UNIVERSIDADE DE LISBOA

FACULDADE DE CIÊNCIAS

DEPARTAMENTO DE INFORMÁTICA

Threat Detection in SIEM Considering Risk Assessment

Ana Mafalda Silva Osório

Mestrado em Engenharia Informática

Sistemas de Informação

Dissertação orientada por:

Profª. Doutora Ana Luísa do Carmo Correia Respício

Engenheiro Pedro da Silva Dias Rodrigues

2018

Acknowledgments

During the development of this work, I relied on the direct or indirect support of multiple people to which I am deeply grateful. My thank you to the DiSIEM project for financing this dissertation.

I would first like to thank my advisers, Prof. Doc. Ana Luísa do Carmo Correia Respício and Engineer Pedro Dias Rodrigues for accepting me for the development of this thesis. All your guidance, availability, support and encouragement in the crucial moments of this journey was indispensable and extremely valuable, either in the growth of the present project, whether in my growth as a person.

I would also like to thank the Security Operation Center experts from EDP. All your help was essential for this thesis development and without it, none of this would have been possible. I would like to give a special thanks to Ricardo Martins, Ivo Rosa, Gonçalo Martins, João Alves and Vanessa Gomes. Thank you very much for your ideas, your availability, all your patience, your jokes and all the laughs we shared in the SOC room.

I am also very grateful for all my friends who accompanied me throughout this academic, and non-academic journey, and with who I shared unforgettable moments. A special thank you to my girls, Margarida Duarte, Anita Santos, Beatriz Riquito, Sara Loureiro and Lúcia Rodrigues. Thank you for all your encouragement on the development of this work, for our random conversations, and especially for all your help and advice throughout the years.

To my not so little brother the biggest thanks of them all. Thank you for your daily rant about life, for sending me a message every day we were apart and thank you for the understanding always manifested despite the lack of attention and absences. After 16 years, you are still the best gift I ever received.

Finally, I am very grateful to my family, especially to my parents for the encouragement received along these years as well as the economic support, to Gonçalo Lima for always believing in me and for all the patience, and to my grandparents for their company and for all our Sunday lunches throughout these five years.

This work is supported by the European Commission through the H2020 programme under grant agreement 700692 (DiSIEM).

Dedicated to my parents and my brother

Resumo

Nos dias de hoje, a segurança informática é cada vez mais um assunto fundamental. Os sistemas informáticos são indispensáveis para o funcionamento das organizações e um dos seus maiores problemas é que estão sujeitos a ficar comprometidos, podendo assim afetar o desempenho e a reputação de toda a organização. As ameaças contra a segurança e a confiabilidade de infraestruturas críticas, nomeadamente redes elétricas, podem resultar em ocorrências fatais para a normal atividade tanto das organizações como da sociedade. Um ciberataque a uma infraestrutura crítica pode afetar a vida de milhares de pessoas, visto que pode ser fruto de um ataque terrorista.

Desta forma, as empresas têm investido em processos de gestão de risco de segurança de informação. Estes processos tornam possível proteger os diversos ativos, monitorizar os serviços, processos e projetos, de forma a conseguir reduzir tanto quanto possível a perda de tempo, esforço e custos com a recuperação de incidentes de segurança.

A gestão de risco tem como objetivo minimizar ou até mesmo eliminar o impacto negativo que os riscos possam ter numa determinada organização. O processo de gestão de risco é habitualmente composto por cinco etapas interligadas entre si: a comunicação e consulta, que ocorre ao longo de todas as etapas deve ser feita em conjunto com as partes interessadas e que deve abordar questões relativas ao risco, tais como as suas causas, consequências e medidas que devem ser usadas para tratar o risco; o estabelecimento de contexto, onde são definidos os critérios utilizados durante o processo de gestão de risco; o processo de avaliação de risco, constituído por fases de identificação, análise e avaliação do risco; o tratamento do risco, onde são selecionadas medidas que podem ser aplicadas com o objetivo de reduzir o risco anteriormente identificado; e por último a etapa de monitorização e revisão de risco, que garante que todo o processo de gestão de risco funciona corretamente, assegurando que as medidas aplicadas são as mais corretas, obtendo mais informações para melhoria do risco, detetando mudanças no contexto e identificando riscos emergentes. No final de todo este processo a organização conseguirá obter o conhecimento do risco a que está sujeita, podendo assim ter um processo de tomada de decisões ajustado às suas necessidades.

Uma das tecnologias mais usadas pelas empresas para realizar a monitorização de eventos de cibersegurança são os sistemas de gestão e correlação de eventos *Security Information and Event Management* (SIEM). Estes sistemas fazem a coleção de

informação proveniente de várias fontes. Depois de recolhidos os dados, como os mesmos são provenientes de diversas fontes, são todos colocados na mesma estrutura, ou seja, são normalizados. Depois de normalizados, através da utilização de filtros e regras para a deteção de padrões de comportamentos maliciosos, é feita a deteção de possíveis anomalias nos sistemas da organização e são gerados alertas. Cabe à equipa responsável pela gestão dos incidentes de cibersegurança analisar e reagir a estes alertas gerados pelo SIEM. Atualmente estes sistemas têm algumas limitações, nomeadamente não conseguem comunicar o risco de uma forma simples e eficaz para os gestores das organizações. Assim, é necessário adicionar a esta tecnologia outros indicadores relevantes, com o objetivo de melhorar a eficiência das equipas de segurança.

Os processos de gestão de risco são, regra geral, básicos e não contemplam caraterísticas inatas das infraestruturas, tais como as dependências e diferenças entre os tipos de ativos monitorizados.

