etc.) is the best solution. Although the quadrant is categorised as low priority and accepts any possible risks, it needs to be monitored closely. In addition, information gathered from low risk incidents can be used as a sample in analysing high impact risks for future prediction. For example in multi-stage attacks, normally a low risk incident like “ICMP PING” is established first before a serious attack is launched. Therefore, information and detail like the source of attackers can be obtained from the first attack and this helps security analysts to efficiently analyse and predict future incidents.

4.2.4 Rating Thresholds

To map risk indexes onto appropriate response strategies, this study considers rating thresholds as illustrated in *Figure 10* and they can be used to determine and differentiate between non-critical and critical incidents.

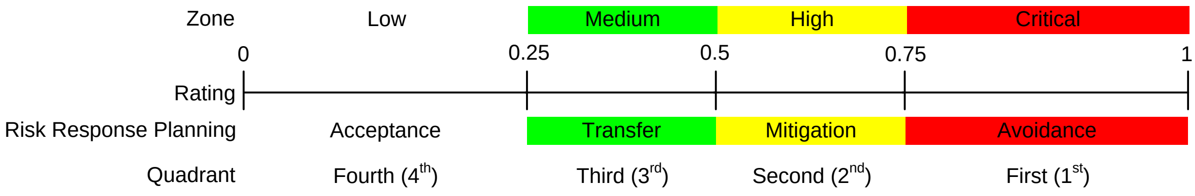


Figure 10. Example of Rating Threshold

In addressing the threshold rating in mapping between incidents and quadrants, with regards to the mapping model, this study compares with other scoring techniques such as CVSS v2 (Mell *et al.*, 2006; Mell *et al.*, 2009), Symantec (2006), US-CERT (2011) and Secunia (2011). Although the latter scoring systems have been widely used, the selection of it may be different from this study because those systems consider a different set of indicators and decision factors to determine the final scores and their priority.

Based upon the Base, Temporal and Environmental metrics, CVSS v2 scores between 0-10. With the score, CVSS v2 maps incidents into three different group of priority: high, medium and low. The thresholds between the groups are clearly defined in the CVSS v2 documentation. Symantec Corporation uses CVSS v2 as their method to identify the threat level of identified vulnerabilities (Symantec, 2010). However, in 2006 Symantec deployed their own rating system and the legacy DeepSight rating system uses 3 differences categories: Risk Rating, Severity Rating and Impact Rating. Each rating has its priority categories. For instance, in risk rating Symantec uses 5 categories, very low, low, moderate, severe and very severe (Symantec, 2006).

US-CERT applies a scoring system based on rating between 0-180 and it is calculated based upon several questions (US-CERT, 2011). Their scoring system is not a linear scoring system and therefore they not apply any categorisation but highlight any vulnerability with a metric greater than 40, which are then candidates for US-CERT Technical Alerts (i.e. a system used to provide timely information about current security issues, vulnerabilities and exploits by Technical Cyber Security Alerts). Finally, using a scale of 5, Secunia applies five levels of categorisation in defining incidents' criticality: extremely criticality (5), highly criticality (4), moderately criticality (3), less critical (2) and not critical (1) (Secunia, 2011).

There is no specific guideline to determine the best threshold between critical or non-critical incidents. However, the proposed framework needs it and therefore it is appropriate to this study to apply suitable rating thresholds. In order to investigate the suitability of the thresholds, the next chapter evaluates the distribution results in comparison with other approaches, such as CVSS v2 and Snort Priority.

4.3 Multi-strategy Incident Prioritisation Framework

To facilitate the response selection process in IRSs, the framework aims to prioritise incidents based upon several strategies together with some relevant decision factors, which were identified earlier in the previous section. Thus, in order to combine them interactively, *Figure 11* shows the active interaction between strategies and modules in the proposed framework.

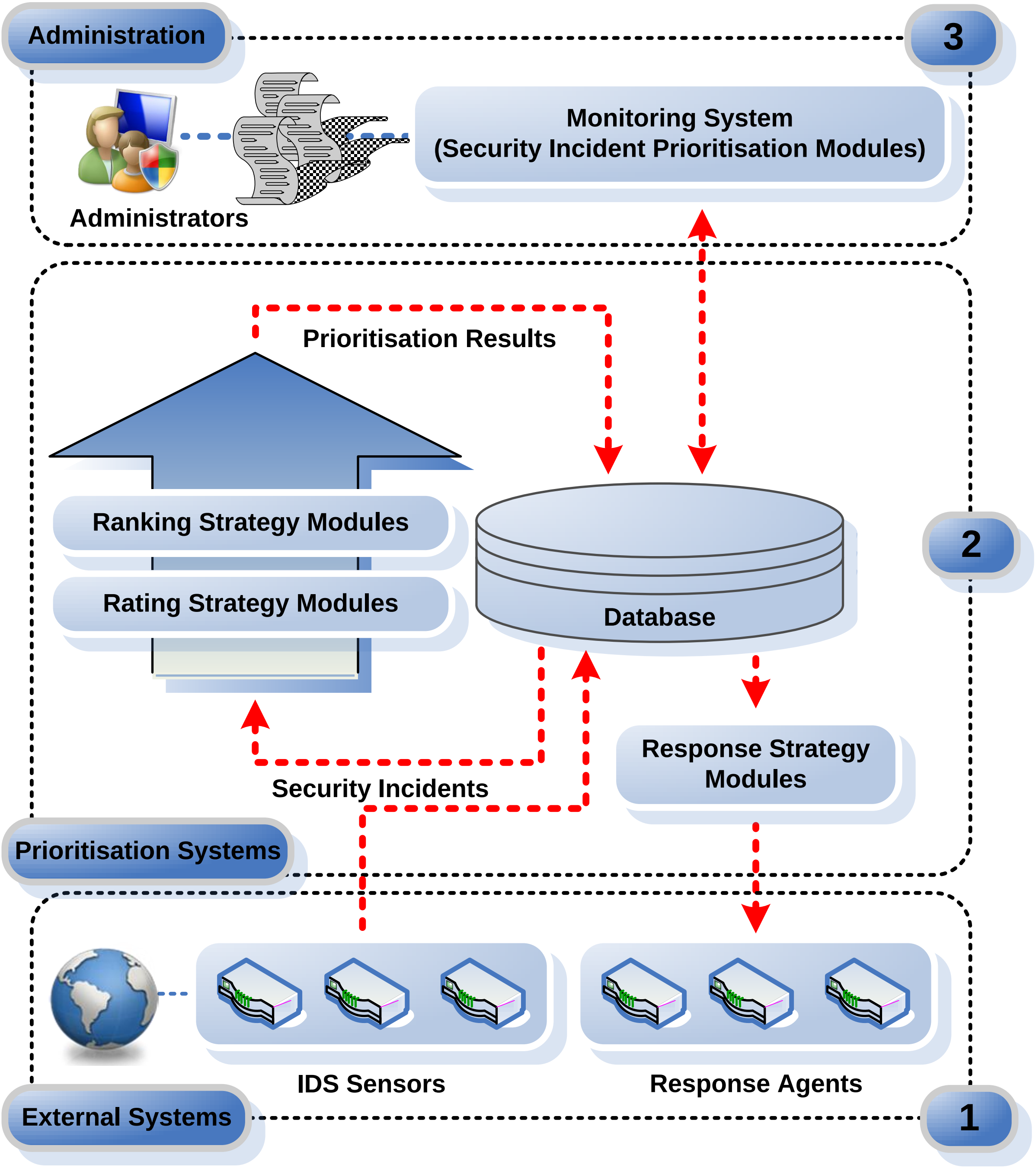


Figure 11. Multi-strategy Incident Prioritisation Framework

The framework comprises three main elements as follows:

(a) ***External Systems***. This is the first part of the proposed framework and it aims to create a relationship between the main systems and other systems externally. The external systems adopt other systems and mostly use open source systems. In addition to the proposed framework, there are two main components as follows:

  (i) *IDS Sensors*. They are security appliances used to monitor network traffic, detect suspicious activities and store them in an appropriate storage system like a centralised database; normally they are called Intrusion Detection Systems. In the case of this study, the Snort IDS was used.

  (ii) *Response Agents.* They are also security appliances, but they operate to respond to specific incidents with a specific type of response option based upon results produced by the prioritisation systems in the second part of the framework. For example, security appliances such as firewall, access control systems and honeypots can be used to help to respond to the incidents appropriately.

(b) ***Prioritisation Systems***. As the main elements in the proposed framework, these provide the main core system by organising several modules in the prioritisation process as follows:

  (i) *Rating Strategy Modules.* With Risk Index Model (RIM) and the aid of the Analytic Hierarchy Process (AHP), the module aims to rate incidents using specific modes selected by security analysts in the rating process. In order to rate and estimate quantitative risk indexes for incidents, there are two modes which can be applied in strategies in the rating process, namely *on-demand* and *static mode*. With methodical and approachable decision making, a result of numerical values for each incident is produced. AHP aids the estimation process by giving weighting for each decision factor and the indicators used in RIM. Finally, the output of the estimation process produces a series of numerical values that have been calculated automatically and changed periodically based upon the framework configurations.

  (ii) *Ranking Strategy Modules.* Aiming to rank incidents, these modules rank incidents quantitatively based upon their risk index values which are taken from the result of the earlier module. With the rating strategy modules, a higher value refers to a higher priority risk which can potentially be considered as a critical incident. Similar to the rating strategy modules, this module updates the ranking between incidents based upon their risk indexes but limited to the strategies planned and configuration configured in the previous procedure.

(iii) *Response Strategy Modules.* The third module in the prioritisation systems aims to create a relationship between incidents and response options. The quantitative results obtained from the previous modules together with the rating thresholds are used to map onto appropriate quadrants in RSM (i.e. avoidance, mitigation, transfer and acceptance); specifically, a mapping of qualitative results into a quantitative group of priorities. The different levels in RSM allow security analysts or automated security appliances (e.g. response agents) to act fast to respond only to true and critical incidents. With this module, incidents are distributed and grouped into several groups immediately and appropriate responses can be launched simultaneously within a similar group. As an implication from that, it allows an easy management (via a monitoring system) and additional advantages to security analysts in making a prompt and manual decision where each quadrant has its own type of response options to be selected.

(c) ***Administration***. As the third element in the proposed framework, it provides functions to interact with end-users and enables *Security Incident Prioritisation Modules*. The module aims to provide a monitoring system based upon results produced by the previous parts. It provides a graphical user interface to security analysts to monitor and configure the proposed framework as well as summarising the results from the other parts of the framework. With this module, security analysts are able to configure as well as monitor the results from the *prioritisation systems* using friendly interfaces. Some of the sub modules are event monitoring, assets management, event query, searching and the detail of the results of the prioritisation process for every single incident, such as its priority with risk index values and its quadrants.

4.3.1 Operational Characteristics

The proposed framework offers the following operational characteristics:

(i) *Multiple strategies*. The proposed framework applies multiple strategies in optimising the incident prioritisation process and incorporating other indicators in making appropriate decisions as well as responding to critical incidents based upon their priority. By implication, different modes in different strategies allow a customisable result.

(ii) *Robust and methodical approaches*. The used of methodical approaches like AHP in estimating the incident risk indexes allows the estimation process to produce a good risk index. The proposed framework estimates the level of their criticality based upon two main decision factors, like the asset criticality and other attributes which relate to incidents. In addition, its robustness allows the estimation process to operate normally in any scenario even with unavailable information for some indicators.

(iii) *Flexible risk scoring*. The estimation of the incident risk indexes covers internal factors such as the criticality of assets and extends its coverage over external factors, such as CVSS and vulnerability risks. This flexibility allows the scoring of the incident risk indexes to be wider than the current scoring systems (e.g. CVSS).

(iv) *Prioritisation of incidents.* Using the ranking strategy modules, the proposed framework has the ability to prioritise incidents based upon their risk indexes. The priority results can be classified into two different types of priorities: a list of incidents with their risk indexes as well as the quadrant group of priorities depending on the rating thresholds.

(v) *Flexible and practical*. The proposed framework allows a flexible configuration and applies a practical strategy in the prioritising and monitoring process. With this operational characteristic it can, potentially, work in a live traffic network with online assessment as well as in a real time environment.

(vi) *User friendly interfaces*. With customisable web modules, the proposed framework allows a simple administration of the summarisation of the results of the framework by providing a friendly graphical user interface system. The web modules also allow security analysts to exhaustively evaluate and examine the incident results from a more comprehensible statistical viewpoint.

4.4 Summary

This chapter has focused upon the conceptual framework for the incident prioritisation process, in order to provide a flawless framework to facilitate the autonomous mode in the response selection process. Its description has included an introduction of the main models, strategies, frameworks and the rationale behind their implementation, as well as their operational characteristics. In conclusion, this chapter highlighted the main point of this study and gave the detail of the framework, as well as discussing how they can be combined as one significant framework. It is important to understand the interrelationship between those strategies and the model in compiling the overall process in prioritising incidents in order to get a useful result from the incident prioritisation process.

Having established the proposed framework using multiple strategies and models, the next chapter presents several evaluations of the framework and is followed by a detailed discussion of them. It is important to understand that the results provide a verification of the usefulness and suitability of the framework in facilitating the autonomous mode in the response selection process. The evaluation study also investigates the feasibility of the proposed framework to operate an online assessment, besides evaluating its flexibility, performance and practicality.

5 Evaluation of the Multi-strategy Incident Prioritisation Framework

The novelty of this study is to propose a framework to conduct a prioritisation process on different types of incident, in order to identify their priority and respond to them appropriately. The aim is to facilitate the autonomous mode in the response selection process. Thus, in order to highlight the feasibility and suitability of the framework, this evaluation study is significant.

Having proposed the Multi-strategy Incident Prioritisation Framework, it is important to design a systematic evaluation phase in order to provide a verification of its feasibility and suitability, in particular for the second part of the framework, which is the prioritisation system.

This chapter presents four evaluation stages based upon the proposed framework which aim to evaluate it in terms of its effectiveness and performances in relation to the models and strategies selected. It is important to this evaluation study to investigate the effectiveness and performance of the proposed framework in order to satisfy its feasibility and suitability, in particular the ability of the framework to facilitate the autonomous mode. Besides, operating with a reasonable processing time in the prioritisation process, reduces false responses to false incidents and applies online assessment capabilities.

The first stage investigates the feasibility of the Risk Index Model (RIM) operation. To make evaluation and comparisons with the results from other studies, the first stage analyses the effectiveness of the rating and ranking process. With the first stage results, the second stage extends the evaluation study by analysing the effect of using different strategies in the rating and ranking process, in order to satisfy process enhancement. In particular, the second stage applies the *on-demand mode* strategy, as opposed to the *static mode* strategy applied in the first stage. Furthermore, the third stage evaluates the suitability of using the Response Strategy Model (RSM) as the response strategy in the framework. The third stage also evaluates the relationship between incidents' priority and the incident classification (e.g. false/true incidents). Finally, the fourth stage investigates the performance of the proposed framework by measuring the processing time in the rating and ranking process. The chapter ends with a summary.

5.1 General Description

There are four stages of the evaluation study in this chapter and each of them has its unique objectives with different results, discussion and conclusion. However, they also share a similar requirement in their experimental procedures. This section discusses the similarities in order to avoid any repetition in the introduction of each evaluation stage, in particular the datasets, tools and experimental assumptions.

In conducting experiments, each stage uses one or two types of dataset, either the MIT 2000 DARPA or Plymouth dataset, and each of them contains a unique characteristic. Their descriptions are as follows:

5.1.1 Dataset 1: MIT DARPA LLDOS 1.0

The main dataset used in this study uses one of the MIT 2000 DARPA data sets; specifically, LLDOS 1.0 with some modification. In addition to the most well-known dataset used in many security studies (Alsubhi *et al.*, 2008; Alserhani *et al.*, 2010), the rationale behind the selection of this specific dataset is due to the multi-stage attacks it contains. This is important as it allows this study to evaluate and analyse the effectiveness of ranking and prioritising incidents over different phases of attacks.

Table 14. Attack Phases

Phase	Attacker Schemes	Description
Phase 1	***IPsweep***	Sending ICMP echo-request for live hosts
Phase 2	***Probe***	Probe of live IP's to look for the sadmind daemon running on Solaris Hosts
Phase 3	***Break-in***	Break-ins via the sadmind vulnerability, both successful and unsuccessful on those hosts
Phase 4	***Install Virus***	Installation of the Trojan mstream DDoS software on three hosts using telnet
Phase 5	***DDos***	Launching the DDoS attacks

Table 15. Attack Phases Detail

Phase		**Time**	**Duration (sec)**	**No. of Packets**	**Total Incidents**
Pre 1		09:21:36 - 09:51:35	1800	154886	25
1	**IPsweep**	09:51:36 - 09:52:00	25	1371	40
Pre 2		09:52:01 - 10:08:06	966	30368	21
2	**Probe**	10:08:07 - 10:18:05	599	34092	243
Pre 3		10:18:06 - 10:33:09	904	43869	4
3	**Break-in**	10:33:10 - 10:35:01	112	4528	64
Pre 4		10:35:02 - 10:50:00	899	40289	28
4	**Install Virus**	10:50:01 - 10:50:54	54	2266	10
Pre 5		10:50:55 - 11:26:14	2120	87564	12
5	**DDos**	11:26:15 - 11:34.21	487	96242	579
Post 5		11:34:22 - 12:35:48	3687	154312	42
Total		09:21:36 - 12:35:48	11653	649787	1068

Fundamentally, the simulation of the intrusion detection data set is simulated using three segments of an Air Force base network: inside, DMZ and outside network (DARPA, 2011). The simulation contains a series of attacks launched by a novice attacker and is divided into five phases. As tabulated in *Table 15*, this study defined 6 additional phases in the scenario which are pre and post the main phase. To provide simplicity in the phases, *Table 14* describes the main attack phase where most of the incidents detected in that phase are considered as true and critical incidents.

The detail of the phases is tabulated in *Table 16*. Unlike the phase's description from the original dataset, *Table 16* extends the dataset into several phases and categorises them into pre-phase, post-phase and critical phase. This categorisation allows a proper evaluation of the effectiveness of the model based on the transition of the rating and ranking process of incidents. The three phases are as follows:

(a) *Pre-Phase*. This is a phase where no critical incident happens before the main phase.

(b) *Critical phase*. This contains a critical incident as well as the other non-critical incidents in the main phase and is highlighted in **bold** in the table.

(c) *Post-phase*. The post-phase is a phase where no critical incident is detected but which happens after the last main phase.

With a total of 649,787 packets, the study detected 1,068 incidents, which can be found mainly in the main attack phases. The detail for the main phases is similar to a recent study by Alserhani *et al.* (2010) except in their study they were unable to detect incidents in the last main phase (i.e. DDoS attack).

Table 16. Attack Phases Detail

Phase	Time	Duration (sec)	No. of Packets	Total Incidents	Signature Name	No. of Incidents
Pre 1	09:21:36 - 09:51:35	1800	154886	25	ATTACK-RESPONSES directory listing	3
					FTP Bad login	1
					TELNET login incorrect	3
					ATTACK-RESPONSES Invalid URL	1
					ATTACK-RESPONSES 403 Forbidden	1
					ICMP Echo Reply	8
					ICMP PING	8
1	09:51:36 - 09:52:00	25	1371	40	**ICMP Echo Reply**	**20**
					ICMP PING	**20**
Pre 2	09:52:01 - 10:08:06	966	30368	21	ATTACK-RESPONSES Invalid URL	1
					ATTACK-RESPONSES 403 Forbidden	2
					ICMP Echo Reply	9
					ICMP PING	9
2	10:08:07 - 10:18:05	599	34092	243	**ICMP Destination Unreachable Port Unreachable**	**72**
					RPC portmap sadmind request UDP	**76**
					RPC portmap Solaris sadmin port query udp request	**76**
					ICMP Echo Reply	8
					ICMP PING	8
					TELNET login incorrect	3
Pre 3	10:18:06 - 10:33:09	904	43869	4	ATTACK-RESPONSES directory listing	4
3	10:33:10 - 10:35:01	112	4528	64	**RPC portmap sadmind request UDP**	**14**
					RPC portmap Solaris sadmin port query udp portmapper sadmin port query attempt	**14**
					RPC portmap Solaris sadmin port query udp request	**14**
					RPC sadmind query with root credentials attempt UDP	**14**
					TELNET login incorrect	**4**
					ATTACK-RESPONSES directory listing	3
					SQL version overflow attempt	1
Pre 4	10:35:02 - 10:50:00	899	40289	28	ATTACK-RESPONSES directory listing	6
					TELNET login incorrect	2
					ATTACK-RESPONSES 403 Forbidden	2
					ICMP Echo Reply	9
					ICMP PING	9
4	10:50:01 - 10:50:54	54	2266	10	**RSERVICES rsh root**	**8**
					ATTACK-RESPONSES 403 Forbidden	2
Pre 5	10:50:55 - 11:26:14	2120	87564	12	ATTACK-RESPONSES 403 Forbidden	2
					TELNET login incorrect	1
					ATTACK-RESPONSES directory listing	4
					ICMP Destination Unreachable Port Unreachable	4
					ATTACK-RESPONSES Invalid URL	1
5	11:26:15 - 11:34.21	487	96242	579	**(snort decoder) Bad Traffic Loopback IP**	**572**
					SNMP AgentX/tcp request	3
					ICMP Echo Reply	1
					ICMP PING	1
					ICMP PING *NIX	1
					ICMP PING BSDtype	1
Post 5	11:34:22 - 12:35:48	3687	154312	42	TELNET login incorrect	4
					ICMP Echo Reply	17
					ICMP PING	17
					ATTACK-RESPONSES 403 Forbidden	3
					ATTACK-RESPONSES Invalid URL	1
Total		11653	649787	1068		1068

Based on the information given in the dataset, the study considers the categories of assets tabulated in *Table 17*. There are three sub networks in the scenario, but to focus on the analysis of the assets included in the dataset, the study examined only the hosts in the inside network. It is important to the study to consider this category as it provides a useful categorisation of the assets' values.

Table 17. Asset Categorisation

Category	Asset	IP Address	Hostname	Operating System
Category 1	*Network Asset*	*172.16.115.1*	*firewall-inside.eyrie.af.mil*	
		172.16.116.1	*firewall-inside.eyrie.af.mil*	
		172.16.117.1	*firewall-inside.eyrie.af.mil*	
		172.16.118.1	*firewall-inside.eyrie.af.mil*	
Category 2	*Host with services*	*172.16.112.20*	*hobbes.eyrie.af.mil*	*Linux Redhat 5.0*
		172.16.115.20	*mill.eyrie.af.mil*	*Solaris 2.7*
Category 3	*Host with non-windows Operating System*	*172.16.112.10*	*locke.eyrie.af.mil*	*Solaris 2.6*
		172.16.112.50	*pascal.eyrie.af.mil*	*Solaris 2.5.1*
		172.16.112.149	*eagle.eyrie.af.mil*	*Linux Redhat 5.0*
		172.16.112.194	*falcon.eyrie.af.mil*	*Solaris 2.5.1*
		172.16.112.207	*robin.eyrie.af.mil*	*SunOS 4.1.4*
		172.16.113.50	*zeno.eyrie.af.mil*	*SunOS 4.1.4*
		172.16.113.84	*duck.eyrie.af.mil*	*SunOS 4.1.4*
		172.16.113.105	*goose.eyrie.af.mil*	*Linux Redhat 5.0*
		172.16.113.204	*goose.eyrie.af.mil*	*Solaris 2.5.1*
		172.16.113.148	*crow.eyrie.af.mil*	*Linux Redhat 5.0*
		172.16.113.168	*finch.eyrie.af.mil*	*SunOS 4.1.4*
		172.16.113.169	*swan.eyrie.af.mil*	*Solaris 2.5.1*
		172.16.113.207	*pigeon.eyrie.af.mil*	*Linux Redhat 5.0*
		172.16.117.103	*pc9.eyrie.af.mil*	*MacOS*
		172.16.117.111	*pc8.eyrie.af.mil*	*MacOS*
		172.16.118.10	*linux1.eyrie.af.mil*	*Linux Redhat 5.2*
		172.16.118.20	*linux2.eyrie.af.mil*	*Linux Redhat 5.0*
		172.16.118.30	*linux3.eyrie.af.mil*	*Linux Redhat 5.0*
		172.16.118.40	*linux4.eyrie.af.mil*	*Linux Redhat 5.0*
		172.16.118.50	*linux5.eyrie.af.mil*	*Linux Redhat 5.0*
		172.16.118.60	*linux6.eyrie.af.mil*	*Linux Redhat 5.0*
		172.16.118.70	*linux7.eyrie.af.mil*	*Linux Redhat 5.0*
		172.16.118.80	*linux8.eyrie.af.mil*	*Linux Redhat 5.0*
		172.16.118.90	*linux9.eyrie.af.mil*	*Linux Redhat 5.0*
		172.16.118.100	*linux10.eyrie.af.mil*	*Linux Redhat 5.0*
Category 4	*Host with any Windows Operating System*	*172.16.112.100*	*hume.eyrie.af.mil*	*Windows NT 4.0*
		172.16.115.5	*pc1.eyrie.af.mil*	*Windows 95*
		172.16.115.87	*pc2.eyrie.af.mil*	*Windows 95*
		172.16.115.234	*pc0.eyrie.af.mil*	*Window NT 4.0*
		172.16.116.44	*pc5.eyrie.af.mil*	*Windows 3.1*
		172.16.116.194	*pc3.eyrie.af.mil*	*Windows 95*
		172.16.116.201	*pc4.eyrie.af.mil*	*Windows 95*
		172.16.117.52	*pc7.eyrie.af.mil*	*Windows 3.1*
		172.16.117.132	*pc6.eyrie.af.mil*	*Windows 3.1*

5.1.2 Dataset 2: Plymouth University Dataset

Although DARPA allows a significant comparison with the results of other studies, it is important to evaluate the proposed framework with a bigger and more recent dataset. As such, this study uses a private dataset, the Plymouth University dataset. The traffic of the dataset was collected on a public network (100-150 Mbps) over a period of 40 days (i.e. starting from 17th May 2007 to 25th June 2007). With a conventional network sniffer tool like tcpdump, the dataset is a collection of real and public traffic flowing into a web server on port 80 within the University extranet. The dataset has been previously used in several studies (Tjhai *et al.*, 2008a; Tjhai *et al.*, 2010; Tjhai, 2011), particularly in the alert correlations and studies on the identification of false incidents. The purpose of using the private dataset as an addition to the DARPA dataset is to evaluate the framework with a more recent and live traffic data set. In fact, the evaluation of the synthetic, data such as the DARPA dataset is inadequate for providing a practical evaluation and implementation in a real life environment.

Table 18. The Plymouth University Dataset

Signature	First Detected	Last Detected	Total	False Alarm	True Alarm
WEB-MISC robots.txt access	17-05-2007 00:04:29	25-06-2007 23:57:08	26971	58.39%	-
(http_inspect) BARE BYTE UNICODE ENCODING	17-05-2007 00:26:26	25-06-2007 21:53:56	6613	14.32%	-
POLICY Google Desktop activity	17-05-2007 00:51:51	25-06-2007 23:59:23	3364	7.28%	-
ICMP L3retriever Ping	17-05-2007 03:07:13	25-06-2007 22:53:40	1143	2.47%	-
SPYWARE-PUT Trackware funwebproducts mywebsearchtoolbar-funtools runtime detection	17-05-2007 03:16:50	25-06-2007 23:43:11	1922	4.16%	-
WEB-CGI calendar access	17-05-2007 04:48:47	17-06-2007 07:18:40	11	0.02%	-
ATTACK-RESPONSES 403 Forbidden	17-05-2007 06:12:42	25-06-2007 21:23:23	745	1.61%	-
(http_inspect) DOUBLE DECODING ATTACK	17-05-2007 06:32:58	25-06-2007 22:36:37	520	1.13%	-
SPYWARE-PUT Hijacker searchmiracle-elitebar runtime detection	17-05-2007 08:50:51	25-06-2007 14:06:48	81	-	0.18%
WEB-IIS view source via translate header	17-05-2007 11:22:12	25-06-2007 09:41:30	3463	7.50%	-
(portscan) TCP Portsweep	17-05-2007 11:58:41	25-06-2007 18:16:41	128	0.28%	-
ICMP Source Quench	17-05-2007 16:22:49	30-05-2007 16:57:05	2	0.00%	-
ICMP Destination Unreachable Communication Administratively Prohibited	17-05-2007 17:25:33	25-06-2007 19:14:12	158	0.34%	-
(http_inspect) WEBROOT DIRECTORY TRAVERSAL	17-05-2007 20:31:25	24-06-2007 15:54:18	37	0.08%	-
WEB-MISC .DS_Store access	18-05-2007 08:03:08	21-06-2007 08:22:09	62	0.13%	-
(http_inspect) IIS UNICODE CODEPOINT ENCODING	18-05-2007 08:31:07	25-06-2007 22:56:40	51	0.11%	-
(portscan) TCP Portscan	18-05-2007 09:36:35	21-06-2007 13:22:33	19	0.04%	-
ICMP redirect host	18-05-2007 11:46:58	16-06-2007 20:57:35	8	0.02%	-
ICMP PING CyberKit 2.2 Windows	18-05-2007 16:16:14	25-06-2007 19:06:03	690	-	1.49%
SPYWARE-PUT Hijacker marketscore runtime detection	18-05-2007 21:43:28	25-06-2007 18:22:30	7	-	0.02%
SPYWARE-PUT Adware hotbar runtime detection - hotbar user-agent	18-05-2007 23:18:58	21-06-2007 11:13:53	29	-	0.06%
ICMP PING NMAP	20-05-2007 05:00:58	20-06-2007 18:24:05	17	0.04%	-
WEB-PHP xmlrpc.php post attempt	20-05-2007 13:54:03	21-06-2007 16:06:17	2	0.00%	-
ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	21-05-2007 08:44:44	14-06-2007 12:10:06	13	0.03%	-
WEB-PHP remote include path	22-05-2007 06:52:06	24-06-2007 09:27:38	4	0.01%	-
SPYWARE-PUT Trackware alexa runtime detection	22-05-2007 10:13:22	23-06-2007 04:38:49	21	-	0.05%
MULTIMEDIA Quicktime User Agent access	24-05-2007 23:03:32	21-06-2007 16:15:55	11	0.02%	-
WEB-MISC WebDAV search access	25-05-2007 09:00:23	25-05-2007 09:01:32	5	0.01%	-
(portscan) Open Port	25-05-2007 16:16:49	18-06-2007 16:52:36	5	0.01%	-
(snort_decoder) WARNING: ICMP Original IP Fragmented and Offset Not 0!	28-05-2007 12:21:15	08-06-2007 20:08:56	6	0.01%	-
WEB-PHP test.php access	28-05-2007 18:45:01	22-06-2007 15:32:46	2	0.00%	-
WEB-CGI formmail access	28-05-2007 23:14:44	02-06-2007 15:12:45	3	-	0.01%
WEB-PHP calendar.php access	29-05-2007 00:22:49	29-05-2007 00:22:49	1	0.00%	-
WEB-MISC Domino webadmin.nsf access	29-05-2007 06:08:55	29-05-2007 06:08:58	2	-	0.00%
WEB-FRONTPAGE /_vti_bin/ access	29-05-2007 11:36:05	05-06-2007 00:41:57	5	0.01%	-
WEB-IIS asp-dot attempt	30-05-2007 21:51:49	25-06-2007 21:44:06	27	0.06%	-
SPYWARE-PUT Trickler teomasearchbar runtime detection	31-05-2007 15:31:58	18-06-2007 19:20:12	2	0.00%	-
WEB-PHP IGeneric Free Shopping Cart page.php access	01-06-2007 05:49:27	21-06-2007 12:56:40	17	0.04%	-
WEB-CLIENT Microsoft wmf metafile access	05-06-2007 15:36:17	21-06-2007 13:47:47	3	0.01%	-
(http_inspect) OVERSIZE CHUNK ENCODING	08-06-2007 11:09:25	08-06-2007 11:10:47	2	0.00%	-
ICMP PING speedera	08-06-2007 14:46:55	08-06-2007 14:47:18	7	0.02%	-
WEB-MISC encoded cross site scripting attempt	12-06-2007 04:02:27	12-06-2007 04:02:27	1	0.00%	-
WEB-MISC cross site scripting attempt	12-06-2007 04:02:27	12-06-2007 04:02:27	1	0.00%	-
WEB-MISC intranet access	19-06-2007 00:48:59	19-06-2007 00:49:10	8	0.02%	-
WEB-FRONTPAGE _vti_inf.html access	21-06-2007 12:13:59	22-06-2007 16:30:27	3	0.01%	-
WEB-PHP admin.php access	22-06-2007 09:05:01	22-06-2007 09:05:01	1	0.00%	-
		Grand Total	46193	98.20%	1.80%

With a fine-tuned signature rule-set, *Table 18* shows the distribution of the related incidents and classifies them into true or false incidents. The classification of the false and true incidents is made manually and supervised by a GCIA Certified Intrusion Analyst (GCIA, 2011). Approximately 98.20% of the incidents (i.e. 45,360) detected are asserted as false positives, while 1.80% of the total incidents (i.e. 833) are affirmed to be irrelevant positives. The classification of these is important as they need to be analysed later in the third stage of the evaluation study

5.1.3 General Tools

To carry out the experiments in the different evaluation stages, this study applied several types of open source software, namely Snort (network intrusion detection), MySQL (database), Apache (HTTP server), PHP (Server-side HTML embedded scripting language) and Tcpreplay. The reasons for utilising these applications were their openness and public availability, as well as being free to use. The descriptions of the applications are briefly explained as follows:

(a) *Snort*. The software is a free and lightweight network-based IDS created by Caswell and Roesch (1998). To monitor network traffic and detect harmful payload or suspicious incidents, such as signature-based IDSs, Snort uses a set of pre-defined rules written in text files. However, to improve the detection mode, security analysts are free to edit and create new rules or even disable built-in rules. This study deployed Snort version 2.8.5.1 to detect incidents based upon the snortrules-snapshot-2853 rules set and default configurations.

(b) *MySQL*. Originally found by David Axmark, Allan Larsson and Michael "Monty" Widenius, MySQL is quoted as the most popular open source database software (MySQL, 2011). As open source software, in addition to being the most affordable software, it also provides a superior speed, security, reliability, ease of use and active improvements by other developers to make sure it is free from bugs. This study used MySQL 5.1.37 as the database to store incidents that were detected by Snort.

(c) *Apache*. Deployed as a web-server, Apache was originally founded in April 1996 and provides a secure, efficient and extensible server to support the current HTTP standards (Apache, 2011). In an effort to develop and maintain the current standards, Apache continues to support various platforms, including operating systems from UNIX and the Windows family. In this study, the Apache web-server is used as a tool to serve HTTP requests and display the experimental result using web browsers, and this study deployed Apache 2.2.13 for that purpose.

(d) *PHP*. Originally created by Rasmus Lerdorf in 1995, PHP is a server-side HTML embedded scripting language, widely-used and designed to support active web development to produce dynamic web pages (PHP, 2011). In addition, it has evolved to include a command-line interface capability and this allows this study to use it as a standalone application which has an ability to run specific functions independently. An advantage is that PHP also can be deployed on most web servers currently freely available in the public domain. This study applied PHP version 5.2.10 running with Apache 2.2.13 for the web server and used it as tool to examine, analyse, estimate, rate, rank and prioritise incidents based upon their risk indexes.

(e) *Tcpreplay*. A tool gives the ability to re-generate network traffic in a simulation mode, using any traffic which was previously captured using a libpcap format. The tool is written by Aaron Turner and has been utilised by many vendors, enterprises, universities, labs and open source projects in order to re-play network traffic (Tcpreplay, 2011). This evaluation study utilised the tool to re-play the captured traffic in the selected datasets, in order to simulate them as live traffic.

5.1.4 Design Assumptions and Rationale

To facilitate and conduct experiments in this study properly, along with the specific model and strategies planned in the proposed framework, some modifications and assumptions were made. Specifically, given the lack of specific information on assets, some assumptions had to be made on the values of assets that related to the incident scenario in the dataset.

Using the category given for the assets, the experiment in this study made an assumption of the indicators' value, particularly for assets; as such information is not available directly from the dataset. The assumption is only to quantify the value of the incident risk index and is exclusively used for the experiment in this study, so the value does not necessarily reflect the actual value of assets in the original dataset. As a simple basis, this study adopted similar values to those given by Lee *et al.* (2002) and the assumed values are based upon the asset's functional role. The criticality, maintainability, replaceability and dependability values are shown in *Table 19*. In addition, the experiment applied zero values for the control indicator for all assets. This assumption stems from the DARPA dataset itself, which assumes a naïve defender.

Table 19. Assumed Asset Value

Category	Criticality	Maintainability	Replaceability	Dependability
Category 1	10	10	5	5
Category 2	8	8	5	5
Category 3	4	2	5	0
Category 4	2	2	5	0

Furthermore, the experiment used five different indicators in evaluating the value for the likelihood of threat and vulnerability. As such, their values are obtained with specific guidelines and a similar description, as described in *Section 4.1.3*.

To facilitate the requirement of the judgement matrices for the decision factors and indicators, this study uses the values tabulated in *Table 7*, *Table 8* and *Table 9* (see *Section 4.1.2*, pp. 63). Based on the value of the consistency index and consistency ratio, all the assessments and values for the indicators' weight in this assumption are considered consistent.

The other requirements and assumptions used in specific stages are discussed separately.

5.2 Risk Index Model Evaluation

The first stage of the evaluation study investigates the use of AHP as a method of prioritising incidents in the Rating Strategy Modules (see *Figure 11*) and aims to satisfy two objectives:

(a) To propose a new Risk Index Model (RIM) as a method of rating, ranking and prioritising incidents, particularly with the aid of the Analytic Hierarchy Process;

(b) To validate the result of RIM, they are compared to existing approaches used as the industry standards, namely CVSS v2 and Snort Priority.

5.2.1 Experiment and Procedure Description

This stage performed two main experiments, based on whether different weightings for indicators are applied. The description of the experiments is as follows:

(a) *Experiment 1*. Using AHP as the model to estimate risk indexes, the first experiment uses same value for all indicators leading to equal weights when calculating risk indexes. This experiment is a control experiment and its results will be used to compare with the Experiment 2 results.

(b) *Experiment 2*. The second experiment uses different weights of indicators and is used to identify the effect different weightings can have on the incident risk indexes. The used of different weightings of indicators in this experiment is an improvement made in order to address one the post-incident prioritisation drawbacks which identified in *Section 3.1.3*.

Since this is a preliminary evaluation, the experiment was conducted using the DARPA dataset only. The experiment inherited all the dataset descriptions as well as experimental assumptions made in the previous section (i.e. *Section 5.1.4*) for the experiment input.

Furthermore, in order to calculate the incident risk indexes, both experiments applied the *static mode* strategy in the rating process and they rated incidents only once, when the incidents are detected. Essentially, the rating for the risk index for each incident is unchanged and remains static until the end of the evaluation phases. Theoretically, the periodic changes of the risk index could give another implication, such as it would affect the performance of the estimation process but perhaps give more accurate risk indexes. However, this first stage would not consider the effect of the changes.

In order to compare the results, and validate the RIM, the experiment was based on some assumptions. In particular, with the DARPA 2000 LLDOS 1.0 dataset, there are different attacks in different phases of attacks, as shown in *Table 16*. Thus, to analyse the dataset, this study made assumptions as follows:

(a) A true incident in any phase is assumed as a critical incident in that particular phase.

(b) Due to the multi-staged attack in the dataset, true incidents in the latest phase are assumed as more critical incidents compared to incidents in other previous phases.

In analysing the ranking of the incident, the experiment ranked each one according to its detection time. All incidents are ranked and no incident was excluded until the end of the phases. In addition, the different weights for the indicators used in Experiment 2 was obtained using estimation in three judgement matrices (see *Section 4.1.2*, pp. 63): the judgement matrix of the influence factor, the judgement matrix of the main indicator for *impact on asset* and the judgement matrix of the main indicator for *likelihood of threat and vulnerability*. The judgement matrices were used to evaluate the different results of the incident risk index. In this particular experiment, the judgement matrices were just an assumption made to manually fit with Risk Index Model. Generally, the judgement matrices can be altered, and the assumption in this particular experiment is not definitive and may be subject to reassessment.

5.2.2 Results

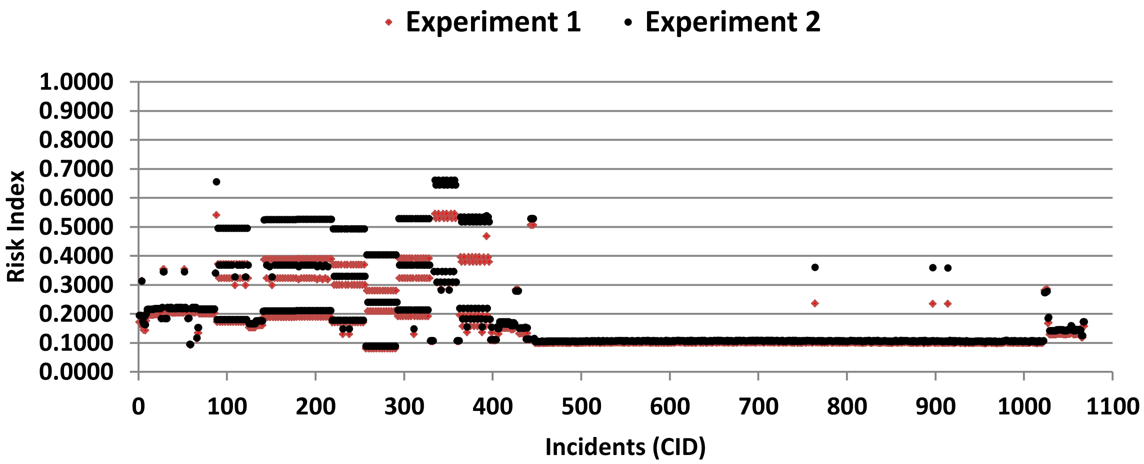


Figure 12. Graph for the distribution of incidents (Experiment 1 and Experiment 2)

Figure 12 shows the results of the two experiments. As can be seen in the graph, Experiment 2 plots higher risk indexes in comparison to Experiment 1. Generally, the distribution of incidents in both experiments was different and it shows significant results. To look at them closer, *Table 20* and *Table 21* tabulate the selected incidents.

Table 20. Partial result of risk index and ranking for Experiment 1

							Time Interval																							
Phase	Incidents' Signature	No. of Incidents	Time		Risk Index		09:51:35		09:52:00		10:08:06		10:18:06		10:33:09		10:35:01		10:50:00		10:50:54		11:26:14		11:34:21		12:23:39		12:35:48	
			Min	Max	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High
Pre 1	FTP Bad login	1	09:32:34	09:32:34	0.3142	0.3142	1	1	4	4	4	4	114	114	114	114	149	149	149	149	149	149	153	153	153	153	153	153	153	153
1	**ICMP Echo Reply**	**20**	**09:51:36**	**09:52:00**	**0.0939**	**0.3542**			**65**	**2**	**86**	**2**	**317**	**66**	**321**	**66**	**385**	**95**	**413**	**95**	**423**	**95**	**435**	**99**	**1014**	**99**	**1042**	**99**	**1056**	**99**
	ICMP PING	**20**	**09:51:36**	**09:52:00**	**0.0942**	**0.3542**			**64**	**1**	**85**	**1**	**316**	**65**	**320**	**65**	**384**	**94**	**412**	**94**	**422**	**94**	**434**	**98**	**1013**	**98**	**1041**	**98**	**1055**	**98**
Pre 2	ATTACK-RESPONSES Invalid URL	1	09:52:10	09:52:10	0.1135	0.1135					84	84	315	315	315	315	376	376	398	398	408	408	415	415	422	422	450	450	464	464
	ATTACK-RESPONSES 403 Forbidden	2	09:54:45	09:58:36	0.1345	0.1345					83	82	311	310	311	310	372	371	392	391	396	395	401	400	408	407	412	411	414	413
2	**RPC portmap sadmind request UDP**	**76**	**10:08:07**	**10:18:05**	**0.0802**	**0.3412**							**329**	**68**	**333**	**68**	**397**	**103**	**425**	**103**	**435**	**103**	**447**	**107**	**1026**	**107**	**1054**	**107**	**1068**	**107**
	RPC portmap Solaris sadmin port query udp request	**76**	**10:08:07**	**10:18:05**	**0.2802**	**0.5412**							**141**	**1**	**141**	**1**	**184**	**7**	**184**	**7**	**188**	**7**	**192**	**7**	**196**	**7**	**196**	**7**	**196**	**7**
Pre 3	ATTACK-RESPONSES directory listing	4	10:22:43	10:31:30	0.1061	0.1061									319	316	380	377	408	405	418	415	430	427	437	434	465	462	479	476
3	**RPC portmap sadmind request UDP**	**14**	**10:33:10**	**10:34:59**	**0.1959**	**0.3462**											**267**	**97**	**267**	**97**	**271**	**97**	**275**	**101**	**282**	**101**	**282**	**101**	**282**	**101**
	RPC portmap Solaris sadmin port query udp request	**14**	**10:33:10**	**10:34:59**	**0.3959**	**0.5462**											**22**	**1**	**22**	**1**	**22**	**1**	**26**	**1**	**26**	**1**	**26**	**1**	**26**	**1**
	RPC sadmind query with root credentials attempt UDP	**14**	**10:33:10**	**10:34:59**	**0.1573**	**0.3076**											**357**	**150**	**357**	**150**	**361**	**150**	**365**	**154**	**372**	**154**	**374**	**154**	**376**	**154**
Pre 4	TELNET login incorrect	2	10:36:34	10:46:04	0.1361	0.1362													390	389	394	393	398	397	405	404	409	408	411	410
	ATTACK-RESPONSES 403 Forbidden	2	10:46:28	10:46:28	0.1315	0.1315													394	393	404	403	411	410	418	417	434	433	441	440
4	**RSERVICES rsh root**	**8**	**10:50:02**	**10:50:38**	**0.1334**	**0.2835**															**400**	**173**	**405**	**177**	**412**	**179**	**416**	**179**	**418**	**179**
	ATTACK-RESPONSES 403 Forbidden	2	10:50:15	10:50:54	0.1318	0.1323															402	401	409	408	416	415	420	419	427	426
Pre 5	TELNET login incorrect	1	11:00:11	11:00:11	0.1355	0.1355																	399	399	406	406	410	410	412	412
	ATTACK-RESPONSES Invalid URL	1	11:05:11	11:05:11	0.1116	0.1116																	416	416	423	423	451	451	465	465
5	**(snort decoder) Bad Traffic Loopback IP**	**572**	**11:27:51**	**11:27:56**	**0.0984**	**0.1027**																			**1012**	**441**	**1040**	**469**	**1054**	**483**
Post 5	TELNET login incorrect	4	11:39:07	12:33:25	0.1578	0.1702																					358	356	368	356

To show the simplicity and difference of the results, *Table 20* tabulates selected incidents detected in Experiment 1 by Snort IDSs and stored in the MySQL database, and most of them are considered as true and critical incidents. The other details related to the dataset can be found in Appendix A.

There were 1,068 incidents detected and the critical incidents are highlighted in bold. *Table 20* and *Table 21* show the incidents tabulated into several phases, groups, number of alerts, time, risk index and the priority of the incident ranked at the specific time. The first column on the left of the table refers to the phases of the dataset and is followed by the incidents, grouped into similar incident types. The number of similar incidents is presented in the third column. In order to analyse the ranking of similar incidents, this study summarises the time detected and the risk index according to two different values (high/max and low/min). The min and max timestamps in the time column refer to the first and last timestamp of the incident detected. The low and high values in the risk index column indicate the lowest and highest values of the incident risk index. The ranking process was ranked at 12 different periods started from 09:51:35 and ended at 12:35:48. To give a simple view, the incidents are grouped into similar types of signature and ranked based on the highest and lowest risk indexes.

The incidents were ranked separately in the experiment as a single event and the total number of incidents increased over time. The lowest rank was at position number 1 at the beginning and 1068 in the end. As tabulated, most of true and critical incidents (except in the last phase) were ranked at the top priority ranking. For example, in the 1st phase at 09:52:00, the critical incident with the signature "*ICMP PING*" and "*ICMP Echo Reply*" were ranked at first and second place. After about 30 minutes, new incidents were detected and the position was changed again. Since the new incidents were considered more critical compared to the previous incidents, the top priority was given to the new incident which was the "*RPC portmap Solaris sadmin port query udp request*". Continuously, a similar scenario happened at 10:35:01, where the new incidents were ranked as top priority compared to the previous incident. This trend is consistent with the assumption made earlier whereby a new critical incident in a new phase is considered more critical to the incident in the previous phases.