O projeto DiSIEM propõe colmatar este problema, através do desenvolvimento de extensões que são instaladas como componentes externas e integradas com os SIEM. No âmbito do projeto já foi desenvolvido um modelo e uma ferramenta, no entanto a ferramenta desenvolvida não foi integrada num ambiente real. A ferramenta consistia num modelo multinível para apreciação de risco, de forma a que fosse possível transmitir uma noção de risco às partes interessadas, utilizando as informações provenientes do SIEM. Esta ferramenta tal como este trabalho, foram desenvolvidos no contexto do projeto DiSIEM através de uma colaboração entre a Faculdade de Ciências da Universidade de Lisboa e a EDP - Energias de Portugal, SA.

O modelo desenvolvido faz uma apreciação de risco em três níveis diferentes: máquinas, aplicações e serviços. Esta apreciação é realizada com base em três versões diferentes do modelo, sendo sempre consideradas três componentes para o cálculo do risco: vulnerabilidades, dependências e incidentes.

Assim, o propósito deste trabalho consistiu em tornar a ferramenta operacional num ambiente empresarial, fazer novos desenvolvimentos na mesma e integrá-la com o SIEM existente na EDP, o Micro Focus ArcSight. Isto irá permitir aumentar a capacidade de comunicação de risco aos gestores da organização por parte das equipas de segurança; auxiliar o processo de tomada de decisão; e atribuir uma maior ou menor relevância aos eventos detetados pelo SIEM, devido à monitorização mais eficaz considerando os resultados da avaliação de risco.

A ferramenta conta com várias informações recolhidas no universo EDP, nomeadamente os ativos, as vulnerabilidades e os incidentes da empresa.

A informação acerca dos ativos foi obtida através de uma extração à base de dados da organização que, dada a grande escala e diversidade de operação, tem uma quantidade

de ativos muito grande, na ordem dos milhares. No processo de identificação dos ativos da empresa foram identificadas algumas incoerências nos dados, o que levou à necessidade de cruzar as informações recolhidas com outras fontes de informação do universo EDP.

As vulnerabilidades são obtidas através da junção de informação de duas fontes diferentes: uma empresa responsável por realizar *pen-testing* e uma fonte adicional de dados, um detetor de vulnerabilidades de infraestrutura, o *Nessus Vulnerability Scanner*. Este *software* é responsável por detetar as vulnerabilidades existentes nas infraestruturas da EDP e, apesar de o mesmo já estar presente no universo EDP antes do desenvolvimento desta ferramenta, as vulnerabilidades detetadas não eram ainda tidas em conta pela equipa de segurança. Ao integrarmos as vulnerabilidades detetadas pelo *Nessus* com todas as detetadas através de *pen-testing* e já existentes no nosso modelo, conseguimos assim avaliar o risco de forma mais rigorosa por termos em conta todas as vulnerabilidades conhecidas no ambiente EDP.

Os incidentes tanto podem ser detetados por utilizadores ou podem surgir da monitorização de eventos por parte da equipa do SOC. Porém, os incidentes que se encontram incluídos na base de dados são apenas os provenientes do SIEM em uso na EDP.

Todos os dados recolhidos, depois de uniformizados e estruturados, são então importados para uma base de dados global, através de um módulo feito para esse propósito. Esta base de dados foi contruída com o objetivo de aglomerar todas as informações recolhidas e a mesma encontra-se adaptada ao ambiente EDP.

Depois de os dados estarem na base de dados, é possível aplicar o processo de avaliação de risco para cada um dos ativos identificados. Dado que o processo tem em conta as dependências entre ativos, inicia-se com o cálculo do risco ao nível das máquinas, passando depois ao nível das aplicações e por fim para o nível dos serviços.

Todos os dados relevantes são depois apresentados num *dashboard* que providencia capacidade para fazer *risk analytics*. Isto é, é possível analisar detalhadamente as componentes associadas ao risco de cada ativo. Este *dashboard* possibilita também que haja uma interação direta com a base de dados na interface, permitindo que as vulnerabilidades e os incidentes abertos possam ser fechados, permitindo inclusive que haja a inserção de novas vulnerabilidades ou incidentes pela equipa de cibersegurança. É ainda possível gerar relatórios pdf com os valores de risco para um determinado período de tempo, de forma a que seja possível auxiliar os decisores nas tomadas de decisão.

Todas estas funcionalidades foram melhorias ao *dashboard* desenvolvido na etapa anterior do projeto.

A ferramenta encontra-se ainda interligada com o SIEM, o que forneceu à equipa de cibersegurança a possibilidade de priorizar os eventos que são detetados pelo SIEM. Esta priorização é feita com base nos resultados do cálculo do risco e permite que a equipa possa analisar e dar prioridade aos ativos que têm um maior nível de risco. Os dados relativos ao risco são importados para o SIEM através de um *connector* que realiza uma *query* à base de dados. Esta *query* faz uma ordenação dos ativos pelo valor do risco, permitindo assim ao SIEM considerar os ativos que têm um valor de risco não aceitável e, como tal, que devem ter especial atenção por parte da equipa de cibersegurança.

No final deste trabalho são ainda apresentados os resultados preliminares obtidos pela integração da ferramenta no universo EDP.

Palavras-chave: Avaliação de Risco, Gestão de Risco, SIEM.

Abstract

Nowadays, security information is fundamental, as computer systems are indispensable to the functioning of organisations and one of their biggest problems is that they may be compromised, which can affect the performance and reputation of the organisations. Therefore, companies invested in risk management processes to monitor their services, processes, and projects, allowing them to avoid cybersecurity incidents.