Table 21. Partial result of risk index and ranking for Experiment 2

							Time Interval																							
Phase	Incidents' Signature	No. of Incidents	Time		Risk Index		09:51:35		09:52:00		10:08:06		10:18:06		10:33:09		10:35:01		10:50:00		10:50:54		11:26:14		11:34:21		12:23:39		12:35:48	
			Min	Max	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High
Pre 1	FTP Bad login	1	09:32:34	09:32:34	0.3135	0.3135	1	1	4	4	4	4	141	141	141	141	176	176	176	176	176	176	180	180	183	183	183	183	183	183
1	**ICMP Echo Reply**	**20**	**09:51:36**	**09:52:00**	**0.0950**	**0.3459**			**65**	**2**	**86**	**2**	**317**	**123**	**321**	**123**	**385**	**158**	**413**	**158**	**423**	**158**	**435**	**162**	**1014**	**165**	**1042**	**165**	**1056**	**165**
	ICMP PING	**20**	**09:51:36**	**09:52:00**	**0.0955**	**0.3459**			**64**	**1**	**85**	**1**	**316**	**122**	**320**	**122**	**384**	**157**	**412**	**157**	**422**	**157**	**434**	**161**	**1013**	**164**	**1041**	**164**	**1055**	**164**
Pre 2	ATTACK-RESPONSES Invalid URL	1	09:52:10	09:52:10	0.1177	0.1177					84	84	315	315	315	315	376	376	398	398	408	408	415	415	422	422	450	450	464	464
	ATTACK-RESPONSES 403 Forbidden	2	09:54:45	09:58:36	0.1531	0.1531					83	82	311	310	311	310	372	371	392	391	396	395	401	400	408	407	412	411	414	413
2	**RPC portmap sadmind request UDP**	**76**	**10:08:07**	**10:18:05**	**0.0891**	**0.3408**							**329**	**125**	**333**	**125**	**397**	**160**	**425**	**160**	**435**	**160**	**447**	**164**	**1026**	**167**	**1054**	**167**	**1068**	**167**
	RPC portmap Solaris sadmin port query udp request	**76**	**10:08:07**	**10:18:05**	**0.4041**	**0.6558**							**76**	**1**	**76**	**1**	**105**	**7**	**105**	**7**	**105**	**7**	**109**	**7**	**109**	**7**	**109**	**7**	**109**	**7**
Pre 3	ATTACK-RESPONSES directory listing	4	10:22:43	10:31:30	0.1086	0.1086									319	316	380	377	408	405	418	415	430	427	484	481	512	509	526	523
3	**RPC portmap sadmind request UDP**	**14**	**10:33:10**	**10:34:59**	**0.2195**	**0.3469**											**220**	**151**	**220**	**151**	**224**	**151**	**228**	**155**	**235**	**158**	**235**	**158**	**235**	**158**
	RPC portmap Solaris sadmin port query udp request	**14**	**10:33:10**	**10:34:59**	**0.5345**	**0.6619**											**22**	**1**	**22**	**1**	**22**	**1**	**22**	**1**	**22**	**1**	**22**	**1**	**22**	**1**
	RPC sadmind query with root credentials attempt UDP	**14**	**10:33:10**	**10:34:59**	**0.1826**	**0.3100**											**325**	**177**	**325**	**177**	**329**	**177**	**333**	**181**	**340**	**184**	**342**	**184**	**342**	**184**
Pre 4	TELNET login incorrect	2	10:36:34	10:46:04	0.1550	0.1552													390	389	394	393	398	397	405	404	409	408	411	410
	ATTACK-RESPONSES 403 Forbidden	2	10:46:28	10:46:28	0.1505	0.1505													394	393	404	403	411	410	418	417	422	421	424	423
4	**RSERVICES rsh root**	**8**	**10:50:02**	**10:50:38**	**0.1526**	**0.2797**															**400**	**185**	**405**	**189**	**412**	**192**	**416**	**192**	**418**	**194**
	ATTACK-RESPONSES 403 Forbidden	2	10:50:15	10:50:54	0.1507	0.1514															402	401	409	408	416	415	420	419	422	384
Pre 5	TELNET login incorrect	1	11:00:11	11:00:11	0.1540	0.1540																	399	399	406	406	410	410	412	412
	ATTACK-RESPONSES Invalid URL	1	11:05:11	11:05:11	0.1161	0.1161																	416	416	423	423	451	451	465	465
5	**(snort decoder) Bad Traffic Loopback IP**	**572**	**11:27:51**	**11:27:56**	**0.1036**	**0.1090**																			**1012**	**434**	**1040**	**462**	**1054**	**476**
Post 5	TELNET login incorrect	4	11:39:07	12:33:25	0.1733	0.1890																					329	327	377	327

In contrast to the previous example, incidents detected in the 3rd phase were ranked at the top priority until the end of the scenario. Although there were new critical incidents (i.e. Bad Traffic Loopback IP) detected in the 5th phase, it was ranked lower than the critical incident in the 3rd Phase because it was considered as not critical enough in comparison. In this particular scenario, the result is consistent with the dataset because the incidents were considered failed (DARPA, 2011).

Furthermore, *Table 21* shows partial results of Experiment 2 and some significant changes compared to the results of Experiment 1. The results are slightly different because the experiment was performed with weighted indicators. In general, Experiment 2 has shown some significant changes in the risk index value as well as the top priority ranking. In order to show the changes, *Table 22* shows the percentage of unchanged rank position between both experiments.

Table 22. The percentage of unchanged rank position between both experiments

Time	Total	Total	Top 10	Top 25	Top 50	Top 100	Top 250
		Percentage					
2000-03-07 09:51:35	25	100.00	100.00	100.00	-	-	-
2000-03-07 09:52:00	65	66.15	100.00	100.00	76.00	-	-
2000-03-07 10:08:06	86	44.19	100.00	100.00	60.00	-	-
2000-03-07 10:18:06	329	54.10	100.00	100.00	96.00	62.00	53.60
2000-03-07 10:33:09	333	54.65	100.00	100.00	96.00	62.00	53.60
2000-03-07 10:35:01	397	45.59	10.00	52.00	72.00	79.00	41.60
2000-03-07 10:50:00	425	46.35	10.00	52.00	72.00	79.00	41.60
2000-03-07 10:50:54	435	45.75	10.00	52.00	72.00	79.00	41.60
2000-03-07 11:26:14	447	41.61	10.00	4.00	26.00	58.00	33.20
2000-03-07 11:34:21	1026	26.71	10.00	4.00	26.00	58.00	33.20
2000-03-07 12:23:39	1054	26.76	10.00	4.00	26.00	58.00	33.20
2000-03-07 12:35:48	1068	26.59	10.00	4.00	26.00	58.00	33.20
Average		48.20	47.50	56.00	58.91	65.89	40.53

Table 22 shows the percentage of the unchanged rank position for all incidents, top 10, top 25, top 50, top 100 and top 250 incidents in 12 different timestamps. As can be seen when considering all incidents, 73.41% of the incidents or the majority of the rank positions was changed. There were on average only 26.59% of the total incidents that remained unchanged. Interestingly for the top priority incident, the average is quite significant where 47.50% for the top 10 and 56.00% and top 25 incidents remained unchanged. For example, at 10:35:01, the total number of incidents was 397 and only 45.59% (181 incidents) of rank positions had remained unchanged; other incidents changed their position. To show some changes in the top priority incidents, 10% of the incidents in the top 10 priority rank remained unchanged and the majority of them were changed; 9 out of 10 incidents. A similar percentage can be seen in the other timestamp where some of the top priority incidents were changed.

In the majority of cases, the change of the risk index affects the ranking of incidents; it represents 73.41% of them. For example, the highest rating for the "ICMP Echo Reply" incident in Experiment 1 was 0.3542, but it significantly decreased to 0.3459 in Experiment 2. At the same time, the ranking for a similar signature was different where the highest position was at the 99th position in Experiment 1 and the 165th position in Experiment 2. However, in a few cases which represent 26.59% of incidents, the use of different weightings had no effect upon the ranking. For example, the risk index for the "*RPC portmap Solaris sadmin port query udp request*" incident was changed from 0.5462 to 0.6619 without modifying its rank.

Table 23. Risk Index and Ranking Comparison

Incidents' Signature Name	No. of Incidents	Time		Risk Index				Ranking			
		Min	Max	Low		High		Low		High	
				E1	E2	E1	E2	E1	E2	E1	E2
ATTACK-RESPONSES directory listing	20	09:29:20	11:03:33	0.1061	0.1083	0.1725	0.1956	482	573	329	323
FTP Bad login	1	09:32:34	09:32:34	0.3142	0.3135	0.3142	0.3135	153	183	153	183
TELNET login incorrect	17	09:32:34	12:33:25	0.1302	0.1484	0.2865	0.2828	447	427	175	190
ATTACK-RESPONSES Invalid URL	4	09:37:05	12:23:39	0.1116	0.1161	0.1442	0.1650	465	465	404	401
ATTACK-RESPONSES 403 Forbidden	12	09:45:34	12:31:13	0.1186	0.1252	0.1429	0.1633	463	463	405	403
ICMP Echo Reply	**72**	**09:45:37**	**12:26:16**	**0.0939**	**0.0950**	**0.3542**	**0.3459**	**1056**	**1056**	**99**	**165**
ICMP PING	**72**	**09:45:37**	**12:26:16**	**0.0942**	**0.0955**	**0.3542**	**0.3459**	**1055**	**1055**	**98**	**164**
ICMP Destination Unreachable Port Unreachable	76	10:08:07	11:04:13	0.2100	0.2402	0.5067	0.5292	211	211	14	35
RPC portmap sadmind request UDP	**90**	**10:08:07**	**10:34:59**	**0.0802**	**0.0891**	**0.3462**	**0.3469**	**1068**	**1068**	**101**	**158**
RPC portmap Solaris sadmin port query udp request	**90**	**10:08:07**	**10:34:59**	**0.2802**	**0.4041**	**0.5462**	**0.6619**	**196**	**109**	**1**	**1**
RPC portmap Solaris sadmin port query udp portmapper sadmin port query attempt	**14**	**10:33:10**	**10:34:59**	**0.3799**	**0.5178**	**0.5303**	**0.6452**	**73**	**73**	**8**	**8**
RPC sadmind query with root credentials attempt UDP	**14**	**10:33:10**	**10:34:59**	**0.1573**	**0.1826**	**0.3076**	**0.3100**	**376**	**342**	**154**	**184**
SQL version overflow attempt	1	10:34:57	10:34:57	0.4679	0.5386	0.4679	0.5386	18	14	18	14
RSERVICES rsh root	**8**	**10:50:02**	**10:50:38**	**0.1334**	**0.1526**	**0.2835**	**0.2797**	**418**	**418**	**179**	**192**
(snort decoder) Bad Traffic Loopback IP	**572**	**11:27:51**	**11:27:56**	**0.0984**	**0.1036**	**0.1027**	**0.1090**	**1054**	**1054**	**483**	**476**
SNMP AgentX/tcp request	3	11:27:54	11:27:55	0.2349	0.3592	0.2366	0.3614	199	157	197	155
ICMP PING *NIX	1	11:28:18	11:28:18	0.2811	0.2739	0.2811	0.2739	184	199	184	199
ICMP PING BSDtype	1	11:28:18	11:28:18	0.2811	0.2739	0.2811	0.2739	183	198	183	198

In comparing the experimental results between the similar and different weights of indicators, *Table 23* summarises the comparison between the two experiments. The table summarises the incidents by grouping them into similar type of signatures with the number of incidents, time when the incident was detected (i.e. min and max), risk indexes and ranking of the related incidents. For the risk index and ranking, the table only shows the lowest and highest values for both experiments; E1 represents Experiment 1 and E2 represents Experiment 2. As mentioned earlier, there were some significant changes in the risk index value as well as some of the top priority ranking. For example, the top priority incidents for both experiments were still in the same position. This scenario can be seen in the "*RPC portmap Solaris sadmin port query udp request"* and the "*RPC portmap Solaris sadmin port query udpportmappersadmin port query attempt*" incidents.

5.2.3 Discussion

The experimental results, presented in the previous section, are encouraging as all the true and critical incidents received appropriate ranking, except the last true incidents. The proposed method was further validated by comparing the experimental results with the industry standards, like Snort priority and the CVSS v2 Base Score.

Table 24. Snort Priority, CVSS v2 Base Score and Exploitability Subscore and Risk Index

						Risk Index			
						Low		High	
Incidents' Signature Name	**Snort Priority**	**CVE ID**	**CVSS v2 Base Score**	**Exploitability Subscore**	**No. of Incidents**	**E1**	**E2**	**E1**	**E2**
ATTACK-RESPONSES directory listing	2	-	-	-	20	0.1061	0.1083	0.1725	0.1956
FTP Bad login	2	-	-	-	1	0.3142	0.3135	0.3142	0.3135
TELNET login incorrect	2	-	-	-	17	0.1302	0.1484	0.2865	0.2828
ATTACK-RESPONSES Invalid URL	2	-	-	-	4	0.1116	0.1161	0.1442	0.1650
ATTACK-RESPONSES 403 Forbidden	2	-	-	-	12	0.1186	0.1252	0.1429	0.1633
ICMP Echo Reply	**3**	**-**	**-**	**-**	**72**	**0.0939**	**0.0950**	**0.3542**	**0.3459**
ICMP PING	**3**	**-**	**-**	**-**	**72**	**0.0942**	**0.0955**	**0.3542**	**0.3459**
ICMP Destination Unreachable Port Unreachable	3	CVE-2005-0068	5	10	76	0.2100	0.2402	0.5067	0.5292
RPC portmap sadmind request UDP	**2**	**-**	**-**	**-**	**90**	**0.0802**	**0.0891**	**0.3462**	**0.3469**
RPC portmap Solaris sadmin port query udp request	**2**	**CVE-2003-0722**	**10**	**10**	**90**	**0.2802**	**0.4041**	**0.5462**	**0.6619**
RPC portmap Solaris sadmin port query udp portmapper sadmin port query attempt	**2**	**CVE-2003-0722**	**10**	**10**	**14**	**0.3799**	**0.5178**	**0.5303**	**0.6452**
RPC sadmind query with root credentials attempt UDP	**2**	**-**	**-**	**-**	**14**	**0.1573**	**0.1826**	**0.3076**	**0.3100**
SQL version overflow attempt	1	CVE-2002-0649	8	10	1	0.4679	0.5386	0.4679	0.5386
RSERVICES rsh root	**1**	**-**	**-**	**-**	**8**	**0.1334**	**0.1526**	**0.2835**	**0.2797**
(snort decoder) Bad Traffic Loopback IP	**2**	**-**	**-**	**-**	**572**	**0.0984**	**0.1036**	**0.1027**	**0.1090**
SNMP AgentX/tcp request	2	CVE-2002-0013	10	10	3	0.2349	0.3592	0.2366	0.3614
ICMP PING *NIX	3	-	-	-	1	0.2811	0.2739	0.2811	0.2739
ICMP PING BSDtype	3	-	-	-	1	0.2811	0.2739	0.2811	0.2739

Table 24 shows the outcome of this comparison. The first column in the table is the type of incident, which is followed by the Snort Priority, as obtained directly by Snort IDS. The next three columns are the CVE-ID, CVSS v2 Base Score and exploitability sub score which were taken directly from National Vulnerability Database (NIST, 2011). The last four columns show the risk indexes that were directly taken from the experimental results.

The experimental results show that the approach in this study is better than the Snort Priority and CVSS v2 Base Score in terms of ranking and prioritising incidents. Based on the experimental result, all incidents were rated and produced risk indexes between 0 and 1. It seems that the results show a significant improvement in terms of the number of the incident rating because the CVSS v2 Base Score can rate only 17.23% or 184 out of 1,068 incidents. The low percentage is because only 5 out of 18 types of incidents have the CVE-ID and CVSS v2 Base Score, the rest have no significant values. This study has identified this as a serious limitation when the CVSS v2 Base Score is used as an approach in ranking incidents; only incidents with a signature that has the CVSS and CVE-ID can be ranked, all others will be excluded.

Furthermore, the ranking approach performed in this study is better than the Snort Priority because the latter prioritises incidents only into several groups, specifically three. With the limitation of the group priority, security analysts will face difficulty in differentiating which incidents are urgent and important. To look at them closer, *Figure 13* plots the distribution of incidents using the incident risk index and Snort Priority. As can be seen, the distribution of incidents is limited to only three groups, as opposed to RIM with risk indexes between 0 and 1. For example, there were 72 incidents for the

"*ICMP Echo reply*" and the Snort Priority labelled all of them as a low priority or 3 within the same groups. However, in this study, with the similar incidents in Experiment 1, the risk indexes given were between 0.0939 and 0.3542. The different risk indexes between the incidents allow security analysts to rank and prioritise incidents more effectively. This limitation of the group priority can also be seen with the CVSS because it groups incidents with a similar type of incident and not according to the incidents' urgency or risk indexes.

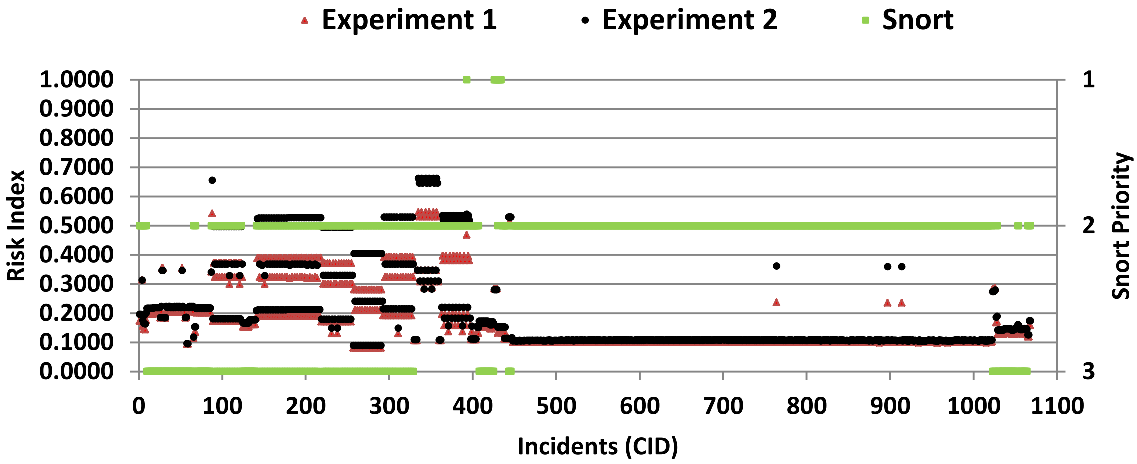


Figure 13. Graph for Experiment 1, Experiment 2 and Snort Priority

In comparison, the position of the ranking in *Table 23* is better compared to the prioritising result in *Table 24* because the incidents were prioritised according to their risk indexes and not into a similar group. Although the rating of the risk index and the ranking of the critical incidents cannot be validated with other studies, the result from the Snort Priority can be considered as an appropriate comparison reference because it is a standard priority which is practically produced by Snort IDS. In particular, the experimental results give a better output in terms of an incident's ranking because each incident can be ranked separately and clearly has a specific position for every single incident. With the identification of the specific position, it helps security analysts to respond only to an appropriate incident; hence it could save time and resources.

Furthermore, using the Snort Priority some of the false incidents were rated as high priority incidents, but using the approach in this study those incidents were rated with a low risk index and a low ranking. To look at them closer, the incident with the "*(snort decoder) – Bad Traffic Loopback IP*" signatures were prioritised as medium in the Snort Priority, but the ranking approach in this study ranked it with a low position of 1,054 in both experiments. Furthermore, the DARPA 2000 LLDOS 1.0 dataset is known as a scenario of multi-stage attack where a series of attacks were launched over a period of time and different stages (as shown in *Table 15*). As expected, the result of the experiment has shown that the rating and ranking for the different stages of attack were apparently in line with the assumption made. The experiments were fairly rated and ranked the critical incidents as the top priority incidents in each stage except the two last stages. They were rated and ranked like that because the incidents in the last two stages were considered as failed attacks.

In comparing the experimental results in this study with other results, this study has shown some improvement in rating as well as ranking and prioritising incidents. In comparison, the model in this study rated incidents at the 5th phase with a low rating and the same time ranked it at a suitable position and placed it better compared to Alsubhi *et al.* (2008) . In contrast, the approach in Alsubhi *et al.* (2008) gave a very high score for similar incidents in the 5th phase, although the incidents were considered as failed incidents. Furthermore, this study is unable to compare the experimental results with others since there is not another recent study in incident prioritisation that uses the same or a similar dataset.

5.2.4 Conclusion and Limitation

The first stage of the evaluation study has shown the integration of risk assessment and AHP in prioritising incidents. The model was introduced as a means to estimate the rating of incidents based on ten indicators derived from two main decision factors: likelihood of event and consequence of event. With a combination of the risk assessment and the aid of AHP, the risk index for each incident is sorted and ranked quantitatively.

A model to rate and rank incident is the Risk Index Model (RIM), which has already been used successfully in this evaluation study. The study also validated the feasibility of the model by using the standard DARPA 2000 LLDOS 1.0 dataset (DARPA, 2011). The investigation of the effectiveness of the model was completed by looking at three aspects:

(a) *Different weightings for indicators*. The straightforward analysis of the result between the two experiments reveals that both are different in terms of valuing risk indexes as well as the position of the non-top priority incidents. To summarise, the use of the different weightings for indicators has shown significant changes only in risk index values and not in the top priority ranking. In particular, when considering all incidents, 73.41% of the incidents or the majority of the rank positions was changed. There were on average only 26.59% of the total incidents which remained unchanged. Interestingly for the top priority incident, the average is quite significant where 47.50% of the top 10 incidents and 56.00% of the top 25 incidents remained unchanged. The experimental result in this stage also showed a reasonable case where incidents can be ranked dynamically using a different or similar weight of indicators. This stage is unable to determine which experiment could produce better results because there are no significant and correct reference results to compare. However, the comparison between the experimental results indicated that the result in Experiment 2 is better than Experiment 1 in terms of their risk indexes.

(b) *Comparison study with other approaches like the Common Vulnerability Scoring System (CVSS) (NIST, 2011) and Snort Priority (Caswell and Roesch, 1998).* To reduce the limitation of the unavailability of other studies to compare with the results, this study made an evaluation study based on two industry standards: Snort Priority and the CVSS. In comparing with the outcomes from them, the model has significantly improved the incident prioritisation by rating and ranking all incidents detected in the dataset. In terms of experimental results, the model rated 100% of the number of incidents compared to only 17.23% of incidents with the CVSS. In addition, the model improves the limitation of group priority in the Snort Priority (e.g. high, medium and low priority) by quantitatively ranking, sorting and listing incidents according to their risk indexes.

(c) *Feasibility of Risk Index Model*. The preliminary results of the experiment demonstrated and validated the feasibility of the model in rating as well as ranking incidents. The preliminary results of the experiment also demonstrated and validated the feasibility of the approach in this study in rating and quantifying incidents using similar and different weights of indicators.

In addition to the main aspects above, the experiment also clearly demonstrated that the approach is practical and can conveniently be used as an alternative approach to rating, ranking and prioritising incidents. Furthermore, the proposed model is suitable to be applied in real life to rank and prioritise incidents.

The model uses selected indicators and they are easy to measure and obtain as well as requiring less computational process. In terms of its configuration, this model has shown that the judgement matrices used are efficient enough for rating, ranking as well as prioritising true and critical incidents. However, the judgement matrices used for full practical use must be configured correctly because it would affect the output of the ranking. For instance, the priority value for the consequence of an event or factor related to an asset could be a small index value when it involves only one asset, for example prioritising incidents in one web server.

In conducting the experiment, this study has found some limitations with regards to the practical aspects. Below are some of the limitations and suggestions for reducing them.

(a) *Quantitative Input*. All inputs in the experiments are quantitative. However, in a practical situation it is difficult to establish such quantitative measures, particularly with asset values. Arguably, therefore, a qualitative input which has a different group of rating (e.g. high, medium and low) would be more meaningful. This study used quantitative values because the model allows incidents to be differentiated among others. It is suggested that a qualitative input needs to be changed to a quantitative input in order to calculate a risk index.

(b) *Reasonable Assumptions*. At present, the experiment has used assumptions to derive the values in estimating risk index, particularly in rating the value of an asset. To reduce this limitation, the future work should focus on strengthening the estimation process for rating every indicator which is involved in the model. It is suggested to extend the indicator by giving a precise and detailed metric for measuring incidents, especially in reducing uncertainty amongst indicators.

(c) *Strategies Performances*. In the experiment, the ranking was based on a small number of incidents (i.e. 1,068 in total). The performance cost of rating and ranking incidents on a larger scale has not been adequately studied, but based on the preliminary results which can be simulated within a few seconds, it is estimated that the effect will be less. In order to evaluate this potential demand, this study has conducted an additional experiment in identifying a better strategy in ranking incidents in the later stages. Although the result of this experiment is convincing in terms of the prioritisation strategy, technically the involvement of a few million incidents may slow the rating and ranking process. Therefore, the fourth stage investigates the processing time between different rating and ranking strategies to compare the performance effectiveness.

(d) *Responses*. The result also provides a clear distinction between the ways incidents are rated, ranked and prioritised. However, the experiments in this stage do not consider any countermeasures or response to control the critical incident. With the promising result in this stage, the third stage in this study also investigated a response strategy which can be used to work with RIM in selecting appropriate responses for incidents with different priorities. An important question for future studies is to determine better strategies if there is another countermeasure or response applied to stop the critical incident.

5.3 Evaluation of the Effect of Using Different Strategies in Ranking and Rating

The first stage highlighted the feasibility of RIM, particularly in the rating and ranking process in order to estimate risk indexes and rank incidents. However, the first stage has not considered the effect of the changes in risk indexes and this second stage extends the evaluation study of the effect of the changes over time.

Therefore, in order to scale down the consideration, this second stage investigates the effect of applying several strategies in the rating and ranking process and also aims to satisfy two objectives:

(a) To investigate the effect of applying a different strategy in the rating process as it offers changes of the incident risk indexes over time.

(b) To investigate the effect of applying a different strategy in the ranking process by using the advantages of time interval.

It is important to understand that the improvement made by applying a different strategy in the rating and ranking process has the potential to improve the prioritisation process, in particular with a new formulation made from some of the indicators used in the proposed framework. This stage is predicted to create an improvement of risk indexes in rating incidents and facilitate a better approach in ranking as well as positioning a critical incident. As mentioned in the previous chapters (see *Section 4.2.3*), the rating and ranking process are the two main modules in the framework and they help to identify the urgency and criticality of incidents. With the identification, they help a security analyst to respond only to an appropriate incident, hence they could save time and avoid a waste of effort.

5.3.1 Experiment and Procedure Description

In order to investigate the effect of the changes made on the strategy planned in the rating and ranking process, this stage considers the following criteria:

(a) The rating process adopts the *on-demand mode* as its strategy, where the incident risk index is updated each time a new incident is detected.

(b) Since the DARPA dataset simulates less than three hours network traffic, the changes of the incident risk indexes are configured to be restricted to three different time intervals: 1 hour, 2 hours and without limitation. The different time intervals are important to demonstrate the different results in different set of configurations.

(c) In the ranking process, the positions of incidents are also ranked dynamically according to the changes of their risk index.

As discussed in *Section 4.1.3*, the changes are predicted to improve the Risk Index Model from two different perspectives: firstly, the use of the *on-demand mode* as the rating strategy will produce a more accurate incidents risk index compared to the previous one, and secondly, the changes of the strategy in the ranking process will eliminate the limitation of ranking too many incidents in one time.

This stage extends the experiments in the first stage; therefore it applies a similar Risk Index Model as well as its descriptions, assumptions, the matrix judgements and models.

5.3.2 Results and Discussion

As expected, the experimental results at this stage were consistent with the results from the first stage in terms of the number of outputs. There were 1,068 incidents detected by the sensor and again all the incidents were rated and ranked. To extend the discussion on the experimental results, this section discusses them in two parts.

(a) The first part discusses the effect of the changes of the incident risk indexes due to the selection mode in the rating strategy.

(b) The second part discusses the effect of the ranking strategy due to the changes of the incident risk indexes in terms of their number, as well as the position of critical incidents.

To show the effect of the changes, *Figure 14* and *Figure 15* plot the distribution of incidents by plotting the lowest, the highest and the average of their risk indexes. As can be seen in *Figure 15*, incidents were plotted with higher risk indexes in comparison to incidents in *Figure 14.* For example, this trend can be seen in between incidents with CID 100 to 450. The distribution is identical with the first stage results except the new graphs contain a range of risk index for each incident. The range is a result of the changes of risk index over time.

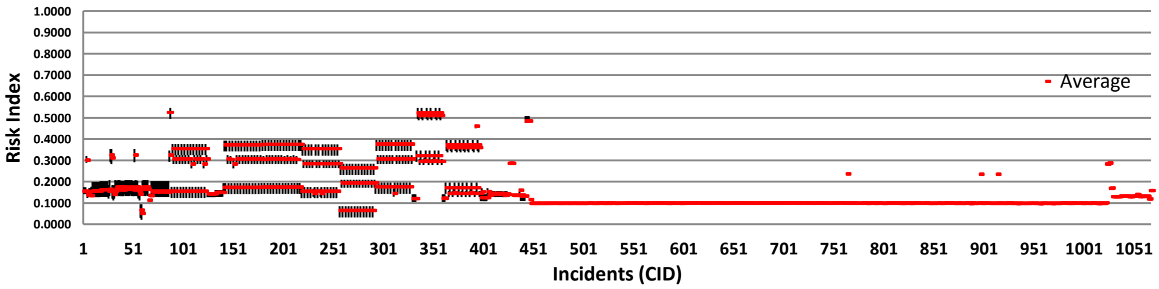


Figure 14. A new graph for Experiment 1

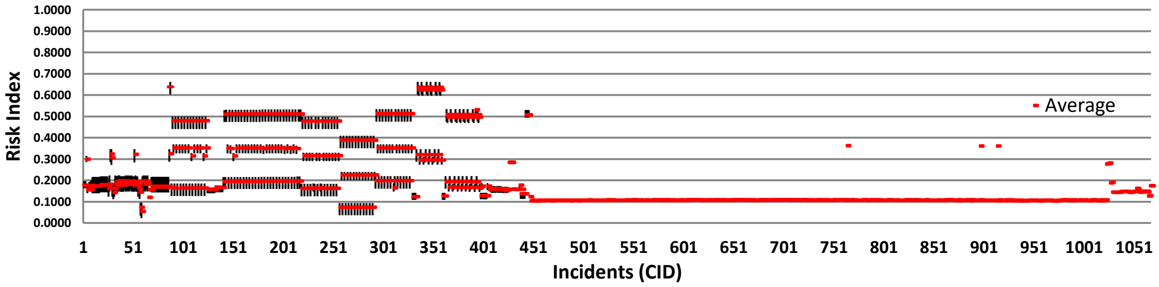


Figure 15. A new graph for Experiment 2

To look at the effect closer, *Table 25* shows some of the selected incidents. In order to show the comparison results and their trend, a selection of the incidents was made based upon their detection time as well as the top incidents in different attack phases.

Table 25. A partial result of the Risk Index upon selected incidents

		Time Interval											
		09:51:35	09:52:00	10:08:06	10:18:06	10:33:09	10:35:01	10:50:00	10:50:54	11:26:14	11:34:21	12:23:39	12:35:48
Incident	Detected	25	40	21	243	4	64	28	10	12	579	28	14
	Total	25	65	86	329	333	397	425	436	447	1026	1054	1068

Experiment 1

Time Detected	**Incident ID**	Risk Index											
09:32:34	CID 4	0.3142	0.2970	0.2951	0.2885	0.2892	0.2898	0.2910	0.2911	0.2920	0.3193	0.3186	0.3183
09:51:36	CID 28		0.3542	0.3504	0.3339	0.3330	0.3334	0.3325	0.3309	0.3301	0.2910	0.2922	0.2926
09:51:56	CID 52		0.3542	0.3504	0.3337	0.3329	0.3318	0.3310	0.3295	0.3285	0.2902	0.2915	0.2919
10:08:07	CID 88				0.5412	0.5402	0.5460	0.5411	0.5393	0.5379	0.4941	0.4936	0.4933
10:33:27	CID 353						0.5462	0.5413	0.5396	0.5381	0.4942	0.4937	0.4934
10:50:03	CID 428								0.2835	0.2834	0.2878	0.2874	0.2872
11:27:52	CID 575										0.1026	0.1002	0.0991

Experiment 2

Time Detected	**Incident ID**	Risk Index											
09:32:34	CID 4	0.3135	0.2954	0.2935	0.2862	0.2869	0.2875	0.2886	0.2888	0.2899	0.3147	0.3140	0.3139
09:51:36	CID 28		0.3459	0.341	0.3327	0.3317	0.3341	0.3325	0.3306	0.3298	0.2854	0.2865	0.2869
09:51:56	CID 52		0.3459	0.3410	0.3325	0.3315	0.3320	0.3305	0.3287	0.3276	0.2844	0.2855	0.2859
10:08:07	CID 88				0.6558	0.6547	0.6615	0.6562	0.6542	0.6527	0.6037	0.6031	0.6028
10:33:27	CID 353						0.6619	0.6565	0.6546	0.6531	0.6038	0.6032	0.6029
10:50:03	CID 428								0.2797	0.2796	0.2856	0.2851	0.2849
11:27:52	CID 575										0.1090	0.1063	0.1052

The experimental results are tabulated into three main tables: the first table on the top tabulates the number of incidents detected and the other two tables show the incident risk indexes based upon two different experiments. In the risk index table, the first column on the left of the table refers the time of the incident detected followed by its ID. In order to analyse the effect of the strategy used in the rating process, the incident risk index was ranked at 12 different periods starting from 09:51:35 and ending at 12:35:48. In a practical situation, they are rated dynamically when a new incident is detected.

With the implementation of the *on-demand mode* in the rating process, the experimental result shows significant changes in the incident risk indexes where all incidents were affected. For example, in following the consideration of the criteria in the rating process, the risk index for “FTP Bad login” with CID 4 was rated at 09:32:34 with 0.3142 for the first time in Experiment 1. The trend for the similar incidents also can be seen in Experiment 2. The risk index was updated from one period to another until the end of the phase. A similar trend can be seen in the other incidents. The changes of the risk indexes are consistent with the claim made earlier in *Section 4.1.3* due to the changes of the formulation in the *frequency* and *similarity* indicator.

In order to show the effect on the implementation of the second criteria of different time limitations (e.g. 1 hour, 2 hours and none), *Table 26* shows the different trend compared to the previous results in *Table 25* using the results of Experiment 2. In particular, a different trend can be seen in incidents with CID 353, 428 and 575. For example, with the 1 hour limitation, the incident with CID 353 was detected at 10:33:27 and at the time rated (i.e. 10:35:01), only incidents detected in between 10:35:01 and 09:35:01 were counted to estimate its risk index. Furthermore, the incident risk index was rated differently with the implementation of two hours limitation. A similar trend can be seen on incidents with CID 428 and 575.

Table 26. The incident risk indexes based upon different time interval limitations

			Time Interval											
			09:51:35	09:52:00	10:08:06	10:18:06	10:33:09	10:35:01	10:50:00	10:50:54	11:26:14	11:34:21	12:23:39	12:35:48
Time Detected	**Incident ID**	**Limitation**	Risk Index											
09:32:34	CID 4	None	0.3135	0.2954	0.2935	0.2862	0.2869	0.2875	0.2886	0.2888	0.2899	0.3147	0.3140	0.3139
		1 hour	0.3135	0.2954	0.2935	0.2862	0.2869							
		2 hours	0.3135	0.2954	0.2935	0.2862	0.2869	0.2875	0.2886	0.2888	0.2899	0.3147		
09:51:36	CID 28	None		0.3459	0.341	0.3327	0.3317	0.3341	0.3325	0.3306	0.3298	0.2854	0.2865	0.2869
		1 hour		0.3459	0.341	0.3327	0.3317	0.3341	0.3325	0.3306				
		2 hours		0.3459	0.341	0.3327	0.3317	0.3341	0.3325	0.3306	0.3298	0.2854		
09:51:56	CID 52	None		0.3459	0.3410	0.3325	0.3315	0.3320	0.3305	0.3287	0.3276	0.2844	0.2855	0.2859
		1 hour		0.3459	0.3410	0.3325	0.3315	0.3320	0.3305	0.3287				
		2 hours		0.3459	0.3410	0.3325	0.3315	0.3320	0.3305	0.3287	0.3276	0.2844		
10:08:07	CID 88	None				0.6558	0.6547	0.6615	0.6562	0.6542	0.6527	0.6037	0.6031	0.6028
		1 hour				0.6558	0.6547	0.6615	0.6562	0.6542	0.6527			
		2 hours				0.6558	0.6547	0.6615	0.6562	0.6542	0.6527	0.6037		
10:33:27	CID 353	None						0.6619	0.6565	0.6546	0.6531	0.6038	0.6032	0.6029
		1 hour						**0.6628**	**0.6572**	**0.6553**	**0.6537**	**0.6038**		
		2 hours						0.6619	0.6565	0.6546	0.6531	0.6038	0.6032	0.6029
10:50:03	CID 428	None								0.2797	0.2796	0.2856	0.2851	0.2849
		1 hour								**0.2802**	**0.2800**	**0.2859**		
		2 hours								0.2797	0.2796	0.2856	0.2851	0.2849
11:27:52	CID 575	None										0.1090	0.1063	0.1052
		1 hour										**0.1590**	**0.1532**	
		2 hours										0.1090	0.1063	0.1052

According to the experimental results, the changes of the incident risk index can be seen only on the incident which was detected after 10:33:00. This is because the restriction was made in the second criteria where the effect can only be seen after 10:29:20, which is one hour after the first incident detected (i.e. 09:29:20).

The changes of the risk indexes over time give additional implications. In particular, the implementation of the different mode and strategies in the processes has made some improvement in two aspects, firstly the position of the critical incidents, and secondly the total number of incidents that need to be ranked.

In order to show the implication for the position of the critical incidents, *Table 27* tabulates the comparison results between the experimental outputs in the first stage. Using Experiment 2 as the reference results for the comparison study, *Table 27* shows the example of some selected incidents using two different studies and the first column lists those incidents. Each incident has three rows; the first row details the risk index of the correspondence incident, the second row shows its position and the last row tabulates its old position which is taken from the experimental results in the first stage. The list contains the critical and non-critical incidents taken from different phases. Similar to the first stage, in order to evaluate the experimental results, the ranking process was ranked at 12 different periods starting from 09:51:35 and ending at 12:35:48.

In general, the changes of risk indexes over time have changed some of the positions of incidents. In comparing the position of incidents, the majority of them were influenced. For example, the position for the *CID 4* incident has changed from the old position at 183rd to the new position at 158th due to the changes of the risk index (i.e. 0.3135 to 0.3139); this trend is consistent with the other incidents. The changes of risk indexes have less significant effect on some of the top priority incidents. For instance, the *CID 88* incident has no effect on the changes and a similar trend can be seen with the *CID 353* incident.

Table 27. Position for critical incidents between two different studies

		Time Interval											
Incident ID		**09:51:35**	**09:52:00**	**10:08:06**	**10:18:06**	**10:33:09**	**10:35:01**	**10:50:00**	**10:50:54**	**11:26:14**	**11:34:21**	**12:23:39**	**12:35:48**
CID 4	Risk Index	0.3135	0.2954	0.2935	0.2862	0.2869	0.2875	0.2886	0.2888	0.2899	0.3147	0.3140	0.3139
	New Position	1	4	4	141	141	182	182	182	186	158	158	158
	Old Position	1	4	4	141	141	176	176	176	180	183	183	183
CID 52	Risk Index		0.3459	0.3410	0.3325	0.3315	0.3320	0.3305	0.3287	0.3276	0.2844	0.2855	0.2859
	New Position		1	2	124	124	159	159	159	163	188	184	184
	Old Position		3	3	124	124	159	159	159	163	166	166	166
CID 88	Risk Index				0.6558	0.6547	0.6615	0.6562	0.6542	0.6527	0.6037	0.6031	0.6028
	New Position				1	1	7	7	7	7	5	7	7
	Old Position				1	1	7	7	7	7	7	7	7
CID 353	Risk Index						0.6619	0.6565	0.6546	0.6531	0.6038	0.6032	0.6029
	New Position						1	1	2	1	3	5	5
	Old Position						1	1	1	1	1	1	1
CID 428	Risk Index								0.2797	0.2796	0.2856	0.2851	0.2849
	New Position								188	191	185	187	187
	Old Position								187	191	194	194	194

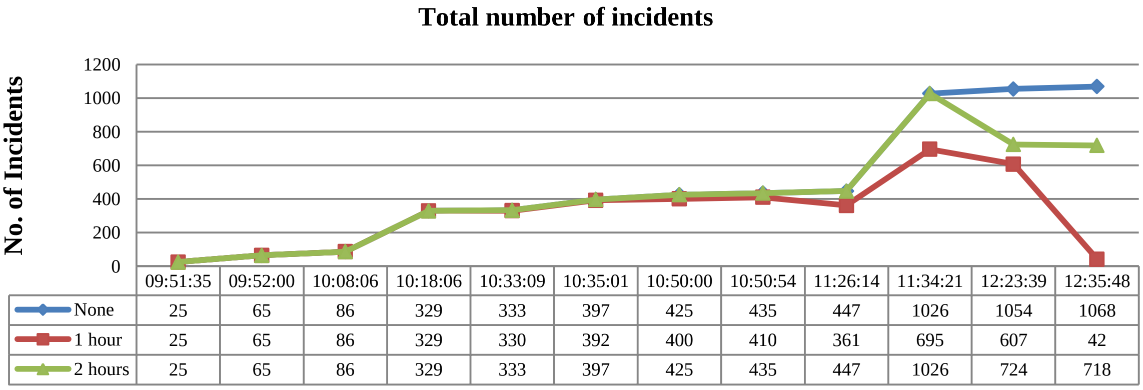
*The new position is based upon the *Section 5.3* experiment and the old position is based on the S*ection 5.2 experimental results.*

In order to show the effect upon the changes of the time limitation upon the incident rank, *Table 28* shows the different trend compared to the results in *Table 27*. As similar to the risk index results in *Table 26*, the different trend can be seen in incidents with CID 353 and 428. For example, with the implementation of a 1 hour limitation, the incident with CID 353 was detected at 10:33:27 and at the time rated (i.e. 10:35:01) it was ranked in 1st position. The position changed to 4th position as opposed to the implementation of 2 hours limitation which showed a similar position to the previous one. This trend has been predicted in the first place because the experimental results in the first stage indicated that only a certain percentage of incidents will be affected in terms of their positions. The changes of the incident position are not too significant because the changes only affect not more than ±10 movements.

In addition, as in *Table 28*, there are a few rows which show some empty spaces. The empty space means some of the incidents have been dropped from being ranked at that specific period. This is consistent with the third criterion mentioned earlier where incidents are ranked only for a few hours; therefore only incidents that have a lifetime less than the configured hours will be ranked, otherwise they will be dropped. For example, the "*FTP Bad Login*" with CID 4 was ranked only in 5 different periods until 10:33:09 and after that it was dropped from being ranked. Similar trends can also be seen with the other incidents. In contrast, without the limitation applied, all the incidents will be ranked until the end of the ranking process. With the improvement, the implementation of the third criterion in the ranking strategy is potentially helpful in assisting security analysts to focus and analyse only a small number of critical incidents, instead of having unnecessary incidents. In addition, since the total number of the incidents changes from time to time, the position of the incident is also improved. For example, at the 11:34:21, instead of having position at 185th for the incident with CID 428, it was located at the position 45th with the 1 hour limitation.

Table 28. The incident ranks based upon different time interval limitations

			Time Interval											
Time Detected	**Incident ID**		**09:51:35**	**09:52:00**	**10:08:06**	**10:18:06**	**10:33:09**	**10:35:01**	**10:50:00**	**10:50:54**	**11:26:14**	**11:34:21**	**12:23:39**	**12:35:48**
09:32:34	CID 4	Risk Index	0.3135	0.2954	0.2935	0.2862	0.2869	0.2875	0.2886	0.2888	0.2899	0.3147	0.3140	0.3139
		Position (None)	1	4	4	141	141	182	182	182	186	158	158	158
		Position (1 Hour)	**1**	**4**	**4**	**141**	**141**							
		Position (2 Hour)	**1**	**4**	**4**	**141**	**141**	**182**	**182**	**182**	**186**	**158**		
09:51:56	CID 52	Risk Index		0.3459	0.3410	0.3325	0.3315	0.3320	0.3305	0.3287	0.3276	0.2844	0.2855	0.2859
		Position (None)		1	2	124	124	159	159	159	163	188	184	184
		Position (1 Hour)		**2**	**1**	**123**	**123**	**158**	**158**	**158**				
		Position (2 Hour)		**2**	**1**	**123**	**123**	**158**	**158**	**158**	**162**	**187**		
10:08:07	CID 88	Risk Index				0.6558	0.6547	0.6615	0.6562	0.6542	0.6527	0.6037	0.6031	0.6028
		Position (None)				1	1	7	7	7	7	5	7	7
		Position (1 Hour)				**1**	**1**	**7**	**7**	**7**	**7**			
		Position (2 Hour)				**1**	**1**	**7**	**7**	**7**	**7**	**5**		
10:33:27	CID 353	Risk Index						0.6619	0.6565	0.6546	0.6531	0.6038	0.6032	0.6029
		Position (None)						1	1	2	1	3	5	5
		Position (1 Hour)						**1**	**4**	**3**	**1**	**4**		
		Position (2 Hour)						**1**	**1**	**2**	**1**	**3**	**1**	**2**
10:50:03	CID 428	Risk Index								0.2797	0.2796	0.2856	0.2851	0.2849
		Position (None)								188	191	185	187	187
		Position (1 Hour)								**184**	**188**	**45**		
		Position (2 Hour)								**188**	**191**	**185**	**47**	**32**



	09:51:35	09:52:00	10:08:06	10:18:06	10:33:09	10:35:01	10:50:00	10:50:54	11:26:14	11:34:21	12:23:39	12:35:48
None	25	65	86	329	333	397	425	435	447	1026	1054	1068
1 hour	25	65	86	329	330	392	400	410	361	695	607	42
2 hours	25	65	86	329	333	397	425	435	447	1026	724	718

Figure 16. The number of incidents using two ranking strategies

In terms of the number of incidents, the total number of incidents rated was dissimilar from the experimental result in the first stage. The graph in *Figure 16* shows the difference between those implementations. The number of incidents rated and ranked was similar only for the first hour (09:29:20 – 10:29:20) and two hours (09:29:20 – 11:29:20), but it was changed after that. As illustrated in *Figure 16*, the number of incidents rated and ranked between 1 hour and without limitation was different starting in the period 10:33:09. The total number of incidents without limitation was increased up to 1,068 incidents at the end of the period but this would be different from the 1 hour limitation results. The total number of incidents that need to be ranked is fluctuating and varies. For example, at 10:35:01 there were 392 incidents that needed to be ranked; this number increased at 10:50:54 to 410 incidents and decreased back at 11:26:14 to 361 incidents. A similar trend can be seen with the implementation of a 2 hour limitation.

The changes in the number of incidents have additional implications. In general, the total number of incidents that need to be ranked is similar to the number that need to be rated. Therefore, if the number of incidents is increased each time the incident is detected, the total number of incidents that need to be ranked is indirectly increased too. As can be seen, the total number of incidents was increased dramatically using the first stage criteria and had the potential to become infinite if there had been other incidents detected after the last period. In some circumstances, arguably the incremental of the number will increase computational processes. It is logical that a high number of incidents use a high processing power; therefore, it is impractical and time-consuming for a huge number of incidents. The implementation of those criteria as a strategy in the rating process to rate incidents as well as in the ranking process to rank them has significantly reduced some of the latter problem. As a result, the total number of incidents that need to be ranked was fairly reduced in the experiment. As noted, the highest number of incidents recorded was only 695 incidents at 11:34:21, which is less 331 incidents if using the first stage criteria.

The investigation into the processing time of the rating and ranking process is discussed in the fourth stage of the evaluation study.

5.3.3 Conclusion

The evaluation study in the second stage highlights some interesting findings as follows:

(a) *Changes of the incident risk index over time*. With the implementation of the *on-demand mode* as a strategy in the rating process, the incident risk indexes change periodically when a new incident is detected and they will be updated as long as they satisfy the conditions in the criteria. As a key to ranking incidents, the changes of the incident risk index are constantly followed by the changes in its position. The study also highlights the effect of the changes over time and the position where the majority of incidents were influenced. The comparison results showed that the change of risk indexes has a small degree of effect upon the position of the incidents. In conclusion, the *on-demand mode* strategy is better than the *static mode* strategy in prioritising incidents, although it may induce an overhead in the processes.

(b) *Different weightings of indicators*. Consistent with the first stage, the experimental result has identified the different value of the risk index between similar and different weights of indicators. The different weights used by the indicators have shown some significant changes in rating and ranking incidents.

(c) *Improve the analysis results*. With the implementation of different modes and strategies in the rating and ranking process, some improvements have been made. In particular, a better position for critical incidents can be produced compared to the strategy used in the first stage. Plus, there is a reduction in terms of the total number of incidents that need to be ranked. This reduction allows security analysts to focus on a small number of incidents and helps to respond only to an appropriate incident; hence it could save time and resources.

(d) *A practical and convenient approach*. As similar to the first stage, the experiment in this study clearly stated that the implementation of different strategies is practical and can conveniently be used as an alternative approach to rate, rank and prioritise incidents.

In improving the strategy, this stage still inherits some limitations similar to the first stage, particularly with the input, response selections and dataset.

5.4 Response Strategy Model Evaluation

The evaluation studies in the first and second stage evaluated the feasibility of RIM as well as the effect of using different strategies in the rating and ranking process. Although both studies have shown significant results in prioritising incidents, they share a similar limitation upon the response selection process. Thus, this stage extends the evaluation study by investigating the suitability of considering the Response Strategy Model (RSM) in the framework.

The third stage aims to investigate the effectiveness of the proposed model as a strategy in the response selection process. One of the criteria to support the response selection process is to consider the ability to distribute incidents into appropriate responses. For example, a serious incident should be mapped with an active response in order to minimise its impact, as opposed to an incident of less impact which it may be appropriate to map with a passive one. This mapping process is important to the proposed framework, as a good mapping strategy increases the reliability of the model in facilitating the autonomous mode. Therefore, in order to satisfy such claims, this stage investigates the ability of the proposed framework to distribute incidents.

Furthermore, this stage also investigates the relationship between the distribution of incidents and their classification (e.g. false/true incidents), as one of the important objectives supporting the response selection process is the consideration of reducing false responses to false incidents.

5.4.1 Experiment and Procedure Description

In order to investigate the effectiveness of the proposed model, this stage discusses two case studies and aims to satisfy three goals.

(a) Firstly, the case studies investigate the distribution of incidents in comparison with other industrial tools like CVSS v2 (Mell *et al.*, 2006; Mell *et al.*, 2009) and Snort Priority (Caswell and Roesch, 1998).

(b) Secondly, the case studies investigate the relationship between the distribution and their ability to classify incidents between true and false incidents.

(c) Thirdly, the case studies extend the investigation into the effect of applying the different weights of the decision factors in the rating and ranking process as well as its relationship with incident classification.

There are two case studies in this stage. The first case study was conducted using the DARPA dataset and the second case study was conducted using the Plymouth University datasets.

The case studies were based upon the results from the first and second stage; therefore they applied a similar Risk Index Model as well as their descriptions, assumptions, the matrix judgements, criteria and models.

To facilitate the distribution of incidents and its mapping process, the case studies consider the following rating threshold, as in *Figure 17*.

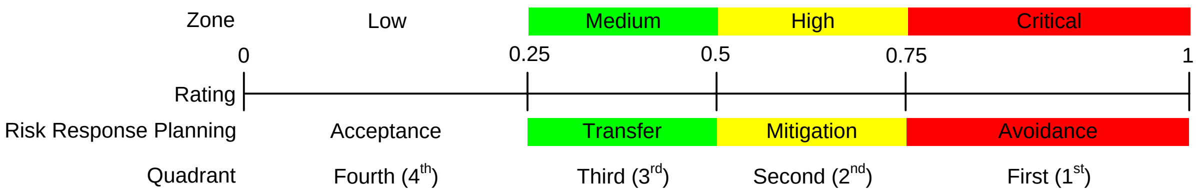


Figure 17. Rating Threshold

Furthermore, the second goal is predicted to satisfy two types of relationship. Firstly, the true positive incidents are likely to be prioritised as high priority incidents and secondly, the false incidents are likely to be prioritised as low priority incidents.

To facilitate the third goal, in order to show different scenarios in the study, this stage applies the following weights for the decision factors. There were five scenarios in the evaluation studies and each scenario has different weights of decision factors, which manually generated in order to simulate different scenarios.

Table 29. Scenario - different weights of decision factors

Scenario	Consequence of Event	Likelihood of Event
1	0.4444	0.5556
2	0.1000	0.9000
3	0.1667	0.8333
4	0.3333	0.6667
5	0.5000	0.5000

5.4.2 Results

Table 30 shows the distribution of incidents using the DARPA dataset. It contains 1,068 incidents. The first column on the left refers to the phases of the dataset and is followed by the total of incidents. The incidents are divided into two classes of incidents: true and false incidents. The other columns summarise the percentage of incidents with regards to specific rows; either they are true or false incidents. The distribution is separated between Snort Priority, CVSS v2 and the Response Strategy Model. The Snort Priority is divided into 3 different priorities which are high, medium and low. With CVSS v2, there are three main categories and there are high, medium and low. However, *Table 30* tabulates 4 columns for CVSS v2 and the last column is an additional column and it refers to incidents without priority. With the proposed framework, the Response Strategy Model (RSM) divides its priority into four quadrants, including avoidance, mitigation, transfer and acceptance.

Table 30. With the DARPA datasets

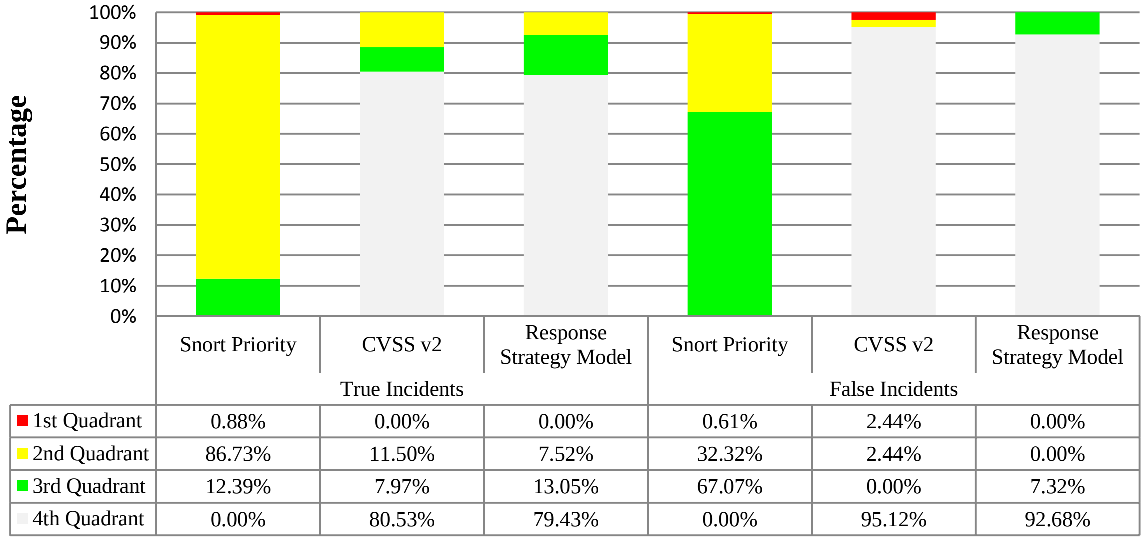
Phase	Time	No. of Incidents	Type	No. of Incidents	Snort Priority			CVSS v2				Response Strategy Model			
					High	Medium	Low	High	Medium	Low	None	Avoidance	Mitigation	Transfer	Acceptance
Pre 1	09:21:36 - 09:51:35	25	TRUE	-	-	-	-	-	-	-	-	-	-	-	-
			FALSE	25	-	36.00%	64.00%	-	-	-	100.00%	-	-	**4.00%**	**96.00%**
1	09:51:36 - 09:52:00	40	TRUE	40	-	-	100.00%	-	-	-	100.00%	-	-	**7.50%**	**92.50%**
			FALSE	-	-	-	-	-	-	-	-	-	-	-	-
Pre 2	09:52:01 - 10:08:06	21	TRUE	-	-	-	-	-	-	-	-	-	-	-	-
			FALSE	21	-	14.29%	85.71%	-	-	-	100.00%	-	-	-	**100.00%**
2	10:08:07 - 10:18:05	243	TRUE	224	-	67.86%	32.14%	33.93%	32.14%	-	33.93%	-	**17.86%**	**43.30%**	**38.84%**
			FALSE	19	-	15.79%	84.21%	-	-	-	100.00%	-	-	-	**100.00%**
Pre 3	10:18:06 - 10:33:09	4	FALSE	4	-	100.00%	-	-	-	-	100.00%	-	-	-	**100.00%**
3	10:33:10 - 10:35:01	64	TRUE	60	-	100.00%	-	46.67%	-	-	53.33%	-	**46.67%**	**23.33%**	**30.00%**
			FALSE	4	25.00%	75.00%	-	25.00%	-	-	75.00%	-	-	-	**100.00%**
Pre 4	10:35:02 - 10:50:00	28	TRUE	-	-	-	-	-	-	-	-	-	-	-	-
			FALSE	28	-	35.71%	64.29%	-	-	-	100.00%	-	-	-	**100.00%**
4	10:50:01 - 10:50:54	10	TRUE	8	100.00%	-	-	-	-	-	100.00%	-	-	**50.00%**	**50.00%**
			FALSE	2	-	100.00%	-	-	-	-	100.00%	-	-	-	**100.00%**
Pre 5	10:50:55 - 11:26:14	12	TRUE	-	-	-	-	-	-	-	-	-	-	-	-
			FALSE	12	-	66.67%	33.33%	-	33.33%	-	66.67%	-	-	**33.33%**	**66.67%**
5	11:26:15 - 11:34.21	579	TRUE	572	-	100.00%	-	-	-	-	100.00%	-	-	-	**100.00%**
			FALSE	7	-	42.86%	57.14%	42.86%	-	-	57.14%	-	-	**100.00%**	-
Post 5	11:34:22 - 12:35:48	42	TRUE	-	-	-	-	-	-	-	-	-	-	-	-
			FALSE	42	-	19.05%	80.95%	-	-	-	100.00%	-	-	-	**100.00%**
Total	09:21:36 - 12:35:48	1068	TRUE	904	0.88%	86.73%	12.39%	11.50%	7.97%	-	80.53%	-	**7.52%**	**13.05%**	**79.43%**
			FALSE	164	0.61%	32.32%	67.07%	2.44%	2.44%	-	95.12%	-	-	**7.32%**	**92.68%**

In general, a total of 904 incidents or 84.64% of incidents are considered as true incidents and this includes critical incidents as well as non-critical incidents. Only 15.36% or 164 incidents are considered as false incidents. As can be seen in the table, there is a clear distribution between true and false incidents. With the proposed framework and RSM, an average of 92.68% of the false incidents was prioritised as the lowest quadrant in the acceptance strategy column. This percentage is better compared to only 67.07% of the false incidents being prioritised under low priority with Snort Priority.

There is a huge percentage or 79.43% of true incidents identified under the acceptance quadrant and this figure can be considered as misclassification, as in the ideal situation a true incident should be classified under the first or second quadrant. However, this percentage clearly shows that those true incidents are not really critical; therefore it is acceptable to be considered under that quadrant. The results are also consistent with the DARPA dataset where most of the true incidents were identified as failed incidents, especially in the last main phase.

Furthermore, the distribution of true incidents using RSM is better compared to Snort Priority and CVSS v2. To look at them closer, in the 3rd phase, the true incidents were prioritised into three different groups using RSM compared to only one group with Snort Priority. In this case, the distribution allows any automated response systems to initiate multiple actions on incidents. This means incidents will have different types of response depending on their criticality and priority.

To summarise the result in *Table 30*, *Figure 18* plots the distribution of incidents. The first quadrant was mapped with the avoidance column and high priority in Snort Priority and CVSS v2, followed by the second quadrant with the mitigation column as well as medium priority in Snort Priority and CVSS v2. Similarly, the third quadrant was mapped with the transfer column and the lowest priority for Snort Priority and CVSS v2. Finally, the last quadrant maps incidents without any CVSS v2's score and the acceptance column. As can be seen in the graph, a better distribution for the high priority incidents in the first quadrant was produced by RSM. Snort Priority distributed 0.88% for true incidents and 0.61% for false incidents, as opposed to zero percentage with RSM. In this particular context, the incident distribution is significant with RSM.



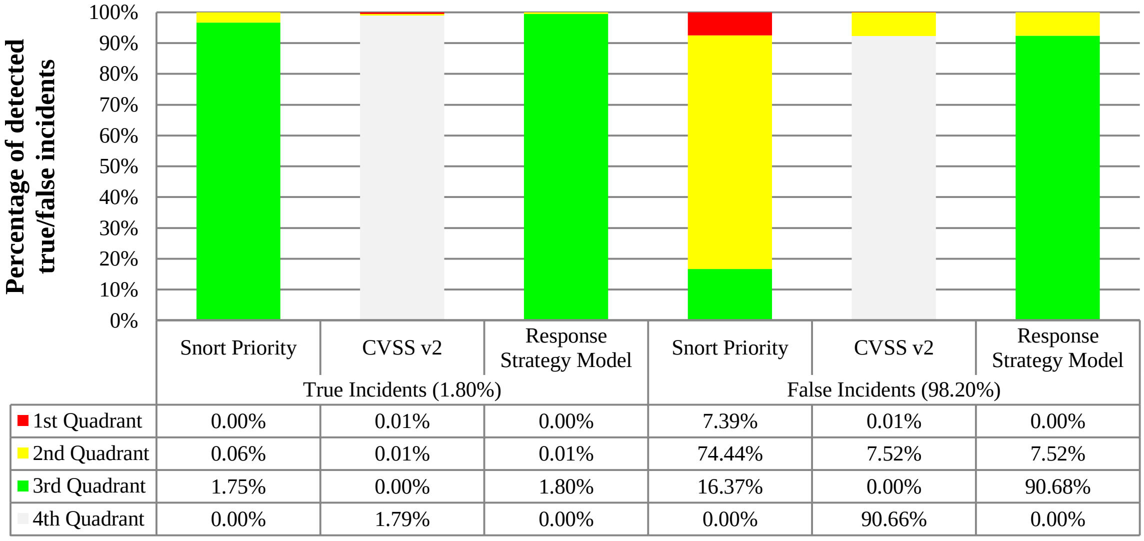
	Snort Priority	CVSS v2	Response Strategy Model	Snort Priority	CVSS v2	Response Strategy Model
	True Incidents			False Incidents		
🟥 1st Quadrant	0.88%	0.00%	0.00%	0.61%	2.44%	0.00%
🟨 2nd Quadrant	86.73%	11.50%	7.52%	32.32%	2.44%	0.00%
🟩 3rd Quadrant	12.39%	7.97%	13.05%	67.07%	0.00%	7.32%
⬜ 4th Quadrant	0.00%	80.53%	79.43%	0.00%	95.12%	92.68%

Figure 18. Graph for the incident distribution with the DARPA dataset

To further the discussion, *Table 31* and *Figure 19* tabulate the distribution of incidents using the private dataset. To recall, 98.20% of the incidents (i.e. 45,360) detected are asserted as false positives, while 1.80% of the total incidents (i.e. 833) are affirmed to be irrelevant positives[3]. With Snort Priority, 46,193 incidents were categorised into three priorities with 7.39% of them being grouped under the high priority, 74.50% under the medium priority and the balance were under the low priority. With CVSS v2, only 7.55% of incidents were able to be categorised under high, medium or low priority. A huge percentage, some 92.45% of incidents, cannot be categorised under any priority. The distribution of false incidents with Snort Priority shows an interesting figure. For instance, the majority of false incidents with 74.44% were categorised under the medium priority and the majority of true incidents with 1.75% were categorised under the low priority. The distribution of false incidents with CVSS v2 shows different figures in comparison to Snort Priority. With a low percentage of incidents with category (i.e. 7.55% as opposed to 92.45% without any category), 7.52% were prioritised as false incidents and under the medium priority and only about 0.01% of incidents were identified as under the high priority.

Table 31. With the Plymouth datasets

Type	Snort Priority			CVSS v2				Response Strategy Model			
	High	**Medium**	**Low**	**High**	**Medium**	**Low**	**None**	**Avoidance**	**Mitigation**	**Transfer**	**Acceptance**
FALSE	7.39%	74.44%	16.37%	0.01%	7.52%	0.00%	90.66%	0.00%	7.52%	90.68%	0.00%
TRUE	0.00%	0.06%	1.75%	0.01%	0.01%	0.00%	1.79%	0.00%	0.01%	1.80%	0.00%
Total	7.39%	74.50%	18.12%	0.02%	7.53%	0.00%	92.45%	0.00%	7.53%	92.47%	0.00%



	True Incidents (1.80%)			False Incidents (98.20%)		
	Snort Priority	CVSS v2	Response Strategy Model	Snort Priority	CVSS v2	Response Strategy Model
🟥 1st Quadrant	0.00%	0.01%	0.00%	7.39%	0.01%	0.00%
🟨 2nd Quadrant	0.06%	0.01%	0.01%	74.44%	7.52%	7.52%
🟩 3rd Quadrant	1.75%	0.00%	1.80%	16.37%	0.00%	90.68%
⬜ 4th Quadrant	0.00%	1.79%	0.00%	0.00%	90.66%	0.00%

Figure 19. Graph for the incidents distribution with the Plymouth dataset

With the Response Strategy Model, incidents were distributed into four quadrants. The highest priority is the avoidance quadrant, followed by the mitigation quadrant. The transfer quadrant is a low priority and the acceptance quadrant is considered as a very low priority, which is suitable for not

[3] There is a small round-off error when the percentages are rounded to 2 decimal places. This is also can be seen in *Figure 19*. For example, the correct value for 0.01% in the CVSS v2 distribution is 0.006%.

critical and not urgent incidents. The graph plots no incident under the avoidance quadrant with RSM. This means that there is no incident that needs an urgent and important response. However, the majority of incidents, with 92.47%, were categorised under the transfer quadrant and indicated that the majority of them were not critical. This percentage is significant because the majority of them (45,360 or 98.20%) are considered as false incidents in the dataset description. In analysing the 98.20%, 90.68% of incidents (i.e. 41,886) were categorised under the transfer quadrant and only 7.52% (i.e. 3,474) were categorised under the mitigation quadrant. Furthermore, there was no incident under the high priority incidents or the first quadrant, as opposed to 7.39% with Snort Priority and 0.01% with CVSS v2. This result is significant because it shows that the distribution of false incidents in RSM is better in comparison to the other two. Moreover, the majority of the false incidents in RSM, or 90.68%, were categorised under the third quadrant as opposed to only 16.37% with Snort Priority. In addition, there was zero percentage with CVSS v2 due to the limitation of its scoring system, and there was a huge percentage of false incidents (90.66%) which were unable to be prioritised.

Although the distribution is significant, the model is unable to categorise the false incidents under the lowest quadrant. In an ideal situation, false incidents should be categorised under the lowest priority. However, with a huge percentage, or 90.68%, of incidents under the transfer quadrant, it satisfies the earlier prediction that false incidents are likely to be prioritised as low priority incidents.

In analysing true incidents, 1.80% of incidents (i.e. 830) were categorised under the third quadrant and only less than 0.01% of incidents (i.e. 3) were categorised under the second quadrant. In an ideal state of affairs, the true incidents are more likely to be categorised under the avoidance or mitigation quadrants. However, the case study is unable to categorise them in the avoidance quadrant, and only a small percentage of them are under the mitigation quadrants. In comparison, the results are almost the same as those of Snort Priority and CVSS v2. The majority of the true incidents in Snort Priority, or 1.75%, were categorised in the third quadrant and 0.06% the second quadrant. With the limitation in the CVSS v2 scoring system, only 0.01% were able to be prioritised correctly in the first and second quadrant, leaving the majority of them (1.79%) in the last quadrant.

Although the distribution of true incidents is less significant because the case study is unable to categorise them in the avoidance quadrant, the percentages of the distribution are consistent with Snort Priority and CVSS v2. This consistency gives a good indicator to show that the true incidents are not really critical and, therefore, they should not be in the first and second quadrants. If this indicator can be considered as a good assumption, therefore, the distribution of true incidents using RSM is significant. To discuss this in detail, an additional comparison study was conducted and is discussed in the next section.

In addition to the case study, the third goal in the experiment description aims to investigate the effect of using different weights in the decision factors. To analyse the results, *Table 32* shows the distribution of incidents using the Plymouth dataset. The table summarises the percentage of the incident distribution. As mentioned in the description of the experiment, there were five scenarios in this case study and the first column on the left lists all of them, followed by two different classes of incidents: true and false incidents. The other columns summarise the percentage of incidents with regards to specific rows. Either they are true or false incidents with the Response Strategy Model. Similar to the representation of the previous result, they are distributed into 4 quadrants: avoidance, mitigation, transfer and acceptance.

Table 32. The incident distribution for Response Strategy Model using the Plymouth dataset

		Response Strategy Model			
Scenario	**Type**	**Avoidance**	**Mitigation**	**Transfer**	**Acceptance**
1	FALSE	0.00%	7.52%	90.68%	0.00%
	TRUE	0.00%	0.01%	1.80%	0.00%
	Total	**0.00%**	**7.53%**	**92.47%**	**0.00%**
2	FALSE	0.00%	7.52%	58.42%	32.26%
	TRUE	0.00%	0.01%	0.00%	1.80%
	Total	**0.00%**	**7.53%**	**58.42%**	**34.06%**
3	FALSE	0.00%	7.52%	59.58%	31.09%
	TRUE	0.00%	0.01%	0.00%	1.80%
	Total	**0.00%**	**7.53%**	**59.58%**	**32.89%**
4	FALSE	0.00%	7.52%	88.75%	1.93%
	TRUE	0.00%	0.01%	1.80%	0.00%
	Total	**0.00%**	**7.53%**	**90.54%**	**1.93%**
5	FALSE	0.00%	7.46%	90.74%	0.00%
	TRUE	0.00%	0.01%	1.80%	0.00%
	Total	**0.00%**	**7.47%**	**92.53%**	**0.00%**

In general, the use of different weights results in a huge difference in the incident distribution. In terms of the distribution of the false incidents, the results in Scenario 2 and 3 are better compared to the original weight as shown in Scenario 1. As can be seen, huge percentages of the false incidents were moved from the transfer quadrant to the acceptance quadrant. This movement is significant because in an ideal situation false incidents are likely to be categorised under the last quadrant or the lowest priority. In this particular result, based on the weights used in the study, the smaller the weight for the *consequence of event (e.g. asset)* decision factor, the better the results for the distribution which can be produced. This is significant because the Plymouth dataset contains only one asset: the web server.

Although the result was influenced by the number of asset in the dataset, a similar scene also affects the distribution of the true incidents. In conclusion, it can be seen that the configurations in Scenarios

2 and 3 are the best configurations for a network environment with only one asset. This is important because the percentage of the *consequence of event (e.g. asset)* decision factor has no significant effect upon one asset.

It is important to note that the proposed framework and RSM might not work in all contexts as they can be changed in a different scenario; a different dataset might produce a different set of results. However, the case studies shown in this study have their own strength in showing that it is possible to categorise and identify false incidents or true incidents using the priority of the incident itself.

5.4.3 Discussion

The results presented in the previous section are encouraging, as the Risk Index Model works well with the Response Strategy Model by mapping all incidents into their appropriate quadrants. The framework has also shown a significant result in mapping between the quantitative indexes with the qualitative group of priorities. Although this study does not have a correct reference result of the critical incidents, the comparisons made in the case study have shown a substantial value in balancing the distribution of incidents when it compared to available industry standards (e.g. CVSS and Snort Priority). The different levels in RSM give an advantage to security analysts or automated security appliances to act fast to respond to only true and critical incidents. As an implication of this, it allows easy management where each quadrant has its own type of response. Besides, this implication also demonstrates the suitability of the framework to be used in facilitating the autonomous mode in the response selection process. Furthermore, its suitability is strengthened by the significant relationship between the priority and classification of incidents.

Similar to other studies, the results in this stage are unable to make a 100% correct classification. Therefore, in order to discuss them further, the case studies were compared with recent studies: Alserhani *et al.* (2010), Ning *et al.* (2004) and Tjhai *et al.* (2010). The selection of these studies is because they used a similar dataset, either the DARPA or Plymouth dataset.

To the best of our knowledge, not much study has been done to compare incident prioritisation studies and incident classification. Therefore, this evaluation study takes the initiative of reducing the gap by comparing the results with a correlation study. One of the objectives in the correlation study is to identify false and true incidents, which are also similar to the results in this stage.

There is a significant relationship between the incident priorities and their classification using the DARPA dataset. In particular, with RSM, 92.68% of false incidents were categorised as under the lowest category and only 7.32% of false incidents were categorised as the third quadrant; both categories are considered as below the medium priority. In order to compare the result, this study made a comparison between two correlation studies: Alserhani *et al.* (2010) and Ning *et al.* (2004).

Ning *et al.* (2004) showed an interesting figure where their method manages to remove unnecessary false alarms in the DARPA dataset. With 60% of detection rates they identified 93.18% of them as true incidents and only 6.82% as false incidents. In comparing with the result in this stage, if RSM removes 92.68% of the incidents under the lowest quadrant, only 7.32% are considered as significant figures for false incidents. Both results are similar in terms of their percentage (i.e. 6.82% and 7.32%), although Ning *et al.* (2004) used a small number of incidents after they had been correlated. In addition, Ning *et al.* (2004) were unable to detect the whole related incident and, in particular, their detection rate was only 60%. Their model also depends on the quality of modelling (i.e. prerequisites and consequences) and they agreed that the process would be very difficult to perform if the attack modelling was weak and inconsistent. Furthermore, they deployed and tested their system in an offline mode, as opposed to online assessments in the proposed framework; hence it gives advantages to the proposed framework.

Due to the low detection rate in Ning *et al.* (2004), the result was compared with the more recent study of Alserhani *et al.* (2010). Their study improved the detection rate as well as the false incidents detection. From the study, 8.1% of the correlated alerts were identified as false incidents. This result is also similar to the false incidents in the framework. Only 7.32% of incidents were categorised under the third quadrants.

Furthermore, there is an irrelevant positive incident in the DARPA dataset. Irrelevant positives refer to incidents from unsuccessful attempts or unrelated vulnerabilities. According to the dataset description, the DDoS attacks in the last phase of the dataset are failed attacks, thus they can be considered as irrelevant positives. There is no discussion about this kind of incident in Alserhani *et al.* (2010) and Ning *et al.* (2004). To highlight a significant result, the case studies have prioritised them as lowest priority incidents and categorised them under the last quadrants.

Similar with the DARPA dataset, the results in the private dataset have shown a significant relationship between low priority incidents and false incidents. As highlighted earlier, the distribution of incidents in RSM is better compared to Snort Priority and CVSS v2. With RSM, 90.68% of incidents were categorised as under the third quadrant and 7.53% of incidents were categorised as under the second quadrant. The results were compared with Tjhai *et al.* (2010). In the study by Tjhai *et al.* (2010), with two stages alarm correlation and filtering system using SOM neutral network and K-mean algorithm, they correctly identified 87% of the false incidents. The study used two stages of correlation, with 78.8% of false incidents being identified in the first stage and 96% of them being identified in the second stage. The result in RSM was considered as a reasonable result and distributed 90.68% of incidents into the third quadrant, as opposed to only 78.80% identified in the first stage in the Tjhai *et al.* (2010) study. However, the second stage in Tjhai *et al.* (2010) has shown an improvement, 96% as opposed to only 90.68% with the framework. Although the second stage in Tjhai *et al.* (2010) indicated a better result, they correlated the incidents using an offline mode, giving an extra advantage to the proposed framework because the operation mode is online.

5.4.4 Conclusion

The third stage of the evaluation study highlights some interesting findings as follows:

(a) *Formal model to map between quadrants and response options*. The establishment of RSM in the proposed framework has shown a significant result in terms of distributing incidents into different levels of priorities. The urgent and important incidents are mapped into the highest quadrant, as opposed to the non-urgent incidents which are mapped into the lowest quadrant. The dynamic formulation in the rating process allows incidents to be mapped dynamically in the ranking process. The case studies have shown a significant result in distributing incidents into appropriate quadrants.

(b) *Significant relationship between incident priorities and their classification*. The case studies in this stage have shown a significant relationship in addressing false and true incidents. There is a relationship between false incidents and their priority. Furthermore, the results in this stage were predicted to be similar because the proposed framework adopts the similarity and frequency indicators, and these indicators use a similar formulation with the correlation study in calculating the similarity between incidents and the frequency of them.

(c) *Balance between qualitative and quantitative results*. We must be aware of the limitations of the results representation discussed in Chapter 3, where the quantitative values used to represent the incident risk indexes are difficult to understand. Thus, RSM provides a seamless way to express the different qualitative level for the incident priorities. Although the numerical values offer advantages in the ranking process, the qualitative representation is important too. In order to give a similar interpretation of incidents, RSM gives a balance by grouping them into four quadrants qualitatively based upon their risk indexes.

(d) *Effect of the different weights in the decision factors*. Similar to the evaluation study in the first stage, the use of different weights in the decision factors also produces different results.

In conclusion, with the highlighted findings above, it can be seen that the proposed framework is suitable for use in facilitating the autonomous mode in the response selection process.

Although this stage has contributed a significant result in distributing incidents, there is a limitation. The main limitation in the case study is the use of a fixed threshold to map incidents. This threshold is not a definitive value and is subject to other reassessments, thus different scales will produce a different distribution. The discussion about the threshold limitation has been discussed in *Section*

4.2.4. To recall, there is no specific guideline to determine the best threshold between critical or non-critical incidents. However, the distribution of incidents in the case studies has shown acceptable results and the comparison results with CVSS v2 and Snort Priority strengthen the scale used in the thresholds.

Furthermore, the threshold limitation is also highlighted in Mu and Li (2010) and Stakhanova *et al.* (2007a). For instance, the adaptive response strategy used by Stakhanova *et al.* (2007a) defined a "*probability threshold*" that indicates an acceptable level of confidence in triggering appropriate responses to counter incidents in progress. Similar to this study, the threshold in Mu and Li (2010) and Stakhanova *et al.* (2007a) is defined manually. Stakhanova *et al.* (2007a) adopted the "*probability threshold*" to set a tolerance in selecting possible responses; the increment of the probability threshold decreased the error of selection.

5.5 The Performance Evaluation

The previous stages evaluated the feasibility of the proposed framework and investigated its models in order to validate them. In addition, the previous stages investigated the effect of using different strategies in the ranking and rating process as well as the distribution of the incidents and their classification with the RSM. The progressive results from one stage to another in the previous studies have shown the feasibility of the framework and strengthened its suitability.

The evaluation stage is continued with the fourth stage and this stage aims to investigate the performance of the framework. One of the criteria to enable the autonomous mode is to consider a fast processing time in order to support real time response. This is also important to the proposed framework, as a good processing time increases the reliability of the model in prioritising incidents. In order to facilitate the autonomous mode, this stage *aims to measure the processing time in the rating and ranking process using real time simulation*.

By measuring the rating and raking process, this study is able to investigate the feasibility of the proposed framework to run in a live traffic network and perform an online assessment. Therefore, it is important to measure how long it takes to rate and rank the incidents. To satisfy the autonomous mode in the response selection process, the rating and ranking process should be able to rate and rank incidents within a reasonable and considerable processing time. With this performance study, it helps security analysts to configure the proposed framework to perform better in assessing a live traffic network, besides supporting an online assessment.

5.5.1 Experiment and Procedure Description

In order to investigate the performance, this stage simulates 12 simulations. Using a personal computer, the simulation was simulated on Intel® Core™ 2 Duo Processor E6320 (4M Cache, 1.86 GHz, 1066 MHz FSB) and 2GB memory. All the running programs, such as the MySQL database, Snort and other applications, run in a similar peripheral.

To maintain the consistency of the results, the simulations were conducted using the DARPA dataset but with some additional configuration. The following descriptions are the additional configurations made from the simulation.

(a) There are two main experiments, one with the DDoS attacks and one without the attack. The main reason for having two types of experiment is to investigate the performance of the framework in relation to the effect of the number of incidents, as the DDoS attack in the dataset produces a burst of incidents per second, in fact more than 500 incidents per second. Since the DARPA dataset contains the DDoS attacks in the last phase of the dataset, it is suitable for showing the different results. The simulation with the DARPA dataset with the DDoS attacks contains 1,074 incidents per cycle and the other one has only 502 incidents per cycle. *Table 33* tabulates the configuration of the simulation set where SET A-F refer to set without the DDoS attacks and SET G-L with the DDoS attacks.

(b) In order to simulate more incidents, the DARPA dataset is repeated several times. For example, in order to simulate 1,506 incidents, the dataset with 502 incidents is simulated 3 times. *Table 33* tabulates the configuration of the simulation.

(c) In order to show the different effect, each set of the simulations contains a different time configuration, as it can be controlled using a simulation tool, namely Tcpreplay. A higher speed of the tool decreases the simulation time and increases the number of incidents per minute. The main reason for having a different time configuration on the simulation is to investigate the performance of the model and to analyse the result relationship between the number of incidents and time. For example, between SET A and SET C, although the total of incidents are similar, they were simulated in two different timeframes, SET A with 2052 seconds while SET C was with 1022 seconds.

(d) In order to maintain the consistency with the previous stage, the simulation also contains five scenarios of configurations similar to the third stage, thus each incident will have 5 different risk indexes based on the different set of scenarios in the configuration.

Table 33. The configuration of the performance simulation

	Set	Speed	No. of incidents	Simulation Time (s)
Without DDoS	A	100	1506	2052
	B	100	3012	4132
	C	1000	1506	1022
	D	1000	3012	2131
	E	10000	1506	644
	F	10000	3012	1465
With DDoS	G	100	1074	689
	H	100	2148	1368
	I	1000	1074	379
	J	1000	2148	797
	K	10000	1074	219
	L	1000	2148	447

The other configurations which are not mentioned in the descriptions are adapted from the previous stages.

5.5.2 Results

Table 34 shows the results of the simulations. There were 12 different simulations, each of them configured according to the experimental descriptions and procedures. *Table 34* shows a summary of the experiment tabulated into two main tables, which are also similar to the configuration table. The first column on the left of the table refers to the type of dataset and whether it contains the DDoS attacks, followed by the label of the name of the set, speed of the simulation tool (i.e. packet replay tool), number of incidents, incidents per minute, the duration of the simulation and average time to rate incidents (i.e. processing time).

Table 34. The average processing time for the rating process

	Set	Speed	No. of incidents	Incidents/minute	Simulation Time (s)	Average (s)
Without DDoS	A	100	1506	44	2052	18.26
	B		3012	44	4132	72.66
	C	1000	1506	88	1022	33.48
	D		3012	85	2131	141.04
	E	10000	1506	140	644	42.30
	F		3012	123	1465	242.46
With DDoS	G	100	1074	94	689	61.95
	H		2148	94	1368	136.34
	I	1000	1074	170	379	71.44
	J		2148	162	797	209.91
	K	10000	1074	294	219	70.59
	L		2148	288	447	281.34
						115.15

In order to measure the performance of the proposed framework in the rating process, the average processing time was calculated. On average, the processing time to calculate the incident risk index was 115.15 seconds or less than 2 minutes per incident. However, the average processing time is not significant because there is a huge difference between the lowest and the highest processing time. The lowest average is 18.26 seconds and the highest is 281.34 seconds. Furthermore, the average processing time is influenced by the number of incidents. In order to investigate the effect of having a different number of incidents in the simulation, the next section discusses the performance results based upon the speed of simulation and type of dataset.

In general, the speed of simulation has a significant effect upon the performance of the rating and ranking process. As can be seen in *Table 34*, the effect was very noticeable, where the higher the speed of the Tcpreplay tool, the higher the average of the processing time. In particular, the higher speed increased the number of incidents per minute. For example, SET A and SET C have a similar number of incidents, but the duration of the simulation was different. The duration for SET C is twice that of SET A, 2052 seconds as compared to 1022 seconds for SET C. SET C has 88 incidents per minute in comparison with 44 incidents for SET A. As a consequence, as can be seen in *Table 34*, the average processing time for SET C was increased 83.35% in comparison to SET A. This trend is consistent with other simulations and is a clear indicator of where the processing time is influenced by the number of incidents. The higher the number of incidents detected per minute, the higher the average time taken to rate incidents.

A similar trend can also be seen when the simulation simulated a burst of incidents with the DDoS attack in the second dataset. For example, in comparing SET E and SET K, both of which simulations run using a similar speed, they were different in terms of the average time. The average processing time to rate incidents in SET K is 70.59 seconds, in comparison with only 42.30 seconds for SET E. This scenario shows that a burst of incidents has also affected the processing time.

Furthermore, there are other factors to consider. Although the number of incidents detected per minute is similar, it can be seen in *Table 34* that the average processing time for the scenarios was different. A higher number of the total of incidents in a simulation increases the processing time. For example, this trend can be seen in comparison between SET A and SET B as well as SET G and SET I. The average time is higher because there was an overhead to calculate the similarity indicators, as can be seen in SET B and SET I. The similarity indicator calculates the similarity of incidents, and in order to satisfy the calculation, it needs to consider the previous incidents. The overhead upon the similarity indicators is increased due to a bigger number of the total of incidents. In particular, the processing time for SET B is increased as double SET A. The similar trend can also be seen in SET G and SET I.

In order to show the similar trend, *Figure 20* combines all the simulations in one graph. Without the simulation time, it shows a processing time graph for each incident. The graph plots the duration taken to rate incidents and is taken from the difference between the detection time and when the processing time ends.

In the first 500 incidents, most of the incidents were rated with less than a second. This result is interesting because the incidents can be rated and ranked immediately after they are detected. However, the case was different after that; the performance of the rating process was decreased. As can be seen in *Figure 20*, it appears that most of the graphs were increased when they reached a higher number of incidents. This trend is consistent with the results presented earlier, where the processing time increases in parallel with the nnuber of incidents.

In order to show the difference between the graphs, the comparison is made between two groups of simulation, one with the DDoS attacks and other one without attacks. For the simulation with the

DDoS attacks, the first group is differentiated between SET H, SET J and SET L. On the other hand, the second group compares SET B, SET D and SET F.

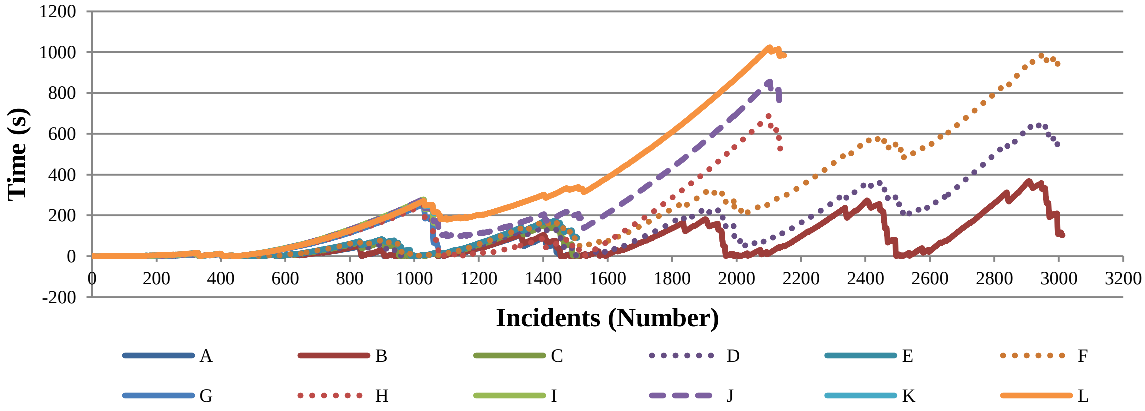


Figure 20. Incidents vs. Time (s)

All the simulations in the first group contain the DDoS attacks and therefore simulated more incidents per minute. The trend of the results can be seen clearly in the graph when the average time for SET L was higher compared to SET J and SET H. The highest peak for the processing time is 1000 seconds in SET L, in comparison to 800 seconds in SET J and 600 seconds in SET H. A similar trend can also be seen with the second group, in SET B, SET D and SET F. The trend of the results is similar to the previous scenario, but they give a better result in terms of their processing time.

In conclusion, the performance of the rating process is influenced by the two factors: the number of incidents detected per minute and the total number of previous incidents. The first factor cannot be controlled since the number of incidents detected per minute is unpredictable, but the second one is slightly different where it can be reduced by limiting the number in the indicator calculation. The *similarity* and *frequency* indicators consider all the previous incidents in their calculation. The second factor has been considered in the proposed framework and the investigation into it has been evaluated in the second stage.

In order to extend the discussion on the effect of the rating process, the following results show the measurement taken of the ranking process. *Table 35* tabulates the results of the simulations. Similar to the rating process, there were 12 different simulations and these were tabulated into two main tables, each of them configured similarly to the previous descriptions. The first column on the left of the table refers to the type of dataset and whether it contains the DDoS attacks, followed by the label of the name of set, the speed of the tool, the number of incidents, the incidents per minute, the duration of the simulation and the average number of ranked incidents per minute.

Table 35. The measurement of the ranking process

	Set	Speed	No. of incidents	Incidents/minute	Simulation Time (s)	Average
Without DDoS	A	100	1506	44	2052	13
	B		3012	44	4132	51
	C	1000	1506	88	1022	49
	D		3012	85	2131	145
	E	10000	1506	140	644	76
	F		3012	123	1465	275
With DDoS	G	100	1074	94	689	82
	H		2148	94	1368	154
	I	1000	1074	170	379	151
	J		2148	162	797	288
	K	10000	1074	294	219	114
	L		2148	288	447	404
						150

Similar to the performance factor in the rating process, the ranking process also has the same effect. An overhead caused by the number of incidents detected and also the previous incidents in the rating process influences the performance of the ranking process. As can be seen in *Table 35*, the effect of having a different number of incidents in the simulation is clearly shown. Furthermore, the result tabulated is also identical with the performance results in the previous analysis in the rating process.

In order to investigate the performance result in the ranking process, *Figure 21* shows two different sets of graphs, SET C and SET E. The graphs were plotted using two values, the blue bar is the number of incidents detected within a minute and the red line is the number of incidents with priority and rank. SET C was simulated for 1022 seconds and with an average of 88 incidents per minute and it ranked an average 49 incidents per minute. The first graph in *Figure 21* shows the ranking performance for SET C. It shows the total number of detected incidents per minute and the total number with priority. The first 6 bars show a better performance compared to the other bars, as all the first 500 incidents in that particular moment were ranked in real time as when they were detected. Immediately after that, the situation was changed where the performance of the ranking process was decreased and caused a bit of a delay. A similar trend can be seen in the second graph in the figure.

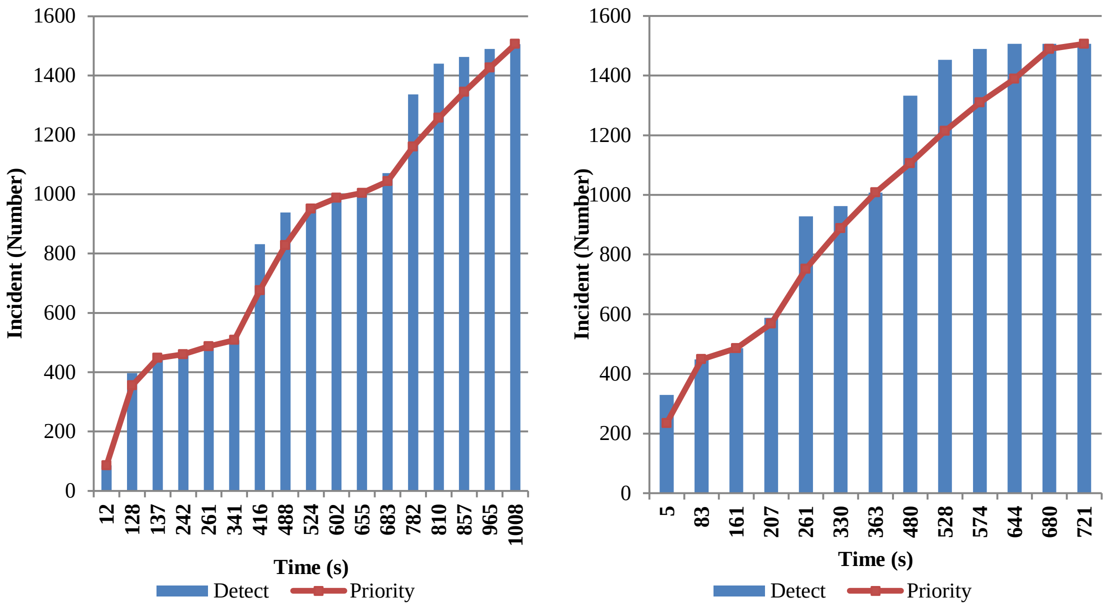


Figure 21. SET C and SET E

Although the graphs show a bit of a delay in the incidents with priority, the delay is not significant because on average each of incidents will be ranked less than a minute.

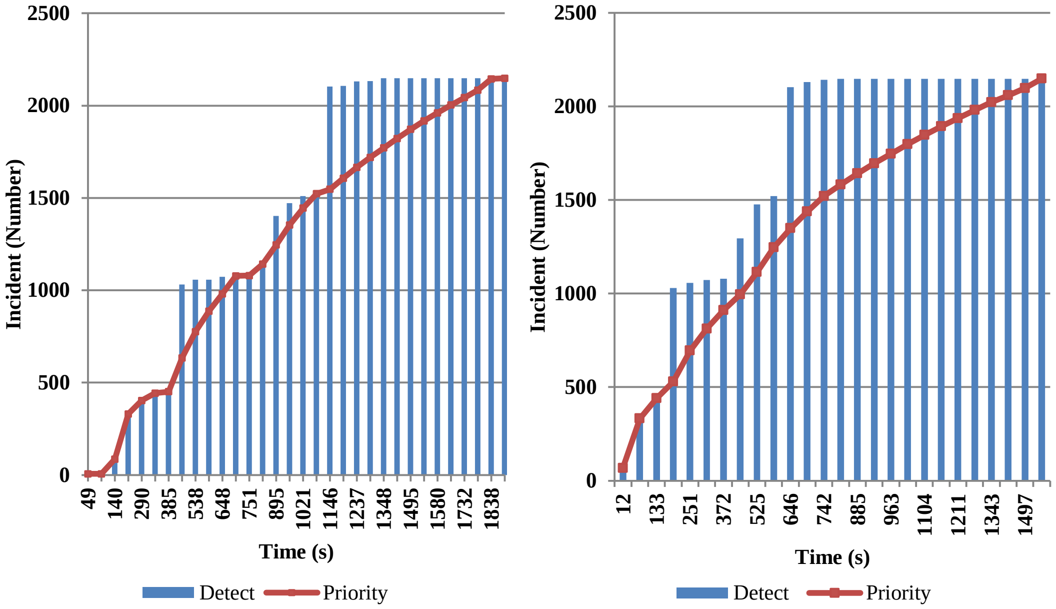


Figure 22. SET H and SET J

A similar trend can also be seen in *Figure 22,* where the first 500 incidents were ranked immediately they were detected. This is similar to the performance results in the rating process, where all the first 500 incidents were rated in real time. The performance was decreased after that, due to the performance of the processing time in the rating process. A burst of incidents in this scenario can clearly be seen when there is a huge difference in the graph after the first 500 incidents.

5.5.3 Discussion

The results presented in the previous section are encouraging as the performance of the rating and ranking process can be achieved in less than a second. It appears from this evidence that the higher number of incidents affects the performance of the processing time in the rating and ranking process.

In particular, the performance is influenced by two main factors, firstly by the total number of incidents detected per second where a burst of incidents increases the processing time and secondly, the total number of previous incidents involved in the similarity indicator calculation. A higher number of both factors cause an extra overhead and slowing down of the processing time in the rating and ranking process. As an implication from this, the framework should consider the limitation as one of the factors in order to facilitate the autonomous mode in the response selection process.

The first factor is hard to control; it depends upon the effectiveness of an IDS sensor and other security appliances, such as firewalls and access controls.

Table 36. Average Time (s)

	Set	Speed	No. of incidents	Incidents/minute	Simulation Time (s)	Average (s)
Without DDoS	Without Limitation	10	3012	18	10283	38.20
	With 1 hour Limitaion	10	3012	18	10122	15.12

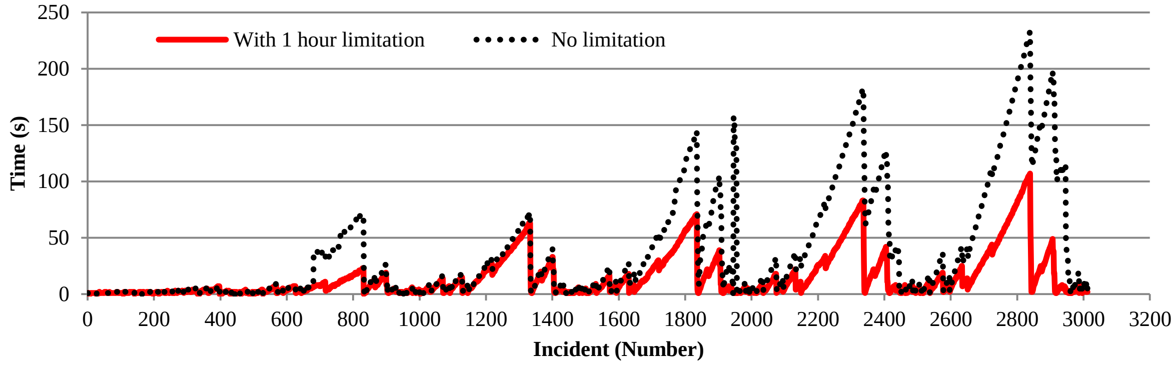


Figure 23. The performance comparison

The second factor, however, has been considered in the design of the framework. *Table 36* and *Figure 23* show the improvement made to the processing time in the rating and ranking process. The graph shows two simulations, one with the implementation of the rating and ranking strategy in the incident prioritisation process. For instance, unlike the previous simulations, the total number of the previous incidents to be considered in the similarity and frequency indicator was limited to one hour. As a consequence, the total number of incidents was decreased and this helped to improve the processing time. The consideration also helps to improve the overall performance. This can be seen clearly in *Table 36*, the average for the processing time was improved 152% with the implementation of the rating strategy, although they were simulated using a similar speed of tools, number of incidents per minute and total number of incidents. It appears that the result is significant and it is also improved the processing time of the ranking process.

Furthermore, in order to compare the performance results with other studies, they are compared with those of Cohen (1999) and Alsubhi *et al.* (2011). To illustrate the importance of timely response, Cohen (1999) highlights that the longer the delay between detection and response, the higher the attack success rate is. In a recent publication, Alsubhi *et al.* (2011) investigated a complexity analysis in the FuzMet system and as a result they found a light overhead in the prioritisation process.