One of the most used tools to monitor and detect security anomalies is the security information and event management system (SIEM). These systems support a team responsible for managing cybersecurity incidents to analyse and react to the alarms generated by the SIEM. However, these systems are expensive and have limitations, especially while assessing security risk in a simple and effective way.

The DiSIEM project aims to address this problem by developing a new model to assess risk hierarchically. A model and a framework have been developed however it was necessary to integrate it in a real environment.

This work consists in integrating the developed framework in the EDP environment so that it is possible to assess risk and communicate a notion of risk between IT managers and C-Level managers. The framework uses information coming from the SIEM and adds the results of the risk assessment it.

Our model has a risk assessment process based on assessing the vulnerabilities, incidents, and dependencies of the assets identified in the organisation. After the risk assessment process, all the relevant data are imported to the SIEM through a connector, so that the cybersecurity team can prioritize events. This will allow to improve the effectiveness of SIEM threat detection considering assets' risk.

This dissertation is part of the H2020 DiSIEM project and results from a collaboration between Faculdade de Ciências da Universidade de Lisboa and EDP - Energias de Portugal, SA.

Keywords: Risk Assessment, Risk Management, SIEM.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

These days, more than ever, companies are concerned with the cybersecurity of their environments. This concern is not only driven by legal issues, but also by the increase of large scale successful cyber-attacks and the influence that the impact of a successful attack, intrusion or illicit access can have on the company's own image and business. The effectiveness of cybersecurity critically depends on the technical and human resources available to support it, and cybersecurity is as much an issue of management as it is a technical issue.

Security risk, if not properly managed, can lead to the complete collapse of an organisation. Organisations are exposed to multiple risks, and if those risks are not identified and treated as part of the risk management process, the organisation might have a poor performance. Therefore, security risk management is a vital process that needs to be executed to maintain a productive IT infrastructure.

To identify and monitor a vast number of cybersecurity events, organisations have Security Operations Centers (SOC) that rely on Security Information and Event Management (SIEM) platforms. The SIEM systems produce detailed and contextualized alarms for possible real-time risks the organisation may have to face and help the SOC team to make security-related decisions.

Nowadays, SIEM systems are a fundamental tool in modern SOC, but current SIEM systems have many limitations on the methods and means used to store data and report information. By integrating the SIEM with other security technologies, this solution can be used as a single pane of glass for the threats and possible breaches that the organisation is facing. Since SIEM systems do not provide an adequate security risk assessment [1], there’s a gap between the SOC team and the business managers, regarding communication of security risk.

One of the objectives of the EU project DiSIEM is to bridge this gap by conceiving and implementing a SIEM extension to assess risk hierarchically. In this context, a framework has been developed.

This work results from a collaboration between Faculdade de Ciências da Universidade de Lisboa and EDP - Energias de Portugal, SA.

EDP is the most important Portuguese company in the energy sector, and to manage the security of its infrastructures, EDP has a Security Operation Center (SOC) that deals with security-related issues.

This work addresses the limitations of an already existing framework for assessing risk in three decision levels [2], services, applications and hosts, aiming to enhance it by embedding it in a real environment like the EDP SOC, and integrating it with the SIEM used by this organisation, the Micro Focus ArcSight. This framework will also consider a new source of information, the Nessus Professional Vulnerability Scanner [3], which is a software already used and operational at EDP.

1.2 Objectives

Considering the aspects referred to in the previous section, the main objective of this work is to enhance the effectiveness of SIEM systems considering the results of risk assessment. With this, we had the objective of adapt and enhance the implementation of an existing risk assessment framework to:

- Contemplate supplementary input sources, the Nessus Professional Vulnerability Scanner [3];
- Integrate the developed component with the SIEM in use at EDP environment, using the risk assessment results to improve risk mitigation;
- Enhance the reporting mechanisms to communicate risk at different management levels.

1.3 Contributions

This work offers three main contributions:

i. An integrated framework to assess risk that can be used in the daily basis of an organisation;
ii. Enhanced reports to support decision making at the C-Levels;
iii. The possibility of risk analytics to know the source of the risk.

As a result of this work, the EDP SIEM now includes the results of risk assessment in their SOC operation. This allows EDP to have a better knowledge regarding the security of its assets since due to the risk assessment process it is now possible to know the risk value associated with each asset. By integrating the results obtained from the risk assessment with SIEM, the SOC team now benefits from the ability to prioritize events that occur in assets with a risk greater than a specific value. In addition to this, EDP also benefits from an improvement in the risk communication process to the top managers, due to the implementation of a dashboard to present the results obtained and due to the possibility of generating pdf reports with the historical values of risk.

This work is based on a database that is integrated with the organisation asset model, as well as diverse sources of information, including the SIEM. This database stores the collected assets, vulnerabilities and incidents and, after the risk assessment process has been completed, links the results obtained in the risk assessment process with the SIEM helping the SOC team in the prioritization of the detected events. The connection with the SIEM is bi-directional since it relies on the information coming from it (regarding incidents and vulnerabilities) and it also feeds it with new information.

As a result of the contributions of this work, the document "Multi-Level Risk Demonstrator" was written to guide DiSIEM partners while installing and using the developed framework.

1.4 Structure of the Document

This document is organized as follows.

Chapter 2 introduces the context of this work. This chapter is divided into three topics: EDP, SIEM and Nessus Vulnerability Scanner. In the first topic we approach the EDP's business and its SOC team; next, we give a little introduction to SIEMs, specifically the Micro Focus ArcSight since it is the one used in EDP; and lastly, we introduce the Nessus Vulnerability Scanner which is the new input source that is used to detect infrastructure vulnerabilities in EDP.

Chapter 3, State of the Art, introduces the security risk management standards and then reviews and discusses current publications and research around the risk analysis and SIEM topics.

Chapter 4, The Risk Assessment Model in DiSIEM, is the chapter where we describe the model upon which this work is based on. We also explain the issues existent in the current model and how it is improved by our development.

Chapter 5, Implementation, gives a global vision of the developed solution. It describes the current framework architecture with all its improvements: it contemplates the developed database used to store all the data and the process used to get the information that populates the database, and it describes the dashboard used to display all the information stored, as well as the SIEM integration.

Chapter 6, Evaluation of the Preliminary Component Integration, presents and discusses the results obtained by the implementation of the framework.

The document ends in Chapter 7 which contains the main conclusions of this work and future developments.

Chapter 2

Context

This work is part of the Diversity in Security Information and Event Management (DiSIEM) [4] project and results from a collaboration between Faculdade de Ciências da Universidade de Lisboa (FCUL) and EDP - Energias de Portugal, S.A., which are two of the partners in the consortium. This project is funded by the European Commission and aims to improve existing SIEM systems with several mechanisms.

The DiSIEM project has four main objectives [4]:

- Improve the quality of the collected events;
- Add support for collecting information;
- Create new methods for visualising the information;
- Allow the use of cloud services for secure event storage.

Since the SIEM tools are expensive, all these improvements have been done as an extension to some of the systems currently available, allowing companies to make better judgment calls without spending a lot of money in additional plugins.

2.1 EDP – Energias de Portugal

EDP was founded in 1976, with the merge of 13 companies in the Portuguese electricity sector. Since then, the EDP Group has not stopped growing and evolving, becoming a multinational company, ranking among Europe's major electricity operators, as well as being one of Portugal's largest non-financial business groups [5].

To monitor and manage the security of its infrastructures, EDP has a Security Operation Center (SOC) that deals with security-related issues. The SOC team is responsible for the detection, collection, analysis, and reaction to cybersecurity events in real-time, using a combination of technology components and a set of defined processes. The SOC team also conducts awareness campaigns and security training sessions for the company employees through the use of case studies that happened in the past.

The existence of a SOC allows organisations to improve the security incident detection through 24/7 monitoring and analysis of security events, which provides an advantage to defend against incidents and intrusions, consequently reducing security risk.

EDP's SOC obtains an integrated view of the monitored infrastructure by employing an ArcSight SIEM system from Micro Focus [6]. All the information about real-time events is constantly being updated and presented in a dashboard, fed by the SIEM, with several security metrics and visualization options. The SOC uses security metrics to analyse the tasks and the results obtained in each month and, to inform the C-level managers about the security status of the organisation, periodic reports are produced with relevant information for the current month and providing a baseline comparison with previous months.

Figure 2.1 shows the dashboard currently used at EDP. This dashboard presents security metrics related to the number of incidents and the number of vulnerabilities detected, as well as the average response time of the SOC team. A history of the last 12 months is also available, which allows the team to understand the evolution of the efforts made to solve the incidents and vulnerabilities detected. Since EDP is an international company, the dashboard also contains a graphic representation of the incidents in Brazil and Spain. Finally, the dashboard includes a module for risk assessment.

To classify the risks EDP is exposed to, the organisation uses the risk categories displayed in Table 1. These categories, along with its associated colour, were the ones used to classify the risks discovered throughout this work.

Figure 2.1 – EDP Dashboard

Qualitative Value	Quantitative Value Range
Critical	90 – 100
High	70 – 89.9
Medium	30 – 69.9
Low	10 – 29.9
Very Low	0 – 9.9

Table 1 - Risk categories used by EDP

2.2 SIEM

A Security Information and Event Management system, or SIEM, has the general purpose to aggregate and manage event log data, allowing companies to monitor security events in real time, but they also have the means to search historical data. This provides more efficient and convenient analysis capabilities, making it easier to detect incidents and respond to them in a timely manner. The use of SIEMs in an organisation is one of the best practices in information security [7].

SIEMs can collect, normalize, filter, aggregate, correlate, and visualize the logs received from the technological components adopted by the organisation.

Firstly, the SIEM makes a collection of all the events obtained from the technological components. These data are obtained through various connectors that interact with the SIEM and retrieve data from the source where they are installed. Secondly, all the data must be normalized so that a common pattern between all types of data is established and, after the normalization phase, a filtration is needed in order to exclude all the unnecessary data. After the filtering phase, it is necessary to aggregate and correlate the data, so that it is possible to identify the most common and relevant events, in order to generate alerts. Lastly, the visualization allows the SOC to have an understandable view of the global cyber context being monitored, ranging from detailed technical data to high-level metrics. The SOC uses the processed information to engage key stakeholders, including C-Level managers, helping their decision-making process.

State-of-the-art SIEM systems present relevant technological advances, but this tool still has some limitations [8]:

- The threat intelligence capability is still very recent and limited;
- The data visualization techniques have low quality;
- It is difficult to extract high-level information from all the correlated data;
- The event correlation capacities of the SIEM depend on the quality of the events that are collected;

- Historical events are difficult to retain for a long duration.

Apart from that, the adoption and implementation of a SIEM by an organisation is expensive.

The DiSIEM project aims to improve the technology available today through the extension of current systems, using their capacity for extension and personalization.

SIEM systems are marketed in a variety of forms and the functionalities offered by the different manufacturers diverge. Therefore, it is up to each organisation to make its own evaluation and decide which SIEM system is the best fit and the most suitable for their needs.

The Micro Focus ArcSight is the SIEM used by the EDP SOC team. The ArcSight SIEM architecture is divided into three main components: Connectors, Loggers and Enterprise Security Management (ESM) (Figure 2.2).