In Cohen (1999), the success of attacks is influenced by the delay between the time of detection and its response. For example, if skilled attackers are given 10 hours after they are detected before a response, the success rate is 80%. If an extra 10 hours are given to them, the success rate is increased to 95% and beyond 30 hours, the attacker never fails. In comparison with the results of this study, the worst processing time taken to rate and rank incidents is less than an hour, which is considered a reasonable result in comparison to Cohen’s study. In this particular case, the performance in the processing time is considered appropriate and reasonable because no incident is rated and ranked more than 30 hours. A reasonable time to rate and rank incidents is important in order to limit the probability of the attacker being successful and reduce their opportunity to attack the system entirely. This result strongly suggests that the framework has shown an appropriate performance in terms of its processing time. With less than an hour, the result is considered a significant result in showing the ability of the proposed framework in facilitating the response selection process, in order to provide an effective active response to respond to incidents.

Alsubhi *et al.* (2011) presented an alert processing time in calculating the alert relationship metric in the FuzMet system. In order to compare the processing time, since they performed the investigation using a small number of alerts, this study considers the performance of the rating process for the first 500 incidents. With 300 incidents, the maximum peak for the processing time in their study is 160ms and they considered this a small overhead, although it might increase an overhead to the system. In order to limit the overhead, they have considered a similar consideration like this study by limiting the number of incidents in the process. In comparison, the performance results tabulated in the figures above are similar for the first 500 incidents. The performance in the proposed framework is working very well by rating and ranking all the first 500 incidents in less than a second and in real time. In conclusion, the performance result presented in this study and time taken to prioritise incidents is considered reasonable. This also satisfies the requirement of an online assessment.

The comparison study shows that the framework has performed in a reasonable situation and, based upon the performance results, it is appropriate for use in facilitating the autonomous mode in the response selection process. However, this is not a full evaluation of the performance and the computational effort required, but it provides a level of comparison with prior studies.

5.5.4 Conclusion

The fourth stage of the evaluation study investigated the performance of the proposed framework. The measurement of the performance investigated two parts of the processing time, in the rating and ranking process. In conclusion, the investigation was done by looking at two main aspects as follows:

(a) *The performance of the rating and ranking process*. The performance of the proposed framework was measured using the processing time in the rating and ranking process. It appears that the performance results are significant with a reasonable processing time in the rating and ranking process. Furthermore, the processing time is influenced by two factors, mainly upon the number of incidents in the process. The higher the number that need to be processed, the slower the processing time. The two factors identified in the investigation are the total number of incidents detected per second and the total number of previous incidents involved in the calculation of the similarity indicator. In particular, a burst of incidents increases the processing time and having too many incidents to calculate the similarity indicators also induces the process.

(b) *In comparison with other performance studies*. In comparison with the performance results of Cohen (1999) and Alsubhi *et al.* (2011), the performance of the proposed framework has shown a reasonable result in the rating and ranking process. In terms of the processing time, the rating process simulated on average 115.15 seconds and also satisfied the proposal made by Cohen (1999). In addition, the performance for the first 500 incidents is similar to the result presented in Alsubhi *et al.* (2011).

In addition, the greatest advantage of the investigation in this study is to analyse the overall performance, with different configurations in the rating and ranking process, in order to evaluate the practicality of the proposed framework. Furthermore, with the main aspects above, the experiment also clearly demonstrated that the performance of the rating and ranking process is reasonable and can be seen as a significant result since it can be achieved in a short time, which benefits the response selection process.

In conducting the experiment, this study has found some limitations and below is some of these along with suggestions on how to reduce them.

(a) *Computing Power*. Although the results presented in this study were considered a reasonable result, they were also influenced by the computing power, where the experiment was conducted using a personal computer and run other non-related applications as well during the simulation. This limitation affected the measurement of the results and, as a consequence, it decreased the processing time. Therefore, in order to reduce the limitation and increase the real time processing, it is suggested to consider other factors such as hardware, algorithms, codes optimisation, processor utilisation and also communication between systems (Stankovic, 1988).

(b) *Responses*. The performance results highlighted a reasonable processing time in terms of the rating and ranking process. However, the processing time presented in this evaluation study does not consider the real response time because the simulation does not include any security appliances, such as firewalls and access control to respond to the incidents. An important question for future studies is to determine the best response time by including the practicality of those security appliances, in order to respond to the incidents.

5.6 Summary

This chapter has discussed the evaluation study of the models, strategies and indicators used in the proposed framework. The progressive results from the first stage to the last stage have demonstrated a combination of different aspects of evaluation, and they highlighted their unique findings and conclusions.

The key objective of describing the evaluation at different stages of studies is to investigate the unique objectives at each stage. The result presented has shown strong evidence to support the ability of the proposed framework to work robustly based upon its operational characteristics. Furthermore, the comparison study in the evaluation studies also strengthens the framework and its suitability to facilitate the autonomous mode in the response selection process in IRSs. In conclusion, the analysis made of the studies clearly defined their contribution as well as stating their limitations.

To further investigate the usefulness and feasibility of the proposed framework in a practical mode, a live traffic network and online assessment, the following chapter presents the prototype of the proposed framework, and evaluates it using a similar dataset to the one used in this chapter.

6 A Prototype implementation of Security Incident Prioritisation Modules

After validating and evaluating the proposed framework, the next stage of the research is to design and implement a prototype system that can demonstrate its key operations and show how these can be implemented in practice. This chapter describes the prototype implementation of the proposed framework, and specifically the administration and prioritisation modules. The main features of the administration module have been embodied in a web interface, which can be used to monitor, configure, and analyse the prioritisation modules. Several modelling languages, including use case diagrams and state diagrams, are used to provide a visual illustration of the prototype. Finally, the incident scenarios that are used in this chapter are based on the DARPA dataset.

6.1 Implementation Overview

There are three main parts in the proposed framework as illustrated in *Figure 24.* The two main parts, the prioritisation and administration modules, have been fully implemented, whereas the external systems have been adopted from other sources. The rationale behind adopting existing IDS sensors and response agents, rather than implementing them from scratch is twofold; firstly implementing these modules would have been out of the scope of the proposed research, and secondly supporting input from existing IDS sensors serves to provide a more realistic environment and strengthen compatibility with existing solutions. Snort, a popular, well documented, and open source IDS tool, was chosen as the IDS sensor in the prototype (Caswell and Roesch, 1998). As for the modules that were fully implemented, their descriptions are as follows:

(a) **Prioritisation Systems.** The three main modules of the prototype are: *Rating Strategy*, *Ranking Strategy* and *Response Strategy*. More details on the functionality of these modules can be found in *Section 4.3*. The modules run independently as application daemons and they are used to prioritise incidents. Similar with the experiment in the previous chapter, their development is based on PHP, a server-side HTML-embedded scripting language. All these modules connect to the same MySQL database, in order to retrieve and upload incident prioritisation and response data. MySQL was chosen to allow compatibility with Snort, which also supports logging to MySQL.

(b) **Administration**. The *Security Incident Prioritisation Modules* provide a graphical user interface to help summarise, visualise prioritisation results, configure, analyse, and monitor the *prioritisation systems*. The design of the modules is inspired by the Snorby[4] (2011) web application and has been developed using the latest web development technologies PHP5 version 5.3.3, HTML5 and CSS3. The combination of these technologies allows the modules to have interactive and friendly interfaces. These modules also share the same database with Snort and the prioritisation systems.

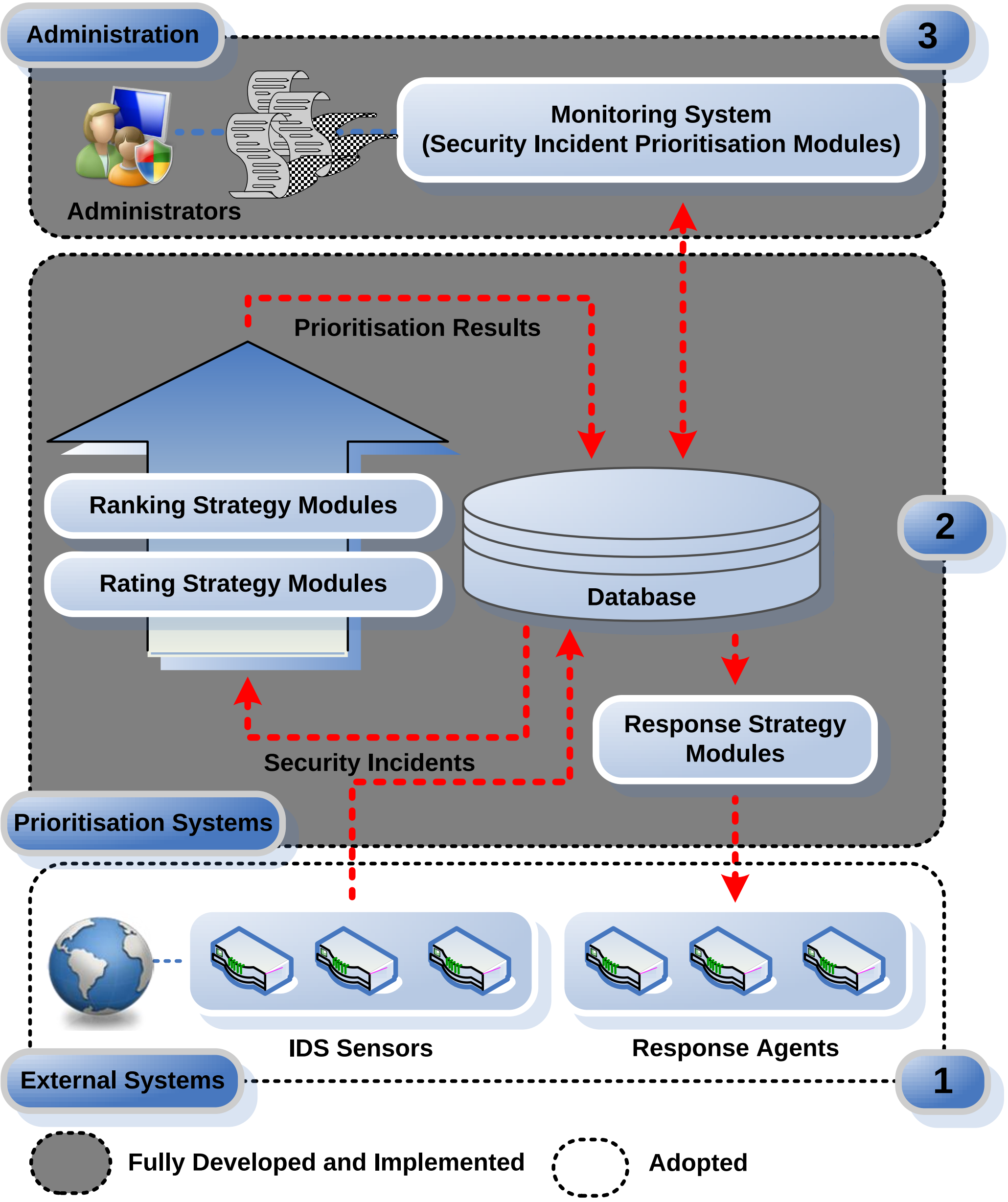


Figure 24. Modules Implementation

[4] Snorby is an open source web application which provides monitoring interfaces for intrusion detection systems. Some of the graphical interfaces in the prototype were designed based on ideas taken from the Snorby interfaces.

6.2 Prototype Functionalities

To gain insight into the main functionality of the proposed framework, modelling languages, such as *use case diagrams* and *state diagrams,* are presented.

6.2.1 Use case diagram

Use case modelling has been widely utilised to graphically portray a functional description of interaction between external entities and systems, as well as their collaborations. They are applied to capture the behaviours of the developed systems, without having to specify how those behaviours are implemented (Booch *et al.*, 2005). *Figure 25* shows the system level, and describes the interaction between external systems and the system itself.

The role of administrator, as presented in *Figure 25,* is given below:

(a) Administrators have the ability to run specific applications as daemons after they have properly configured the configuration files. The configuration files can be found in the second part of the proposed framework, *Prioritisation Systems* (see *Section 4.3*). The applications run until they are stopped manually by administrators.

(b) Administrators have the ability to manage the web modules, which represent the third part of the proposed framework, *Security Incident Prioritisation Modules (SIPM)*[5]. This includes the ability to visualise incidents, analyse them and configure the web modules.

(c) Apart from running applications in a daemon mode, administrators are also given privileges to stop and re-run them again manually.

(d) Administrators also have an ability to reset databases and it allows them to restart the applications and web modules in different environments.

[5] For the remainder of this chapter, the terms "*Security Incident Prioritisation Modules*" and "web modules" will be interchangeable.

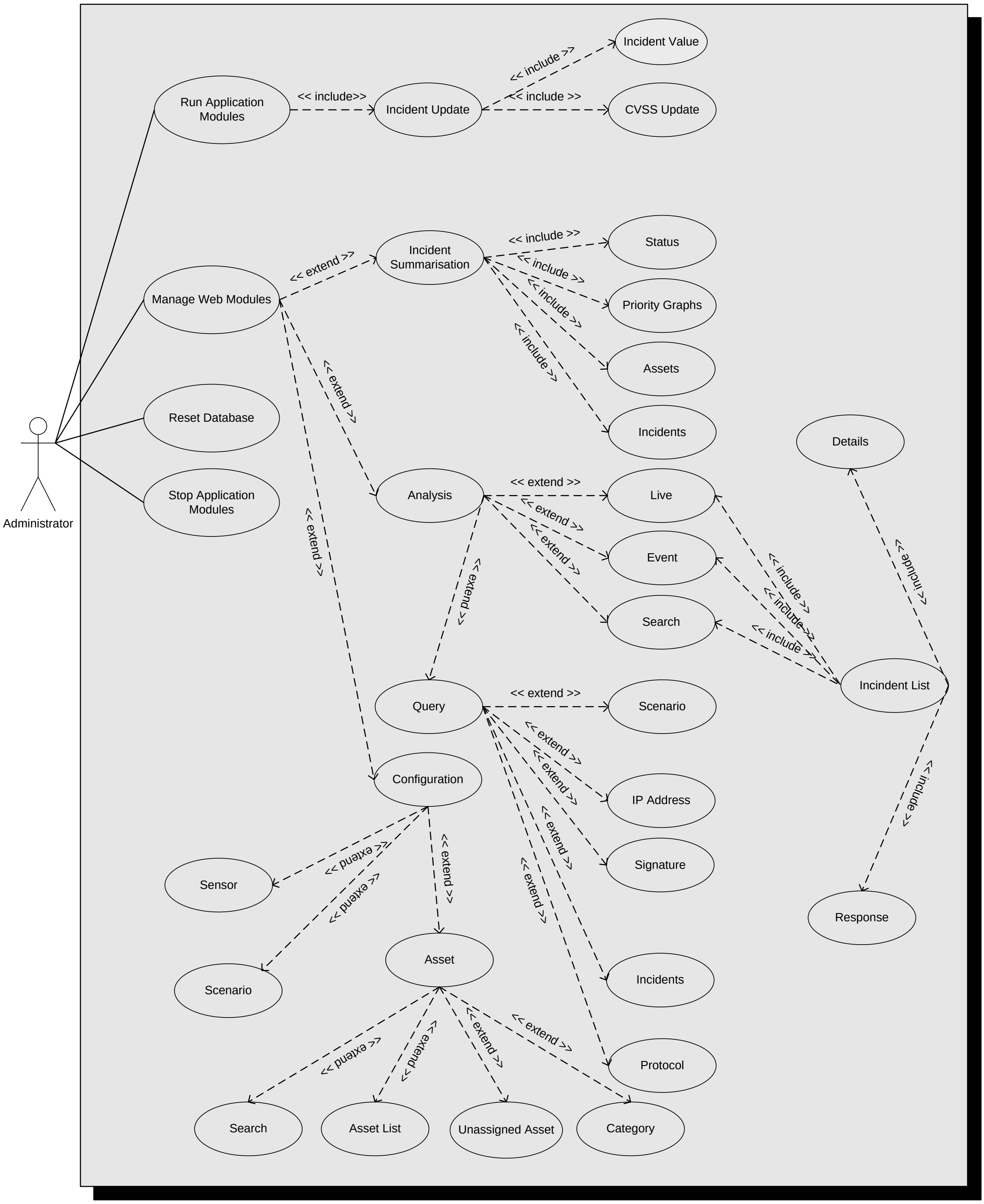


Figure 25. SIPM Use case diagram

Although the use case diagram has provided a brief overview of the modules' functionality, it does not clarify how those modules are performed. For this purpose, state diagrams are presented in the next sub-section.

6.2.2 State diagrams

A state diagram describes all the possible states of an object as events occur, and is used to demonstrate the behaviour of an object through many use cases of a system, as well as to emphasise the flow of control from one state to another (Booch *et al.*, 2005).

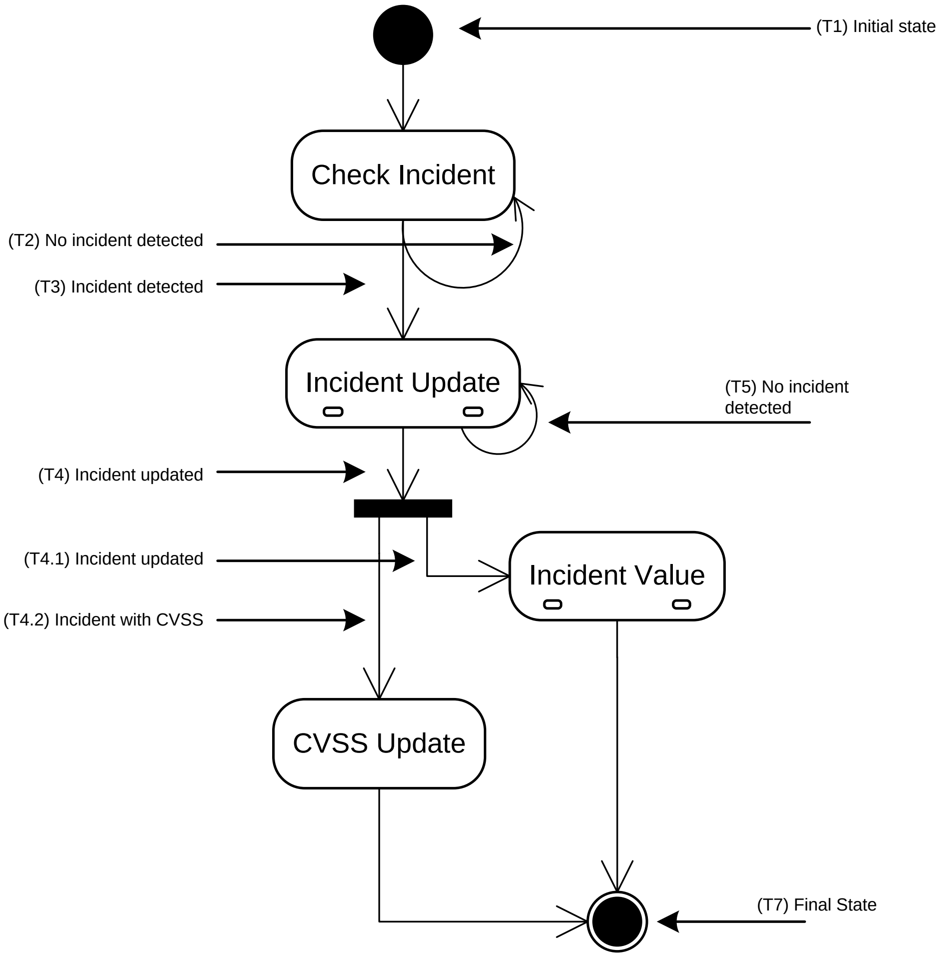


Figure 26. Super State

Figure 26 shows all the possible states in the proposed framework and it summarises the behaviours of the running system. As a super-state, there are four main states and brief descriptions of them are given below:

(a) *Check Incident.* The initial state (T1) starts when administrators run the application daemons and it remains in the same state as long as no incidents are detected (T2). The transition of the state occurs only when there is a detected incident (T3); when triggered, it goes to the *Incident Update* state.

(b) *Incident Update*. This is a continuous state from *Check Incident*, where the state starts when there is an incident (T3), which an output comes from it; or otherwise it remains in the same state (T5). As illustrated in *Figure 27*, this state is built up from three main sub-states, which run in succession: *Update Incident Detail*, *Update Similarity* and *Update Frequency*. The outputs of this state will be used in the next states, *Incident Value* and *CVSS Update*, which run in parallel. The *Update Incident Detail* state updates the details of incident such as its source address, destination address, type of attack, time occurring and signature. The *Update Similarity* state calculates the similarity of each incident and updates it in the database. Similarly, the *Update Frequency* state updates the quantitative values which relate to signature similarity.

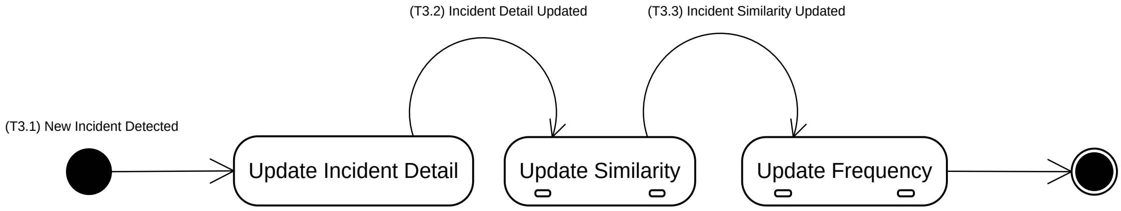

(T3.2) Incident Detail Updated
(T3.3) Incident Similarity Updated
(T3.1) New Incident Detected
Update Incident Detail
Update Similarity
Update Frequency

Figure 27. Incident Update State

(c) *Incident Value*. This particular state starts when there is an updated incident as a result of a previous state (i.e. the *Incident Update* state) (T4.1). There are four sub-states in this particular state, as illustrated in *Figure 28*: *Get Last Incident, Retrieve Incident Value, Update Incident Value* and *Update Scenario.* The transition from one state to another is dependent upon the output from the state before them; for instance, the transition from the *Get Last Incident* state to the *Retrieve Incident Value* state depends upon the output of the *Get Last Incident* state. To detail out the related processes, the *Get Last Incident* state (T4.1.1) retrieves the last incident in the stored database and uses it as a key to retrieve other new incidents, as it helps to minimise time to update every single incident. As a result from the previous state, it triggers the *Retrieve Incident Value* state (T4.1.2), and, in this particular state, the indicator values for incidents are calculated and the calculation is based upon the configuration made earlier, which is why it is also called the calculation phase. Once the calculation phase has been done (T4.1.3), the state moves to the *Update Incident Value* state and updates (or stores) the indicator values for each incident involved in the calculation phase. Continuously, the state is repeated (T4.1.4) until there are no other incidents to update (T4.1.5). Once the incident value is updated, it moves to a new state, the *Update Scenario* state, to update the new risk index values based upon the scenario setting and indicator values. In cases where there are more than one scenario, the state is repeated (T4.1.6) until all the scenario values are calculated and, as results to this state, the risk index values are updated.

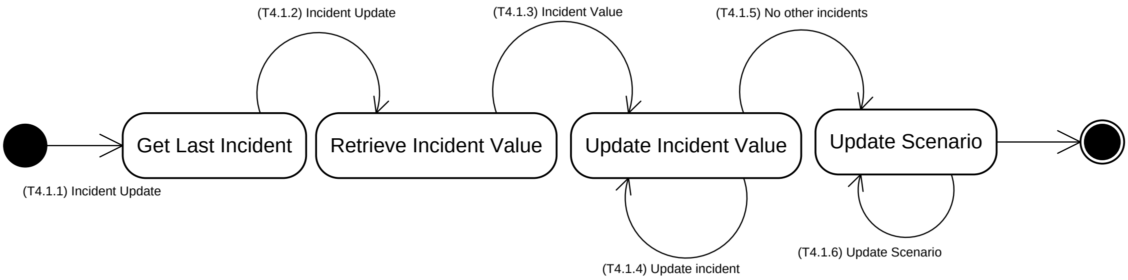


Figure 28. Incident Value State

(d) *CVSS update.* Similar to the *Incident Value* state, the transition to enter this stage is dependent upon the output from the previous state (T4.2); in cases where this is an incident with CVSS. This state runs simultaneously with the *Incident Value* state and it retrieves input for the CVSS v2 value from NVD (NIST, 2011) and stores it appropriately onto a specific table in a database.

On top of the super state, the *Manage Web Modules* state is an independent state and used for the administration modules. This state starts when there is an initial login from authorised administrators (T8.1) and it remains in the same state until they choose to logout from the web modules (T8.4). In this particular state, there is a sub-state where administrators are authorised to browse any web pages as they wish (T8.2) and return back to the main menu (T8.3) when they like. There are many web pages that can be selected at this particular stage, as described in the next sections.

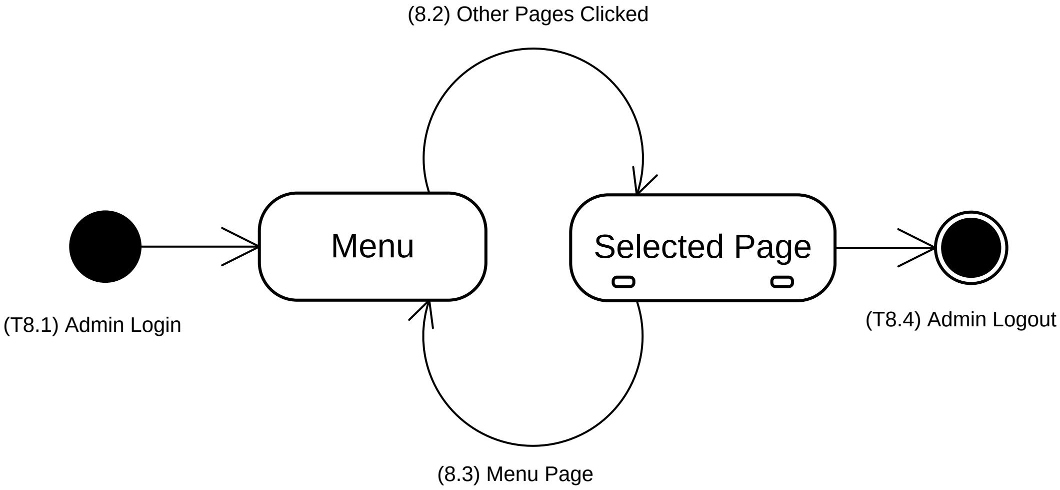


Figure 29. Manage Web Modules State

6.2.3 Web Modules

The web modules provide a graphical user-friendly interface that allows administrators to view and configure the modules. The web modules provide a web analytics solutions that give rich insights into the incident prioritisation process and analysis simpleness. Simplicity, easy-to-use, customisable, flexible and optimisation of results features allow administrators to analyse the entire prioritisation process. The web modules provide various types of custom results and give a broader view of the current situation related to incidents and IDSs. Their functionality can be summarised into three key functions:

(a) **Incident Summarisation**. This category provides the summarisation of the incident prioritisation results in the front page. As highlighted in the use case diagram in *Section 6.2.1*, examples of outputs that can be presented include:

   a. *Incident Status*. The current status provides a summative view of the incident risk index, by providing information such as the number of incidents in each risk index category.

   b. *Priority Graphs*. These show the distribution of risk indexes based upon their priority and the summarisation of results in graphs.

   c. *Assets*. The web modules show the available asset in the systems. It also highlights critical assets and summarise the most attacked assets.

   d. *Incidents*. As it is important information, the web modules show the current incidents and their priority. It also highlights top incidents based upon their type of signatures.

(b) **Analysis**. This category examines results from the prioritisation process. The analysis processes are performed as follows:

   a. *Event.* The event page allows the user to view details of live events, based on criteria such as priority level. The information provided for each event includes: detection time, sensor ID, incident priority, source IP address, destination IP address and generated IDS rule. This page also allows "*marking*" of specific incidents for further analysis on the *Live* page (please see item b below). In addition, the user can access response options in this page, by following links to pages: *show response, and insert response*. The *show response* page allows administrators to show all the actions that have been taken in response to the selected incident. The *insert response* page allows the administrator to issue responses using a simple form.

b. *Live*. This page presents the incidents that have been marked for further review in the *Event* page. It follows the same format as the *Event* page.

c. *Search.* This page allows queries based on criteria such as source address, destination address, signature name, signature class. It follows the same format as the *Event* page, but it is not refreshed.

d. *Query*. This page provides more in-depth queries based on scenarios, IP addresses, signatures, incidents and protocols. The query results are displayed in a table, which typically contains the incidents priority as well as associated graphs.

(c) **Configuration**. This interface enables the configuration of several parameters, such as the sensitivity of sensors, asset categories, indicator values and thresholds for different scenarios. An illustration of how these configuration parameters can be used is given in the next section.

This section has provided the prototype functionalities. Furthermore, to facilitate the usage and visualisation of the web modules, print screens for the prototype can be viewed in the next section.

6.3 Demonstrating the Security Incident Prioritisation Modules (SIPM) Prototype

Having presented the main features of the proposed framework and its web modules, this section demonstrates some examples of how incidents can be prioritised, ranked and grouped according to their priorities. It also presents the details of the prioritisation results using the relevant features to show the incident priorities with two different dimensions: a group of the incident priorities and a list of the incident risk indexes with a quantitative value. The prioritised incidents, which are stored in a database, are detected in a real-time simulation using the DARPA datasets and Tcpreplay (2011) with Snort IDS. The rationale for demonstrating only one dataset instead of two is that the prioritisation results using other scenarios will produce a similar visual upon the related pages.

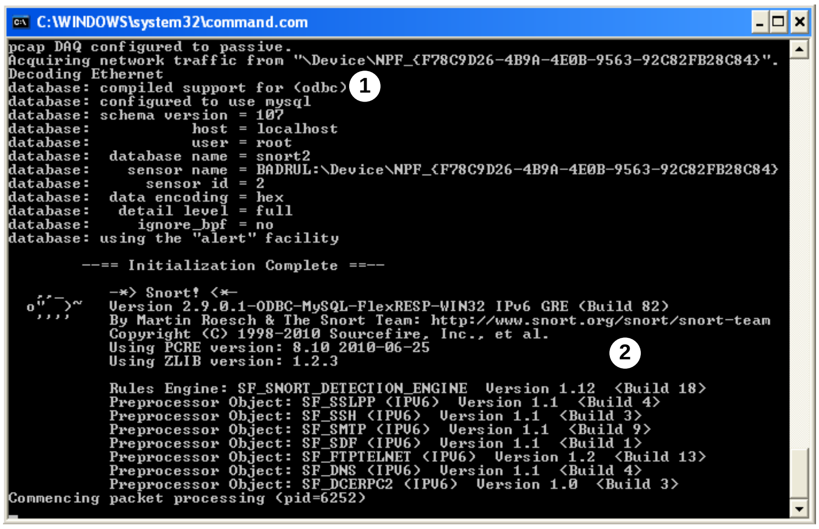
The prototype contains two separate modules: the application daemons (i.e. for the back end and run as a service) and web modules (i.e. for the front end). To demo the prototype, there are four sections and the details of their descriptions are as follows:

6.3.1 The Application Daemons

In order for the application daemons of the prototype to operate properly, Snort and Tcpreplay need to be running first:

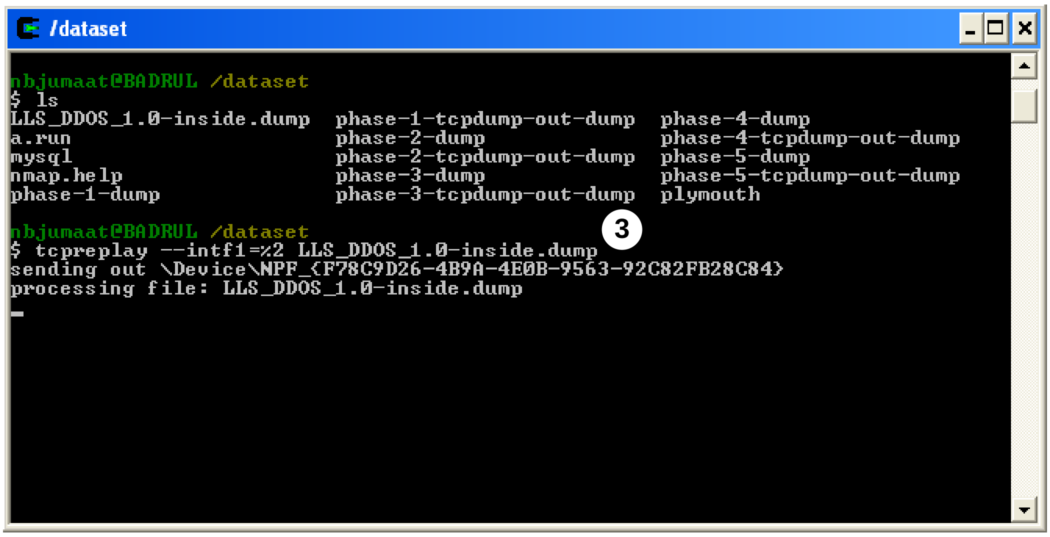
(a) *Snort and its database*. As illustrated in *Figure 30*, Snort IDS is executed to listen to a virtual network interface *"\Device\NPF_{F78C9D26-4B9A-4E0B-9563-92C82FB28C8*". Label 1 in *Figure 30* shows the details of its configuration and, as stated in the figure, the suspicious incidents detected will be stored in the *localhost* database, namely *Snort2*.

(b) *Tcpreplay* (2011). In order to inject packets in the network and simulate a realistic monitoring environment, the demonstration used the *Tcpreplay* application. As illustrated in Label 3 in *Figure 31*, *Tcpreplay* replays the simulation files (e.g. a pcap format file) and pumps them into a similar interface listened to by Snort IDS (i.e. *Figure 30*).



```
pcap DAQ configured to passive.
Acquiring network traffic from "\Device\NPF_{F78C9D26-4B9A-4E0B-9563-92C82FB28C84}".
Decoding Ethernet
database: compiled support for (odbc)
database: configured to use mysql
database: schema version = 107
database:           host = localhost
database:           user = root
database:  database name = snort2
database:    sensor name = BADRUL:\Device\NPF_{F78C9D26-4B9A-4E0B-9563-92C82FB28C84}
database:      sensor id = 2
database:  data encoding = hex
database:   detail level = full
database:     ignore_bpf = no
database: using the "alert" facility

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.0.1-ODBC-MySQL-FlexRESP-WIN32 IPv6 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-team
           Copyright (C) 1998-2010 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 1.12  <Build 18>
           Preprocessor Object: SF_SSLPP (IPV6)  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSH (IPV6)  Version 1.1  <Build 3>
           Preprocessor Object: SF_SMTP (IPV6)  Version 1.1  <Build 9>
           Preprocessor Object: SF_SDF (IPV6)  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET (IPV6)  Version 1.2  <Build 13>
           Preprocessor Object: SF_DNS (IPV6)  Version 1.1  <Build 4>
           Preprocessor Object: SF_DCERPC2 (IPV6)  Version 1.0  <Build 3>
Commencing packet processing (pid=6252)
```

Figure 30. Snort IDSs

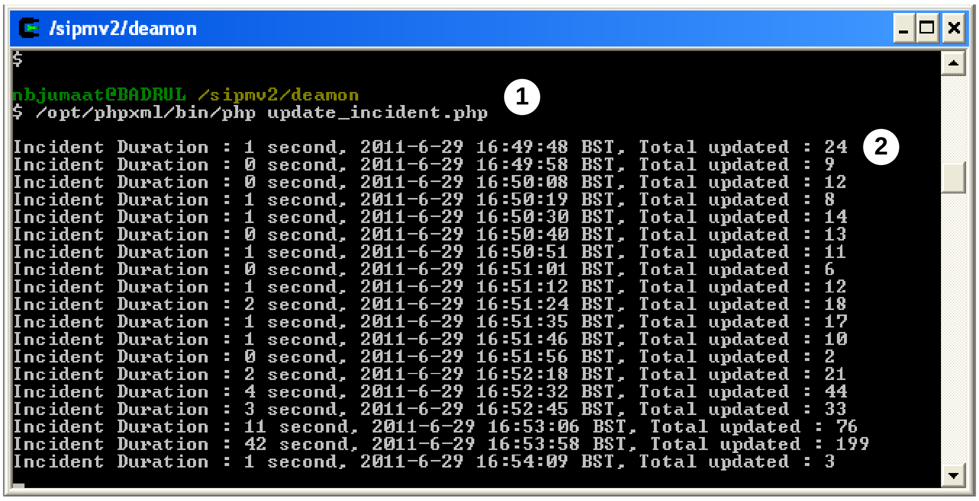


```
nbjumaat@BADRUL /dataset
$ ls
LLS_DDOS_1.0-inside.dump  phase-1-tcpdump-out-dump  phase-4-dump
a.run                     phase-2-dump              phase-4-tcpdump-out-dump
mysql                     phase-2-tcpdump-out-dump  phase-5-dump
nmap.help                 phase-3-dump              phase-5-tcpdump-out-dump
phase-1-dump              phase-3-tcpdump-out-dump  plymouth

nbjumaat@BADRUL /dataset
$ tcpreplay --intf1=%2 LLS_DDOS_1.0-inside.dump
sending out \Device\NPF_{F78C9D26-4B9A-4E0B-9563-92C82FB28C84}
processing file: LLS_DDOS_1.0-inside.dump
```

Figure 31. The use of TCPreplay

The results of the simulation are stored in a database based upon the Snort IDS configuration file which is manually set by administrators. To continue the demonstration process, the calculation of the incident risk indexes and other processes are done using two applications which are also independently executed in a daemon mode:

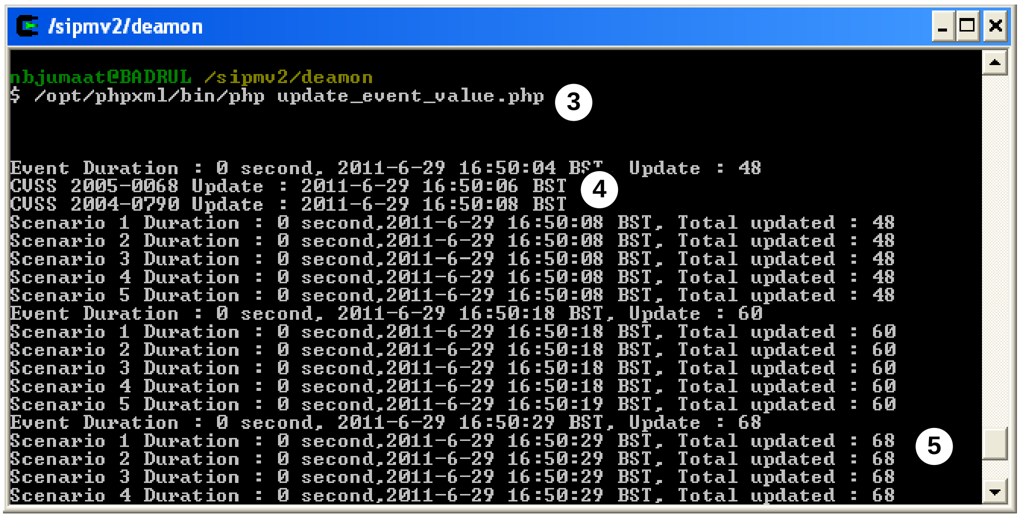
(a) *Incident Update*. *Figure 32* shows a running application as it waits for new incidents to be analysed. It is a process of checking that a new incident is running periodically and stops only when administrators end the application manually. Label 1 in the figure shows a command typed by administrators to execute the application and, in this particular example, a file named "*update_incident.php*" was used. As mentioned in *Section 6.2.2*, the application daemon calls three different functions – *Update Initial Detail*, *Update Similarity* and *Update Frequency* – and, Label 2 shows the related output. Within the output, there is some interesting information that can be used as a tracker for administrators to monitor the application daemon so that it runs seamlessly, such as incident duration, which shows the update process duration, timestamp and the total number of incidents.



```
$

nbjumaat@BADRUL /sipmv2/deamon
$ /opt/phpxml/bin/php update_incident.php

Incident Duration : 1 second, 2011-6-29 16:49:48 BST, Total updated : 24
Incident Duration : 0 second, 2011-6-29 16:49:58 BST, Total updated : 9
Incident Duration : 0 second, 2011-6-29 16:50:08 BST, Total updated : 12
Incident Duration : 1 second, 2011-6-29 16:50:19 BST, Total updated : 8
Incident Duration : 1 second, 2011-6-29 16:50:30 BST, Total updated : 14
Incident Duration : 0 second, 2011-6-29 16:50:40 BST, Total updated : 13
Incident Duration : 1 second, 2011-6-29 16:50:51 BST, Total updated : 11
Incident Duration : 0 second, 2011-6-29 16:51:01 BST, Total updated : 6
Incident Duration : 1 second, 2011-6-29 16:51:12 BST, Total updated : 12
Incident Duration : 2 second, 2011-6-29 16:51:24 BST, Total updated : 18
Incident Duration : 1 second, 2011-6-29 16:51:35 BST, Total updated : 17
Incident Duration : 1 second, 2011-6-29 16:51:46 BST, Total updated : 10
Incident Duration : 0 second, 2011-6-29 16:51:56 BST, Total updated : 2
Incident Duration : 2 second, 2011-6-29 16:52:18 BST, Total updated : 21
Incident Duration : 4 second, 2011-6-29 16:52:32 BST, Total updated : 44
Incident Duration : 3 second, 2011-6-29 16:52:45 BST, Total updated : 33
Incident Duration : 11 second, 2011-6-29 16:53:06 BST, Total updated : 76
Incident Duration : 42 second, 2011-6-29 16:53:58 BST, Total updated : 199
Incident Duration : 1 second, 2011-6-29 16:54:09 BST, Total updated : 3
```

Figure 32. The *Incident Update* application daemon

(b) *Incident Value*. This application daemon starts the updating process only when there is an output from the previous application. The application aims to satisfy two objectives: i) to update the incident risk indexes based upon settings in the configuration file (see Label 5 for the updating process tracker) and ii) to retrieve information and other related scores from CVSS v2 as marked with Label 4.



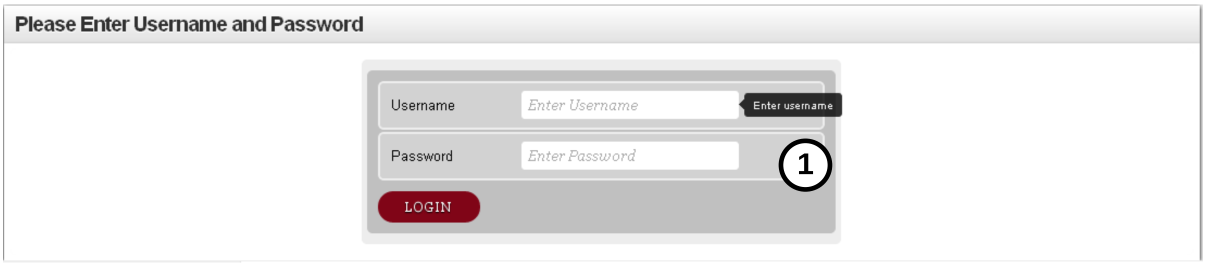
```
nbjumaat@BADRUL /sipmv2/deamon
$ /opt/phpxml/bin/php update_event_value.php


Event Duration : 0 second, 2011-6-29 16:50:04 BST, Update : 48
CVSS 2005-0068 Update : 2011-6-29 16:50:06 BST
CVSS 2004-0790 Update : 2011-6-29 16:50:08 BST
Scenario 1 Duration : 0 second,2011-6-29 16:50:08 BST, Total updated : 48
Scenario 2 Duration : 0 second,2011-6-29 16:50:08 BST, Total updated : 48
Scenario 3 Duration : 0 second,2011-6-29 16:50:08 BST, Total updated : 48
Scenario 4 Duration : 0 second,2011-6-29 16:50:08 BST, Total updated : 48
Scenario 5 Duration : 0 second,2011-6-29 16:50:08 BST, Total updated : 48
Event Duration : 0 second, 2011-6-29 16:50:18 BST, Update : 60
Scenario 1 Duration : 0 second,2011-6-29 16:50:18 BST, Total updated : 60
Scenario 2 Duration : 0 second,2011-6-29 16:50:18 BST, Total updated : 60
Scenario 3 Duration : 0 second,2011-6-29 16:50:18 BST, Total updated : 60
Scenario 4 Duration : 0 second,2011-6-29 16:50:18 BST, Total updated : 60
Scenario 5 Duration : 0 second,2011-6-29 16:50:19 BST, Total updated : 60
Event Duration : 0 second, 2011-6-29 16:50:29 BST, Update : 68
Scenario 1 Duration : 0 second,2011-6-29 16:50:29 BST, Total updated : 68
Scenario 2 Duration : 0 second,2011-6-29 16:50:29 BST, Total updated : 68
Scenario 3 Duration : 0 second,2011-6-29 16:50:29 BST, Total updated : 68
Scenario 4 Duration : 0 second,2011-6-29 16:50:29 BST, Total updated : 68
```

Figure 33. The *Incident Value* application daemon

Once the suspicious incidents are detected and stored in a database, they can be visualised using any web browser with the web modules and the next section visualises the related pages.

6.3.2 Incident Summarisation

To log into the web modules, administrators need to use a legitimate username and password; otherwise the web modules will not allow them to visualise the other analytics pages. Label 1 in *Figure 34* illustrates the login form that needs to be filled in by administrators before they can browse the web modules. The password in the database is stored using the MD5 Message-Digest algorithms.



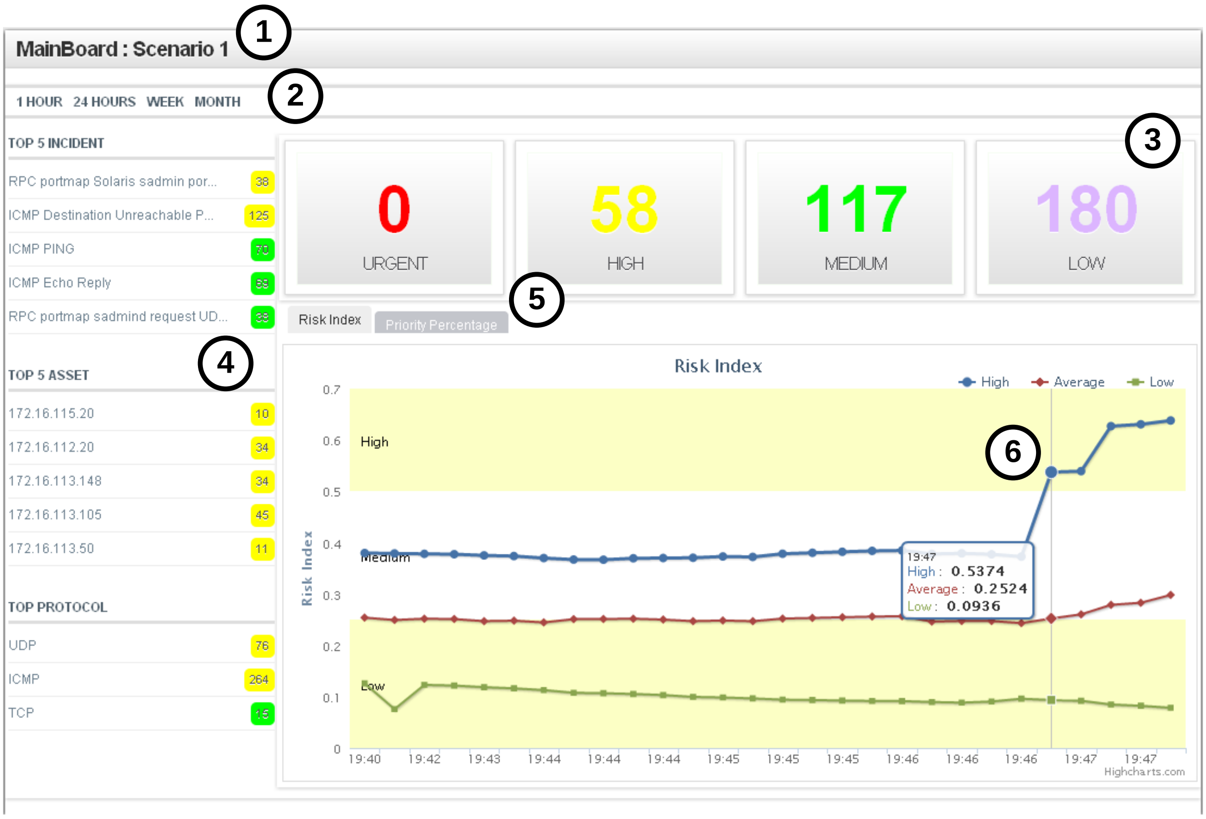
Please Enter Username and Password

Username: Enter Username

Password: Enter Password

Figure 34. Login page

Once the login process is successful, administrators are redirected to the first page of the web modules which is the main board of the modules. *Figure 35* illustrates the board.



MainBoard : Scenario 1

1 HOUR 24 HOURS WEEK MONTH

TOP 5 INCIDENT	
RPC portmap Solaris sadmin por...	38
ICMP Destination Unreachable P...	125
ICMP PING	70
ICMP Echo Reply	69
RPC portmap sadmind request UD...	38

TOP 5 ASSET	
172.16.115.20	10
172.16.112.20	34
172.16.113.148	34
172.16.113.105	45
172.16.113.50	11

TOP PROTOCOL	
UDP	76
ICMP	264
TCP	15

URGENT	HIGH	MEDIUM	LOW
0	58	117	180

19:47
High : 0.5374
Average : 0.2524
Low : 0.0936

Figure 35. Main Board

The main board provides very useful information such as a summarisation and snapshot of the current status of the prioritisation results. As mentioned in *Section 6.2.3*, it also displays information including the current scenario, distribution of incidents and graphs. Label 1 summarises the page and it shows the current scenario in the main board. The scenario is a set of settings for any configuration where each configuration is used to generate the incident risk index. Each scenario has a different configuration for specifics such as colours (e.g. red, green, yellow), priority wording (e.g. high, low, medium) and also the weight of indicators used to calculate the incident risk index. Depending on how many scenarios are created, the page can be changed easily by administrators. In this particular main board, the graph shown on the page was based on *Scenario 1*. To add a new scenario, the administrator can use the *configuration* page.

To show the distribution of incidents, Label 3 refers to four boxes with different colours and the boxes summarise the total number of incidents based on their priority. Each box contains an active link and it can be used to navigate the administrator to the *Event* page, in order to make a further analysis on specific incidents based upon their priority. The boxes are coloured using different colours to differentiate their priorities and this can be configured using the configuration page. In this example, the red colour with “0” represents an urgent priority incident with no incident under it, followed by other priorities. In order to increase the customisation of the page, the name and colour of the boxes are also customisable – for example, ‘urgent’ can be changed to ‘important’ and so on.

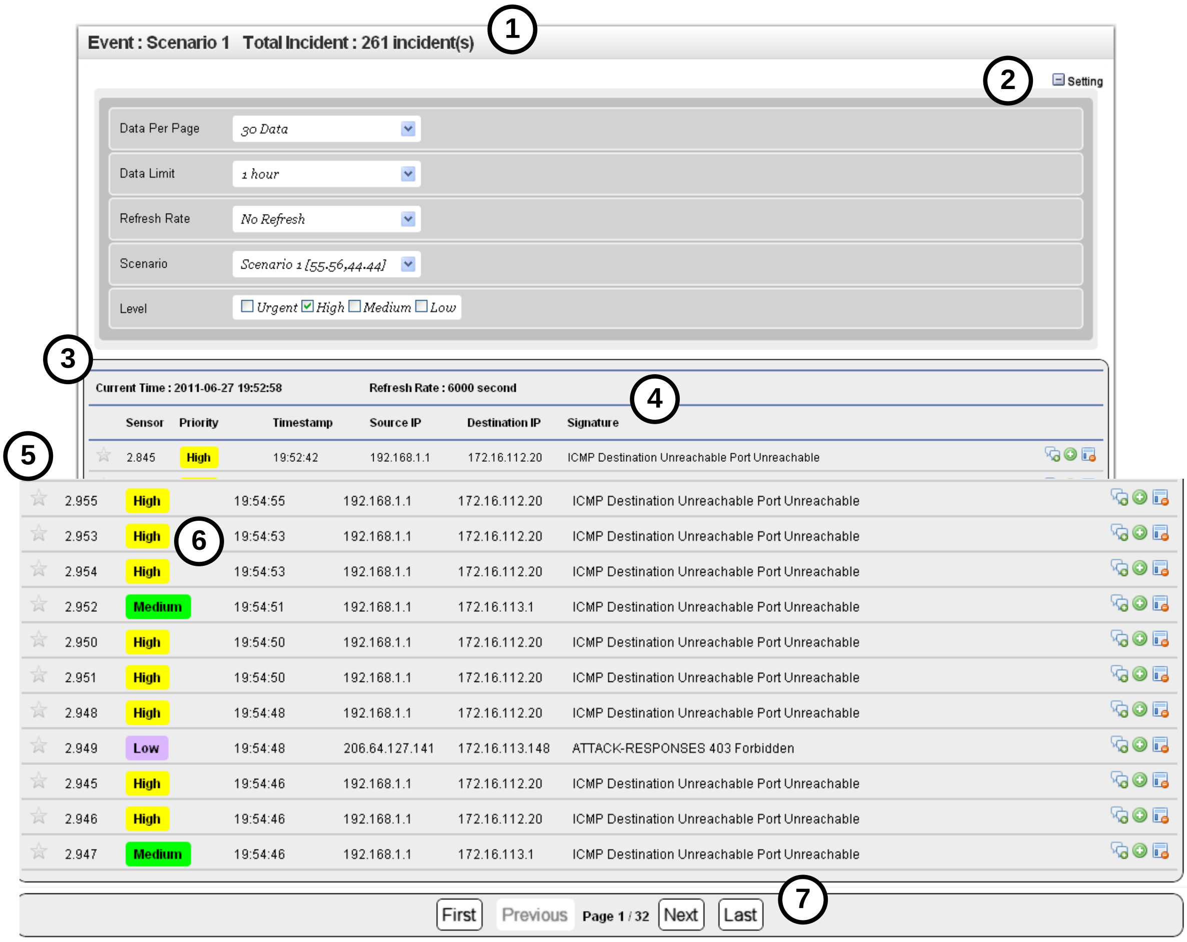
In order to show the current scenario using other representation, additional graphs as in Label 6 are generated in real time, giving an opportunity to administrators to update the current scenario. The graph is interactive and there is a vertical line to show the current risk index in any particular time. For example, at 19:47, Label 6 shows the current level of the incident priorities, such as 0.5374 for the highest index, 0.2524 for the average index and 0.0936 for the lowest index.

To provide an interactive page, all the wording in the main board is active; hence they allow easy navigation within the module. For example, Label 2 allows administrators to summarise the results within the last 1 hour, 24 hours, one week and one month. On top of that, Label 4 summarises lists for the top incidents, assets and protocols, and administrators are allowed to navigate to other pages such as the *scenario* and *event* pages.

To analyse each incident in further detail or to thoroughly examine assets and events, the next section illustrates the other related visuals.

6.3.3 Analysis

Using a similar scenario as the previous example, *Figure 36* shows a live event for the *Event* page. In this particular example, there were 261 incidents and most of them were labelled as a high priority. The priority of the incidents can be differentiated using the customisable colours, such as yellow for high and green for the medium priority (see Label 6).



Event : Scenario 1 Total Incident : 261 incident(s)

Data Per Page	30 Data
Data Limit	1 hour
Refresh Rate	No Refresh
Scenario	Scenario 1 [55.56,44.44]
Level	□ Urgent ☑ High □ Medium □ Low

Current Time : 2011-06-27 19:52:58 Refresh Rate : 6000 second

	Sensor	Priority	Timestamp	Source IP	Destination IP	Signature
☆	2.845	High	19:52:42	192.168.1.1	172.16.112.20	ICMP Destination Unreachable Port Unreachable
☆	2.955	High	19:54:55	192.168.1.1	172.16.112.20	ICMP Destination Unreachable Port Unreachable
☆	2.953	High	19:54:53	192.168.1.1	172.16.112.20	ICMP Destination Unreachable Port Unreachable
☆	2.954	High	19:54:53	192.168.1.1	172.16.112.20	ICMP Destination Unreachable Port Unreachable
☆	2.952	Medium	19:54:51	192.168.1.1	172.16.113.1	ICMP Destination Unreachable Port Unreachable
☆	2.950	High	19:54:50	192.168.1.1	172.16.112.20	ICMP Destination Unreachable Port Unreachable
☆	2.951	High	19:54:50	192.168.1.1	172.16.112.20	ICMP Destination Unreachable Port Unreachable
☆	2.948	High	19:54:48	192.168.1.1	172.16.112.20	ICMP Destination Unreachable Port Unreachable
☆	2.949	Low	19:54:48	206.64.127.141	172.16.113.148	ATTACK-RESPONSES 403 Forbidden
☆	2.945	High	19:54:46	192.168.1.1	172.16.112.20	ICMP Destination Unreachable Port Unreachable
☆	2.946	High	19:54:46	192.168.1.1	172.16.112.20	ICMP Destination Unreachable Port Unreachable
☆	2.947	Medium	19:54:46	192.168.1.1	172.16.113.1	ICMP Destination Unreachable Port Unreachable

Page 1 / 32

Figure 36. The *Event* page

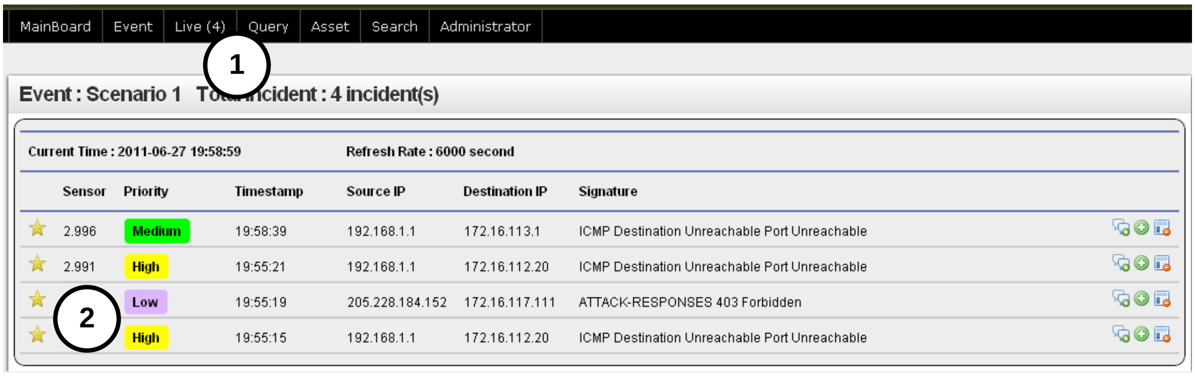
The *event* page provides insight information related to the prioritised incidents. The page provides two main functions including the setting and summarisation functions.

In order to display the settings menu, the drop-down button in Label 2 gives a shortcut to administrators to exhibit and close the settings menu. The settings menu allows the output in the *Event* page to be represented in a combination of five different settings include data per page (e.g. 30 events showed on each page), data limit (the time limit of events, e.g. 1 hour), refresh rate (the web page is refreshed periodically based upon this setting, e.g. no refresh rate is selected), the selection scenario and the priority level, which can be used to filter the level of priority of an event (e.g. administrators have the ability to set it to have a high incident only).

Based on the settings, the page updates the modules periodically and this can be seen in Label 3, as it shows a list of incidents by indicating the current time and refresh rate used by the page. The table in the page displays information related to incidents such as priority, source IP address, destination IP address and signatures (i.e. Label 4); each of them can be used to navigate to the *query* page in order to investigate them further.

Since the page updates periodically, it provides additional functions to 'mark incidents'. The first column of the list in the table shows a star – this function allows administrator to highlight incidents in case they want to revise them again in future (see Label 5). The revision page can be found on the *Live* page, as illustrated in *Figure 37*.

In order to facilitate the usability of the page, there are additional navigation functions on the page. The four buttons ( ) are used to load other pages as mentioned in *Section 6.2.3*; the pages are the *show response*, *insert response* and *show details* page. In addition, at the bottom of the page, there are four buttons: the first, previous, next and last button. These buttons can be used to navigate throughout the list in order to analyse all the incidents; for example, in the page there are 32 pages (Label 7).



Event : Scenario 1 Total incident : 4 incident(s)

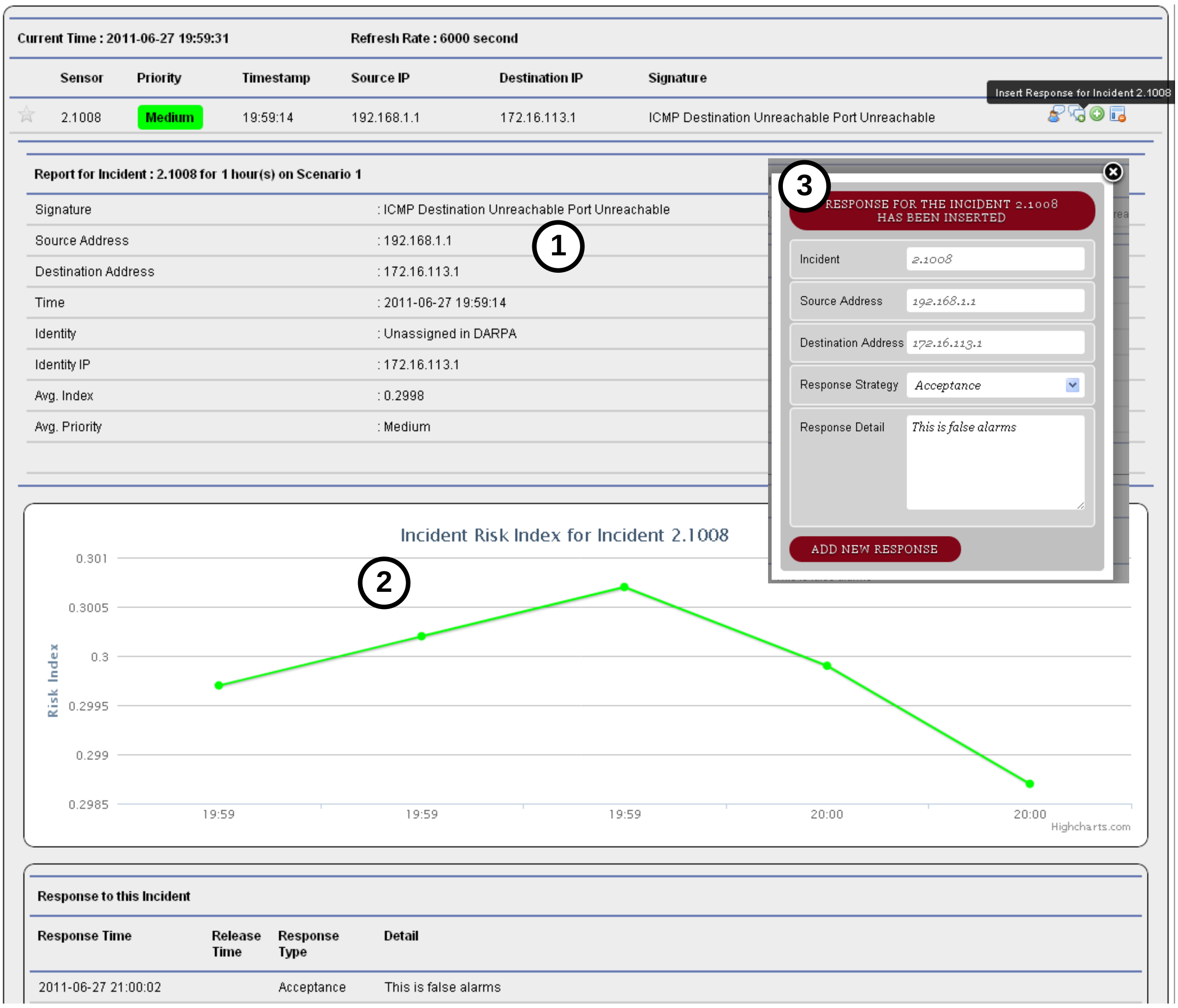
Current Time : 2011-06-27 19:58:59 Refresh Rate : 6000 second

	Sensor	Priority	Timestamp	Source IP	Destination IP	Signature
☆	2.996	Medium	19:58:39	192.168.1.1	172.16.113.1	ICMP Destination Unreachable Port Unreachable
☆	2.991	High	19:55:21	192.168.1.1	172.16.112.20	ICMP Destination Unreachable Port Unreachable
☆		Low	19:55:19	205.228.184.152	172.16.117.111	ATTACK-RESPONSES 403 Forbidden
☆		High	19:55:15	192.168.1.1	172.16.112.20	ICMP Destination Unreachable Port Unreachable

Figure 37. The *Live* page

In order to revise marked incidents, *Figure 37* shows a snapshot of the page. As can be seen in Label 1, the page summarises the total number of marked incidents from other pages, such as the *Event* page and *Search* page. In particular, this page shows four incidents. Furthermore, the first column of the page lists yellowish stars and they show highlighted incidents that have been marked previously on the other pages, such as the *Event* page and *Search* page (i.e. Label 2). Like other pages, all the wording in this page is also an active link which can be used to navigate directly to the *query* page.

In addition to the *Event* and *Live* page, to analyse the detail of each incident, it is recommended that administrators load additional pages like the *Response* and *Detail* page, as illustrated in *Figure 38*. For example, the figure shows details of an incident with ID 1008 which was detected in Sensor 2.



Current Time : 2011-06-27 19:59:31 Refresh Rate : 6000 second

	Sensor	Priority	Timestamp	Source IP	Destination IP	Signature
☆	2.1008	Medium	19:59:14	192.168.1.1	172.16.113.1	ICMP Destination Unreachable Port Unreachable

Insert Response for Incident 2.1008

Report for Incident : 2.1008 for 1 hour(s) on Scenario 1

Signature	: ICMP Destination Unreachable Port Unreachable
Source Address	: 192.168.1.1
Destination Address	: 172.16.113.1
Time	: 2011-06-27 19:59:14
Identity	: Unassigned in DARPA
Identity IP	: 172.16.113.1
Avg. Index	: 0.2998
Avg. Priority	: Medium

RESPONSE FOR THE INCIDENT 2.1008 HAS BEEN INSERTED

Incident	2.1008
Source Address	192.168.1.1
Destination Address	172.16.113.1
Response Strategy	Acceptance
Response Detail	This is false alarms

Response to this Incident

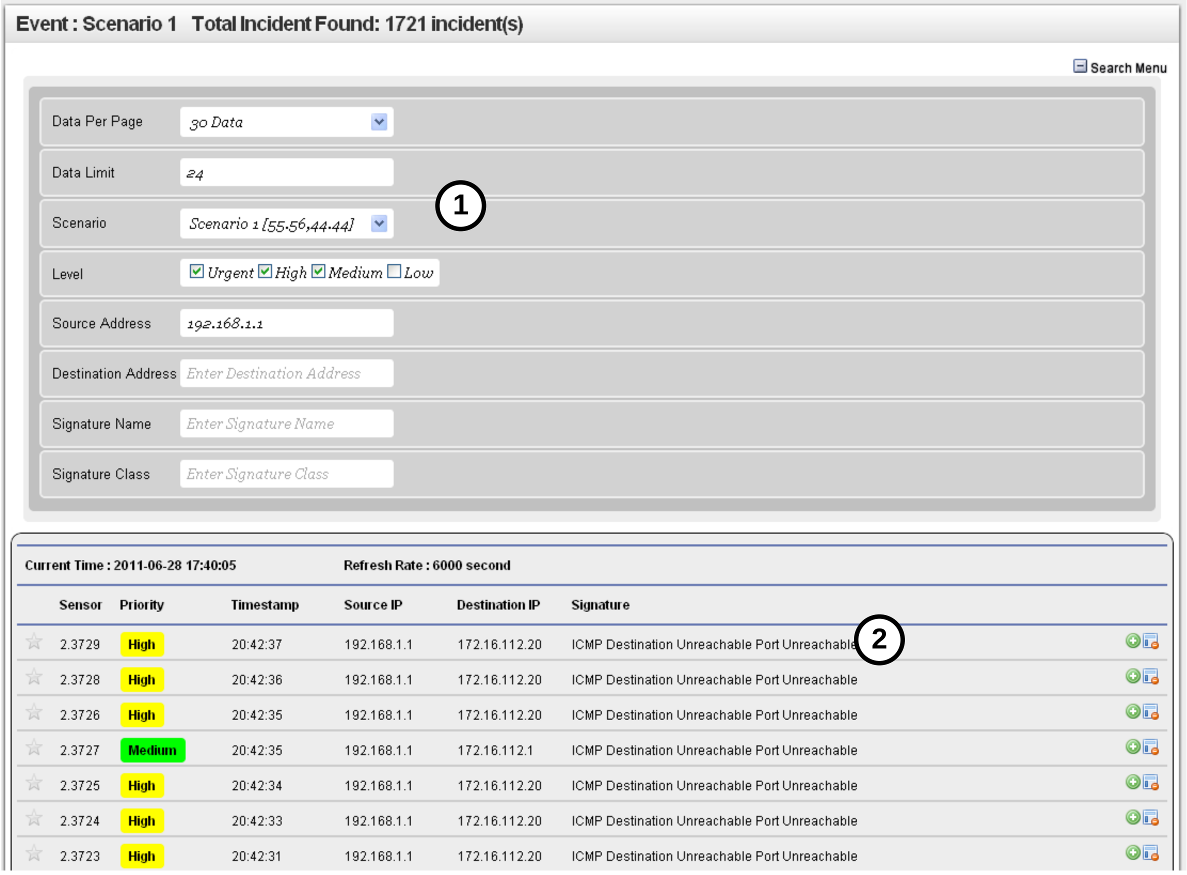
Response Time	Release Time	Response Type	Detail
2011-06-27 21:00:02		Acceptance	This is false alarms

Figure 38. The additional pages

The *Detail* page shows other information related to the selected incidents. For example, the page summary tabulates useful information such as sensor ID, incident priority, time detected, source and destination IP as well as its signature (see Label 1). Every single detail has an active link which can be used as a reference for administrators to navigate to a new page such as the *Query* page. In addition to that, in order to give additional information, there is a graph below the incident information (i.e. Label 2). The graph is temporal and shows the history of risk indexes which are taken periodically within a specific period of time (i.e. the time period itself is configured by administrators manually – the interval limitation). As the graph grows periodically over time, it allows administrators to make an additional judgement upon the selected incident. For example, the illustrated graph in the figure shows a declining graph and, arguably, it therefore shows that the incident itself is not really as critical in time as when it was first detected.

The *response* page in Label 3 is a form loaded after the response button is clicked. It provides a manual input from administrators; for example, if there is a case of false incidents, it can be noted as it is. At the bottom of the page, there is a list of responses and it shows the previous responses entered manually by administrators or automatically by response agents. This list allows administrators to analyse the selected incident thoroughly, and other further actions could be planned based upon the list.

To extend the analysis upon incidents, it is recommended that administrators extend their investigation by searching a specific type of incident and this can be done using the *Search* page. As illustrated in *Figure 39*, the search facilities allow administrators to focus upon a specific type of incident based on their attributes such as source IP address, destination IP address or even with their signatures.



Event : Scenario 1   Total Incident Found: 1721 incident(s)

Search Menu

Data Per Page	30 Data
Data Limit	24
Scenario	Scenario 1 [55.56,44.44]
Level	☑ Urgent ☑ High ☑ Medium □ Low
Source Address	192.168.1.1
Destination Address	Enter Destination Address
Signature Name	Enter Signature Name
Signature Class	Enter Signature Class

Current Time : 2011-06-28 17:40:05   Refresh Rate : 6000 second

	Sensor	Priority	Timestamp	Source IP	Destination IP	Signature
☆	2.3729	High	20:42:37	192.168.1.1	172.16.112.20	ICMP Destination Unreachable Port Unreachable
☆	2.3728	High	20:42:36	192.168.1.1	172.16.112.20	ICMP Destination Unreachable Port Unreachable
☆	2.3726	High	20:42:35	192.168.1.1	172.16.112.20	ICMP Destination Unreachable Port Unreachable
☆	2.3727	Medium	20:42:35	192.168.1.1	172.16.112.1	ICMP Destination Unreachable Port Unreachable
☆	2.3725	High	20:42:34	192.168.1.1	172.16.112.20	ICMP Destination Unreachable Port Unreachable
☆	2.3724	High	20:42:33	192.168.1.1	172.16.112.20	ICMP Destination Unreachable Port Unreachable
☆	2.3723	High	20:42:31	192.168.1.1	172.16.112.20	ICMP Destination Unreachable Port Unreachable

Figure 39. The *Search* Page

The searching form allows administrators to enter a specific query manually. The query can be made using 8 attributes such as source address, destination address and signature. In this example, a new query using the source address has been entered with "*192.168.1.1*" as the input (i.e. Label 1). The output of the query uses similar attributes to the other pages, such as the heading of the page and its table. On this particular page, the table displays the search results using 6 main columns including the sensor with incidents' ID, its priority, timestamp, source and destination address as its reference of signatures (i.e. Label 2).

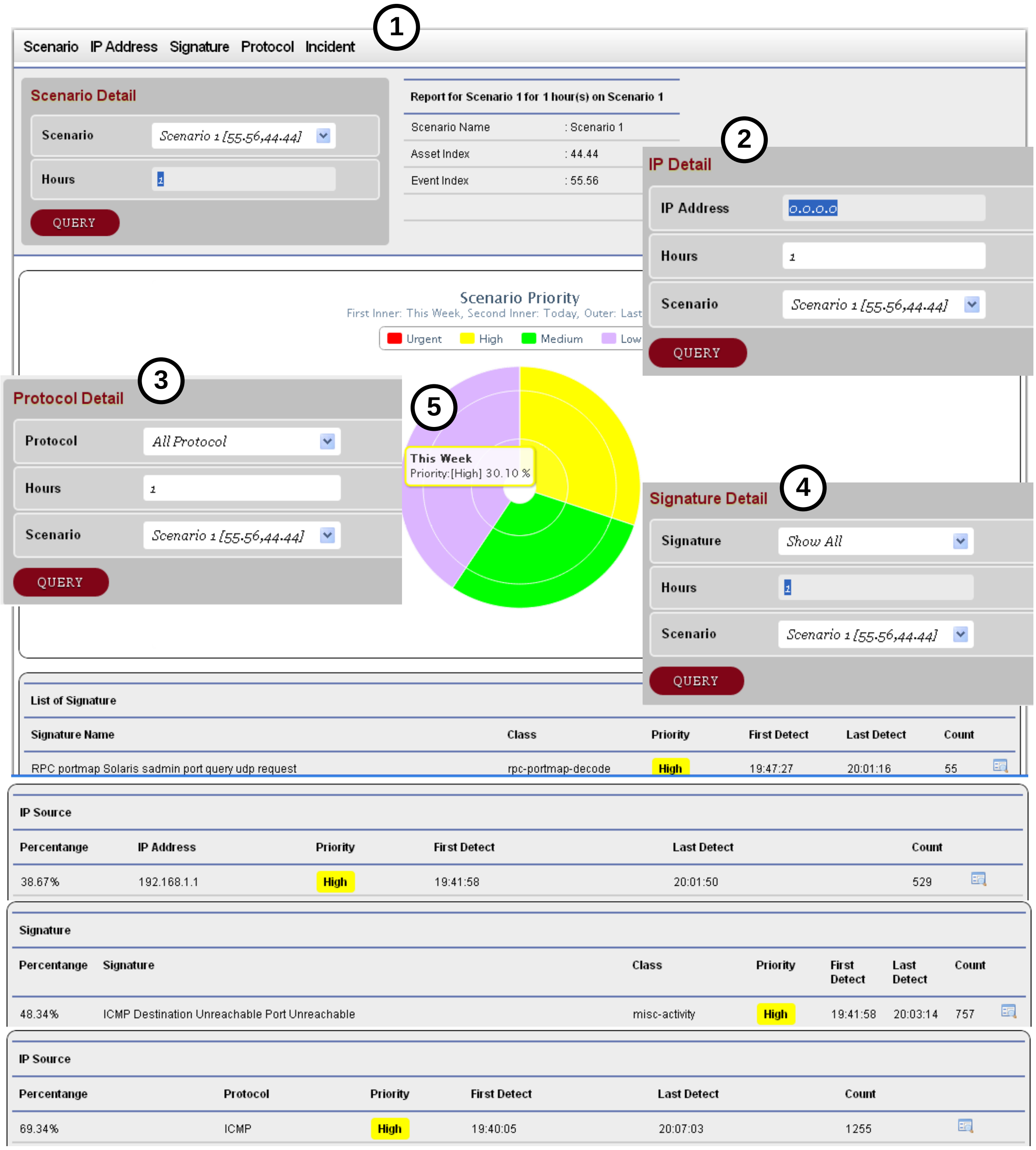
The analysis function in the web modules also provides the additional query page, on top of what the *Search* page provides. To analyse the details of the incidents, *Figure 40* shows the *Query* page. It is similar to the *Search* page except that this page allows administrators to focus on and summarise the similar incidents based upon specific attributes. The attributes can be categorised into five fields: scenario, IP address, signature, protocol and specific incidents (i.e. Label 1 – Label 4).

With the scenario query, administrators are allowed to summarise the results based upon a specific timeline; for example, a summarisation of a scenario for the last 30 hours and so on. In addition, the page provides a graph to summarise the percentages of incidents and it categorises them into different levels of priority based on the settings made on the *configuration* page (i.e. Label 5). Using this visualisation, it summarises a general view of what is the current status compared to the previous days. The result of the query is tabulated into six columns include signatures, class, priority and time detected as well as the total number of incidents.

In addition, in order to provide more specific queries, administrators are allowed to make a query based on incidents' protocol, such as TCP and UDP. Furthermore, the query can also be made using signatures and the query form only lists signatures which can be obtained automatically from databases.

The result of the query is displayed according to the selection category. For example, a query made based upon IP address attributes tabulates the percentage of similar IP addresses together with the total number of incidents.

Similar with other pages, every single result on the page has an active link which can be used to navigate from one page to others; for example, if there is an "IP address" attribute, it is possible to click to navigate to the *Query* page using IP address as its attribute.


1
Scenario IP Address Signature Protocol Incident
2
3
4
5
QUERY
Scenario Priority
First Inner: This Week, Second Inner: Today, Outer: Last
Urgent
High
Medium
Low
This Week
Priority:[High] 30.10 %

Scenario Detail

Scenario: *Scenario 1 [55.56,44.44]*

Hours: 1

Report for Scenario 1 for 1 hour(s) on Scenario 1

Scenario Name	: Scenario 1
Asset Index	: 44.44
Event Index	: 55.56

IP Detail

IP Address: 0.0.0.0

Hours: 1

Scenario: *Scenario 1 [55.56,44.44]*

Protocol Detail

Protocol: *All Protocol*

Hours: 1

Scenario: *Scenario 1 [55.56,44.44]*

Signature Detail

Signature: *Show All*

Hours: 1

Scenario: *Scenario 1 [55.56,44.44]*

List of Signature

Signature Name	Class	Priority	First Detect	Last Detect	Count
RPC portmap Solaris sadmin port query udp request	rpc-portmap-decode	High	19:47:27	20:01:16	55

IP Source

Percentange	IP Address	Priority	First Detect	Last Detect	Count
38.67%	192.168.1.1	High	19:41:58	20:01:50	529

Signature

Percentange	Signature	Class	Priority	First Detect	Last Detect	Count
48.34%	ICMP Destination Unreachable Port Unreachable	misc-activity	High	19:41:58	20:03:14	757

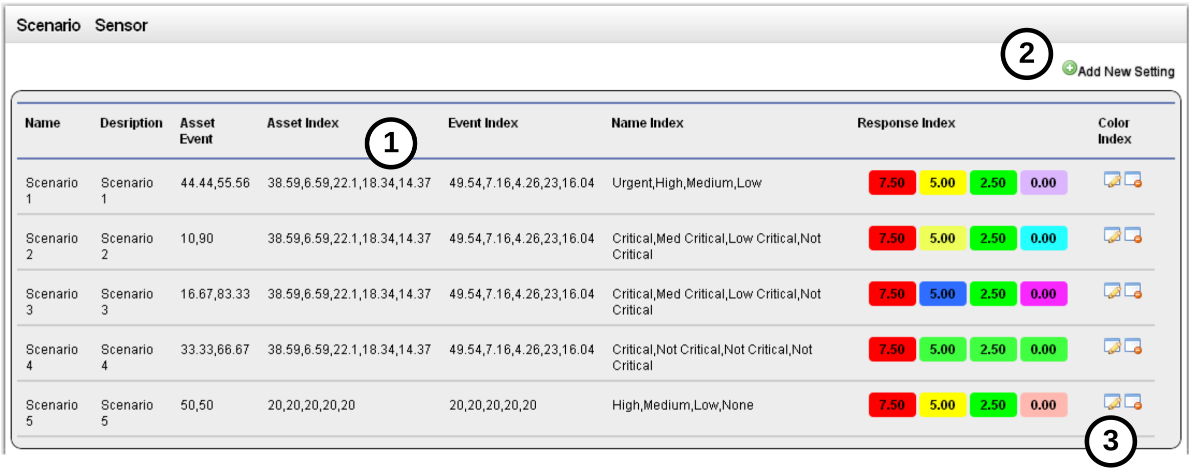
IP Source

Percentange	Protocol	Priority	First Detect	Last Detect	Count
69.34%	ICMP	High	19:40:05	20:07:03	1255

Figure 40. The *Query* Page

6.3.4 Configuration

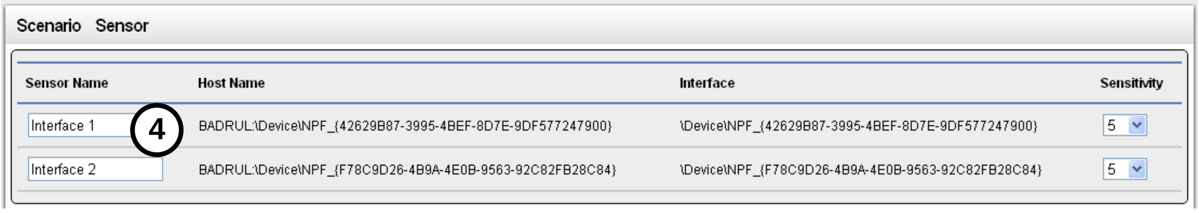
To facilitate the analysis and visualisation of the web modules, the *configuration* page plays an important role; in particular, the page provides various settings such as colours, weightings for indicators, assets configuration, sensor indicators and scenario settings. These configurations are illustrated in *Figure 41* through to *Figure 46*.



Name	Desription	Asset Event	Asset Index	Event Index	Name Index	Response Index	Color Index
Scenario 1	Scenario 1	44.44,55.56	38.59,6.59,22.1,18.34,14.37	49.54,7.16,4.26,23,16.04	Urgent,High,Medium,Low	7.50 5.00 2.50 0.00	
Scenario 2	Scenario 2	10,90	38.59,6.59,22.1,18.34,14.37	49.54,7.16,4.26,23,16.04	Critical,Med Critical,Low Critical,Not Critical	7.50 5.00 2.50 0.00	
Scenario 3	Scenario 3	16.67,83.33	38.59,6.59,22.1,18.34,14.37	49.54,7.16,4.26,23,16.04	Critical,Med Critical,Low Critical,Not Critical	7.50 5.00 2.50 0.00	
Scenario 4	Scenario 4	33.33,66.67	38.59,6.59,22.1,18.34,14.37	49.54,7.16,4.26,23,16.04	Critical,Not Critical,Not Critical,Not Critical	7.50 5.00 2.50 0.00	
Scenario 5	Scenario 5	50,50	20,20,20,20,20	20,20,20,20,20	High,Medium,Low,None	7.50 5.00 2.50 0.00	

Figure 41. The *Configuration* Page - Scenario

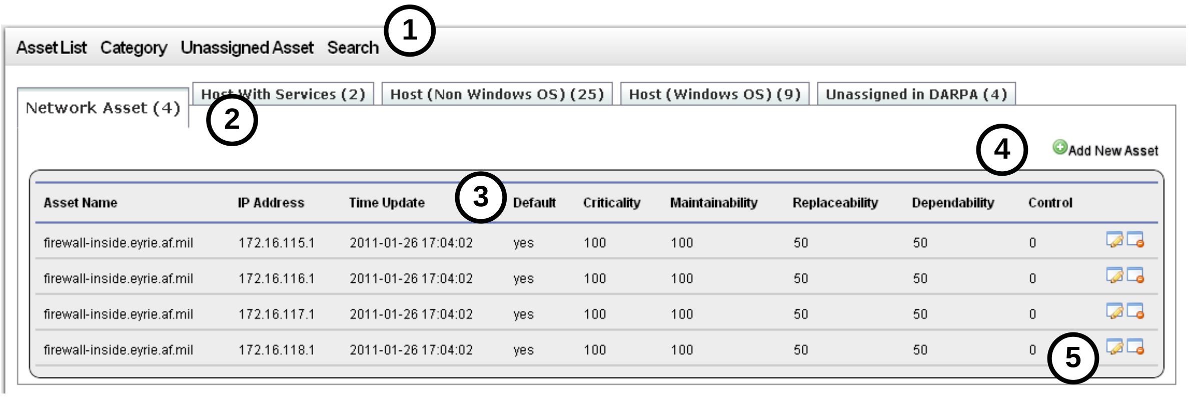
Figure 41 shows the *configuration* page for scenarios used in the web modules, as they can be added and removed depending on the administrators' desire. As can be seen in Label 1, the summarisation of the configuration is tabulated into several columns such as scenario name, descriptions, weight of indicators, custom names for the priority level and appropriate thresholds with their colours. In order to add a new scenario, administrators are allowed to click the button with Label 2 and a form will be loaded to be filled. To optimise the navigation process, there are two buttons for each scenario (i.e. Label 3). The first button allows administrators to navigate the edit page and updates the selected configuration setting. In addition, the current setting can be deleted using the second button.



Sensor Name	Host Name	Interface	Sensitivity
Interface 1	BADRUL:\Device\NPF_{42629B87-3995-4BEF-8D7E-9DF577247900}	\Device\NPF_{42629B87-3995-4BEF-8D7E-9DF577247900}	5
Interface 2	BADRUL:\Device\NPF_{F78C9D26-4B9A-4E0B-9563-92C82FB28C84}	\Device\NPF_{F78C9D26-4B9A-4E0B-9563-92C82FB28C84}	5

Figure 42. The *Configuration* Page – Sensor

In addition to the *configuration* page for the scenario setting, *Figure 42* shows an example page of the sensor setting which is used to configure the sensor indicator. In addition to the interface's original name stored in databases, the sensor name itself can be renamed as an alias (see Label 4). The custom name gives an additional attribute to administrators when monitoring the entire modules. Furthermore, the sensitivity of the sensor can be configured using the drop-down menu on the page.



Asset Name	IP Address	Time Update	Default	Criticality	Maintainability	Replaceability	Dependability	Control
firewall-inside.eyrie.af.mil	172.16.115.1	2011-01-26 17:04:02	yes	100	100	50	50	0
firewall-inside.eyrie.af.mil	172.16.116.1	2011-01-26 17:04:02	yes	100	100	50	50	0
firewall-inside.eyrie.af.mil	172.16.117.1	2011-01-26 17:04:02	yes	100	100	50	50	0
firewall-inside.eyrie.af.mil	172.16.118.1	2011-01-26 17:04:02	yes	100	100	50	50	0

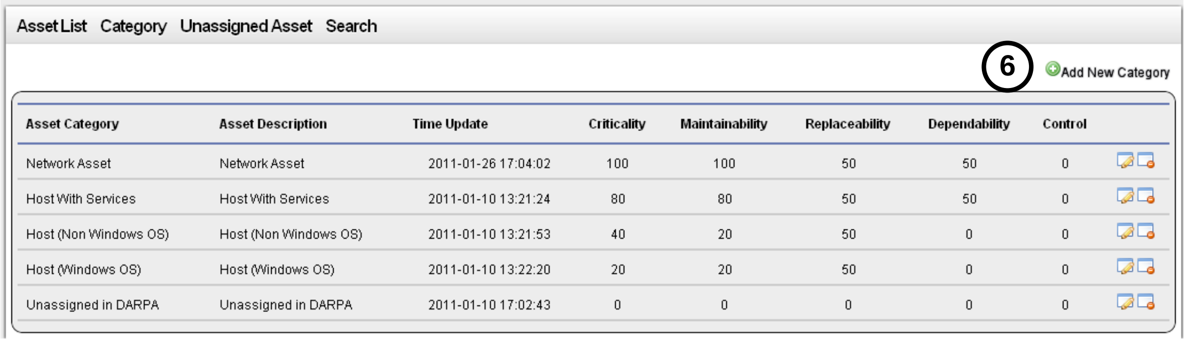
Figure 43. The *Configuration* Page – Asset

The configuration page also allows administrator to configure assets. There are four main configuration pages for the asset setting: asset list, category, unassigned asset and search. On the top of *Figure 43*, there are several shortcuts and these are active links used to load other pages such as the asset list, category, unassigned asset and search page (see Label 1).

The page contains customisable tabs and these allow administrators to navigate from one category to another in order to view the asset settings. In this particular example, there are five tabs which represent five categories, namely: *network asset, host with services, host for non-Windows OS, host with Widows OS* and *unassigned in the DARPA dataset* (see Label 2).

The table highlights all the settings which are configured manually by administrators and a simple view like this allows them to view all the assets thoroughly. Similar to other pages, the list shows the weight for each indicator represented by the corresponding assets. In addition, the button on the right of the page (i.e. Label 4) gives a hand to administrators to add a new asset and administrators need to enter the appropriate input in a form loaded after the button is clicked, such as asset name, IP address and indicators’ values (see Label 3).

Similar to the other configuration pages, there are two buttons (i.e. Label 5). The first one allows administrators to navigate to the edit page in order to update the current configuration setting. The current setting can also be deleted using the second button.

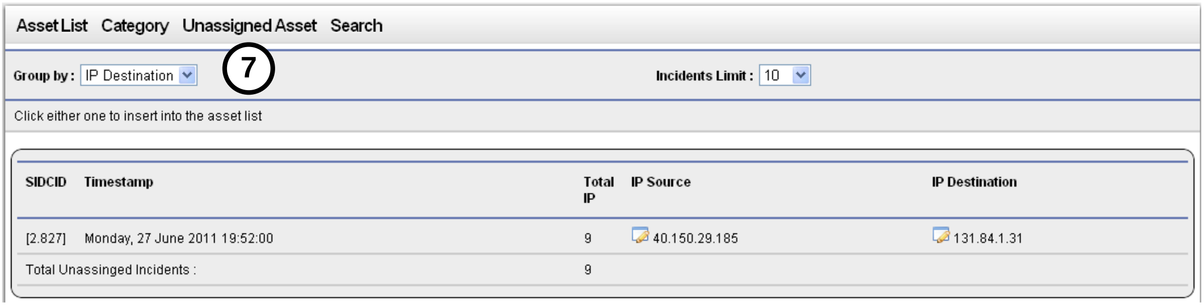


Asset Category	Asset Description	Time Update	Criticality	Maintainability	Replaceability	Dependability	Control
Network Asset	Network Asset	2011-01-26 17:04:02	100	100	50	50	0
Host With Services	Host With Services	2011-01-10 13:21:24	80	80	50	50	0
Host (Non Windows OS)	Host (Non Windows OS)	2011-01-10 13:21:53	40	20	50	0	0
Host (Windows OS)	Host (Windows OS)	2011-01-10 13:22:20	20	20	50	0	0
Unassigned in DARPA	Unassigned in DARPA	2011-01-10 17:02:43	0	0	0	0	0

Figure 44. The *Configuration* Page – Asset Category

Furthermore, using the category menu link, administrators are allowed to configure and update the category of assets. *Figure 44* tabulates a list of the category configuration settings and contains details about them. It shows only the appropriate category which is entered manually by administrators and each of them will be used as a reference to calculate the incident risk indexes.

Similar to other the configuration pages, the button on the right allow administrators to add a new category (i.e. Label 6). Input such as asset category, descriptions and indicators' values are particularly useful pieces of information.



Group by : IP Destination

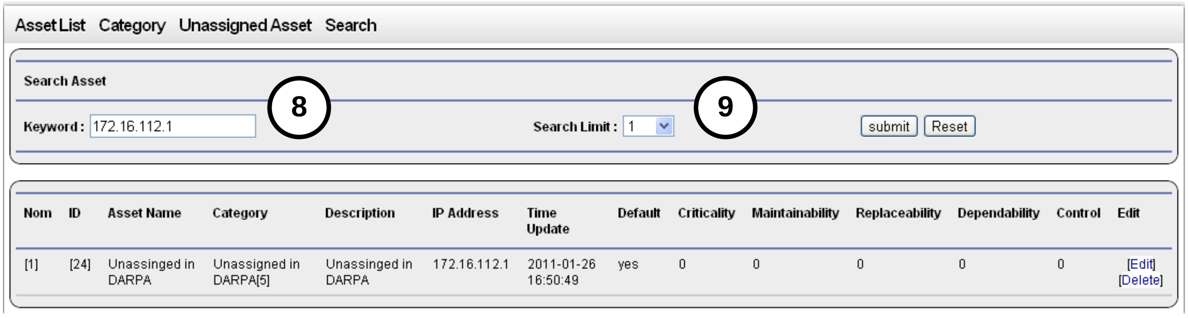
Incidents Limit : 10

Click either one to insert into the asset list

SIDCID	Timestamp	Total IP	IP Source	IP Destination
[2.827]	Monday, 27 June 2011 19:52:00	9	40.150.29.185	131.84.1.31
Total Unassinged Incidents :		9		

Figure 45. The *Configuration* Page – Unassigned Asset

With the *unassigned asset* page, administrators are allowed to list the unassigned assets as this is important to the proposed framework because the appropriate values for indicators are needed in the calculation process. *Figure 45* shows an example and lists only one asset; it shows only the total number of incidents which relate to the reference assets and its IP addresses. The page also allows administrators to make a custom list on the page. For example, administrators are allowed to display the unassigned assets by grouping them using similar an IP destination or source (see Label 7).



Keyword : 172.16.112.1

Search Limit : 1

Nom	ID	Asset Name	Category	Description	IP Address	Time Update	Default	Criticality	Maintainability	Replaceability	Dependability	Control	Edit
[1]	[24]	Unassinged in DARPA	Unassigned in DARPA[5]	Unassinged in DARPA	172.16.112.1	2011-01-26 16:50:49	yes	0	0	0	0	0	[Edit] [Delete]

Figure 46. The *Configuration* Page – Asset Search

Finally, to find any assets, and in order to view or update their settings, it is recommended that administrators load the search asset page as it provides an easy way to locate a desired asset. As illustrated in *Figure 46*, the keyword form can be used to enter the desired IP address in order to make a query (i.e. Label 8). To give an additional facility to administrators, it allows a query made using a wildcard character (%) and, with it, appropriate results will be returned by listing several assets according to the query made. To limit the query results, administrators can use the drop-down menu which allows them to choose a number between 1 to 200 assets (i.e. Label 9).

6.4 Advantages and Limitations

In providing a flexible platform to administrators to configure, analyse and make a wise decision using the prioritisation results, the web modules give the following advantages:

(a) *Analytics results*. The web modules provide a web analytics solutions that give rich insights into the incident prioritisation process and analysis simpleness. Simplicity, easy-to-use, customisable, flexible and optimisation of results features allow administrators to analyse the entire prioritisation process and their results examined in online assessment mode. The web modules provide various types of custom results and give a broader view of the current situation related to incidents and IDSs.

(b) *Simplicity with graphical interfaces.* Instead of having numerical values, the web modules simplify reporting and analytics by providing graphical interfaces in interpreting the incident priorities with the aid of the usage of different colours and graphs. The use of different colours allows administrators to interpret the meaning of the prioritisation process results easily and also gives additional advantage to high-level management and non-technical people to understand the current situation easily because the representation of results are displayed in a combination between qualitative and qualitative results.

(c) *Easy management and user friendly interfaces*. The use of the web modules provides user friendly interfaces because administrators have an ability to manage any human-computer interaction such as customisation upon settings, change the configuration setting, analyse the prioritisation results and make a decision via any web browsers. With the openness of the web modules, they can be accessed from any platforms anywhere, and all these can be done without any hassle.

(d) *Flexible setting to optimise the prioritisation results*. The web modules provide a flexibility mode upon the module configurations which allows administrators to modify them dynamically, in order to optimise the view of the prioritisation results. With the result optimisation, the web modules provide comprehensive summarisations of the incident priorities and for example, the web modules summarise the top incidents, top assets as well as to customise the incident priorities. By having this, it is also improve the understanding by giving different perspective in interpreting the incidents because they are initially using numerical values to represent theirs priority.

(e) *Live traffic network and online assessment mode*. With the capabilities of the proposed framework to examine a live traffic network, the web modules provide a direct access management system as well as run them in online assessment mode, in order to analyse the incident risk indexes. Unlike other offline systems, the web modules allow administrators to make a wise decision instantly based upon the online results without have to wait for the entire information to be collected using batch systems.

(f) *Practical and cost effective*. With the openness of the web modules, they can be viewed and browsed using any web browsers. A practical solution for enterprises, to extend the usage to have a large audience of analysts is considered cheap and very cost effective as it does not require any cost since web browsers are free to download.

In addressing the advantages of the web modules, they also inherit some limitations as follows:

(a) *Applications Dependent*. As the web modules are served using a web server, they rely on the efficiency of the web server itself, in case of the server offline, the prioritisation process cannot be done and other analyses are halted. In addition, as the nature of the World Wide Web, they also rely upon the network consistency to communicate and exchange information.

(b) *Inherit other vulnerabilities*. Due to the used of web applications, the web modules are vulnerable with the web application vulnerabilities such as HTTP Parameter Pollution (HPP) , SQL injection, cross-site scripting and session hijacking. In addition to that, the web modules also vulnerable to the other vulnerabilities such as hardware (e.g. web server) and software (e.g. browsers); as they can be used as a weak point to exploit the entire modules.

Therefore, to provide a better service in the future, it is important to address thus limitations using other security precautions and countermeasures.

6.5 Summary

This chapter demonstrated the implementation stage of the proposed framework by providing some examples and snapshots from Security Incident Prioritisation Modules. The details of its modules, system architecture, state diagrams and web modules have been presented to show how they interact.

The key objective of demonstrating and describing the details of the modules is to enable a better understanding of how the proposed framework works, and how its internal modules are affected by the external environment. Due to time constraints, it was not possible to fully implement the operation of some modules, such as response agents. This limitation, among others, is discussed in the following chapter.

This page intentionally left blank

7 Conclusion

This chapter summarises the study by reviewing the achievements of the research. It highlights its most important findings, as well as its limitations. It then discusses the potential of new studies within the domain, showing how the proposed framework could be enhanced in the future.