The connectors are software components that collect events from each connected device, normalize the data to a common standard format, apply filtering and aggregation rules and then send the processed data to the Logger and ESM components. EDP uses two types of connectors: the *SmartConnector* and the *FlexConnector*. The *SmartConnector* is the more standard connector since it does not require any adaptation and it is developed by ArcSight. The *FlexConnector* is adaptable to the organisation's needs but requires high implementation effort. This type of connector is the only option to gather and parse information from legacy systems or from custom applications.

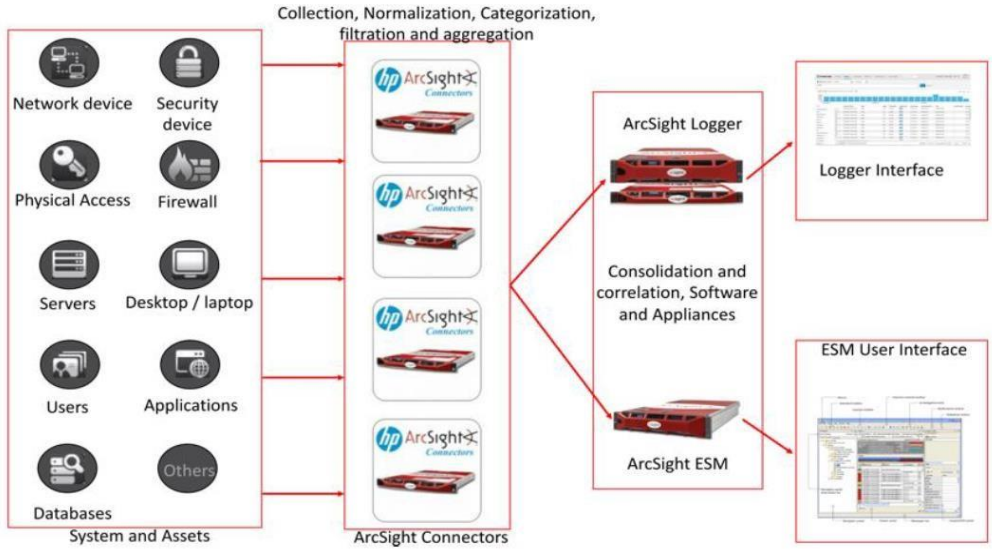

Figure 2.2 – ArcSight Architecture at EDP, extracted from [1]

The Logger component consolidates and stores all the events fetched by the connectors, and it also allows normalization and analysis of the events. A web interface is supplied with the purpose of helping the SOC team analysing the data collected. At EDP, the Logger processes about 3000 events per second.

The Enterprise Security Management (ESM) is a software component that correlates the data coming from the connectors and the loggers. It provides an interface where the SOC team can monitor the current security threats, offering visualization of alerts. This interface helps the team dealing with all the collected data, allowing them to monitor and analyse the events or the alerts generated.

2.3 Nessus Professional Vulnerability Scanner

A vulnerability scanner is used for the automated identification and detection of vulnerabilities in a company's IT infrastructure, which may have misconfigured assets or even flawed software. The scanner digs through the organisation infrastructure and looks for open ports, outdated software or default passwords. The scanner uses a list of known vulnerabilities, already known by the security community, hackers, and the software vendors.

The Nessus Professional Vulnerability Scanner software [3] is the product most used and recommended for the vulnerability scanning process. This software provides asset coverage for the widest variety of network devices. Like the vulnerability scanners existent in the market, Nessus scans for viruses, malware, backdoor hosts and malicious processes to identify vulnerabilities. This software covers more technologies comparatively with other software in the market which allows it to have a detection rate higher than other solutions. It also provides a high-speed scanning with low false positives which allows the companies to quickly identify the vulnerabilities that need fixing first. The results of the scan are reported in the XML format, but the software also provides a dashboard to consult the scanned data, although this dashboard is not used by EDP.

Although Nessus is already operational in the EDP environment, the results from the scans were not used or included in the operation of the SOC team. The infrastructure vulnerabilities detected by the software, when added to the other vulnerabilities detected in EDP, are important for a better understanding of the risk of certain assets. An asset that previously had no risk, with the inclusion of this new tool, can see its risk changed if it has infrastructural vulnerabilities.

Chapter 3

State of the Art

We begin this chapter by introducing the security risk management standards. Nowadays, the use of these standards by organisations has become usual since they aim to guide organisations in how to deal with risks.

Then we review scientific literature related to hierarchical models that deal with dependencies between assets and related to risk propagation. At the end of the Literature Review section, we also introduce the previously developed model that was improved and integrated as result of this work.

3.1 Security Risk Management Standards

Risk is part of everything organisations do nowadays. Thus, security risk management is an essential process for the proper function of organisations because it allows them to identify potential risks in advance, taking precautionary steps to reduce them.

Security risk management is a cyclic process that focuses on discovering and assessing the risks inside an organisation and determining how those risks can be controlled or mitigated. Its main purpose is to identify the information assets of an organisation and their vulnerabilities, as well as to rank them according to the need for protection. Risk management plays a critical role in protecting an organisation's information assets, and therefore its mission.

Information security risk management standards have been established by the National Institute of Standards and Technology (NIST) [9] and the International Organisation for Standardization (ISO) [10] with the purpose of helping organisations to implement an effective information security risk management program, allowing them to reduce risk.

The ISO/IEC 27005:2011 - Information Security Risk Management [11] is the ISO standard that provides guidelines for information security risk management process. Figure 3.1 displays the process recommended by the standard.

This standard divides the process into six phases. The first one is the context establishment phase, where the purpose of the information security risk management is

determined. In this phase, the organisation should be able to define the internal and external context for risk management, specify the basic criteria and the scope and boundaries for the information security risk management process.

In the basic criteria definition phase, four criteria are defined: risk management approach, risk evaluation, impact, and risk acceptance. The risk management approach depends on the scope and objectives of the risk management and it is the phase where the decisions regarding the risk management approach are made. The risk evaluation criteria are used to evaluate the organisation's information security risk based on the value of the business processes, the criticality of the assets, legal requirements, operational and business importance of availability, confidentiality, integrity and the expectations from the stakeholders. The impact criteria are used to specify the degree of damage or costs to the organisation caused by a security event. The risk acceptance criteria depend on the organisation's policies and objectives but consist of the definition of risk acceptance rules for the company.

The risk assessment process is the second phase, where the identification, analysis, and evaluation of the risks are made.

The risk treatment is the third phase and consists in selecting the controls that should be applied to make a modification, retention, avoidance or sharing of the risk.

The fourth phase is the risk acceptance, where based on the risk acceptance criteria defined in the context establishment phase, a list of accepted risks should be made, with justification for those that do not meet the criteria defined. An acceptable risk is a risk that is understood and tolerated usually because the cost or difficulty of implementing an effective countermeasure exceeds the expectation of loss.

Risk Assessment is a process that analyses what can go wrong, how likely it is to happen, what are the consequences if it happens and how tolerable the identified risk is. It assigns a risk rating to each specific information asset of a company and allows the organisation to measure relative risk, which enables one to compare ratings later in the risk control process.

The risk assessment process is divided into three phases following the ISO 27005: risk identification, risk analysis, and risk evaluation (Figure 3.1). The risk identification phase has the purpose to identify what could cause a potential loss to the organisation and it should include all the risks, including the ones that are not under the control of the organisation. Managers must do a process of "self-examination" to identify the organisation assets. An asset classification scheme to categorize the assets should be developed, and it should be based on the sensitivity and security needs of the assets. After the identification of all the assets, an identification of all the threats and their sources

should be made, as well as an identification of the vulnerabilities that can be exploited by the threats and cause harm to the assets identified, followed by an identification of the controls already implemented by the organisation. Lastly, an identification of the possible consequences of the exploitation of a vulnerability should also be assessed. This phase leads to identifying the weaknesses and threats that the organisation is subjected to.

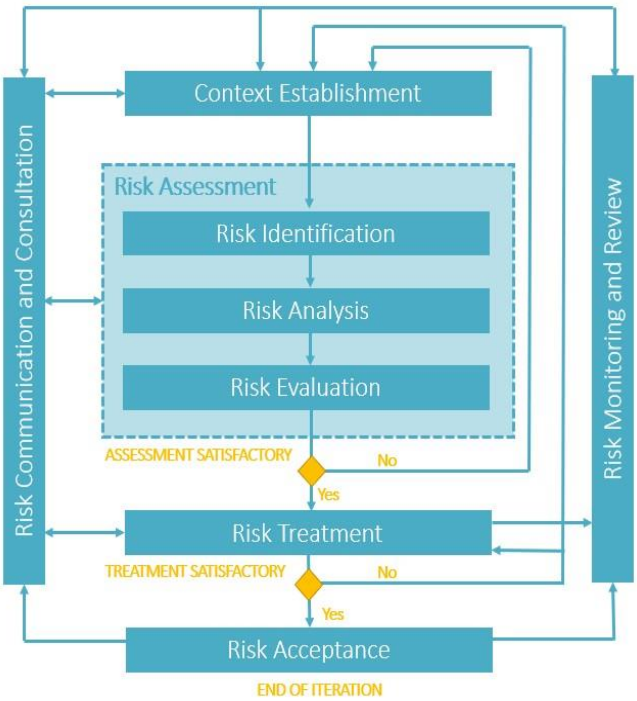

Figure 3.1 – Risk Management Process adapted from ISO 27005

The risk analysis phase is where each identified risk is classified. There are three types of risk analysis methodology: qualitative, quantitative or a combination of these. The qualitative risk assessment is usually used first to obtain an indication of the level of risk and to reveal major risks. It uses a scale of qualifying attributes (e.g., Low, Medium, High) and its advantage is that this approach makes the analysis simpler and more understandable, but it also has the disadvantage that the analysis becomes more imprecise. The quantitative risk assessment uses a numeric scale to determine risk (e.g., 0,2,4,6,8,10). The quality of the assessment depends on the accuracy of the values used in the analysis, which means that even though the analysis becomes more precise, it also becomes more complex. The combination of these two types of analysis, the semiquantitative method, uses a scale in which each qualitative value corresponds to one single quantitative value. After the classification of the identified risks, an assessment of consequences, an assessment of incidents likelihood and a level of risk determination are also made.

Risk evaluation is the last phase of the risk assessment process and it relates the results of the risk analysis process with the criteria and risk acceptance defined in the

context establishment phase. Decisions made in the risk evaluation phase should include whether an activity should be undertaken and the priorities for risk treatment considering estimated levels of risks.

The ISO/IEC 31000:2009 – Risk Management [12], is a standard created by ISO and IEC that provides some guidelines for general risk management in an organisation and for dealing with processes. There are 11 principles that allow the risk management process to be more effective for the organisations:

- It must create value for the organisation;
- It is an integral part of all organisational processes;
- It is part of decision making;
- Explicitly addresses uncertainty;
- It is a systematic, structured and timely process;
- It is based on the best available information;
- It is tailored to the organisation that is being applied;
- Takes human and cultural factors into account;
- It is transparent and inclusive;
- It must be dynamic, iterative and responsive to change;
- It facilitates the continual improvement of the organisation.