7.1 Achievements of the study

The study commenced with an investigation into the different types of response options, exploring issues related to the incident response and prioritisation process. It also identified the generic decision factors needed to facilitate the estimation of the level of risk of incidents, using a methodically approach in the ranking and rating process. The study proposed a novel framework in order to address the incident prioritisation process and to facilitate an autonomous mode in the response selection process in IRSs. Several models and strategies were explored and their capabilities evaluated in order to satisfy the aims of this study.

Literally, the overall goal of this study is to establish a novel approach to prioritising incidents for different types of response options in network environments. Within the proposed framework, which included experiments as well as the prototypes of web modules, this study has been successful. Details are as follows:

1. *A response model for Intrusion Response Systems*. This study has established a model which categorises several response options such as proactive, reactive and passive responses. Using a new perspective, the establishment of the model allows the proposed framework to be designed to respond to and prioritise different levels of incident (See *Chapter 4*). The model helps the proposed framework to work flawlessly in mapping different types of incident, each of which has its own unique characteristics. A survey study was conducted to investigate the correlation between the model and its response options when applied to commercial and research products (see *Chapter 2*). To show the feasibility and suitability of the model, as well as other models, several experiments were conducted and their results suggested positive outcomes (see *Chapter 5*).

2. *Issues in incident response and prioritisation studies*. In Chapter 3, this study established a critical analysis of different perspectives when addressing the significant problems of the incident prioritisation and response selection process, as well as its challenges. With an aim to

establish a framework to prioritise incidents, several issues were exposed in the rating and ranking of, and responses to, incidents. By presenting the strengths and weaknesses of these issues, several strategies were identified which address the limitations of the previous approaches, by enhancing the incident prioritisation process so that it is more systematic in the response selection process.

3. *Generic indicators required to estimate risk indexes of incidents*. The study proposed generic indicators to assist the estimation process and to rate the incident risk indexes, as they are important in the designing of the proposed framework. Two important decision factors were considered - the *impact on assets* and the *likelihood of threats and vulnerability* (see *Section 3.2.3*) - in order to address the incident prioritisation process.

4. *A novel framework which addresses the incident prioritisation process*. Using models and multi-strategies in rating, ranking and response incidents, this study proposed a novel framework to methodically address the incident prioritisation and response selection process. With the aid of the Analytic Hierarchy Process (AHP) and its generic indicators, a new risk estimation model was established: Risk Index Model (RIM). Simultaneously, the proposed framework facilitated the response selection process, which also offered a flawless approach in mapping different types of response options with different priorities of incident; this is done by using the Response Strategy Model (See *Section 4.2.3*).

5. *Comprehensive evaluation stages for the proposed framework*. In addressing the incident prioritisation and response selection process in IRSs, the proposed framework outlined several models and strategies. These need to be evaluated. The objective of the evaluation is to examine the proposed framework and to decide whether it is sufficiently applicable to facilitate the response selection process in a live traffic network with on-line assessment capabilities. The evaluation presented four stages: the proposed framework was analysed in terms of its effectiveness and performances when related to the models and strategies selected (See *Chapter 5*). The progressive results presented from one stage to another demonstrated the suitability and feasibility of the proposed framework in facilitating the selection process in IRSs. More importantly, the evaluation stages satisfied the main criteria to support the selection process, in particular, the ability of the framework to facilitate the autonomous mode, besides to operate with a reasonable processing time in the prioritisation process and reduce false responses upon false incidents.

6. *Implementation of the proposed framework*. To extend the investigation upon the feasibility of the proposed framework, and demonstrate its practical application in a live traffic network with on-

line assessment mode, a proof-of-concept study was designed and realised (See *Chapter 6*). As an extension to the evaluation study, the implementation stage has developed a web-based system, which concentrates on the web modules of the proposed framework, together with its application daemons. In order to illustrate the implementation stage, the detail of the proposed framework was presented using several modelling languages. These included case diagrams and state diagrams, as well as some snapshots of the prototype pages.

To conclude, it is believed that this study has achieved its aims and objectives as stated in Chapter 1.

7.2 Limitations of the study

The discussions of the previous chapters have demonstrated that this research has adequately achieved its aims and objectives: the establishment of a novel framework to use when prioritising incidents in an intrusion response environment. However, a number of limitations and challenges were encountered during the study and they are listed here for future reference:

1. *Quantitative measurements*. In conducting the experiment during the evaluation phase (see *Chapter 5*), this study found some practical limitations. In particular, all input to the experiments is quantitative. However, in a practical situation, it is difficult to establish such quantitative measures, particularly on asset values. Arguably, a qualitative input which has a different group of rating (e.g. high, medium and low) would be more meaningful. This study used quantitative values because the proposed framework allows incidents to be differentiated. Because of this limitation, it is suggested that, in future studies, a qualitative input needs to be changed to a quantitative input, in order to calculate and estimate the incident risk indexes.

2. *A rational assumption.* At present, the evaluation study used assumption to obtain the indicator values when estimating the incident risk indexes, particularly in rating the values which related to assets and the judgement matrices. Although this study has presented positive results, future work should focus on strengthening the estimation process for rating every indicator which is involved in the proposed framework, in particular in the RIM. As decision factors, it is suggested that the indicator input be extended by giving a precise and detailed metric for measuring incidents. This will ensure the reduction of uncertainty amongst indicators.

3. *The evaluation of the study of incidents from the signature-based IDS only*. This evaluation study optimised the use of incidents based on the detection of signature-based IDS only, particularly Snort IDS. The available time did not permit the development of those modules which focus on other IDS's such as anomaly-based IDS or other signature-based examples. The proposed framework is not widely applicable and is limited to Snort only. However, it is considered valuable since Snort is the world's most widely-used IDS in both practising and research communities. Furthermore, the proposed framework operates with post-incident prioritisation process, which considers incidents after the detection process. Thus, theoretically it is possible to rate those incidents even with anomaly-based IDS.

4. *A practical proof-of-concept and response agents*. Although a practical evaluation study using web modules and a live traffic simulation has been presented in *Chapter 6*, it is important to perform the entire prototype in a live traffic network with actual response agents, in order to

strengthen the feasibility of the proposed framework. Furthermore, the results in this study have provided a clear distinction between the ways incidents are rated, ranked and prioritised. However, no practical consideration is given to counter-measures in order to control critical incidents. Although, in the proposed frameworks, there are response agents that can be used to respond to incidents, this is not fully implemented due to the lack of the availability of such security appliances (e.g. firewall) and insufficient time to perform the evaluation study. There are some response feedbacks from the agents, which have a potential to adjust risk indexes, however, this study does not consider it as the main objective. Thus, an important issue for future studies is how to improve strategies when deciding whether other counter-measures or responses would stop the critical incident.

5. *The usability of web modules.* The evaluation study extended the implementation stage to demonstrate the practicality of the web modules. However, the usability of such modules is not evaluated in this study. Although the usability evaluation of the modules is important, in order to demonstrate its easiness and navigation friendly, it is not the main objective of this study. However, the snapshots of the prototype pages presented in *Chapter 6* are considered adequate in order to demonstrate the usage of the web modules in practice.

7.3 Suggestions and Scope for Future Work

A number of suggestions for future work outside the scope of this study have been identified. Several issues have arisen and they are as follows:

1. *Anomaly IDS alarms*. As mentioned above, the input for the application daemon used in the evaluation study and implementation stage is limited to Snort-based alerts. Given this limitation, it would be beneficial that future works be directed towards increasing input from heterogeneous alerts which come from different types of IDS's, such as other signature-based IDS and anomaly-based IDS.

2. *Correlation between false incidents and prioritisation*. The result of the evaluation study in the third stage demonstrated a significant relationship between the classification of incidents and their priorities. Further analysis to investigate the correlation between them would be useful, especially on dealing with a live traffic network. This investigation is significant because it be can used to strengthen the proposed framework as well as to improve the response strategy in responding to false incidents.

3. *Visualisation of the critical incidents*. Figures, tables and graphs would benefit security analysts in terms of an easy and interactive approach when monitoring critical incidents. The other recommendation for future studies is to consider a visualisation domain of critical incidents (e.g. Human-Computer Interaction). Instead of using numbers, graphical images would be accessible and would give more information to security analysts. Most experiments were initially simulated and analysed using PHP. Therefore, revising the web modules and summarising the prioritisation results, using different types of graph models, could offer further opportunities for future studies.

4. *Response agents*. One of the limitations mentioned in the previous section was the use of response feedback from response agents. Future studies could use other approaches, such as machine learning domains; feedback mechanisms would be more meaningful if they were integrated into the current approach to responding to critical incidents.

7.4 Summary – The Future for Automated Response Systems

With thousands of incidents identified every day, relying upon manual processes to identify their importance and urgency is complicated, difficult, error-prone and time-consuming. This study has presented a novel framework that focuses upon the process of prioritising and responding to incidents using a methodically models and strategies. The framework helps security analysts to prioritise them automatically. In fact, the entire study has shown the advantages of using the proposed framework to facilitate the response selection process in IRSs, which not only focuses on critical incidents, but also provides a way to differentiate between incidents, assessing whether they are genuine, or not, and allowing an appropriate response to respond to them. Most importantly, the study has focused on enhancing the prioritisation scheme of identifying critical incidents, in order to provide a way to respond to them methodically. The important concept behind the proposed framework is the methodically steps, which include the rating, ranking and response selection process.

With models and strategies such as the Risk Index Model (RIM) and the Response Strategy Model (RSM), the adoption of the proposed framework in IRS's has given new perspectives in rating, ranking, and responding as well as in prioritising incidents, with generic indicators introduced in the proposed framework. Literally, the future of an automated response in IRS's is a step forward from the prioritisation scheme proposed in this study, because with all its positive results, it contributes significantly to the identification of critical incidents, based upon their importance and urgency. It means that only appropriate events are responded to and, at the same time, allows other legitimate users. Also, the use of web modules in visualising the prioritisation results means that online assessment mode can be employed. Additional visualisation studies would be beneficial, as they would be able to summarise thousands of results (i.e. not just the prioritisation results) in a single image.

In reality, the future of the automated response in Intrusion Response Systems still relies on human intervention, and it is normal with any management systems. However, with modern technology and introduction of an autonomous mode, such interventions are decreasing and this study has contributed in some significant degree to that domain. Although, the human intervention is needed in creating a check-and-balance situation, an automated system is important in order to ensure the survival of the interconnected systems. With more studies working to address the human intervention, it is hoped that one day, a better technology could improve the autonomous mode.

This page intentionally left blank

References

This thesis cites 216 references.

Abedin, M., Nessa, S., Al-Shaer, E. and Khan, L. (2006), "Vulnerability analysis for evaluating quality of protection of security policies", *Proceedings of the 2nd ACM workshop on Quality of protection*, Alexandria, Virginia, USA, pp. 49-52.

Ahmed, M.S., Al-Shaer, E. and Khan, L. (2008), "A Novel Quantitative Approach For Measuring Network Security", *Proceedings of the 27th IEEE Conference on Computer Communications (INFOCOM 2008)*, Phoenix, AZ, pp. 1957-1965.

Aickelin, U., Bentley, P., Cayzer, S., Kim, J. and McLeod, J. (2003), "Danger theory: The link between AIS and IDS?", *Proceedings of the 2nd International Conference on Artificial Immune Systems*, Edinburgh, UK, Vol. 2787, pp. 147-155.

Al-Mamory, S.O. and Zhang, H. (2009), "Intrusion detection alarms reduction using root cause analysis and clustering", *Computer Communications*, Vol. 32 No. 2, pp. 419-430.

Alberts, C. and Dorofee, A. (2004), "Security incident response: rethinking risk management", *International Congress Series*, Vol. 1268, pp. 141-146.

Alserhani, F., Akhlaq, M., Awan, I.U., Cullen, A.J. and Mirchandani, P. (2010), "MARS: Multi-stage Attack Recognition System", *Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications (AINA)*, Perth, Australia, pp. 753-759.

Alsubhi, K., Aib, I. and Boutaba, R. (2011), "FuzMet: a fuzzy-logic based alert prioritization engine for intrusion detection systems", *International Journal of Network Management*, pp. n/a-n/a.

Alsubhi, K., Al-Shaer, E. and Boutaba, R. (2008), "Alert prioritization in intrusion detection systems", *Proceedings of the IEEE Network Operations and Management Symposium*, Salvador, Brazil, pp. 33-40.

Anderson, J.P. (1980), *"Computer Security Threat Monitoring and Surveillance"*, James P. Anderson Co., Box 42, Fort Washington, PA, 19034, USA.

Anuar, N.B., Yaacob, M. and Idna, M.Y. (2004), "RedAlert: Approach for Firewall Policies Update Mechanism", *Wseas Transaction on Computer*, Vol. 3 No. 5, pp. 1451-1454.

Apache (2011), "Apache: HTTP Server Project", Available at: http://httpd.apache.org/ (Accessed: 10 April 2011).

Årnes, A., Sallhammar, K., Haslum, K., Brekne, T., Moe, M.E.G. and Knapskog, S.J. (2005), "Real-time risk assessment with network sensors and intrusion detection systems", *Proceedings of the International Conference on Computational Intelligence and Security*, Xian, China, Vol. 3802, pp. 388-397.

Årnes, A., Valeur, F., Vigna, G. and Kemmerer, R. (2006), "Using Hidden Markov Models to Evaluate the Risks of Intrusions: System Architecture and Model Validation", *Proceedings of the International Symposium on Recent Advances in Intrusion Detection (RAID)*, Hamburg, Germany, pp. 145–164.

Aussibal, J. and Gallon, L. (2008), "A New Distributed IDS Based on CVSS Framework", *Proceedings of the IEEE International Conference on Signal Image Technology and Internet Based Systems (SITIS '08)*, Bali, Indonesia, pp. 701-707.

Ayad, H.G. and Kamel, M.S. (2008), "Cumulative Voting Consensus Method for Partitions with Variable Number of Clusters", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 30 No. 1, pp. 160-173.

Baker, S., Ponniah, D. and Smith, S. (1999), "Risk response techniques employed currently for major projects", *Construction Management and Economics*, Vol. 17, pp. 205-213.

Balepin, I., Maltsev, S., Rowe, J. and Levitt, K. (2003), "Using specification-based intrusion detection for automated response", *Proceedings of the Recent Advances in Intrusion Detection*, Pittsburgh, PA, USA, Vol. 2820, pp. 136-154.

Barker, T.J. and Zabinsky, Z.B. (2011), "A multicriteria decision making model for reverse logistics using analytical hierarchy process", *Omega*, Vol. 39 No. 5, pp. 558-573.

Bejtlich, R. (2004), "*The Tao of Network Security Monitoring: Beyond Intrusion Detection",* Addison Wesley.

Ben-David and Raz, T. (2001), "An integrated approach for risk response development in project planning", *Journal of the Operational Research Society*, Vol. 52, pp. 14-25.

Berander, P. and Jönsson, P. (2006), "Hierarchical Cumulative Voting (HCV) Prioritization of Requirements in Hierarchies", *International Journal of Software Engineering & Knowledge Engineering*, Vol. 16 No. 6, pp. 819-849.

Bhagat, S. and Brickley, J.A. (1984), "Cumulative Voting: The Value of Minority Shareholder Voting Rights", *Journal of Law and Economics*, Vol. 27 No. 2, pp. 339-365.

Blakley, B., McDermott, E. and Geer, D. (2001), "Information security is information risk management", *Proceedings of the 2001 workshop on New security paradigms*, Cloudcroft, New Mexico, pp. 97-104.

Boehm, B.W. and Ross, R. (1989), "Theory-W Software Project Management Principles and Examples", *IEEE Transactions on Software Engineering*, Vol. 15 No. 7, pp. 902-916.

Booch, G., Rumbaugh, J. and Jacobson, I. (2005), "*The Unified Modeling Language User Guide ",* 2nd Edition edition, Addison Wesley Professional.

Butler, S.A. (2002), "Security attribute evaluation method: a cost-benefit approach", *Proceedings of the 24th International Conference on Software Engineering*, Orlando, Florida, pp. 232-240.

Calder, A. and Watkins, S. (2010), "*Information Security Risk Management for ISO27001/ISO27002 ",* IT Governance Publishing.

Campbell, R.P. and Sands, G.A. (1979), "A modular approach to computer security risk management", *Proceedings of the AFIPS Conference*, NY, USA, pp. 293-303.

Carver, C., Hill, J.M., Surdu, J.R. and Pooch, U.W. (2000), "A Methodology for using Intelligent Agents to Provide Automated Intrusion Response", *Proceedings of the IEEE Workshop on Information Assurance and Security*, West Point, NY, pp. 110–116.

Carver, C.A. (2000), *"Intrusion Response Systems: A Survey"*, Department of Computer Science, Texas A&M University.

Carver, C.A. (2001), "*Adaptive Agent-Based Intrusion Response*". PhD Dessertation. Texas A&M University.

Caswell, B. and Beale, J. (2004), "*Snort 2.1 Intrusion Detection"*, 2nd edition, Syngress.

Caswell, B. and Roesch, M. (1998), "Snort: The open source network intrusion detection system", Available at: http://www.snort.org (Accessed: 20 August 2010).

CERT (2009), "OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation", Available at: http://www.cert.org/octave/approach_intro.pdf (Accessed: 14 March 2009).

Chan, J.W.K. and Tong, T.K.L. (2007), "Multi-criteria material selections and end-of-life product strategy: Grey relational analysis approach", *Materials & Design*, Vol. 28 No. 5, pp. 1539-1546.

Chen, C.M., Jeng, B.C., Yang, C.R. and Lai, G.H. (2006), "Tracing denial of service origin: Ant colony approach", *Proceedings of the EvoWorkshops 2006*, Budapest, Hungary, pp. 286-295.

Chu, C.W., Liang, G.S. and Liao, C.T. (2008), "Controlling inventory by combining ABC analysis and fuzzy classification", *Computers & Industrial Engineering*, Vol. 55 No. 4, pp. 841-851.

CIS (2009), *"The CIS Security Metrics: Consensus Metrics Definitions v1.0.0"*, The Center for Internet Security.

CIS (2010), *"The CIS Security Metrics: Consensus Metrics Definitions v1.1.0"*, The Center for Internet Security. Available at: http://benchmarks.cisecurity.org (Accessed: 12th September 2011).

Cisco Systems Inc (2009), "Signature Engines", Available at: http://www.cisco.com/en/US/docs/security/ips/5.1/configuration/guide/idm/dmSgEng.pdf (Accessed: 11 August 2009).

Cisco Systems Inc (2011), "Risk Rating and Threat Rating: Simplify IPS Policy Management", Available at: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/prod_white_paper0900aecd806e7299.html (Accessed: 12th September 2011).

Clark, J.W. and Stavrou, A. (2011), "Breaching & Protecting an Anonymizing Network System", *Proceedings of the 6th Annual Symposium on Information Assurance*, New York, USA, pp. 32-44.

Cohen, F. (1999), "Simulating cyber attacks, defences, and consequences", *Computers & Security*, Vol. 18 No. 6, pp. 479-518.

CORAS (2001), "CORAS - A plattform for Risk Analysis of Security Critical Systems", Available at: http://www2.nr.no/coras/ (Accessed: 16 July 2011).

Covey, S.R. (2004), "*7 Habits of Highly Effective People"*, 15th Anniversary edition, Simon & Schuster Ltd.

CRAMM (1987), "CCTA Risk Analysis and Management Method", Available at: http://www.cramm.com (Accessed: 16 July 2011).

Crawford, G. and Williams, C. (1985), *"The Analysis of Subjective Judgment Matrices (R-2572-1-AF)"*, RAND Corporation.

Cuppens, F. and Miege, A. (2002), "Alert correlation in a cooperative intrusion detection framework", *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, California, USA, pp. 202-215.

DARPA (2011), "DARPA Intrusion Detection Data Sets", Available at: http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/index.html (Accessed: 1 July 2011).

Davis, C., Schiller, M. and Wheeler, K. (2007), "*IT Auditing: Using Controls to Protect Information Assets*", McGraw-Hill.

Debar, H., Dacier, M. and Wespi, A. (1999), "Towards a taxonomy of intrusion-detection systems", *Computer Networks*, Vol. 31 No. 9, pp. 805-822.

Debar, H. and Wespi, A. (2001), "Aggregation and Correlation of Intrusion-Detection Alerts", *Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection*, Davis, CA, USA, pp. 85-103.

Denning, D. (1987a), "An Intrusion-Detection Model", *IEEE Transaction on software engineering*, Vol. 13 No. 2, pp. 222-232.

Denning, D. (1987b), *"A Prototype IDES: A Real Time Intrusion Detection Expert System"*, Technical Report, Computer Science Laboratory, SRI International.

Denning, D.E. and Neumann, P.G. (1985), *"Requirements and Model for IDES - A Real-time Intrusion Detection Expert System"*, Technical Report, CSL, SRI International.

Dondo, M.G. (2008), "A vulnerability prioritization system using a fuzzy risk analysis approach", *Proceedings of the 23rd International Information Security Conference*, Milano, Italy, pp. 525-539.

Dong, Y., Xu, Y., Li, H. and Dai, M. (2008), "A comparative study of the numerical scales and the prioritization methods in AHP", *European Journal of Operational Research*, Vol. 186 No. 1, pp. 229-242.

Dunlap, G.W., King, S.T., Cinar, S., Basrai, M.A. and Chen, P.M. (2002), "ReVirt: enabling intrusion analysis through virtual-machine logging and replay", *SIGOPS Oper. Syst. Rev.*, Vol. 36 No. SI, pp. 211-224.

Ekelhart, A., Fenz, S., Klemen, M. and Weippl, E. (2007), "Security Ontologies: Improving Quantitative Risk Analysis", *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*, Waikoloa, HI, USA, pp. 156-162.

Ekelhart, A., Fenz, S. and Neubauer, T. (2009), "AURUM: A Framework for Information Security Risk Management", *Proceedings of the 42nd Hawaii International Conference on System Sciences*, HI, USA, pp. 1-10.

Esmaili, M., Balachandran, B., Safavi-Naini, R. and Pieprzyk, J. (1996), "Case-based reasoning for intrusion detection", *Proceedings of the 12th Annual Computer Security Applications Conference*, San Diego, CA , USA, pp. 214-223.

Feng, Z., Shijie, Z., Zhiguang, Q. and Jinde, L. (2003), "Honeypot: a supplemented active defense system for network security", *Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies*, Chengdu, China, pp. 231-235.

Fenz, S. and Neubauer, T. (2009), "How to determine threat probabilities using ontologies and Bayesian networks", *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies*, New York, NY, USA, pp. 1-11.

Fessi, B.A., Ben Abdallah, S., Hamdi, M. and Boudriga, N. (2009), "A new genetic algorithm approach for intrusion response system in computer networks", *Proceedings of the IEEE Symposium on Computers and Communications*, Sousse, Tunisia, pp. 342-347.

Fessi, B.A., Hamdi, M., Benabdallah, S. and Boudriga, N. (2007), "A decisional framework system for computer network intrusion detection", *European Journal of Operational Research*, Vol. 177 No. 3, pp. 1824-1838.

FIRST (2011), "CVSS Adopters", Available at: http://www.first.org/cvss/eadopters.html (Accessed: 16 Jun 2011).

Fisch, E.A. (1996), "*Intrusion Damage Control and Assessment: A Taxonomy and Implementation of Automated Responses to Intrusive Behavior"*. Ph.D. Dissertation, Texas A&M U.

Foo, B., Wu, Y.S., Mao, Y.C., Bagchi, S. and Spafford, E. (2005), "ADEPTS: adaptive intrusion response using attack graphs in an e-commerce environment", *Proceedings of the International Conference on Dependable Systems and Networks (DSN 2005)*, Yokohama, Japan, pp. 508-517.

Forman, E.H. and Gass, S.I. (2001), "The Analytic Hierarchy Process--An Exposition", *Operations Research*, Vol. 49 No. 4, pp. 469–487.

Forrest, S., Hofmeyr, S.A., Somayaji, A. and Longstaff, T.A. (1996), "A sense of self for Unix processes", *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA, USA, pp. 120-128.

Fuchsberger, A. (2005), "Intrusion Detection Systems and Intrusion Prevention Systems", *Information Security Technical Report*, Vol. 10 No. 3, pp. 134-139.

Gangadharan, M. and Kai, H. (2001), "Intranet security with micro-firewalls and mobile agents for proactive intrusion response", *Proceedings of the International Conference on Computer Networks and Mobile Computing*, Los Alamitos, CA , USA, pp. 325-332.

GCIA (2011), "GIAC Certified Intrusion Analyst (GCIA)", Available at: http://www.giac.org/certifications/security/gcia.php (Accessed: 1 March 2011).

Gehani, A. and Kedem, G. (2004), "RheoStat: Real-time risk management", *Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection*, Sophia Antipolis, France, pp. 296-314.

Gonzalez, V.M., Galicia, L. and Favela, J. (2008), "Understanding and supporting personal activity management by IT service workers", *Proceedings of the 2nd ACM Symposium on Computer Human Interaction for Management of Information Technology*, San Diego, California, pp. 1-10.

Gregg, M. and Kim, D. (2005), "*Inside Network Security Assessment: Guarding your IT Infrastructure"*, Sams.

Haimes, Y.Y. (2001), "Risk Analysis, Systems Analysis, and Covey's Seven Habits Perspectives", *Risk Analysis*, Vol. 21 No. 2, pp. 217-224.

Haimes, Y.Y. (2009), "*Risk Modeling, Assessment, and Management (Wiley Series in Systems Engineering and Management) ",* 3rd edition, Wiley-Blackwell.

Hamdi, M. and Boudriga, N. (2005), "Computer and network security risk management: Theory, challenges, and countermeasures", *International Journal of Communication Systems*, Vol. 18 No. 8, pp. 763-793.

Han, H., Lu, X.L., Ren, L.Y. and Chen, B. (2006), "Taichi: An Open Intrusion Automatic Response System Based on Plugin", *Proceedings of the International Conference on Machine Learning and Cybernetics*, Dalian, China, pp. 66-77.

Harker, P.T. (1987), "Incomplete pairwise comparisons in the analytic hierarchy process", *Mathematical Modelling*, Vol. 9 No. 11, pp. 837-848.

Haslum, K., Abraham, A. and Knapskog, S. (2007), "DIPS: A Framework for Distributed Intrusion Prediction and Prevention Using Hidden Markov Models and Online Fuzzy Risk Assessment", *Proceedings of the Third International Symposium on Information Assurance and Security*, Trondheim, Norway, pp. 183-190.

Haslum, K. and Årnes, A. (2007), "Multisensor Real-Time Risk Assessment Using Continuous-Time Hidden Markov Models", *Proceedings of the International Conference on Computational Intelligence and Security*, Guangzhou, China, Vol. 4456, pp. 694-703.

Hausrath, N.L. (2011), "*Methods for Hospital Network and Computer Security"*. M.Sc. University of Cincinnati.

Herman, M.W. and Koczkodaj, W.W. (1996), "A Monte Carlo study of pairwise comparison", *Journal Information Processing Letters*, Vol. 57 No. 1, pp. 25-29.

Herrmann, A. and Daneva, M. (2008), *"Requirements Prioritization Based on Benefit and Cost Prediction: A Method Classification Framework"*, Technical Report, Software Engineering Group, University of Heidelberg.

Heyman, T., Scandariato, R., Huygens, C. and Joosen, W. (2008), "Using Security Patterns to Combine Security Metrics", *Proceedings of the 3rd International Conference on Availability, Reliability and Security (ARES 08)*, Barcelona, Spain, pp. 1156-1163.

Hillson, D. (1999), "Developing Effective Risk Responses", *Proceedings of the 30th Annual Project Management Institute 1999 Seminars & Symposium*, Philadelphia, Pennsylvania, USA.

Hillson, D. (2002), "Extending the risk process to manage opportunities", *International Journal of Project Management*, Vol. 20 No. 3, pp. 235-240.

Hofmeyr, S.A., Forrest, S. and Somayaji, A. (1998), "Intrusion detection using sequences of system calls", *Journal of Computer Security*, Vol. 6 No. 3, pp. 151-180.

Houmb, S.H. and Franqueira, V.N.L. (2009), "Estimating ToE Risk Level Using CVSS", *Proceedings of the International Conference on Availability, Reliability and Security (ARES '09)*, Fukuoka, Japan, pp. 718-725.

Houmb, S.H., Franqueira, V.N.L. and Engum, E.A. (2009), "Quantifying security risk level from CVSS estimates of frequency and impact", *Journal of Systems and Software*, Vol. 83. No. 9, pp. 1622-1634.

Huang, P.C., Tong, L.I., Chang, W.W. and Yeh, W.C. (2011), "A two-phase algorithm for product part change utilizing AHP and PSO", *Expert Systems with Applications*, Vol. 38 No. 7, pp. 8458-8465.

IEC (2006), *"IEC 60812: Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)"*, International Electrotechnical Commission. Available at: http://webstore.iec.ch/preview/info_iec60812%7Bed2.0%7Den_d.pdf (Accessed: 16 July 2011).

Jackson, K. (1999), *"Intrusion detection system product survey"*, Technical Report LA-UR-99-3883, Los Alamos National Laboratory.

Jang, H. and Kim, S. (2002), "Real-time intruder tracing through self-replication", *Proceedings of the 5th International Information Security Conference (ISC)*, Sao Paulo, Brazil, pp. 1-16.

Kaplan, S. (1997), "The Words of Risk Analysis", *Risk Analysis*, Vol. 17 No. 4, pp. 407-417.

Kaplan, S. and Garrick, B.J. (1981), "On The Quantitative Definition of Risk", *Risk Analysis*, Vol. 1 No. 1, pp. 11-27.

Karlsson, J., Wohlin, C. and Regnell, B. (1998), "An evaluation of methods for prioritizing software requirements", *Information and Software Technology*, Vol. 39, pp. 939-947.

Karlsson, L., Höst, M. and Regnell, B. (2006), "Evaluating the practical use of different measurement scales in requirements prioritisation", *Proceedings of the 2006 ACM/IEEE International Symposium on Empirical Software Engineering*, Rio de Janeiro, Brazil, pp. 326-335.

Karlsson, L., Thelin, T., Regnell, B., Berander, P. and Wohlin, C. (2007), "Pair-wise comparisons versus planning game partitioning--experiments on requirements prioritisation techniques", *Empirical Software Engineering*, Vol. 12 No. 1, pp. 3-33.

Kheir, N., Cuppens-Boulahia, N., Cuppens, F. and Debar, H. (2010), "A service dependency model for cost-sensitive intrusion response", *Proceedings of the 15th European Conference on Research in Computer Security*, Athens, Greece, pp. 626-642.

Kruegel, C., Valeur, F. and Vigna, G. (2004), "*Intrusion Detection and Correlation: Challenges and Solutions"*, University of California, Santa Barbara: Springer.

Kumar, S. and Spafford, E.H. (1994), *"A Pattern Matching Model for Misuse Intrusion Detection"*, Computer Science Technical Reports, Purdue University. Available at: http://docs.lib.purdue.edu/cstech/1170/ (Accessed: 10 June 2009).

Kwon, M., Jeong, K. and Lee, H. (2008), "PROBE: A Process Behavior-Based Host Intrusion Prevention System", *Proceedings of the 4th International Conference on Information Security Practice and Experience*, Sydney, Australia, Vol. 4991, pp. 203-217.

Lai, Y.P. and Hsia, P.L. (2007), "Using the vulnerability information of computer systems to improve the network security", *Computer Communications*, Vol. 30 No. 9, pp. 2032-2047.

Lazarevic, A., Ozgur, A., Ertoz, L., Srivastava, J. and Kumar, V. (2003), "A comparative study of anomaly detection schemes in network intrusion detection", *Proceedings of the 3rd SIAM International Conference on Data Mining*, San Francisco, CA, USA, pp. 25-36.

Lee, W., Fan, W., Miller, M., Stolfo, S.J. and Zadok, E. (2002), "Toward cost-sensitive modeling for intrusion detection and response", *Journal of Computer Security*, Vol. 10 No. 1-2, pp. 5-22.

Lee, W. and Qin, X. (2003), "Statistical causality analysis of INFOSEC alert data", *Proceedings of the Recent Advances in Intrusion Detection*, Pittsburgh, PA, USA, Vol. 2820/2003, pp. 73-93.

Leffingwell, D. and Widrig, D. (2003), "*Managing Software Requirements: A Use Case Approach",* Addison-Wesley Professional.

Lewandowski, S.M., Van Hook, D.J., O'Leary, G.C., Haines, J.W. and Rossey, L.M. (2001), "SARA: Survivable Autonomic Response Architecture", *Proceedings of the DARPA Information Survivability Conference & Exposition II (DISCEX '01)*, Anaheim, California, Vol. 1, pp. 77-88.

Libeau, F. (2008), "Automating security events management", *Network Security*, Vol. 2008 No. 12, pp. 6-9.

Lin, C.H., Chen, C.H. and Laih, C.S. (2008), "A Study and Implementation of Vulnerability Assessment and Misconfiguration Detection", *Proceedings of the IEEE Asia-Pacific Services Computing Conference (APSCC '08)*, Yilan, Taiwan, pp. 1252-1257.

Lunt, T.F., Tamaru, A., Gilham, F., Jagannathan, R., Jalali, C. and Neumann, P.G. (1989), *"A real-time intrusion-detection expert system (IDES)",* SRI International. Available at: http://www.csl.sri.com/papers/9sri/9sri.pdf (Accessed: 10 June 2009).

Lye, K. and Wing, J.M. (2005), "Game strategies in network security", *International Journal of Information Security*, Vol. 4 No. 1, pp. 71-86.

Manktelow, J. (2003), "*Mind Tools Practical Thinking Skills for an Excellent Life!",* 1st edition, West Sussex: Mind Tools Ltd.

McHugh, J., Christie, A. and Allen, J. (2000), "Defending yourself: the role of intrusion detection systems", *IEEE Software*, Vol. 17 No. 5, pp. 42-51.

Mell, P., Scarfone, K. and Romanosky, S. (2006), "Common Vulnerability Scoring System", *IEEE Security & Privacy*, Vol. 4 No. 6, pp. 85-89.

Mell, P., Scarfone, K. and Romanosky, S. (2009), "A Complete Guide to the Common Vulnerability Scoring System Version 2.0", Available at: http://www.first.org/cvss/cvss-guide.html (Accessed: 14 January 2009).

Miller, D.R., Harris, S., Harper, A., Vandyke, S. and Blask, C. (2010), "*Security Information and Event Management (SIEM) Implementation",* 1st Edition edition, McGraw-Hill Osborne.

Mu, C. and Li, Y. (2010), "An intrusion response decision-making model based on hierarchical task network planning", *Expert Systems with Applications*, Vol. 37 No. 3, pp. 2465-2472.

Mu, C.P., Li, X.J., Huang, H.K. and Tian, S.F. (2008), "Online Risk Assessment of Intrusion Scenarios Using D-S Evidence Theory", *Proceedings of the 13th European Symposium on Research in Computer Security*, Malaga, Spain, pp. 35-48.

Mukherjee, B., Heberlein, L.T. and Levitt, K.N. (1994), "Network intrusion detection", *IEEE Network*, Vol. 8 No. 3, pp. 26-41.

Munteanu, A.B. (2006), "Information Security Risk Assessment: The Qualitative Versus Quantitative Dilemma", *Proceedings of the 6th International Business Information Management Association (IBIMA) Conference*, Bonn, Germany, pp. 227-232.

MyCERT (2011), "Malaysian Computer Emergency Response Team", Available at: http://www.mycert.org.my/en/ (Accessed: 16 July 2011).

MySQL (2011), "MySQL: An open source database software", Available at: http://www.mysql.com/ (Accessed: 10 April 2011).

Neumann, P.G. and Parker, D.B. (1989), "A summary of computer misuse techniques", *Proceedings of the 12th National Computer Security Conference*, Baltimore, Maryland, pp. 396-407.

Nicol, D.M., Sanders, W.H. and Trivedi, K.S. (2004), "Model-based evaluation: from dependability to security", *IEEE Transactions on Dependable and Secure Computing*,, Vol. 1 No. 1, pp. 48-65.

Nicolett, M. and Kavanagh, K. (2009), *"Magic Quadrant for Security Information and Event Management"*, Gartner RAS Core Research Note G00167782.

Ning, P., Cui, Y. and Reeves, D.S. (2002), "Analyzing intensive intrusion alerts via correlation", *Proceedings of the 5th International Symposium Recent Advances in Intrusion Detection (RAID 2002)*, Zurich, Switzerland, pp. 74-94.

Ning, P., Cui, Y., Reeves, D.S. and Xu, D. (2004), "Techniques and tools for analyzing intrusion alerts", *ACM Transactions on Information System Security*, Vol. 7 No. 2, pp. 274-318.

Ning, P., Reeves, D.S. and Cui, Y. (2001), *"Correlating Alerts Using Prerequisites of Intrusions"*, Technical Report TR-2001-13, North Carolina State University, Department of Computer Science.

NIST (2009), *"Information Security"*, National Institute of Standards and Technology. Available at: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf (Accessed: 16 July 2011).

NIST (2011), "National Vulnerability Database version 2.0", Available at: http://nvd.nist.gov/ (Accessed: 1 April 2011).

Noel, S. and Jajodia, S. (2008), "Optimal IDS Sensor Placement and Alert Prioritization Using Attack Graphs", *Journal of Network and Systems Management*, Vol. 16 No. 3, pp. 259-275.

Pak, C. and Cannady, J. (2009), "Asset priority risk assessment using hidden markov models", *Proceedings of the 10th ACM conference on SIG-information technology education*, Fairfax, Virginia, USA, pp. 65-73.

Papadaki, M. (2004), "*Classifying and Responding to Network Intrusions*". PhD. University of Plymouth.

Papadaki, M. and Furnell, S. (2004), "IDS or IPS: what is best?", *Network Security*, Vol. 2004 No. 7, pp. 15-19.

Papadaki, M. and Furnell, S.M. (2005), "Informing the decision process in an automated intrusion response system", *Information Security Technical Report*, Vol. 10 No. 3, pp. 150-161.

Patel, A., Qassim, Q. and Wills, C. (2010), "A survey of intrusion detection and prevention systems", *Information Management & Computer Security*, Vol. 18 No. 4, pp. 277-290.

Paulson, L.D. (2002), "Stopping intruders outside the gates", *Computer*, Vol. 35 No. 11, pp. 20-22.

PHP (2011), "PHP: Hypertext Preprocessor", Available at: http://www.php.net/ (Accessed: 10 April 2011).

Porras, P.A., Fong, M.W. and Valdes, A. (2002), "A mission-impact-based approach to INFOSEC alarm correlation", *Proceedings of the 5th International Symposium Recent Advances in Intrusion Detection*, Zurich, Switzerland, Vol. 2516, pp. 95-114.

Porras, P.A. and Neumann, P.G. (1997), "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances", *Proceedings of the 20th NIST-NCSC National Information Systems Security Conference*, Baltimore, MD, pp. 353-365.

PricewaterhouseCoopers (2008), *"Information Security Breaches Survey 2008 - Technical Report"*, Department for Business Enterprise and Regulatory Reform. Available at: http://www.pwc.co.uk/pdf/BERR_ISBS_2008(sml).pdf (Accessed: 16 November 2009).

PricewaterhouseCoopers (2010), *"Information Security Breaches Survey 2010 - Technical Report"*. Available at: http://www.pwc.co.uk/eng/publications/isbs_survey_2010.html (Accessed: 16 July 2011).

Ragsdale, D.J., Carver, C.A., Jr., Humphries, J.W. and Pooch, U.W. (2000), "Adaptation techniques for intrusion detection and intrusion response systems", *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics*, Nashville, Tennessee, USA, Vol. 4, pp. 2344-2349.

Richardson, R. (2011), *"2010/2011 Computer Crime and Security Survey"*, Computer Security Institute. Available at: http://analytics.informationweek.com/abstract/21/7377/Security/research-2010-2011-csi-survey.html (Accessed: 14 July 2011).

Rogers, R., Fuller, E., Miles, G. and Cunningham, B. (2005), "*Network Security Evaluation Using the NSA IEM "*, Syngress.

Roy, B. (1991), "The outranking approach and the foundations of ELECTRE methods", *Theory and Decision*, Vol. 31 No. 1, pp. 49-73.

Saaty, T.L. (2008a), "Decision making with the analytic hierarchy process", *International Journal of Services Sciences*, Vol. 1 No. 1, pp. 83-98.

Saaty, T.L. (2008b), "Relative Measurement and Its Generalization in Decision Making Why Pairwise Comparisons are Central in Mathematics for the Measurement of Intangible Factors The Analytic Hierarchy/Network Process", *RACSAM. Rev. R. Acad. Cien. Serie A. Mat*, Vol. 102 No. 2, pp. 251-318.

Savola, R.M. and Abie, H. (2009), "Identification of Basic Measurable Security Components for a Distributed Messaging System", *Proceedings of the 3rd International Conference on Emerging Security Information, Systems and Technologies (SECURWARE '09)*, Athens, Greece, pp. 121-128.

Schouwenberg, R. (2008), "Attacks on banks", Available at: http://www.viruslist.com/en/analysis?pubid=204792037 (Accessed: 18 October 2008).

Schultz, E.E. (2002), "A framework for understanding and predicting insider attacks", *Computers & Security*, Vol. 21 No. 6, pp. 526-531.

SECTOOLS (2010), "Top 5 Intrusion Detection Systems", Available at: http://sectools.org/ids.html (Accessed: 1 May 2010).

Secunia (2011), "Terminology : Explanation of terms used in Secunia Advisories.", Available at: http://secunia.com/community/advisories/terminology/ (Accessed: 1 March 2011).

Sherif, J.S., Ayers, R. and Dearmond, T.G. (2003), "Intrusion detection: the art and the practice. Part I", *Information Management & Computer Security*, Vol. 11, pp. 175-186.

Sherif, J.S. and Dearmond, T.G. (2002), "Intrusion detection: systems and models", *Proceedings of the 11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE 2002)*, Pittsburgh, PA, USA, pp. 115-133.

Smaha, S.E. (1988), "Haystack: an intrusion detection system", *Proceedings of the Fourth Aerospace Computer Security Applications Conference*, Orlando, FL , USA pp. 37-44.

Snorby (2011), "Snorby - All about Simplicity", Available at: http://snorby.org/ (Accessed: 11 July 2011).

Stakhanova, N., Basu, S. and Wong, J. (2007a), "A Cost-Sensitive Model for Preemptive Intrusion Response Systems", *Proceedings of the 21st International Conference on Advanced Information Networking and Applications (AINA '07)*, Niagara Falls, Canada, pp. 428-435.

Stakhanova, N., Basu, S. and Wong, J. (2007b), "A taxonomy of intrusion response systems", *International Journal of Information and Computer Security*, Vol. 1 No. 1/2, pp. 169-184.

Stakhanova, N., Strasburg, C., Basu, S. and Wong, J.S. (2008), "On Evaluation of Response Cost for Intrusion Response Systems", *Proceedings of the 11th international symposium on Recent Advances in Intrusion Detection*, Cambridge, MA, USA, pp. 290-291.

Stankovic, J.A. (1988), "Misconceptions about real-time computing: a serious problem for next-generation systems", *Computer*, Vol. 21 No. 10, pp. 10-19.

Stevens, S.S. (1946), "On the Theory of Scales of Measurement", *Science*, Vol. 103 No. 2684, pp. 677-680.

Stoneburner, G., Goguen, A. and Feringa, A. (2002), *"Risk Management Guide for Information Technology Systems"*, National Institute of Standards and Technology. Available at: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (Accessed: 16 July 2011).

Strasburg, C., Stakhanova, N., Basu, S. and Wong, J.S. (2009a), "A Framework for Cost Sensitive Assessment of Intrusion Response Selection", *Proceedings of the 33rd Annual IEEE International Computer Software and Applications Conference*, Seattle, Washington, USA, Vol. 1, pp. 355-360.

Strasburg, C., Stakhanova, N., Basu, S. and Wong, J.S. (2009b), "Intrusion response cost assessment methodology", *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, Sydney, Australia, pp. 388-391.

Subramanian, D., Le, H.T. and Loh, P.K.K. (2009), "Fuzzy Heuristic Design for Diagnosis of Web-Based Vulnerabilities", *Proceedings of the 4th International Conference on Internet Monitoring and Protection (ICIMP '09)*, Venice, Italy, pp. 103-108.

Symantec (2006), "Symantec DeepSight Threat Ratings Guide", Available at: ftp://ftp.symantec.com/public/english_us_canada/products/deepsight_alert_svcs/7.0/manuals/DS-threat-ratings-guide-2006.pdf (Accessed: 1 March 2011).

Symantec (2009), *"Symantec Internet Security Threat Report Trends for 2008 Volume XIV"*, Symantec Corporation. Available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf (Accessed: 16 November 2009).

Symantec (2010), "Symantec Product Vulnerability Management Process", Available at: http://www.symantec.com/security/Symantec-Product-Vulnerability-Response.pdf (Accessed: 1 March 2011).

Symantec (2011), *"Symantec Internet Security Threat Report - Trends for 2010"*. Available at: http://www.symantec.com/business/threatreport/index.jsp (Accessed: 16 July 2011).

Tcpreplay (2011), "Tcpreplay: Pcap Editing and Replay Tools for *NIX", Available at: http://tcpreplay.synfin.net/ (Accessed: 1 April 2011).

Teng, H.S., Chen, K. and Lu, S.C. (1990), "Security audit trail analysis using inductively generated predictive rules", *Proceedings of the 6th Conference on Artificial Intelligence Applications*, pp. 24-29.

Thames, J.L., Abler, R. and Keeling, D. (2008a), "A distributed active response architecture for preventing SSH dictionary attacks", *Proceedings of the IEEE Southeastcon 2008*, Huntsville, Alabama, Vol. 1 and 2, pp. 84-89.

Thames, J.L., Abler, R. and Keeling, D. (2008b), "A Distributed Firewall and Active Response Architecture Providing Preemptive Protection", *Proceedings of the 46th ACM Southeast Conference 2008*, Auburn, AL, USA, pp. 220-225.

Thurstone, L.L. (1927), "A law of comparative judgement", *Psychological Review*, Vol. 34 No. 4, pp. 273-286.

Tian, Z., Zhang, W., Ye, J., Yu, X. and Zhang, H. (2008), "Reduction of False Positives in Intrusion Detection via Adaptive Alert Classifier", *Proceedings of the IEEE International Conference on Information and Automation*, Changsha, China, pp. 1599-1602.

Tjhai, G.C. (2011), "*Anomaly-based Correlation of IDS Alarms"*. PhD. University of Plymouth.

Tjhai, G.C., Furnell, S.M., Papadaki, M. and Clarke, N.L. (2010), "A preliminary two-stage alarm correlation and filtering system using SOM neural network and K-means algorithm", *Computers & Security*, Vol. 29 No. 6, pp. 712-723.

Tjhai, G.C., Papadaki, M., Furnell, S.M. and Clarke, N.L. (2008a), "Investigating the problem of IDS false alarms: An experimental study using Snort", *Proceedings of the IFIP TC 11 23rd International Information Security Conference*, Milano, Italy, Vol. 278, pp. 253-267.

Tjhai, G.C., Papadaki, M., Furnell, S.M. and Clarke, N.L. (2008b), "The Problem of False Alarms: Evaluation with Snort and DARPA 1999 Dataset", *Proceedings of the 5th International Conference on Trust, Privacy and Security in Digital Business*, Turin, Italy, pp. 139-150.

Toth, T. and Kruegel, C. (2002), "Evaluating the impact of automated intrusion response mechanisms", *Proceedings of the 18th Annual Computer Security Applications Conference*, Las Vegas, Nevada, pp. 301-310.

US-CERT (2011), "Vulnerability Notes Database Field Descriptions", Available at: http://www.kb.cert.org/vuls/html/fieldhelp#metric (Accessed: 1 March 2011).

Valdes, A. and Skinner, K. (2001), "Probabilistic Alert Correlation", *Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection*, Davis, CA, USA, pp. 54-68.

Verwoerd, T. and Hunt, R. (2002), "Intrusion detection techniques and approaches", *Computer Communications*, Vol. 25 No. 15, pp. 1356-1365.

Vigna, G. and Kemmerer, R.A. (1998), "NetSTAT: a network-based intrusion detection approach", *Proceedings of the 14th Annual Computer Security Applications Conference*, Scottsdale, Arizona, USA, pp. 25-34.

Wagner, D. and Soto, P. (2002), "Mimicry attacks on host-based intrusion detection systems", *Proceedings of the 9th ACM conference on Computer and communications security*, Washington, DC, USA, pp. 255-264.

Wang, C. and Wulf, W.A. (1997), "Towards A Framework for Security Measurement", *Proceedings of the 20th National Information Systems Security Conference*, Baltimore, MD, USA, pp. 522-533.

Wang, H.Q., Wang, G.F., Lan, Y., Wang, K. and Liu, D.X. (2006), "A new automatic intrusion response taxonomy and its application", *Proceedings of the 8th Asia-Pacific Web Conference and Workshops (APWeb 2006)*, Harbin, People R China, pp. 999-1003.

Wang, S.H., Tseng, C.H., Levitt, K. and Bishop, M. (2007), "Cost-sensitive intrusion responses for mobile ad hoc networks", *Proceedings of the Recent Advances in Intrusion Detection*, Gold Goast, Australia, Vol. 4637, pp. 127-145.

Wang, X., Reeves, D.S., Wu, S.F. and Yuill, J. (2001a), "Sleepy Watermark Tracing: An Active Network-Based Intrusion Response Framework", *Proceedings of the IFIP TC11 Sixteenth Annual Working Conference on Information Security*, Paris, France, Vol. 193, pp. 369 - 384.