These principles were used throughout the development of this work.

3.2 Literature Review

Our literature review focuses mainly on works considering hierarchical relationships between assets, taking into account the dependencies between them and the spread of risk throughout the hierarchy. We also introduce a previous work developed for the DiSIEM project in collaboration with EDP.

3.2.1 Risk Dependencies and Risk Propagation

In [13] a management methodology to address risk dependencies is proposed. This methodology has procedures to estimate each identified risk by taking account of risk dependency effects and enhances a set of risk management practices to manage the estimated risk. A risk dependency refers to an effect due to the occurrence of a risk and this effect can either increase or decrease the probability of occurrence of another risk(s). Risk dependencies can be detected by examining each pair of risks within a project or across other concurrent projects in an organisation and determining whether there is any dependency relationship between them.

The paper proposes three approximation methods to compute the combined risk dependency effect: the conservative method, that picks the highest value from among all the risk dependency values; the optimistic method, that picks the smallest value among all of the risk dependency values and minimizes the dependency effect to a risk or maximizes the dependency effect to an opportunity; and the weighted method that assigns a relative weighted value to each of the dependencies in order to calculate the combined dependency effect.

It is also defined a Risk Dependency Graph (RDG) in which nodes represent risks and edges represent the dependency between risks. From RDG, several useful metrics are defined for evaluating the extent of dependencies among identified risks. The first two metrics, the total number of Direct Successors (NDS) and the total number of Direct Predecessors (NDP), measure the dependency for a specific risk, while the other two metrics, the Total Risk Dependency Count (TRDC) and the Risk Dependency Index (RDI), measure dependency at the project level.

The risk dependency concept was applied to three case studies, which were managed by three different project teams within the organisation. These three projects aimed to enhance three independent systems that involved complicated system environments, and all three projects adopted the same common practices of risk identification and management. The case studies allowed to confirm that dependencies between risks do exist, especially if the risks were identified by different groups of stakeholders. The enhanced and new risk management practices for evaluating, prioritizing, and responding to risk and risk dependencies, as well as the designated metrics, showed valuable and supportive results.

Although the methodology had some benefits it also had some limitations, namely the fact that it does not consider opportunities that occur in IT projects; the process of identifying dependencies needs to be improved so that it can be applied to a larger amount of dependencies; and a management tool to simplify tracking and evaluating risks and risk dependencies is also needed.

A cascading failure model of risk propagation is described in [14]. This paper analyses the robustness of an assembly supply chain network (ASCN) when it suffers from catastrophe events, and its goal is to quantify the robustness index (RI) of ASCN against disruption, to provide a scientific basis for network protection. The robustness index measurement is based on production capacity loss, i.e., the quantity of product that can be delivered to customers after the risk propagates in the network.

An ASCN is composed of manufacturers located in different regions, therefore, the effects of risk are transferred to other organisations, affecting their supply chain partners indirectly. Every entity in a supply chain network faces risk, so the goal is to secure the

uninterrupted flow of materials. A supply chain network is formed by entities that represent network nodes. These nodes are connected by links, and those links can propagate risk, especially when one of the nodes of the network fails. Figure 3.2Figure 3.2 shows the process of risk propagation in a supply chain network.

The innovations of studying the cascading failure of ASCN are the risk propagation mode and the RI of ASCN. By applying the cascading failure theory, the paper describes the concept of risk propagation in an ASCN, constructs a cascading failure model to represent the process of risk propagation, and uses different disruption scenarios to assess the robustness of ASCN.

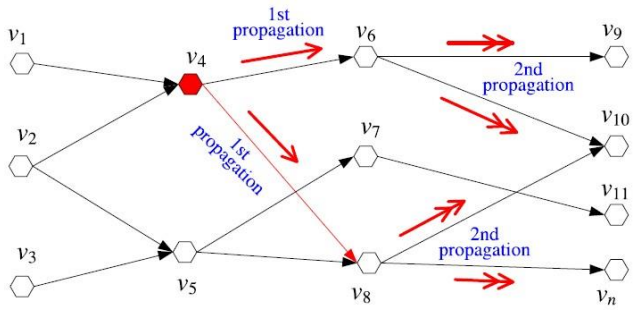

Figure 3.2 – Risk Propagaton in a supply chain network, extracted from [14]

An approach to quantitatively measure the risk of interdependence is presented in [15]. This paper constructs a model for selecting risk response strategies considering expected risk loss and risk interdependencies. As stated before, project risks are not always independent so, this leads to the need to consider risk interdependences as a part of risk analysis. These interdependencies are very important since they define the complexity of the projects, and with complexity comes the issues in decision-making about prioritization of risks. If the risk interdependences are correctly analysed, the project managers will be able to take more effective risk response decisions.

The paper provides a way to measure risk interdependence using a discrete random variable with a probability distribution, which allows the strength of risk interdependence to be measured by the comparison of random variables. Further, an optimization model for selecting risk response strategies considering the interdependences is constructed. The model was applied to a substation during an engineering project of renovation to solve the problems of risk response strategy selection, considering the risk interdependence, costs of implementing strategies and risk response strategy selection. Critical risks were identified by experts involved in the case study, expected losses were estimated and each expert gave evaluations on the interdependent relationships between the risks. A risk network based on the analysis of the strength of risk interdependence was built and based

on the analysis of the risk events and the interdependences, the expert panel discussed and proposed risk response strategies.

To select risk response strategies and further investigate the effects of the risk interdependence, an integer programming model was constructed. This model considers the expected risk loss, risk interdependence, and their two directions by defining a weighting function. The results obtained after applying the model to a case study shows the necessity of considering risk interdependence in risk response analysis in pursuit of organisational benefits maximization.