Wang, X.Y., Reeves, D.S. and Wu, S.F. (2001b), "Tracing Based Active Intrusion Response", *Journal of Information Warefare*, Vol. 1 No. 1, pp. 50–61.

White, G.B., Fisch, E.A. and Pooch, U.W. (1996), "Cooperating security managers: A peer-based intrusion detection system", *IEEE Network*, Vol. 10 No. 1, pp. 20-23.

Wiegers, K.E. (1999), "*Software Requirements*", Redmont, Washington: Microsoft Press.

Wotring, B. (2005), "*Host integrity monitoring: using Osiris and Samhain*", Syngress.

Wu, X., Fu, Y. and Wang, J. (2009), "Information systems security risk assessment on improved fuzzy AHP", *Proceedings of the ISECS International Colloquium on Computing, Communication, Control, and Management*, Sanya, China, Vol. 4, pp. 365-369.

Wu, Y.S., Foo, B., Mao, Y.C., Bagchi, S. and Spafford, E.H. (2007), "Automated adaptive intrusion containment in systems of interacting services", *Computer Networks*, Vol. 51 No. 5, pp. 1334-1360.

Wu, Z., Xiao, D., Xu, H., Peng, X. and Zhuang, X. (2008), "Automated Intrusion Response Decision Based on the Analytic Hierarchy Process", *Proceedings of the IEEE International Symposium on Knowledge Acquisition and Modeling Workshop*, Beijing, China, pp. 574-577.

Xi, Z., Chen, H., Wang, X., Sheng, J. and Fan, Y. (2009), "Evaluation Model for Computer Network Information Security Based on Analytic Hierarchy Process", *Proceedings of the 3rd International Symposium on Intelligent Information Technology Application*, NanChang, China, Vol. 3, pp. 186-189.

Xiao, S.S., Zhang, Y.G., Liu, X.J. and Gao, J.J. (2008), "Alert Fusion Based on Cluster and Correlation Analysis", *Proceedings of the International Conference on Convergence and Hybrid Information Technology*, Daejeon, South Korea, pp. 163-168.

Xu, D. and Ning, P. (2005), "Privacy-preserving alert correlation: a concept hierarchy based approach", *Proceedings of the 21st Annual Computer Security Applications Conference,* Tucson, AZ, pp. 537-546.

Xu, X. (2001), "The SIR method: A superiority and inferiority ranking method for multiple criteria decision making", *European Journal of Operational Research*, Vol. 131 No. 3, pp. 587-602.

Yoo, S. (2010), "*Machine Learning Methods for Personalized Email Prioritization"*. PhD. Carnegie Mellon University.

Young, G. and Pescatore, J. (2009), *"Magic Quadrant for Network Intrusion Prevention System Appliances",* Gartner RAS Core Research Note G00167309.

Yu, D. and Frincke, D. (2005), "Alert confidence fusion in intrusion detection systems with extended Dempster-Shafer theory", *Proceedings of the 43rd annual Southeast regional conference*, Kennesaw, Georgia, Vol. 2, pp. 142-147.

Yu, J., Reddy, Y.V.R., Selliah, S., Kankanahalli, S., Reddy, S. and Bharadwaj, V. (2004), "A collaborative architecture for intrusion detection systems with intelligent agents and knowledge-based alert evaluation", *Proceedings of the 8th International Conference on Computer Supported Cooperative Work in Design*, Xiamen, China, Vol. 2, pp. 271-276.

Yu, S. and Rubo, Z. (2008), "Automatic intrusion response system based on aggregation and cost", *Proceedings of the International Conference on Information and Automation (ICIA)*, Hunan, China, pp. 1783-1786.

Yue, W.T. and Cakanyildirim, M. (2007), "Intrusion prevention in information systems: Reactive and proactive responses", *Journal of Management Information Systems*, Vol. 24, pp. 329-353.

Zahedi, F. (1986), "The Analytic Hierarchy Process: A Survey of the Method and Its Applications", *Interfaces*, Vol. 16 No. 4, pp. 96-108.

Zhang, Z., Abdesselam, F.N., Lin, X. and Ho, P.H. (2008), "A model-based semi-quantitative approach for evaluating security of enterprise networks", *Proceedings of the 2008 ACM symposium on Applied computing*, Fortaleza, Ceara, Brazil, pp. 1069-1074.

Zhang, Z., Ho, P. and He, L. (2009), "Measuring IDS-estimated attack impacts for rational incident response: A decision theoretic approach", *Computers & Security*, Vol. 28 No. 7, pp. 605-614.

Zhang, Z., Lin, X. and Ho, P.H. (2007), "Measuring Intrusion Impacts for Rational Response: A State-based Approach", *Proceedings of the 2nd International Conference on Communications and Networking in China (CHINACOM '07)*, Kunming, China, pp. 317-321.

Zonouz, S.A., Khurana, H., Sanders, W.H. and Yardley, T.M. (2009), "RRE: A game-theoretic intrusion Response and Recovery Engine", *Proceedings of the IEEE/IFIP International Conference on Dependable Systems & Networks*, Lisbon, Portugal, pp. 439-448.

Appendix A

Results of the first stage of the evaluation study

Appendix A extends the experimental results in the first stage of the evaluation study (see *Section 5.2*). There were two experiments conducted in the first stage and their full results as follows.

A.1 Full result of the incident risk index and its position for Experiment 1 (Using similar weight of indicators)

							Time Interval																							
Phase	Incident's Signature	No. of Incidents	Time		Risk Index		09:51:35		09:52:00		10:08:06		10:18:06		10:33:09		10:35:01		10:50:00		10:50:54		11:26:14		11:34:21		12:23:39		12:35:48	
			Min	Max	Min	Max	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High
Pre 1	ATTACK-RESPONSES directory listing	3	09:29:20	09:29:24	0.1725	0.1725	21	19	59	57	77	75	265	263	265	263	316	314	316	314	320	318	324	322	331	329	331	329	331	329
	FTP Bad login	1	09:32:34	09:32:34	0.3142	0.3142	1	1	4	4	4	4	114	114	114	114	149	149	149	149	149	149	153	153	153	153	153	153	153	153
	TELNET login incorrect	3	09:32:34	09:45:36	0.1561	0.1764	23	18	61	56	79	74	299	262	299	262	358	313	364	313	368	317	372	321	379	328	381	328	383	328
	ATTACK-RESPONSES Invalid URL	1	09:37:05	09:37:05	0.1442	0.1442	24	24	62	62	80	80	308	308	308	308	367	367	385	385	389	389	393	393	400	400	402	402	404	404
	ATTACK-RESPONSES 403 Forbidden	1	09:45:34	09:45:34	0.1429	0.1429	25	25	63	63	81	81	309	309	309	309	368	368	386	386	390	390	394	394	401	401	403	403	405	405
	ICMP Echo Reply	8	09:45:37	09:45:37	0.1990	0.1990	9	2	41	34	59	52	208	201	208	201	251	244	251	244	255	248	259	252	266	259	266	259	266	259
	ICMP PING	8	09:45:37	09:45:37	0.1970	0.1970	17	10	49	42	67	60	216	209	216	209	259	252	259	252	263	256	267	260	274	267	274	267	274	267
1	**ICMP Echo Reply**	**20**	**09:51:36**	**09:52:00**	**0.0939**	**0.3542**			**65**	**2**	**86**	**2**	**317**	**66**	**321**	**66**	**385**	**95**	**413**	**95**	**423**	**95**	**435**	**99**	**1014**	**99**	**1042**	**99**	**1056**	**99**
	ICMP PING	**20**	**09:51:36**	**09:52:00**	**0.0942**	**0.3542**			**64**	**1**	**85**	**1**	**316**	**65**	**320**	**65**	**384**	**94**	**412**	**94**	**422**	**94**	**434**	**98**	**1013**	**98**	**1041**	**98**	**1055**	**98**
Pre 2	ATTACK-RESPONSES Invalid URL	1	09:52:10	09:52:10	0.1135	0.1135					84	84	315	315	315	315	376	376	398	398	408	408	415	415	422	422	450	450	464	464
	ATTACK-RESPONSES 403 Forbidden	2	09:54:45	09:58:36	0.1345	0.1345					83	82	311	310	311	310	372	371	392	391	396	395	401	400	408	407	412	411	414	413
	ICMP Echo Reply	9	10:01:41	10:01:41	0.2031	0.2031					42	34	191	183	191	183	234	226	234	226	238	230	242	234	249	241	249	241	249	241
	ICMP PING	9	10:01:41	10:01:41	0.2013	0.2013					51	43	200	192	200	192	243	235	243	235	247	239	251	243	258	250	258	250	258	250
2	ICMP Destination Unreachable Port Unreachable	72	10:08:07	10:18:05	0.2100	0.3235							153	69	153	69	196	104	196	104	200	104	204	108	211	108	211	108	211	108
	RPC portmap sadmind request UDP	**76**	**10:08:07**	**10:18:05**	**0.0802**	**0.3412**							**329**	**68**	**333**	**68**	**397**	**103**	**425**	**103**	**435**	**103**	**447**	**107**	**1026**	**107**	**1054**	**107**	**1068**	**107**
	RPC portmap Solaris sadmin port query udp request	**76**	**10:08:07**	**10:18:05**	**0.2802**	**0.5412**							**141**	**1**	**141**	**1**	**184**	**7**	**184**	**7**	**188**	**7**	**192**	**7**	**196**	**7**	**196**	**7**	**196**	**7**
	ICMP Echo Reply	8	10:11:05	10:11:05	0.1612	0.1612							298	291	298	291	349	342	349	342	353	346	357	350	364	357	366	359	366	359
	ICMP PING	8	10:11:05	10:11:05	0.1529	0.1529							307	300	307	300	366	359	375	368	379	372	383	376	390	383	392	385	394	387
	TELNET login incorrect	3	10:15:28	10:17:38	0.1302	0.1303							314	312	314	312	375	373	397	395	407	405	414	412	421	419	437	435	447	445
Pre 3	ATTACK-RESPONSES directory listing	4	10:22:43	10:31:30	0.1061	0.1061									319	316	380	377	408	405	418	415	430	427	437	434	465	462	479	476
3	**RPC portmap sadmind request UDP**	**14**	**10:33:10**	**10:34:59**	**0.1959**	**0.3462**											**267**	**97**	**267**	**97**	**271**	**97**	**275**	**101**	**282**	**101**	**282**	**101**	**282**	**101**
	RPC portmap Solaris sadmin port query udp portmapper sadmin port query attempt	**14**	**10:33:10**	**10:34:59**	**0.3799**	**0.5303**											**69**	**8**	**69**	**8**	**69**	**8**	**73**	**8**	**73**	**8**	**73**	**8**	**73**	**8**
	RPC portmap Solaris sadmin port query udp request	**14**	**10:33:10**	**10:34:59**	**0.3959**	**0.5462**											**22**	**1**	**22**	**1**	**22**	**1**	**26**	**1**	**26**	**1**	**26**	**1**	**26**	**1**
	RPC sadmind query with root credentials attempt UDP	**14**	**10:33:10**	**10:34:59**	**0.1573**	**0.3076**											**357**	**150**	**357**	**150**	**361**	**150**	**365**	**154**	**372**	**154**	**374**	**154**	**376**	**154**
	TELNET login incorrect	4	10:33:18	10:34:57	0.1363	0.2865											370	171	388	171	392	171	396	175	403	175	407	175	409	175
	ATTACK-RESPONSES directory listing	3	10:33:33	10:34:09	0.1061	0.1061											383	381	411	409	421	419	433	431	440	438	468	466	482	480
	SQL version overflow attempt	1	10:34:57	10:34:57	0.4679	0.4679											14	14	14	14	14	14	18	18	18	18	18	18	18	18
Pre 4	ATTACK-RESPONSES directory listing	6	10:36:29	10:43:57	0.1090	0.1090													404	399	414	409	426	421	433	428	461	456	475	470
	TELNET login incorrect	2	10:36:34	10:46:04	0.1361	0.1362													390	389	394	393	398	397	405	404	409	408	411	410
	ATTACK-RESPONSES 403 Forbidden	2	10:46:28	10:46:28	0.1315	0.1315													394	393	404	403	411	410	418	417	434	433	441	440
	ICMP Echo Reply	9	10:49:00	10:49:18	0.1469	0.1511													384	376	388	380	392	384	399	391	401	393	403	395
	ICMP PING	9	10:49:00	10:49:18	0.1550	0.1571													367	358	371	362	375	366	382	373	384	375	386	377
4	**RSERVICES rsh root**	**8**	**10:50:02**	**10:50:38**	**0.1334**	**0.2835**															**400**	**173**	**405**	**177**	**412**	**179**	**416**	**179**	**418**	**179**
	ATTACK-RESPONSES 403 Forbidden	**2**	**10:50:15**	**10:50:54**	**0.1318**	**0.1323**															**402**	**401**	**409**	**408**	**416**	**415**	**420**	**419**	**427**	**426**
Pre 5	ATTACK-RESPONSES 403 Forbidden	2	10:58:16	11:00:32	0.1327	0.1331																	407	406	414	413	418	417	420	419
	TELNET login incorrect	1	11:00:11	11:00:11	0.1355	0.1355																	399	399	406	406	410	410	412	412
	ATTACK-RESPONSES directory listing	4	11:00:16	11:03:33	0.1109	0.1109																	420	417	427	424	455	452	469	466
	ICMP Destination Unreachable Port Unreachable	4	11:03:38	11:04:13	0.5067	0.5067																	17	14	17	14	17	14	17	14
	ATTACK-RESPONSES Invalid URL	1	11:05:11	11:05:11	0.1116	0.1116																	416	416	423	423	451	451	465	465
5	**(snort decoder) Bad Traffic Loopback IP**	**572**	**11:27:51**	**11:27:56**	**0.0984**	**0.1027**																			**1012**	**441**	**1040**	**469**	**1054**	**483**
	SNMP AgentX/tcp request	3	11:27:54	11:27:55	0.2349	0.2366																			199	197	199	197	199	197
	ICMP Echo Reply	1	11:28:18	11:28:18	0.2857	0.2857																			177	177	177	177	177	177
	ICMP PING	1	11:28:18	11:28:18	0.2838	0.2838																			178	178	178	178	178	178
	ICMP PING *NIX	1	11:28:18	11:28:18	0.2811	0.2811																			184	184	184	184	184	184
	ICMP PING BSDtype	1	11:28:18	11:28:18	0.2811	0.2811																			183	183	183	183	183	183
Post 5	TELNET login incorrect	4	11:39:07	12:33:25	0.1578	0.1702																					358	356	368	356
	ICMP Echo Reply	17	11:51:56	12:26:16	0.1290	0.1316																					432	421	449	428
	ICMP PING	17	11:51:56	12:26:16	0.1285	0.1326																					449	438	461	421
	ATTACK-RESPONSES 403 Forbidden	3	12:14:18	12:31:13	0.1186	0.1393																					404	404	463	406
	ATTACK-RESPONSES Invalid URL	1	12:23:39	12:23:39	0.1373	0.1373																					405	405	407	407

A.2 Full result of the incident risk index and its position for Experiment 2 (Using different weights of indicators)

					Time Interval																									
Phase	Incident's Signature	No. of Incidents	Time		Risk Index		09:51:35		09:52:00		10:08:06		10:18:06		10:33:09		10:35:01		10:50:00		10:50:54		11:26:14		11:34:21		12:23:39		12:35:48	
			Min	Max	Min	Max	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High
Pre 1	ATTACK-RESPONSES directory listing	3	09:29:20	09:29:24	0.1956	0.1956	21	19	53	51	71	69	259	257	259	257	310	308	310	308	314	312	318	316	325	323	325	323	325	323
	FTP Bad login	1	09:32:34	09:32:34	0.3135	0.3135	1	1	4	4	4	4	141	141	141	141	176	176	176	176	176	176	180	180	183	183	183	183	183	183
	TELNET login incorrect	3	09:32:34	09:45:36	0.1747	0.2007	23	18	61	50	79	68	299	256	299	256	358	307	358	307	362	311	366	315	373	322	375	322	375	322
	ATTACK-RESPONSES Invalid URL	1	09:37:05	09:37:05	0.1650	0.1650	24	24	62	62	80	80	308	308	308	308	367	367	382	382	386	386	390	390	397	397	399	399	401	401
	ATTACK-RESPONSES 403 Forbidden	1	09:45:34	09:45:34	0.1633	0.1633	25	25	63	63	81	81	309	309	309	309	368	368	384	384	388	388	392	392	399	399	401	401	403	403
	ICMP Echo Reply	8	09:45:37	09:45:37	0.2188	0.2188	9	2	38	31	38	31	187	180	187	180	238	231	238	231	242	235	246	239	253	246	253	246	253	246
	ICMP PING	8	09:45:37	09:45:37	0.2162	0.2162	17	10	49	42	58	51	207	200	207	200	258	251	258	251	262	255	266	259	273	266	273	266	273	266
1	**ICMP Echo Reply**	**20**	**09:51:36**	**09:52:00**	**0.0950**	**0.3459**			65	2	86	2	317	123	321	123	385	158	**413**	**158**	**423**	**158**	**435**	**162**	**1014**	**165**	**1042**	**165**	**1056**	**165**
	ICMP PING	**20**	**09:51:36**	**09:52:00**	**0.0955**	**0.3459**			64	1	85	1	316	122	320	122	384	157	**412**	**157**	**422**	**157**	**434**	**161**	**1013**	**164**	**1041**	**164**	**1055**	**164**
Pre 2	ATTACK-RESPONSES Invalid URL	1	09:52:10	09:52:10	0.1177	0.1177					84	84	315	315	315	315	376	376	398	398	408	408	415	415	422	422	450	450	464	464
	ATTACK-RESPONSES 403 Forbidden	2	09:54:45	09:58:36	0.1531	0.1531					83	82	311	310	311	310	372	371	392	391	396	395	401	400	408	407	412	411	414	413
	ICMP Echo Reply	9	10:01:41	10:01:41	0.2175	0.2175					50	42	199	191	199	191	250	242	250	242	254	246	258	250	265	257	265	257	265	257
	ICMP PING	9	10:01:41	10:01:41	0.2153	0.2153					67	59	216	208	216	208	267	259	267	259	271	263	275	267	282	274	282	274	282	274
2	ICMP Destination Unreachable Port Unreachable	72	10:08:07	10:18:05	0.2402	0.3684							153	77	153	77	196	106	196	106	200	106	204	110	211	110	211	110	211	110
	RPC portmap sadmind request UDP	**76**	**10:08:07**	**10:18:05**	**0.0891**	**0.3408**							329	125	333	125	397	160	**425**	**160**	**435**	**160**	**447**	**164**	**1026**	**167**	**1054**	**167**	**1068**	**167**
	RPC portmap Solaris sadmin port query udp request	**76**	**10:08:07**	**10:18:05**	**0.4041**	**0.6558**							76	1	76	1	105	7	**105**	**7**	**105**	**7**	**109**	**7**	**109**	**7**	**109**	**7**	**109**	**7**
	ICMP Echo Reply	8	10:11:05	10:11:05	0.1769	0.1769							298	291	298	291	357	350	357	350	361	354	365	358	372	365	374	367	374	367
	ICMP PING	8	10:11:05	10:11:05	0.1662	0.1662							307	300	307	300	366	359	375	368	379	372	383	376	390	383	392	385	394	387
	TELNET login incorrect	3	10:15:28	10:17:38	0.1484	0.1485							314	312	314	312	375	373	397	395	407	405	414	412	421	419	425	423	427	425
Pre 3	ATTACK-RESPONSES directory listing	4	10:22:43	10:31:30	0.1086	0.1086									319	316	380	377	408	405	418	415	430	427	484	481	512	509	526	523
3	**RPC portmap sadmind request UDP**	**14**	**10:33:10**	**10:34:59**	**0.2195**	**0.3469**											220	151	**220**	**151**	**224**	**151**	**228**	**155**	**235**	**158**	**235**	**158**	**235**	**158**
	RPC portmap Solaris sadmin port query udp portmapper sadmin port query attempt	**14**	**10:33:10**	**10:34:59**	**0.5178**	**0.6452**											69	8	**69**	**8**	**69**	**8**	**73**	**8**	**73**	**8**	**73**	**8**	**73**	**8**
	RPC portmap Solaris sadmin port query udp request	**14**	**10:33:10**	**10:34:59**	**0.5345**	**0.6619**											22	1	**22**	**1**	**22**	**1**	**22**	**1**	**22**	**1**	**22**	**1**	**22**	**1**
	RPC sadmind query with root credentials attempt UDP	**14**	**10:33:10**	**10:34:59**	**0.1826**	**0.3100**											325	177	**325**	**177**	**329**	**177**	**333**	**181**	**340**	**184**	**342**	**184**	**342**	**184**
	TELNET login incorrect	4	10:33:18	10:34:57	0.1558	0.2828											370	183	388	183	392	183	396	187	403	190	407	190	409	190
	ATTACK-RESPONSES directory listing	3	10:33:33	10:34:09	0.1083	0.1083											383	381	411	409	421	419	433	431	531	529	559	557	573	571
	SQL version overflow attempt	1	10:34:57	10:34:57	0.5386	0.5386											14	14	14	14	14	14	14	14	14	14	14	14	14	14
Pre 4	ATTACK-RESPONSES directory listing	6	10:36:29	10:43:57	0.1114	0.1114													404	399	414	409	426	421	433	428	461	456	475	470
	TELNET login incorrect	2	10:36:34	10:46:04	0.1550	0.1552													390	389	394	393	398	397	405	404	409	408	411	410
	ATTACK-RESPONSES 403 Forbidden	2	10:46:28	10:46:28	0.1505	0.1505													394	393	404	403	411	410	418	417	422	421	424	423
	ICMP Echo Reply	9	10:49:00	10:49:18	0.1601	0.1654													386	376	390	380	394	384	401	391	404	393	406	395
	ICMP PING	9	10:49:00	10:49:18	0.1704	0.1731													367	359	371	363	375	367	382	374	384	376	386	378
4	**RSERVICES rsh root**	**8**	**10:50:02**	**10:50:38**	**0.1526**	**0.2797**															**400**	**185**	**405**	**189**	**412**	**192**	**416**	**192**	**418**	**192**
	ATTACK-RESPONSES 403 Forbidden	**2**	**10:50:15**	**10:50:54**	**0.1507**	**0.1514**															**402**	**401**	**409**	**408**	**416**	**415**	**420**	**419**	**422**	**421**
Pre 5	ATTACK-RESPONSES 403 Forbidden	2	10:58:16	11:00:32	0.1516	0.1522																	407	406	414	413	418	417	420	419
	TELNET login incorrect	1	11:00:11	11:00:11	0.1540	0.1540																	399	399	406	406	410	410	412	412
	ATTACK-RESPONSES directory listing	4	11:00:16	11:03:33	0.1136	0.1136																	420	417	427	424	455	452	469	466
	ICMP Destination Unreachable Port Unreachable	4	11:03:38	11:04:13	0.5292	0.5292																	38	35	38	35	38	35	38	35
	ATTACK-RESPONSES Invalid URL	1	11:05:11	11:05:11	0.1161	0.1161																	416	416	423	423	451	451	465	465
5	**(snort decoder) Bad Traffic Loopback IP**	**572**	**11:27:51**	**11:27:56**	**0.1036**	**0.1090**																			**1012**	**434**	**1040**	**462**	**1054**	**476**
	SNMP AgentX/tcp request	3	11:27:54	11:27:55	0.3592	0.3614																			157	155	157	155	157	155
	ICMP Echo Reply	1	11:28:18	11:28:18	0.2786	0.2786																			196	196	196	196	196	196
	ICMP PING	1	11:28:18	11:28:18	0.2762	0.2762																			197	197	197	197	197	197
	ICMP PING *NIX	1	11:28:18	11:28:18	0.2739	0.2739																			199	199	199	199	199	199
	ICMP PING BSDtype	1	11:28:18	11:28:18	0.2739	0.2739																			198	198	198	198	198	198
Post 5	TELNET login incorrect	4	11:39:07	12:33:25	0.1733	0.1890																					329	327	377	327
	ICMP Echo Reply	17	11:51:56	12:26:16	0.1426	0.1460																					437	426	449	433
	ICMP PING	17	11:51:56	12:26:16	0.1421	0.1472																					449	438	461	428
	ATTACK-RESPONSES 403 Forbidden	3	12:14:18	12:31:13	0.1252	0.1605																					402	402	463	404
	ATTACK-RESPONSES Invalid URL	1	12:23:39	12:23:39	0.1580	0.1580																					405	405	407	407

Appendix B

Results of the second stage of the evaluation study

Appendix B extends the experimental results in the second stage of the evaluation study (see *Section 5.3*).

B.1 Full comparison result between the incident risk index and its position – CID 4

			Time Interval											
			09:51:35	09:52:00	10:08:06	10:18:06	10:33:09	10:35:01	10:50:00	10:50:54	11:26:14	11:34:21	12:23:39	12:35:48
		Incident Detected	25	40	21	243	4	64	28	10	12	579	28	14
		Total	25	65	86	329	333	397	425	435	447	1026	1054	1068
Experiment 1	Stage 1	Risk Index	0.314	0.3142	0.3142	0.3142	0.3142	0.3142	0.3142	0.3142	0.3142	0.3142	0.3142	0.3142
		Position	1	4	4	114	114	149	149	149	153	153	153	153
	Stage 2	Risk Index	0.314	0.2970	0.2951	0.2885	0.2892	0.2898	0.2910	0.2911	0.2920	0.3193	0.3186	0.3183
	(No limit)	Position	1	4	4	129	129	170	167	167	159	98	98	98
	Stage 2	Risk Index	0.314	0.2970	0.2951	0.2885	0.2892							
	(1 Hour)	Position	1	4	4	129	129							
	Stage 2	Risk Index	0.314	0.2970	0.2951	0.2885	0.2892	0.2898	0.2910	0.2911	0.2920	0.3193		
	(2 Hours)	Position	1	4	4	129	129	170	167	167	159	98		
Experiment 2	Stage 1	Risk Index	0.314	0.3135	0.3135	0.3135	0.3135	0.3135	0.3135	0.3135	0.3135	0.3135	0.3135	0.3135
		Position	1	4	4	141	141	176	176	176	180	183	183	183
	Stage 2	Risk Index	0.314	0.2954	0.2935	0.2862	0.2869	0.2875	0.2886	0.2888	0.2899	0.3147	0.3140	0.3139
	(No limit)	Position	1	4	4	141	141	182	182	182	186	158	158	158
	Stage 2	Risk Index	0.314	0.2954	0.2935	0.2862	0.2869							
	(1 Hour)	Position	1	4	4	141	141							
	Stage 2	Risk Index	0.314	0.2954	0.2935	0.2862	0.2869	0.2875	0.2886	0.2888	0.2899	0.3147		
	(2 Hours)	Position	1	4	4	141	141	182	182	182	186	158		

B.2 Full comparison result between the incident risk index and its position – CID 28

			Time Interval											
			09:51:35	09:52:00	10:08:06	10:18:06	10:33:09	10:35:01	10:50:00	10:50:54	11:26:14	11:34:21	12:23:39	12:35:48
		Incident Detected	25	40	21	243	4	64	28	10	12	579	28	14
		Total	25	65	86	329	333	397	425	435	447	1026	1054	1068
Experiment 1	Stage 1	Risk Index		0.3542	0.3542	0.3542	0.3542	0.3542	0.3542	0.3542	0.3542	0.3542	0.3542	0.3542
		Position		1	1	65	65	94	94	94	98	98	98	98
	Stage 2	Risk Index		0.3542	0.3504	0.3339	0.3330	0.3334	0.3325	0.3309	0.3301	0.2910	0.2922	0.2926
	(No limit)	Position		2	1	66	66	101	101	101	105	108	108	108
	Stage 2	Risk Index		0.3542	0.3504	0.3339	0.3330	0.3334	0.3325	0.3309				
	(1 Hour)	Position		2	1	66	66	101	101	101				
	Stage 2	Risk Index		0.3542	0.3504	0.3339	0.3330	0.3334	0.3325	0.3309	0.3301	0.2910		
	(2 Hours)	Position		2	1	66	66	101	101	101	105	108		
Experiment 2	Stage 1	Risk Index		0.3459	0.3459	0.3459	0.3459	0.3459	0.3459	0.3459	0.3459	0.3459	0.3459	0.3459
		Position		1	1	122	122	157	157	157	161	164	164	164
	Stage 2	Risk Index		0.3459	0.3410	0.3327	0.3317	0.3341	0.3325	0.3306	0.3298	0.2854	0.2865	0.2869
	(No limit)	Position		2	1	123	123	158	158	158	162	187	183	183
	Stage 2	Risk Index		0.3459	0.3410	0.3327	0.3317	0.3341	0.3325	0.3306				
	(1 Hour)	Position		2	1	123	123	158	158	158				
	Stage 2	Risk Index		0.3459	0.3410	0.3327	0.3317	0.3341	0.3325	0.3306	0.3298	0.2854		
	(2 Hours)	Position		2	1	123	123	158	158	158	162	187		

B.3 Full comparison result between the incident risk index and its position – CID 52

			Time Interval											
			09:51:35	09:52:00	10:08:06	10:18:06	10:33:09	10:35:01	10:50:00	10:50:54	11:26:14	11:34:21	12:23:39	12:35:48
		Incident Detected	25	40	21	243	4	64	28	10	12	579	28	14
		Total	25	65	86	329	333	397	425	435	447	1026	1054	1068
Experiment 1	Stage 1	Risk Index		0.3542	0.3542	0.3542	0.3542	0.3542	0.3542	0.3542	0.3542	0.3542	0.3542	0.3542
		Position		3	3	67	67	96	96	96	100	100	100	100
	Stage 2	Risk Index		0.3542	0.3504	0.3337	0.3329	0.3318	0.3310	0.3295	0.3285	0.2902	0.2915	0.2919
	(No limit)	Position		1	2	67	67	102	102	102	106	109	109	109
	Stage 2	Risk Index		0.3542	0.3504	0.3337	0.3329	0.3318	0.3310	0.3295				
	(1 Hour)	Position		1	2	67	67	102	102	102				
	Stage 2	Risk Index		0.3542	0.3504	0.3337	0.3329	0.3318	0.3310	0.3295	0.3285	0.2902		
	(2 Hours)	Position		1	2	67	67	102	102	102	106	109		
Experiment 2	Stage 1	Risk Index		0.3459	0.3459	0.3459	0.3459	0.3459	0.3459	0.3459	0.3459	0.3459	0.3459	0.3459
		Position		3	3	124	124	159	159	159	163	166	166	166
	Stage 2	Risk Index		0.3459	0.3410	0.3325	0.3315	0.3320	0.3305	0.3287	0.3276	0.2844	0.2855	0.2859
	(No limit)	Position		1	2	124	124	159	159	159	163	188	184	184
	Stage 2	Risk Index		0.3459	0.3410	0.3325	0.3315	0.3320	0.3305	0.3287				
	(1 Hour)	Position		1	2	124	124	159	159	159				
	Stage 2	Risk Index		0.3459	0.3410	0.3325	0.3315	0.3320	0.3305	0.3287	0.3276	0.2844		
	(2 Hours)	Position		1	2	124	124	159	159	159	163	188		

B.4 Full comparison result between the incident risk index and its position – CID 88

			Time Interval											
			09:51:35	09:52:00	10:08:06	10:18:06	10:33:09	10:35:01	10:50:00	10:50:54	11:26:14	11:34:21	12:23:39	12:35:48
		Incident Detected	25	40	21	243	4	64	28	10	12	579	28	14
		Total	25	65	86	329	333	397	425	435	447	1026	1054	1068
Experiment 1	Stage 1	Risk Index				0.5412	0.5412	0.5412	0.5412	0.5412	0.5412	0.5412	0.5412	0.5412
		Position				1	1	7	7	7	7	7	7	7
	Stage 2	Risk Index				0.5412	0.5402	0.5460	0.5411	0.5393	0.5379	0.4941	0.4936	0.4933
	(No limit)	Position				1	1	7	7	7	7	7	5	5
	Stage 2	Risk Index				0.5412	0.5402	0.5460	0.5411	0.5393	0.5379			
	(1 Hour)	Position				1	1	7	7	7	7			
	Stage 2	Risk Index				0.5412	0.5402	0.5460	0.5411	0.5393	0.5379	0.4941		
	(2 Hours)	Position				1	1	7	7	7	7	7		
Experiment 2	Stage 1	Risk Index				0.6558	0.6558	0.6558	0.6558	0.6558	0.6558	0.6558	0.6558	0.6558
		Position				1	1	7	7	7	7	7	7	7
	Stage 2	Risk Index				0.6558	0.6547	0.6615	0.6562	0.6542	0.6527	0.6037	0.6031	0.6028
	(No limit)	Position				1	1	7	7	7	7	5	7	7
	Stage 2	Risk Index				0.6558	0.6547	0.6615	0.6562	0.6542	0.6527			
	(1 Hour)	Position				1	1	7	7	7	7			
	Stage 2	Risk Index				0.6558	0.6547	0.6615	0.6562	0.6542	0.6527	0.6037		
	(2 Hours)	Position				1	1	7	7	7	7	5		

B.5 Full comparison result between the incident risk index and its position – CID 353

			Time Interval											
			09:51:35	09:52:00	10:08:06	10:18:06	10:33:09	10:35:01	10:50:00	10:50:54	11:26:14	11:34:21	12:23:39	12:35:48
		Incident Detected	25	40	21	243	4	64	28	10	12	579	28	14
		Total	25	65	86	329	333	397	425	435	447	1026	1054	1068
Experiment 1	Stage 1	Risk Index						0.5462	0.5462	0.5462	0.5462	0.5462	0.5462	0.5462
		Position						5	5	5	5	5	5	5
	Stage 2	Risk Index						0.5462	0.5413	0.5396	0.5381	0.4942	0.4937	0.4934
	(No limit)	Position						1	6	4	2	5	3	3
	Stage 2	Risk Index						0.5471	0.5421	0.5403	0.5388	0.4942		
	(1 Hour)	Position						1	2	3	3	1		
	Stage 2	Risk Index						0.5462	0.5413	0.5396	0.5381	0.4942	0.4937	0.4934
	(2 Hours)	Position						1	6	4	2	5	3	2
Experiment 2	Stage 1	Risk Index						0.6619	0.6619	0.6619	0.6619	0.6619	0.6619	0.6619
		Position						1	1	1	1	1	1	1
	Stage 2	Risk Index						0.6619	0.6565	0.6546	0.6531	0.6038	0.6032	0.6029
	(No limit)	Position						1	1	2	1	3	5	5
	Stage 2	Risk Index						0.6628	0.6572	0.6553	0.6537	0.6038		
	(1 Hour)	Position						1	4	3	1	4		
	Stage 2	Risk Index						0.6619	0.6565	0.6546	0.6531	0.6038	0.6032	0.6029
	(2 Hours)	Position						1	1	2	1	3	1	2

B.6 Full comparison result between the incident risk index and its position – CID 428

			Time Interval											
			09:51:35	09:52:00	10:08:06	10:18:06	10:33:09	10:35:01	10:50:00	10:50:54	11:26:14	11:34:21	12:23:39	12:35:48
		Incident Detected	25	40	21	243	4	64	28	10	12	579	28	14
		Total	25	65	86	329	333	397	425	435	447	1026	1054	1068
Experiment 1	Stage 1	Risk Index								0.2835	0.2835	0.2835	0.2835	0.2835
		Position								175	179	181	181	181
	Stage 2	Risk Index								0.2835	0.2834	0.2878	0.2874	0.2872
	(No limit)	Position								173	177	112	112	113
	Stage 2	Risk Index								0.2840	0.2838	0.2880		
	(1 Hour)	Position								174	173	45		
	Stage 2	Risk Index								0.2835	0.2834	0.2878	0.2874	0.2872
	(2 Hours)	Position								173	177	112	44	33
Experiment 2	Stage 1	Risk Index								0.2797	0.2797	0.2797	0.2797	0.2797
		Position								187	191	194	194	194
	Stage 2	Risk Index								0.2797	0.2796	0.2856	0.2851	0.2849
	(No limit)	Position								188	191	185	187	187
	Stage 2	Risk Index								0.2802	0.2800	0.2859		
	(1 Hour)	Position								184	188	45		
	Stage 2	Risk Index								0.2797	0.2796	0.2856	0.2851	0.2849
	(2 Hours)	Position								188	191	185	47	32

B.7 Full comparison result between the incident risk index and its position – CID 575

			Time Interval											
			09:51:35	09:52:00	10:08:06	10:18:06	10:33:09	10:35:01	10:50:00	10:50:54	11:26:14	11:34:21	12:23:39	12:35:48
		Incident Detected	25	40	21	243	4	64	28	10	12	579	28	14
		Total	25	65	86	329	333	397	425	435	447	1026	1054	1068
Experiment 1	Stage 1	Risk Index										0.1026	0.1026	0.1026
		Position										444	472	486
	Stage 2	Risk Index										0.1026	0.1002	0.0991
	(No limit)	Position										444	469	483
	Stage 2	Risk Index										0.1499	0.1444	
	(1 Hour)	Position										65	12	
	Stage 2	Risk Index										0.1026	0.1002	0.0991
	(2 Hours)	Position										444	156	149
Experiment 2	Stage 1	Risk Index										0.1090	0.1090	0.1090
		Position										434	462	476
	Stage 2	Risk Index										0.1090	0.1063	0.1052
	(No limit)	Position										441	469	483
	Stage 2	Risk Index										0.1590	0.1532	
	(1 Hour)	Position										83	19	
	Stage 2	Risk Index										0.1090	0.1063	0.1052
	(2 Hours)	Position										441	157	150

Appendix C

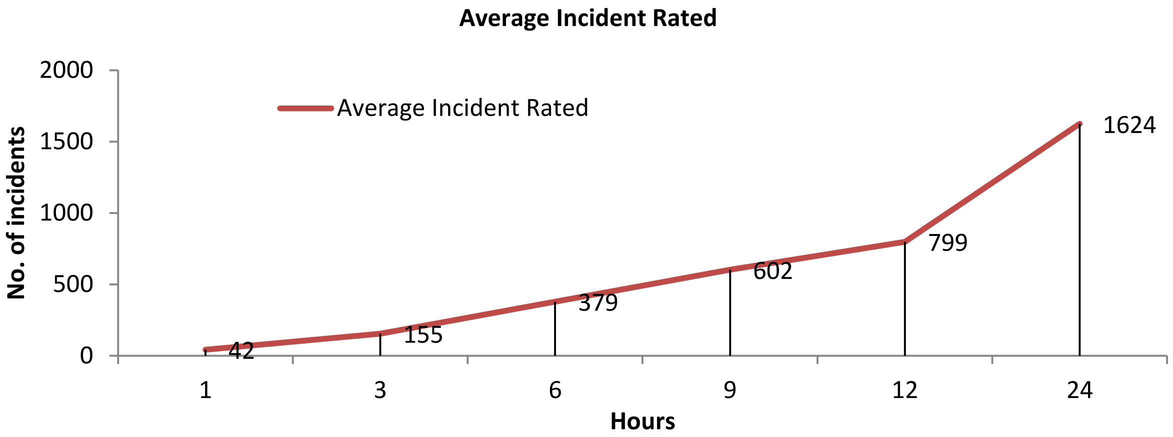
Results of the third stage of the evaluation study

Appendix C extends the experimental results in the third stage of the evaluation study (see *Section 5.4*).

C.1 Different scenario in the third stage experiment

	Consequence of Event	Likelihood of Event	criticality	maintainability	replaceability	dependability	control	severity	exploitability	sensitivity	similarity	frequency
Scenario 1	0.4444	0.5556	0.3859	0.6590	0.2210	0.1834	0.1437	0.4954	0.0716	0.0426	0.2300	0.1604
Scenario 2	0.1000	0.9000	0.3859	0.6590	0.2210	0.1834	0.1437	0.4954	0.0716	0.0426	0.2300	0.1604
Scenario 3	0.1667	0.8333	0.3859	0.6590	0.2210	0.1834	0.1437	0.4954	0.0716	0.0426	0.2300	0.1604
Scenario 4	0.3333	0.6667	0.3859	0.6590	0.2210	0.1834	0.1437	0.4954	0.0716	0.0426	0.2300	0.1604
Scenario 5	50.0000	50.0000	0.2000	0.2000	0.2000	0.2000	0.2000	0.2000	0.2000	0.2000	0.2000	0.2000

C.2 Number of incidents updated using different time limitation.



C.3 The incident distribution with the Plymouth dataset.

Type	Snort Priority			CVSS v2				Response Strategy Model			
	High	Medium	Low	High	Medium	Low	None	Avoidance	Mitigation	Transfer	Acceptance
FALSE	7.39%	74.44%	16.37%	0.01%	7.52%	0.00%	90.66%	0.00%	7.52%	90.68%	0.00%
TRUE	0.00%	0.06%	1.75%	0.01%	0.01%	0.00%	1.79%	0.00%	0.01%	1.80%	0.00%
Total	7.39%	74.50%	18.12%	0.02%	7.53%	0.00%	92.45%	0.00%	7.53%	92.47%	0.00%

C.4 The incident distribution with the Plymouth dataset – different limitation and scenario.

		Response Strategy Model (Time Limitation: 1 Hour)				Response Strategy Model (Time Limitation: 3 Hours)				Response Strategy Model (Time Limitation: 6 Hours)			
Scenario	**Type**	**Avoidance**	**Mitigation**	**Transfer**	**Acceptance**	**Avoidance**	**Mitigation**	**Transfer**	**Acceptance**	**Avoidance**	**Mitigation**	**Transfer**	**Acceptance**
1	FALSE	-	7.55%	90.01%	0.63%	-	7.52%	90.68%	-	-	7.52%	90.68%	-
	TRUE	-	0.01%	1.80%	-	-	0.01%	1.80%	-	-	0.01%	1.80%	-
	Total	**-**	**7.56%**	**91.81%**	**0.63%**	**-**	**7.53%**	**92.47%**	**-**	**-**	**7.53%**	**92.47%**	**-**
2	FALSE	-	7.24%	65.21%	25.75%	-	7.42%	56.74%	34.03%	-	7.49%	56.25%	34.46%
	TRUE	-	0.01%	0.27%	1.52%	-	0.01%	-	1.80%	-	0.01%	-	1.80%
	Total	**-**	**7.25%**	**65.48%**	**27.27%**	**-**	**7.43%**	**56.74%**	**35.83%**	**-**	**7.49%**	**56.25%**	**36.26%**
3	FALSE	-	7.29%	72.10%	18.81%	-	7.44%	69.76%	20.99%	-	7.51%	67.74%	22.94%
	TRUE	-	0.01%	0.46%	1.33%	-	0.01%	0.01%	1.79%	-	0.01%	-	1.80%
	Total	**-**	**7.30%**	**72.57%**	**20.14%**	**-**	**7.45%**	**69.77%**	**22.78%**	**-**	**7.52%**	**67.74%**	**24.74%**
4	FALSE	-	7.47%	89.46%	1.27%	-	7.52%	88.84%	1.83%	-	7.52%	88.78%	1.89%
	TRUE	-	0.01%	1.80%	-	-	0.01%	1.80%	-	-	0.01%	1.80%	-
	Total	**-**	**7.47%**	**91.25%**	**1.27%**	**-**	**7.53%**	**90.64%**	**1.83%**	**-**	**7.53%**	**90.58%**	**1.89%**
5	FALSE	-	6.81%	91.38%	-	-	7.10%	91.09%	-	-	7.35%	90.85%	-
	TRUE	-	0.00%	1.80%	-	-	0.00%	1.80%	-	-	0.01%	1.80%	-
	Total	**-**	**6.82%**	**93.18%**	**-**	**-**	**7.11%**	**92.89%**	**-**	**-**	**7.35%**	**92.65%**	**-**

		Response Strategy Model (Time Limitation: 9 Hours)				Response Strategy Model (Time Limitation: 12 Hours)				Response Strategy Model (Time Limitation: 24 Hours)			
Scenario	**Type**	**Avoidance**	**Mitigation**	**Transfer**	**Acceptance**	**Avoidance**	**Mitigation**	**Transfer**	**Acceptance**	**Avoidance**	**Mitigation**	**Transfer**	**Acceptance**
1	FALSE	-	7.52%	90.68%	-	-	7.52%	90.68%	-	-	7.52%	90.68%	-
	TRUE	-	0.01%	1.80%	-	-	0.01%	1.80%	-	-	0.01%	1.80%	-
	Total	**-**	**7.53%**	**92.47%**	**-**	**-**	**7.53%**	**92.47%**	**-**	**-**	**7.53%**	**92.47%**	**-**
2	FALSE	-	7.51%	57.69%	33.00%	-	7.52%	58.20%	32.47%	-	7.52%	58.42%	32.26%
	TRUE	-	0.01%	-	1.80%	-	0.01%	-	1.80%	-	0.01%	-	1.80%
	Total	**-**	**7.52%**	**57.69%**	**34.80%**	**-**	**7.53%**	**58.20%**	**34.27%**	**-**	**7.53%**	**58.42%**	**34.06%**
3	FALSE	-	7.52%	64.65%	26.03%	-	7.52%	61.55%	29.13%	-	7.52%	59.58%	31.09%
	TRUE	-	0.01%	-	1.80%	-	0.01%	-	1.80%	-	0.01%	-	1.80%
	Total	**-**	**7.53%**	**64.65%**	**27.83%**	**-**	**7.53%**	**61.55%**	**30.93%**	**-**	**7.53%**	**59.58%**	**32.89%**
4	FALSE	-	7.52%	88.72%	1.96%	-	7.52%	88.69%	1.98%	-	7.52%	88.75%	1.93%
	TRUE	-	0.01%	1.80%	-	-	0.01%	1.80%	-	-	0.01%	1.80%	-
	Total	**-**	**7.53%**	**90.52%**	**1.96%**	**-**	**7.53%**	**90.49%**	**1.98%**	**-**	**7.53%**	**90.54%**	**1.93%**
5	FALSE	-	7.27%	90.93%	-	-	7.40%	90.80%	-	-	7.46%	90.74%	-
	TRUE	-	0.01%	1.80%	-	-	0.01%	1.80%	-	-	0.01%	1.80%	-
	Total	**-**	**7.28%**	**92.72%**	**-**	**-**	**7.41%**	**92.59%**	**-**	**-**	**7.47%**	**92.53%**	**-**

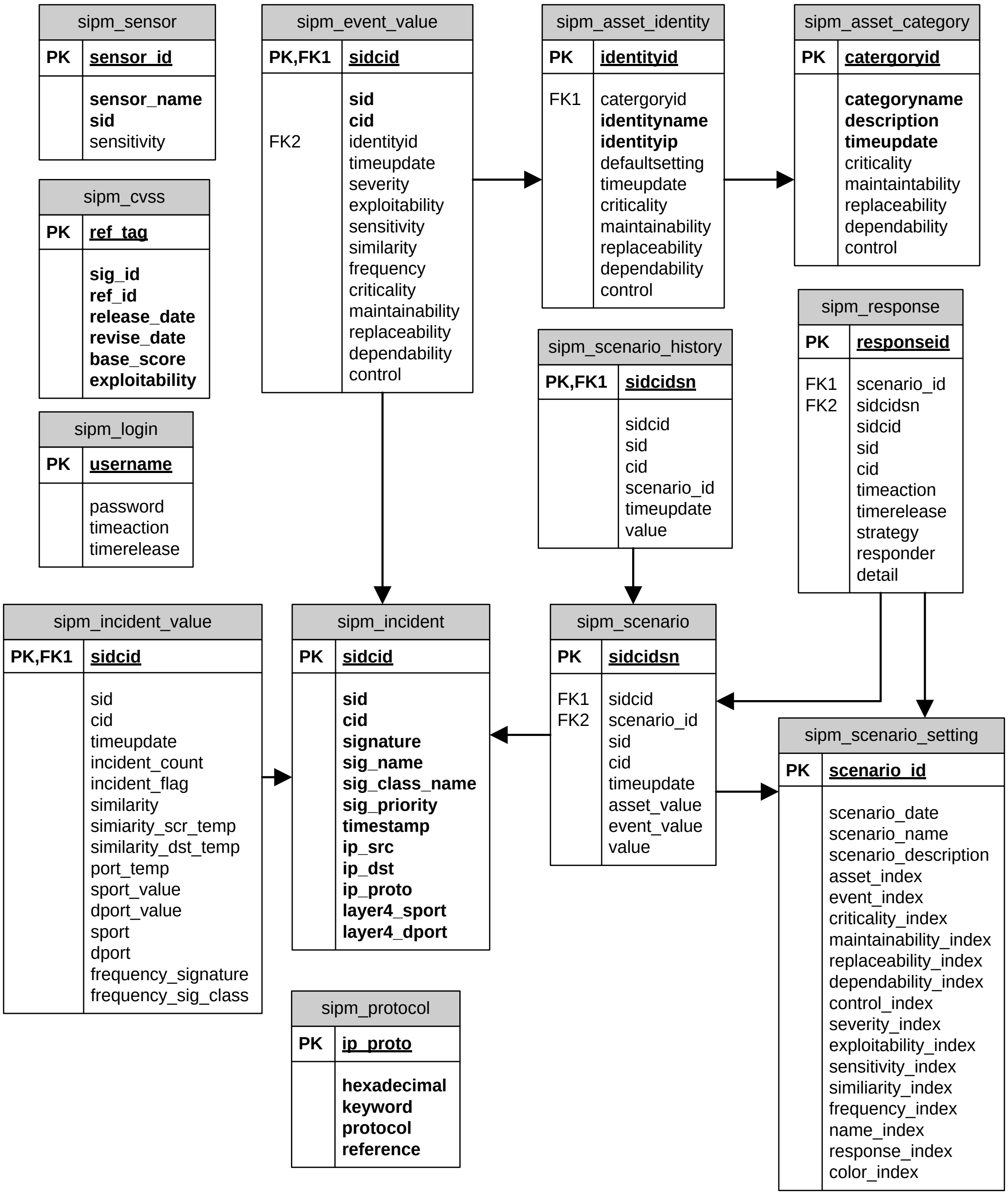
C.5 The incident distribution with the Plymouth dataset – Scenario 1 with 24 hours limitation

Date	Total Alert	Snort Priority			CVSS v2				Response Strategy Model			
		High	Medium	Low	High	Medium	Low	None	Avoidance	Mitigation	Transfer	Acceptance
17 May 2007	1149	9.40	65.01	25.59	0.00	0.70	0.00	99.30	0.00	0.70	99.30	0.00
18 May 2007	1774	5.19	76.10	18.71	0.00	32.47	0.00	67.53	0.00	32.41	67.59	0.00
19 May 2007	1166	4.20	91.51	4.29	0.00	28.73	0.00	71.27	0.00	28.73	71.27	0.00
20 May 2007	856	8.18	86.68	5.14	0.12	0.35	0.00	99.53	0.00	0.47	99.53	0.00
21 May 2007	1165	6.61	66.09	27.30	0.00	10.56	0.00	89.44	0.00	10.56	89.44	0.00
22 May 2007	1100	9.09	65.27	25.64	0.00	0.36	0.00	99.64	0.00	0.36	99.64	0.00
23 May 2007	1296	7.41	68.83	23.77	0.00	15.43	0.00	84.57	0.00	15.43	84.57	0.00
24 May 2007	1324	6.27	69.86	23.87	0.00	13.44	0.00	86.56	0.00	13.44	86.56	0.00
25 May 2007	1129	6.64	68.29	25.07	0.00	1.51	0.00	98.49	0.00	1.51	98.49	0.00
26 May 2007	846	8.63	87.12	4.26	0.00	0.24	0.00	99.76	0.00	0.24	99.76	0.00
27 May 2007	1038	7.42	88.54	4.05	0.00	15.99	0.00	84.01	0.00	15.99	84.01	0.00
28 May 2007	1137	7.74	83.55	8.71	0.09	14.34	0.00	85.57	0.00	14.34	85.66	0.00
29 May 2007	1097	10.76	72.47	16.77	0.09	2.01	0.00	97.90	0.00	2.01	97.99	0.00
30 May 2007	1534	5.93	75.62	18.45	0.00	13.17	0.00	86.83	0.00	13.17	86.83	0.00
31 May 2007	1228	6.84	70.93	22.23	0.00	4.40	0.00	95.60	0.00	4.40	95.60	0.00
01 June 2007	1386	7.14	71.50	21.36	0.00	12.63	0.00	87.37	0.00	12.63	87.37	0.00
02 June 2007	1022	6.46	89.43	4.11	0.10	9.88	0.00	90.02	0.00	9.88	90.12	0.00
03 June 2007	899	7.23	86.65	6.12	0.00	1.33	0.00	98.67	0.00	1.33	98.67	0.00
04 June 2007	1141	9.03	70.03	20.95	0.00	0.09	0.00	99.91	0.00	0.09	99.91	0.00
05 June 2007	1238	7.59	71.24	21.16	0.08	0.73	0.00	99.19	0.00	0.81	99.19	0.00
06 June 2007	1466	6.07	70.12	23.81	0.00	11.05	0.00	88.95	0.00	11.05	88.95	0.00
07 June 2007	1080	8.89	72.04	19.07	0.00	0.74	0.00	99.26	0.00	0.74	99.26	0.00
08 June 2007	1158	6.13	71.76	22.11	0.00	0.09	0.00	99.91	0.00	0.09	99.91	0.00
09 June 2007	1027	5.36	90.94	3.70	0.00	9.25	0.00	90.75	0.00	9.25	90.75	0.00
10 June 2007	1079	8.71	85.82	5.47	0.00	6.30	0.00	93.70	0.00	6.30	93.70	0.00
11 June 2007	1334	7.50	75.64	16.87	0.00	12.22	0.00	87.78	0.00	12.22	87.78	0.00
12 June 2007	1275	8.63	69.02	22.35	0.08	0.55	0.00	99.37	0.00	0.63	99.37	0.00
13 June 2007	1367	8.19	64.67	27.14	0.00	0.15	0.00	99.85	0.00	0.15	99.85	0.00
14 June 2007	1202	7.40	68.72	23.88	0.00	2.25	0.00	97.75	0.00	2.25	97.75	0.00
15 June 2007	1494	5.29	75.30	19.41	0.00	20.08	0.00	79.92	0.00	20.08	79.92	0.00
16 June 2007	1101	5.99	89.55	4.45	0.00	18.53	0.00	81.47	0.00	17.89	82.11	0.00
17 June 2007	1007	7.55	85.70	6.75	0.00	0.50	0.00	99.50	0.00	0.50	99.50	0.00
18 June 2007	1176	10.97	60.29	28.74	0.00	0.09	0.00	99.91	0.00	0.09	99.91	0.00
19 June 2007	1103	8.52	63.46	28.01	0.00	1.36	0.00	98.64	0.00	1.36	98.64	0.00
20 June 2007	1175	8.85	64.09	27.06	0.00	4.85	0.00	95.15	0.00	4.85	95.15	0.00
21 June 2007	1078	6.59	66.88	26.53	0.19	0.65	0.00	99.16	0.00	0.83	99.17	0.00
22 June 2007	977	6.86	68.47	24.67	0.10	0.20	0.00	99.70	0.00	0.31	99.69	0.00
23 June 2007	797	7.40	86.32	6.27	0.00	0.13	0.00	99.87	0.00	0.13	99.87	0.00
24 June 2007	813	7.87	85.49	6.64	0.00	0.12	0.00	99.88	0.00	0.12	99.88	0.00
25 June 2007	959	8.34	65.48	26.17	0.00	0.21	0.00	99.79	0.00	0.21	99.79	0.00

Appendix D

Database Design

The database design in this section is a part of the prototype presented in Chapter 6.



sipm_sensor	
PK	**sensor_id**
	sensor_name
	sid
	sensitivity

sipm_event_value	
PK,FK1	**sidcid**
	sid
	cid
FK2	identityid
	timeupdate
	severity
	exploitability
	sensitivity
	similarity
	frequency
	criticality
	maintainability
	replaceability
	dependability
	control

sipm_asset_identity	
PK	**identityid**
FK1	catergoryid
	identityname
	identityip
	defaultsetting
	timeupdate
	criticality
	maintainability
	replaceability
	dependability
	control

sipm_asset_category	
PK	**catergoryid**
	categoryname
	description
	timeupdate
	criticality
	maintaintability
	replaceability
	dependability
	control

sipm_cvss	
PK	**ref_tag**
	sig_id
	ref_id
	release_date
	revise_date
	base_score
	exploitability

sipm_login	
PK	**username**
	password
	timeaction
	timerelease

sipm_scenario_history	
PK,FK1	**sidcidsn**
	sidcid
	sid
	cid
	scenario_id
	timeupdate
	value

sipm_response	
PK	**responseid**
FK1	scenario_id
FK2	sidcidsn
	sidcid
	sid
	cid
	timeaction
	timerelease
	strategy
	responder
	detail

sipm_incident_value	
PK,FK1	**sidcid**
	sid
	cid
	timeupdate
	incident_count
	incident_flag
	similarity
	simiarity_scr_temp
	similarity_dst_temp
	port_temp
	sport_value
	dport_value
	sport
	dport
	frequency_signature
	frequency_sig_class

sipm_incident	
PK	**sidcid**
	sid
	cid
	signature
	sig_name
	sig_class_name
	sig_priority
	timestamp
	ip_src
	ip_dst
	ip_proto
	layer4_sport
	layer4_dport

sipm_scenario	
PK	**sidcidsn**
FK1	sidcid
FK2	scenario_id
	sid
	cid
	timeupdate
	asset_value
	event_value
	value

sipm_scenario_setting	
PK	**scenario_id**
	scenario_date
	scenario_name
	scenario_description
	asset_index
	event_index
	criticality_index
	maintainability_index
	replaceability_index
	dependability_index
	control_index
	severity_index
	exploitability_index
	sensitivity_index
	similiarity_index
	frequency_index
	name_index
	response_index
	color_index

sipm_protocol	
PK	**ip_proto**
	hexadecimal
	keyword
	protocol
	reference

Appendix E

PHP Source Codes

E.1 The *update_incident* application daemon source code

```php
<?php
  /*****************************************************
  * This application daemon runs in background and
  * update information in the sipm database
  * ***************************************************/
include ("../conf/configuration.inc");
include ("update_similarity_v3.php");
include ("update_frequency_v3.php");


function getNullIncident()
{
        $count = 0;
        $sql_temp =     "SELECT event.sid,event.cid FROM event " .
                        "LEFT JOIN sipm_incident " .
                        "ON event.cid = sipm_incident.cid ".
                        "AND event.sid = sipm_incident.sid " .
                        "where sig_name is NULL $sql ";

        $sql_query = mysql_query($sql_temp);

        while($alert = mysql_fetch_assoc($sql_query))
        {
                $count++;
                if($count==1)
                        {
                        $timestart = time();
                        }
        updateIncidentDetail($alert['sid'],$alert['cid']);
        };


        if($count>1)
        {
                $timeend = time();
                $time_diff = $timeend - $timestart;
                echo    "Incident Duration : $time_diff " . "second, " .
                        " date('Y-n-d G:i:s T') . ", Total updated : $count \n";
        }

        return $count;
}



function updateIncidentDetail($sid,$cid)
{

        $sql_temp =     " SELECT timestamp,signature, sig_name, sig_class_name, ".
                        " sig_priority, ip_src, ip_dst, ip_proto " .
                        " FROM (((event " .
                        " LEFT JOIN ".
                        " signature ON signature.sig_id = event.signature) " .
                        " LEFT JOIN ".
                        " iphdr ON iphdr.cid = event.cid AND iphdr.sid = event.sid) ".
                        " LEFT JOIN ".
                        " sig_class ON sig_class.sig_class_id = signature.sig_class_id) ".
                        " where event.cid = $cid " .
                        " AND event.sid = $sid " .
                        " limit 1" ;

        $sql_query = mysql_query($sql_temp);

        $alert = mysql_fetch_assoc($sql_query);
        $timestamp = $alert['timestamp'];
        $sig_name = $alert['sig_name'];
        $signature = $alert['signature'];
        $sig_class_name = $alert['sig_class_name'];
        $sig_priority = $alert['sig_priority'];
        $ip_src = $alert['ip_src'];
        $ip_dst = $alert['ip_dst'];
        $ip_proto = $alert['ip_proto'];
        $layer4_sport = "-";
        $layer4_dport = "-";

        if($ip_proto==6 || $ip_proto==17)
        list($layer4_sport,$layer4_dport) = getLayer4Protocol($sid,$cid,$ip_proto);

        $sidcid = "$sid.$cid";

        if($ip_proto==6 || $ip_proto==17)
        {
        $sql_insert =  " INSERT INTO sipm_incident" .
                       " (sidcid,sid,cid,signature,sig_name,sig_class_name, ".
                       " sig_priority,timestamp,ip_src,ip_dst,ip_proto, ".
                       " layer4_sport,layer4_dport) " .
                       " VALUES " .
                       " ('$sidcid','$sid','$cid','$signature','$sig_name',".
                       " '$sig_class_name', ".
                       " '$sig_priority','$timestamp','$ip_src','$ip_dst',".
                       " '$ip_proto',".
                       " '$layer4_sport','$layer4_dport') ";
        }
        else
        {
        $sql_insert =  " INSERT INTO sipm_incident" .
                       " (sidcid,sid,cid,signature,sig_name,sig_class_name,".
                       " sig_priority, ".
                       " timestamp,ip_src,ip_dst,ip_proto,layer4_sport,".
                       " layer4_dport) " .
                       " VALUES " .
                       " ('$sidcid','$sid','$cid','$signature','$sig_name',".
                       " '$sig_class_name',".
                       " '$sig_priority','$timestamp','$ip_src','$ip_dst',".
                       " '$ip_proto',".
                       " NULL,NULL) ";
        }
        mysql_query($sql_insert);

        //insert into new table sipm_incident_value
        $sql_insert =  " INSERT INTO sipm_incident_value" .
                       " (sidcid,sid,cid) " .
                       " VALUES " .
                       " ('$sidcid','$sid','$cid') ";
        mysql_query($sql_insert);

        $sql_insert =  " INSERT INTO sipm_incident_false" .
                       " (sidcid,sid,cid) " .
                       " VALUES " .
                       " ('$sidcid','$sid','$cid') ";
        mysql_query($sql_insert);

        //insert into new table sipm_incident_value
updateSimilarity($sid,$cid,$timestamp,$ip_proto,$ip_src,$ip_dst,$layer4_sport,$layer4_dport);
updatefrequency($sid,$cid,$timestamp,$signature, $sig_class_name);

}
function getLayer4Protocol($sid,$cid,$ip_proto)
{

        if($ip_proto== 6)
        $sql_temp =    " SELECT tcp_sport as layer4_sport, tcp_dport as layer4_dport ".
                       " FROM tcphdr where cid = " .
                       " $cid . " AND sid =" . $sid . " limit 1";
        if($ip_proto == 17)
        $sql_temp =    " SELECT udp_sport as layer4_sport, udp_dport as layer4_dport ".
                       " FROM udphdr where cid = " .
                       " $cid . " AND sid =" . $sid . " limit 1";

        $sql_query = mysql_query($sql_temp);
        while($alert = mysql_fetch_assoc($sql_query))
        {
                $layer4_sport = $alert['layer4_sport'];
                $layer4_dport = $alert['layer4_dport'];
        };

        return array($layer4_sport,$layer4_dport);

}

?>
<?php

        while(1)
        {
                        getNullIncident();
                        sleep($sipm_period_update_incident);
        }
?>
```

E.2 The *update_similarity_v3.php* source code

```
<?php

function
updateSimilarity($sid,$cid,$timestamp,$ip_proto,$ip_src,$ip_dst,$layer4_sport,$layer4_dport)
{

        $interval = $GLOBALS['sipmIntervalTime'];

        if($ip_proto == 6 || $ip_proto == 17)
        {
        $value = 0.5;
        $value2 = 0.25;
        $total =
        calculateSimilarity($sid,$cid,$timestamp,$interval,$ip_proto,$ip_src,$ip_dst,$value);
        $total += calculatePortSimilarity
        ($sid,$cid,$timestamp,$interval,$ip_proto,$layer4_sport,$layer4_dport,$value2);
        }
        else
        {
        $value = 0.5;
        $total =

        calculateSimilarity($sid,$cid,$timestamp,$interval,$ip_proto,$ip_src,$ip_dst,$value);

        }

        $sql_update =  " SELECT count(sipm_incident_value.cid) as total ".
                       " FROM sipm_incident_value " .
                       " LEFT JOIN ".
                       " sipm_incident ON sipm_incident.sidcid = sipm_incident_value.sidcid "
.

                       " WHERE timestamp ".
                       " BETWEEN '". $timestamp ."' - INTERVAL ". $interval .
                       " HOUR and '". $timestamp ."' " .
                       " AND sipm_incident.sid = $sid " .
                       " AND sipm_incident.cid < $cid " ;

        $sql_query = mysql_query($sql_update) or die(mysql_error());
        $alert = mysql_fetch_assoc($sql_query);
        $incident_count = $alert['total'];

        $total = round($total,4);
        $sql_update =  " UPDATE sipm_incident_value " .
                       " SET incident_count=$incident_count, similarity = $total " .
                       " WHERE cid = $cid" .
                       " AND sid = $sid ";
        $sql_query = mysql_query($sql_update) or die(mysql_error());
}

function
calculatePortSimilarity($sid,$cid,$timestamp,$interval,$ip_proto,$layer4_sport,$layer4_dport,$
value)
{
        $sql_update =  " UPDATE sipm_incident_value " .
                       " LEFT JOIN sipm_incident ".
                       " ON sipm_incident.sidcid = sipm_incident_value.sidcid "   .
                       " SET similarity = similarity + $value ".
                       " WHERE timestamp ".
                       " BETWEEN '". $timestamp ."' - INTERVAL ". $interval .
                       " HOUR and '". $timestamp ."' " .
                       " AND layer4_sport = $layer4_sport " .
                       " AND sipm_incident.ip_proto = $ip_proto " .
                       " AND sipm_incident.sid = $sid " .
                       " AND sipm_incident.cid <= $cid " ;

        $sql_query = mysql_query($sql_update) or die(mysql_error());
        $count_src_similarity = ($sql_query ? mysql_affected_rows() : 0);

        $sql_update =  " UPDATE sipm_incident_value " .
                       " LEFT JOIN sipm_incident ".
                       " ON sipm_incident.sidcid = sipm_incident_value.sidcid "   .
                       " SET similarity = similarity + $value ".
                       " WHERE timestamp ".
                       " BETWEEN '". $timestamp ."' - INTERVAL ". $interval .
```

```
                      " HOUR and '". $timestamp ."' " .
                      " AND layer4_dport = $layer4_dport " .
                      " AND sipm_incident.ip_proto = $ip_proto " .
                      " AND sipm_incident.sid = $sid " .
                      " AND sipm_incident.cid <= $cid " ;

       $sql_query = mysql_query($sql_update) or die(mysql_error());
       $count_dst_similarity = ($sql_query ? mysql_affected_rows() : 0);

       $total = ($value*$count_dst_similarity) + ($value*$count_src_similarity);
   /****************************************************************************************/
       $sql_when =    " AND (timestamp BETWEEN '". $timestamp ."' - INTERVAL ". $interval .
                      " HOUR and '". $timestamp ."') " .
                      " AND sipm_incident.ip_proto = $ip_proto " .
                      " AND sipm_incident.sid = $sid " .
                      " AND sipm_incident.cid <= $cid " ;

       $sql_update =  " UPDATE sipm_incident_value " .
                      " LEFT JOIN sipm_incident ON ".
                      " sipm_incident.sidcid = sipm_incident_value.sidcid "   .
                      " SET dport = " .
                      " CASE WHEN (layer4_dport > $layer4_dport ".
                      " AND layer4_dport != $layer4_dport $sql_when ) ".
                      " THEN layer4_dport - $layer4_dport ".
                      " ELSE $layer4_dport - layer4_dport END, ".
                      " sport =  ".
                      " CASE WHEN (layer4_sport > $layer4_sport ".
                      " AND layer4_sport != $layer4_sport $sql_when ) ".
                      " THEN layer4_sport - $layer4_sport ".
                      " ELSE $layer4_sport - layer4_sport END " ;

       $sql_query = mysql_query($sql_update) or die(mysql_error());


       $sql_update =  " UPDATE sipm_incident_value " .
                      " LEFT JOIN sipm_incident ON ".
                      " sipm_incident.sidcid = sipm_incident_value.sidcid "   .
                      " SET dport_value = " .
                      " CASE ".
                      " WHEN " .
                      " (dport > 0 AND dport <= 1024 $sql_when ) ".
                      " THEN round((1-(dport/1024)),4) ".
                      " WHEN ".
                      " (dport > 1024 AND dport <= 49151 $sql_when ) ".
                      " THEN round((1-(dport/49151)),4) ".
                      " WHEN ".
                      " (dport > 49151 AND dport <= 65535 $sql_when ) ".
                      " THEN round((1-(dport/65535)),4) ".
                      " ELSE 0 END, ".
                      " sport_value = ".
                      " CASE ".
                      " WHEN ".
                      " (sport > 0 AND sport <= 1024 $sql_when ) ".
                      " THEN round((1-(sport/1024)),4) ".
                      " WHEN ".
                      " (sport > 1024 AND sport <= 49151 $sql_when ) ".
                      " THEN round((1-(sport/49151)),4) ".
                      " WHEN ".
                      " (sport > 49151 AND sport <= 65535 $sql_when ) ".
                      " THEN round((1-(sport/65535)),4) ".
                      " ELSE 0 END " ;

       $sql_query = mysql_query($sql_update) or die(mysql_error());

       $sql_update =  " UPDATE sipm_incident_value " .
                      " LEFT JOIN ".
                      "  sipm_incident ON sipm_incident.sidcid = sipm_incident_value.sidcid "
.
                      " SET port_temp = round(($value*sport_value + $value*dport_value),4), "
                      " similarity = ".
                      " similarity + round(($value*sport_value + $value*dport_value),4) " .
                      " WHERE timestamp ".
                      " BETWEEN '". $timestamp ."' - INTERVAL ". $interval .
                      " HOUR and '". $timestamp ."' " .
                      " AND sport_value < 1 AND dport_value < 1 " .
                      " AND sipm_incident.ip_proto = $ip_proto " .
                      " AND sipm_incident.sid = $sid " .
```

```
                       " AND sipm_incident.cid <= $cid " ;

        $sql_query = mysql_query($sql_update) or die(mysql_error());

        $sql_update =  " SELECT sum(port_temp) as total FROM sipm_incident_value " .
                       " LEFT JOIN sipm_incident ".
ON sipm_incident.sidcid = sipm_incident_value.sidcid "   .
                       " WHERE timestamp ".
                       " BETWEEN '". $timestamp ."' - INTERVAL ". $interval .
                       " HOUR and '". $timestamp ."' " .
                       " AND sport_value < 1 AND dport_value < 1 " .
                       " AND sipm_incident.ip_proto = $ip_proto " .
                       " AND sipm_incident.sid = $sid " .
                       " AND sipm_incident.cid <= $cid " ;

        $sql_query = mysql_query($sql_update) or die(mysql_error());
        $alert = mysql_fetch_assoc($sql_query);
        $total_unsimilar = $alert['total'];

        return ($total+$total_unsimilar);
}



function calculateSimilarity($sid,$cid,$timestamp,$interval,$ip_proto,$ip_src,$ip_dst,$value)
{
        $value2 = round($value/2,2);

        $sql_update =  " UPDATE sipm_incident_value " .
                       " LEFT JOIN sipm_incident ".
                       " ON sipm_incident.sidcid = sipm_incident_value.sidcid "   .
                       " SET similarity =  ".
                       " CASE ".
                       " WHEN ((ip_proto = $ip_proto) AND (ip_proto = 6 OR ip_proto = 17)) ".
                       " THEN similarity + $value2 " .
                       " ELSE similarity + $value END, ".
                       " similarity_src_temp =  ".
                       " CASE ".
                       " WHEN ((ip_proto = $ip_proto) AND (ip_proto = 6 OR ip_proto = 17)) ".
                       " THEN $value2 " .
                       " ELSE $value END ".
                       " WHERE timestamp ".
                       " BETWEEN '". $timestamp ."' - INTERVAL ". $interval .
                       " HOUR and '". $timestamp ."' " .
                       " AND ip_src = $ip_src " .
                       " AND sipm_incident.sid = $sid " .
                       " AND sipm_incident.cid <= $cid " ;

        $sql_query = mysql_query($sql_update) or die(mysql_error());


        $sql_update =  " UPDATE sipm_incident_value " .
                       " LEFT JOIN sipm_incident ".
                       " ON sipm_incident.sidcid = sipm_incident_value.sidcid "   .
                       " SET similarity = ".
                       " CASE ".
                       " WHEN ((ip_proto = $ip_proto) AND (ip_proto = 6 OR ip_proto = 17)) ".
                       " THEN similarity + $value2 " .
                       " ELSE similarity + $value END, ".
                       " similarity_dst_temp =  ".
                       " CASE ".
                       " WHEN ((ip_proto = $ip_proto) AND (ip_proto = 6 OR ip_proto = 17)) ".
                       " THEN $value2 " .
                       " ELSE $value END ".
                       " WHERE timestamp ".
                       " BETWEEN '". $timestamp ."' - INTERVAL ". $interval .
                       " HOUR and '". $timestamp ."' " .
                       " AND ip_dst = $ip_dst " .
                       " AND sipm_incident.sid = $sid " .
                       " AND sipm_incident.cid <= $cid " ;

        $sql_query = mysql_query($sql_update) or die(mysql_error());

        list($rangemin,$rangemax) = getClass($ip_src);

        $sql_update =  " UPDATE sipm_incident_value " .
                       " LEFT JOIN sipm_incident ".
                       " ON sipm_incident.sidcid = sipm_incident_value.sidcid "  .
                       " SET similarity = ".
                       " CASE ".
                       " WHEN ((ip_proto =  $ip_proto) AND (ip_proto = 6 OR ip_proto = 17)) ".
                       " THEN similarity + round(($value2/2),4) " .
                       " ELSE similarity + $value2 END, ".
                       " similarity_src_temp = ".
                       " CASE ".
                       " WHEN ((ip_proto = $ip_proto) AND (ip_proto = 6 OR ip_proto = 17)) ".
                       " THEN similarity_src_temp + round(($value2/2),4) " .
                       " ELSE similarity_src_temp + $value2 END ".
                       " WHERE timestamp ".
                       " BETWEEN '". $timestamp ."' - INTERVAL ". $interval .
                       " HOUR and '". $timestamp ."' " .
                       "  AND (ip_src >=$rangemin AND ip_src <=$rangemax AND ip_src != $ip_src
)".
                       " AND sipm_incident.sid = $sid " .
                       " AND sipm_incident.cid <= $cid " ;

        $sql_query = mysql_query($sql_update) or die(mysql_error());


        list($rangemin,$rangemax) = getClass($ip_dst);

        $sql_update =  " UPDATE sipm_incident_value " .
                       " LEFT JOIN sipm_incident ON ".
                       " sipm_incident.sidcid = sipm_incident_value.sidcid "  .
                       " SET similarity = ".
                       " CASE ".
                       "  WHEN  ((ip_proto =  $ip_proto) AND (ip_proto = 6 OR ip_proto = 17) )
".
                       " THEN similarity + round(($value2/2),4) " .
                       " ELSE similarity + $value2 END, ".
                       " similarity_dst_temp = ".
                       " CASE ".
                       "  WHEN  ((ip_proto =  $ip_proto) AND (ip_proto = 6 OR ip_proto = 17) )
".
                       " THEN similarity_dst_temp + round(($value2/2),4) " .
                       " ELSE similarity_dst_temp + $value2 END ".
                       " WHERE timestamp ".
                       " BETWEEN '". $timestamp ."' - INTERVAL ". $interval .
                       " HOUR and '". $timestamp ."' " .
                       "  AND (ip_dst>= $rangemin AND ip_dst <=$rangemax AND ip_dst != $ip_dst
)".
                       " AND sipm_incident.sid = $sid " .
                       " AND sipm_incident.cid <= $cid " ;

        $sql_query = mysql_query($sql_update) or die(mysql_error());


        $sql_update =  " SELECT sum(similarity_dst_temp) as total, ".
                       " sum(similarity_src_temp) as total2 " .
                       " FROM  sipm_incident_value " .
                       " LEFT JOIN sipm_incident ON ".
                       " sipm_incident.sidcid = sipm_incident_value.sidcid "  .
                       " WHERE timestamp ".
                       " BETWEEN '". $timestamp ."' - INTERVAL ". $interval .
                       " HOUR and '". $timestamp ."' " .
                       " AND sipm_incident.sid = $sid " .
                       " AND sipm_incident.cid <= $cid " ;

        $sql_query = mysql_query($sql_update) or die(mysql_error());
        $alert = mysql_fetch_assoc($sql_query);
        $total = $alert['total'] + $alert['total2'] ;

        $sql_update =  " UPDATE sipm_incident_value ".
                       " LEFT JOIN sipm_incident ON ".
                       " sipm_incident.sidcid = sipm_incident_value.sidcid "  .
                       " SET similarity_dst_temp = 0, similarity_src_temp=0 ".
                       " WHERE timestamp ".
                       " BETWEEN '". $timestamp ."' - INTERVAL ". $interval .
                       " HOUR and '". $timestamp ."' " .
                       " AND sipm_incident.sid = $sid " .
                       " AND sipm_incident.cid <= $cid " ;

        $sql_query = mysql_query($sql_update) or die(mysql_error());
        return  ($total);
}

function getClass($ip_address)
{
        $ip_address_ = explode(".", sipmLong2IP($ip_address));

        if($ip_address >= 0 && $ip_address <=2147483647)
                $class =  "A";
        else if($ip_address >= 2147483648 && $ip_address <= 3221225471)
                $class =  "B";
        else if($ip_address >= 3221225472 && $ip_address <=3758096383)
                $class =  "C";
        else if($ip_address >= 3758096384 && $ip_address <=4026531839)
                $class =  "D";
        else if($ip_address >= 4026531840 && $ip_address <=4294967295)
                $class =  "E";

        switch ($class)
        {
        case "A":
                $localip =  $ip_address_[0] . "." . "0.0.0";
                $rangemax = sipmIP2Long($localip) + 16777216;
                break;
        case "B":
                $localip =  $ip_address_[0] . "." . $ip_address_[1] . ".0.0";
                $rangemax = sipmIP2Long($localip) + 65536;
                break;
        case "C":
                $localip = $ip_address_[0] . "." . $ip_address_[1] . "." . $ip_address_[2] .
".0";
                $rangemax = sipmIP2Long($localip) + 256;
                break;
        case "D":
                $localip =  $ip_address_[0] . "." . $ip_address_[1] . ".0.0";
                $rangemax = sipmIP2Long('239.255.255.255');
                break;
        case "E":
                $localip =  $ip_address_[0] . "." . $ip_address_[1] . ".0.0";
                $rangemax = sipmIP2Long('255.255.255.255');
                break;
}
        $rangemin = sipmIP2Long($localip);
        return array($rangemin,$rangemax);
}
?>
```

E.3 The update_frequecy_v3.php source code

```
<?php

function updatefrequency($sid,$cid,$timestamp,$signature,$sig_class_name)
{

        $signature_count_self = 0;
        $sig_class_id_count_self = 0 ;

        $interval = $GLOBALS['sipmIntervalTime'];

        $sql_update =  " UPDATE sipm_incident_value ".
                       " LEFT JOIN sipm_incident ON ".
                       " sipm_incident.sidcid = sipm_incident_value.sidcid ".
                       " SET frequency_signature = frequency_signature + 1 ".
                       " WHERE timestamp BETWEEN '". $timestamp .
                       " ' - INTERVAL ". $interval . " HOUR and '". $timestamp ."' " .
                       " AND signature = '$signature' " .
                       " AND sipm_incident.sid = $sid " .
                       " AND sipm_incident.cid <= $cid " ;

        $sql_query = mysql_query($sql_update) or die(mysql_error());
        $count_frequency_signature = ($sql_query ? mysql_affected_rows() : 0);

        $sql_update =  " UPDATE sipm_incident_value " .
                       " LEFT JOIN sipm_incident ".
                       " ON sipm_incident.sidcid = sipm_incident_value.sidcid "  .
                       " SET frequency_sig_class = frequency_sig_class + 1 ".
                       " WHERE timestamp BETWEEN '". $timestamp .
                       " ' - INTERVAL ". $interval . " HOUR and '". $timestamp ."' " .
                       " AND sig_class_name = '$sig_class_name' " .
                       " AND sipm_incident.sid = $sid " .
                       " AND sipm_incident.cid <= $cid " ;
        $sql_query = mysql_query($sql_update) or die(mysql_error());
        $count_frequency_sig_class = ($sql_query ? mysql_affected_rows() : 0);

        $sql_update =  " UPDATE sipm_incident_value " .
                       " SET timeupdate=NOW(),".
                       " frequency_signature = $count_frequency_signature   " .
                       " , frequency_sig_class = $count_frequency_sig_class " .
                       " WHERE cid = $cid" .
                       " AND sid = $sid ";

        $sql_query = mysql_query($sql_update) or die(mysql_error());

        $sql_update =  " UPDATE sipm_incident_value " .
                       " LEFT JOIN sipm_incident ".
                       " ON sipm_incident.sidcid = sipm_incident_value.sidcid "  .
                       " SET incident_count = incident_count + 1 ".
                       " WHERE timestamp BETWEEN '". $timestamp .
                       " ' - INTERVAL ". $interval . " HOUR and '". $timestamp ."' " .
                       " AND sipm_incident.sid = $sid " .
                       " AND sipm_incident.cid <= $cid " ;

        $sql_query = mysql_query($sql_update) or die(mysql_error());
}
?>
```

E.4 The update_event_value application daemon source code

```php
<?php
/****************************************************
* This application daemon runs in background
* and update information in the sipm database
* ****************************************************/
include ("../conf/configuration.inc");
include ("update_scenario_value.php");
include ("cvss.php");

function checkLastEventValue()
{

        $count = 0;
        $sql_temp =    " SELECT sipm_incident_value.sid, " .
                       " sipm_incident_value.cid, sipm_incident.timestamp " .
                       " FROM ((sipm_incident_value " .
                       " LEFT JOIN sipm_event_value " .
                       " ON sipm_event_value.sidcid = sipm_incident_value.sidcid) " .
                       " LEFT JOIN sipm_incident " .
                       " ON sipm_incident_value.sidcid = sipm_incident.sidcid) " .
                       " WHERE sipm_event_value.timeupdate is NULL " .
                       " ORDER BY sipm_incident.timestamp DESC " .
                       " limit 1";

        $sql_query = mysql_query($sql_temp);
        while($alert = mysql_fetch_assoc($sql_query))
        {
                retrieveEventvalue($alert['timestamp']);
        };

}

function retrieveEventValue($timestamp)
{
        $count = 0;

        $interval = $GLOBALS['sipmIntervalTime'];

        $sql_temp =    " SELECT sipm_incident_value.sid, " .
                       " sipm_incident_value.cid, signature,timestamp " .
                       ",ip_src, ip_dst " .
                       " FROM sipm_incident_value ".
                       " LEFT JOIN sipm_incident " .
                       " ON sipm_incident.sidcid = sipm_incident_value.sidcid " .
                       " WHERE timestamp BETWEEN '". $timestamp .
                       "' - INTERVAL ". $interval . " HOUR and '". $timestamp ."' " ;

        $sql_query = mysql_query($sql_temp);

        while($alert = mysql_fetch_assoc($sql_query))
        {
        $count++;
        if($count==1)
        {
                $timestart = time();
        }

updateEventValue($alert['sid'],$alert['cid'],$alert['signature'],$alert['ip_src'],$alert['ip_dst'],$timestamp);
        };


        if($count>1)
        {
        $timeend = time();
        $time_diff = $timeend - $timestart;
        echo "\nEvent Duration : $time_diff " . "second, " . date('Y-n-d G:i:s T') .", Update : $count";
        checkEmptyCvss();
        }
}

function updateEventValue($sid,$cid,$signature, $ip_src, $ip_dst, $timeupdate)
{
  //get the asset detail on the event

        $sql_temp =    " SELECT identityid, identityip, " .
                       " max(criticality) as criticality, " .
                       " max(maintainability) as maintainability, " .
                       " max(replaceability) as replaceability, " .
                       " max(dependability) as dependability,      max(control) as control ".
                       " FROM sipm_asset_identity " .
                       " WHERE identityip LIKE '$ip_src' " .
                       " OR identityip LIKE '$ip_dst' ";

        $sql_query = mysql_query($sql_temp);
        $alert = mysql_fetch_assoc($sql_query);


        if(is_NULL($alert['identityip']))
        {
                $criticality   = 0 ;
                $maintainability       = 0 ;
                $replaceability = 0;
                $dependability = 0;
                $control = 0 ;
                $identityid = 0 ;
        }
        else
        {
                $criticality = round(($alert['criticality']/100),4);
                $maintainability = round(($alert['maintainability']/100),4);
                $replaceability = round(($alert['replaceability']/100),4);
                $dependability = round(($alert['dependability']/100),4);
                $control = round(($alert['control']/100),4);
                $identityid = $alert['identityid'];
        }




        $sql_temp =    " SELECT avg(base_score) as base_score, " .
                       " avg(exploitability) as exploitability FROM sipm_cvss " .
                       " WHERE sig_id = $signature limit 1";

        $sql_query = mysql_query($sql_temp);
        $alert = mysql_fetch_assoc($sql_query);
        if(is_NULL($alert['base_score']))
        {
                $severity = 0;
                $exploitability = 0;
        }
        else
        {
                $severity = round(($alert['base_score']/10),4);
                $exploitability = round(($alert['exploitability']/10),4);
        }

        $sql_temp =    " SELECT similarity, frequency_signature, " .
                       " frequency_sig_class, sensitivity, incident_count " .
                       " FROM sipm_incident_value " .
                       " LEFT JOIN sipm_sensor " .
                       " on sipm_incident_value.sid = sipm_sensor.sid " .
                       " WHERE sipm_incident_value.cid = $cid " .
                       " AND sipm_incident_value.sid = $sid limit 1";


        $sql_query = mysql_query($sql_temp);
        $alert = mysql_fetch_assoc($sql_query);

        $sensitivity = round(($alert['sensitivity']/10),4);
        $similarity = round(($alert['similarity']/$alert['incident_count']),4);
        $frequency   =  0.5*(round(($alert['frequency_signature']/$alert['incident_count']),4))
+ 0.5*(round(($alert['frequency_sig_class']/$alert['incident_count']),4));
        $frequency = round($frequency,4);

        $sidcid = $sid . "." . $cid;

        $sql_update_2 = " INSERT INTO sipm_event_value " .
                        " (sidcid,sid,cid,timeupdate,severity, " .
                        " exploitability,sensitivity,similarity,frequency, " .
                        " identityid,criticality,maintainability, " .
                        " replaceability,dependability,control) ".
                        " VALUES "  .
                        " ('$sidcid',$sid,$cid,'$timeupdate', " .
                        " $severity,$exploitability,$sensitivity,$similarity,$frequency, ".
                        " $identityid,$criticality,$maintainability, " .
                        " $replaceability,$dependability,$control) " .
                        " ON DUPLICATE KEY " .
                        " UPDATE timeupdate= '$timeupdate', severity = $severity " .
                        ", exploitability = $exploitability " .
                        ", sensitivity = $sensitivity " .
                        ", similarity = $similarity " .
                        ", frequency = $frequency " .
                        ", identityid = $identityid " .
                        ", criticality = $criticality " .
                        ", maintainability = $maintainability " .
                        ", replaceability = $replaceability " .
                        ", dependability = $dependability " .
                        ", control = $control " ;

        mysql_query($sql_update_2);
}

while(1)
        {
        checkLastEventValue();
        GetScenario();
        sleep($sipm_period_update_incident);
        }
?>
```

E.5 The update_scenario_value.php source code

```
<?php

/****************************************************
* This application is triggered to update incidents’ value
*****************************************************/
function checkLastScenarioValue($scenario_id)
{
        $flag == 0;

        $sql_temp =    " SELECT min(value) as value " .
                       " FROM sipm_scenario ".
                       " WHERE timeupdate = " .
                       " (SELECT timestamp from sipm_incident order by timestamp DESC limit 1)
".
                       " AND scenario_id = $scenario_id " .
                       " limit 1" ;

        $sql_query = mysql_query($sql_temp);
        $alert = mysql_fetch_assoc($sql_query);

        if($alert['value'] == 0)
        {
                doUpdate($scenario_id);
                $flag = 1;
        };

}

function doUpdate($scenario_id)
{

        $sql_temp ="SELECT timestamp from sipm_incident order by timestamp DESC limit 1";
        $sql_query = mysql_query($sql_temp);
        $alert = mysql_fetch_assoc($sql_query);
        $timestamp =  $alert['timestamp'];

        $count = retrieveScenarioValue($timestamp,$scenario_id);
        echo date('Y-n-d G:i:s T');
        echo ", Total updated : $count";
}

function retrieveScenarioValue($timestamp,$scenario_id)
{
        $count = 0;

        $interval = $GLOBALS['sipmIntervalTime'];

        $sql_temp =    " SELECT " .
                       " asset_index, event_index, " .
                       " criticality_index, maintainability_index,  replaceability_index,
                               " dependability_index, control_index, " .
                       " severity_index, exploitability_index, sensitivity_index,".
                       " similarity_index, frequency_index " .
                       " FROM sipm_scenario_setting ".
                       " WHERE scenario_id = $scenario_id " ;

        $sql_query = mysql_query($sql_temp);
        $alert = mysql_fetch_assoc($sql_query);

        $event_index =  $alert['event_index'];
        $asset_index =  $alert['asset_index'];
        $total_event_index =
array($alert['severity_index'],$alert['exploitability_index'],$alert['sensitivity_index'],$ale
rt['similarity_index'],$alert['frequency_index']);
        $total_asset_index =
array($alert['criticality_index'],$alert['maintainability_index'],$alert['replaceability_index
'],$alert['dependability_index'],$alert['control_index']);

        $sql_temp =    "SELECT sipm_incident.sid,sipm_incident.cid " .
                       " FROM sipm_incident " .
                       " WHERE timestamp BETWEEN '". $timestamp .
                       "' - INTERVAL ". $interval . " HOUR and '". $timestamp ."'" ;

        $sql_query = mysql_query($sql_temp);
        while($alert = mysql_fetch_assoc($sql_query))
        {
                $count++;
                if($count==1)
                        $timestart = time();
        updateScenarioValue($scenario_id, $alert['sid'],
$alert['cid'],$event_index,$asset_index,$total_event_index,$total_asset_index,$timestamp);
        };


        if($count>1)
        {
                $timeend = time();

                $time_diff = $timeend - $timestart;
                echo "\nScenario $scenario_id Duration : $time_diff " . "second,";
        }

        return $count;

}

function
updateScenarioValue($scenario_id,$sid,$cid,$event_index,$asset_index,$total_event_index,$total
_asset_index,$timestamp)
{

        $sql_temp =     " SELECT ".
                        " severity, exploitability, sensitivity, similarity, frequency, " .
                        " criticality, ".
                        " maintainability, replaceability , dependability, control " .
                        " FROM sipm_event_value " .
                        " WHERE sipm_event_value.cid = $cid " .
                        " AND sipm_event_value.sid = $sid limit 1";


        $sql_query = mysql_query($sql_temp);
        $alert = mysql_fetch_assoc($sql_query);


        $severity   = round(($total_event_index[0]/100 * $alert['severity']),4);
        $exploitability  = round(($total_event_index[1]/100 * $alert['exploitability']),4);
        $sensitivity  = round(($total_event_index[2]/100 * $alert['sensitivity']),4);
        $similarity  = round(($total_event_index[3]/100 * $alert['similarity']),4);
        $frequency  = round(($total_event_index[4]/100 * $alert['frequency']),4);
        $event_value_list  = $severity  .  ","  .  $exploitability  .  ","  .  $sensitivity  .  ","
.$similarity  . "," . $frequency;

        $criticality  = round(($total_asset_index[0]/100 * $alert['criticality']),4);
        $maintainability  = round(($total_asset_index[1]/100 * $alert['maintainability']),4);
        $replaceability  = round(($total_asset_index[2]/100 * $alert['replaceability']),4);
        $dependability  = round(($total_asset_index[3]/100 * $alert['dependability']),4);
        $control  = round(($total_asset_index[4]/100 * $alert['control']),4);
        $asset_value_list = $criticality  .  ","  .  $maintainability  .  ","  .  $replaceability  .
"," .$dependability  . "," . $control ;

        $scenario_value                                                                          =
(round($event_index/100,4)*($severity+$exploitability+$sensitivity+$similarity  +  $frequency))
+
(round($asset_index/100,4)*($criticality+$maintainability+$replaceability+$dependability+$cont
rol));
        $scenario_value = round($scenario_value,4);
        $sidcidsn = "$sid.$cid.$scenario_id";
        $sidcid = "$sid.$cid";




        $sql_update_2 =         " INSERT INTO sipm_scenario ".
                                " (sidcidsn,sidcid,sid,cid,scenario_id,timeupdate, ".
                                " asset_value,event_value,value) " .
                                " VALUES  ('$sidcidsn','$sidcid',$sid,$cid,$scenario_id,  ".
                                " '$timestamp','$asset_value_list','$event_value_list',  ".
                                " $scenario_value) " .
                                " ON DUPLICATE KEY UPDATE ".
                                " timeupdate= '$timestamp', sidcid=$sidcid,  ".
                                " asset_value='$asset_value_list', ".
                                " event_value='$event_value_list', value=$scenario_value ";

        mysql_query($sql_update_2);

        $sql_update_3 =         " INSERT INTO sipm_scenario_history " .
                                " (sidcidsn,sidcid,sid,cid,scenario_id,timeupdate,value) " .
                                " VALUES ('$sidcidsn','$sidcid',$sid,$cid, ".
                                " $scenario_id,'$timestamp',$scenario_value) " ;
        mysql_query($sql_update_3);
 }

?>
<?php

function GetScenario()
{
        $sql_temp =     " SELECT scenario_id  " .
                        " FROM sipm_scenario_setting" ;

        $sql_query = mysql_query($sql_temp);
        if ($sql_query)
        {
                while($alert = mysql_fetch_assoc($sql_query))
                {
                        $scenario_id = $alert['scenario_id'];
                        checkLastScenarioValue($scenario_id);
                };
        }
        else
        {
                print('MySQL query failed with error: ' . mysql_error());
        }

}

?>
```

E.6 The update_scenario_value.php source code

```
<?php

/****************************************************
 * This function retrieves the base score
 * and exploitability of incidents using CVE ID
 ****************************************************/


function retrieveCvss($cve)
{

        $file = "http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-" . $cve;
        $doc = new DOMDocument();
        $doc->loadHTMLFile($file);
        $xpath = new DOMXpath($doc);
        $elements = $xpath->query("//div[@class='row']");

        $count=0;
        if (!is_null($elements))
        {
                foreach ($elements as $element)
                {
                $count++;

          //get Original release date
                if($count== 1)
                {
                        $nodes = $element->childNodes;
                        $i=0;
                        foreach ($nodes as $node)
                        {
                        $i++;
                                //echo "$i " . $node->nodeValue . "\n";
                        if($i==2)
                        $release_date = trim($node->nodeValue);
                        }
                }

                //get Original revise date
                if($count== 2)
                {
                        $nodes = $element->childNodes;
                        $i=0;
                        foreach ($nodes as $node)
                        {
                                $i++;
                                //echo "$i " . $node->nodeValue . "\n";
                                if($i==2)
                                $revise_date = trim($node->nodeValue);

                        }
                }

                //get CVSS
                if($count== 4)
                {
                        $nodes = $element->childNodes;
                        $i=0;
                        foreach ($nodes as $node)
                        {
                        $i++;
                        // echo "$i " . $node->nodeValue . "\n";
                        if($i==2)
                        $base_score = trim($node->nodeValue);

                 }
                }

                //get   $exploitability
                if($count== 6)
                {
                        $nodes = $element->childNodes;
                        $i=0;
                        foreach ($nodes as $node)
                        {
                                $i++;
                                if($i==2)
                                $exploitability = trim($node->nodeValue);
                        }
                }
                }
        }

        return array($release_date,$revise_date,$base_score,$exploitability);
}



function checkEmptyCvss()
{

        $sql_temp =     " SELECT sig_id,ref_tag,reference.ref_id " .
                        " FROM ((reference " .
                        " LEFT JOIN reference_system " .
                        " ON reference_system.ref_system_id = reference.ref_system_id) " .
                        " LEFT JOIN sig_reference on sig_reference.ref_id = reference.ref_id) "
.
                        " WHERE ref_system_name LIKE '%cve%' " .
                        " AND ref_tag NOT IN ".
                        " (SELECT ref_tag FROM sipm_cvss)";

        $sql_query = mysql_query($sql_temp);

        while($alert = mysql_fetch_assoc($sql_query))
        {

          $ref_tag  = $alert['ref_tag'];
          $sig_id   = $alert['sig_id'];
          $ref_id   = $alert['ref_id'];

        list($release_date,$revise_date,$base_score,$exploitability) = retrieveCvss($ref_tag);

        $date = explode("/",$release_date);
        $release_date =   $date[2] .  "-" . $date[0] .  "-" . $date[1];
        $date = explode("/",$revise_date);
        $revise_date =   $date[2] .  "-" . $date[0] .  "-" . $date[1];

        $sql_insert =   " INSERT INTO sipm_cvss ".
                        " (ref_tag,sig_id,ref_id,release_date, ".
                        " revise_date,base_score,exploitability) " .
                        " VALUES " .
                        " ('$ref_tag','$sig_id','$ref_id','$release_date', ".
                        " '$revise_date','$base_score','$exploitability') ";

        mysql_query($sql_insert);

        echo "\nCVSS $ref_tag Update : " . date('Y-n-d G:i:s T') ;

        };

}


?>
```

Appendix F

Publication

1. Anuar, N.B., Papadaki, M., Furnell, S. and Clarke, N. (2009), "Response Mechanisms for Intrusion Response Systems (IRSs)", Proceedings of the Fifth Collaborative Research Symposium on Security, E-learning, Internet and Networking (SEIN 2009), Darmstadt, Germany, ISBN: 978-1-84102-236-9, pp3-14.

2. Anuar, N.B., Papadaki, M., Furnell, S. and Clarke, N. (2010), "An investigation and survey of response options for Intrusion Response Systems (IRSs)", Proceedings of the Information Security for South Africa (ISSA), Johannesburg, South Africa, pp. 1-8.

3. Anuar, N.B., Furnell, S., Papadaki, M., and Clarke, N. (2011), "A Risk Index Model for Security Incident Prioritisation", Proceedings of the 9th Australian Information Security Management Conference (AISM 2011), Perth, Western Australia, pp. 25-29.