The limitation of this paper is that the impact of the risk interdependence needs to be studied with greater depth and the paper conclusions lack verification. In addition, the author stated that more empirical field work is needed to study the risks and their interdependences.

A Service Dependency Framework (SDF) to assist the response process in selecting the policy enforcement points (PEPs) capable of applying a dynamic response rule is described in [16]. The uniqueness of this framework resides in its capacity to define dependency attributes, instead of assigning static dependency parameters as in most of the current models. The SDF specifies dependencies by modelling the data exchanged in each dependency, the paths followed by these data, the sequencing of dependencies during the operation of the dependent service and the impact due to the unfulfillment of each dependency. There are three dependency characteristics: dependency type, that defines the path of the network flow, and describes the data assets exchanged between the dependent and the antecedent service; dependency mode, that makes precise the occurrence of a dependency within the lifecycle and workflow of the dependent service; and dependency impact that evaluates the influence of the insatisfaction of the relation between antecedent and dependent services. A dependency type may be either service-side, user-side or proxy dependency. This paper demonstrates that service dependencies can be used for more than only a-posteriori evaluation of intrusion response impacts after these have been selected. It describes an apriori use of service dependencies, notably for the selection of suitable means to apply an intrusion response. One of the limitations of this work is that the treatment of responses is separated from the dependencies search.

In [17], a model for email malware propagation is reviewed. This paper aims to explore the impact of connection topologies along with the distribution of user action malware, amongst a population of computers and its associated users. It also explores the impact these factors have when patching or blocking interventions are applied to the population.

The model designates hosts to be in one of three compartments or states: Susceptible (S), Infected (I), or Removed/Recovered (R). User interaction is usually required for

email malware to spread, thus each node in the model has an associated human user. An important user aspect included in the model is the probability that a user will open an infected message. For modelling purposes, each user has an assigned probability threshold value for opening an infected message.

The model was applied to three email malware incident types and for the model types tested and the range of parameter values explored, model types using an exponential based distribution of user likelihood of opening infected messages produced a higher percentage of best-fit values. This shows that by using exponential based distributions of user likelihoods in models, this may provide a better estimation of the distribution compared to using random uniform distributions. Despite the obtained results, this model can be improved by expanding the types of distribution used to model the probability of users to open infected messages and exploring accuracy and robustness of model selection and parameter inference.

A framework for attack modelling and security evaluation in SIEM systems is proposed in [18]. This framework considers attack modelling security evaluation processes, intended to be implemented for the security analysis in SIEM systems. The implemented prototype of the Attack Modelling and Security Evaluation Component (AMSEC) can generate an attack tree and calculate security metrics for a predefined network. After constructing the attack graph, the AMSEC provides the malefactor knowledge after all possible attacks, the attack tree in the graphic form and the log of the malefactor's actions.

In [19] a risk assessment methodology for information systems security with the application of Group Decision Making (GDM) and Analytic Hierarchy Process (AHP) methods is proposed. The proposed methodology is designed in four main sections:

(1) Identifying key assets, threats, and vulnerabilities;

(2) Data gathering of a_i , t_{ij}, v_{ik}, where a_i ($i = 1,2,\ldots, m$) is the value of an asset, t_{ij} ($j = 1,2,\ldots,m$) represents the threat t_j to the asset a_i and v_{jk} represents the danger degree of vulnerability k in the asset a_i;

(3) Calculating risk value R_{ijk} and prioritizing risk incidents, where R_{ijk} is the risk value of asset a_i caused by threat t_j due to the vulnerability k.

The GAHP (GDM and AHP) model proposed in this paper was tested and, according to the test case, the priority of risk incidents was obtained. The proposed assessment methodology provides information from each unique risk incidents respective to the whole system view, which can better support the risk management activity compared with the original methods.

The issues identified with this framework are the need to develop techniques that can cope with large networks and the generation of attack trees must also be optimized to expand the list of parameters, characterizing the hosts and the network, to improve the malefactor model, and to add currently unrealized components.

3.2.2 Risk Assessment in the DiSIEM project

In previous work, a multi-level risk assessment tool model to support the EDP SOC team making decisions and communicating with the organisation top managers was developed [2].

This model considers three layers of assets, it is based on three levels of decision making and it has three main objectives: calculate assets risk, supply information, and support the decision-making process. The three layers of assets considered in this model are Hosts, Applications, and Services, where the services' layer is an abstract representation of the actions or functions supported by applications, and these applications are supported by hosts. The approach to assessing risk is bottom-up, which means that to be able to assess the risk of a service, it is required to assess all the applications that support it and the hosts that support the applications.

The model also considers three different models to assess risk: Generic Additive (GA), Modified Additive (MA) and Maximum Score (MS). The GA model adds all the vulnerabilities, dependencies, or incidents scores and it is compared with the risk appetite that the organisation considers for each variable. The MA model takes into account the impact that might exist when different levels of relevance for different factors are given.

The MS model is the simplest since it assesses the risk by considering only the highest scores in terms of vulnerabilities, dependencies, and incidents.

The model also calculates risk for each asset of the organisation identified. This risk is calculated through three components: vulnerabilities, dependencies, and incidents. The dependencies variable is very important because it allows to consider the existence of two types of risk: imported risk (the risk that is inherited from other assets due to the dependency on them) and intrinsic risk (the risk of the asset itself). The assessment of the risk was based on numerically scoring the variables and was not based on a probabilistic model since there is some difficulty to determine the probability of a vulnerability to be exploited.

A quantitative approach was adopted in this model since this type of risk analysis methodology allows a better recognition of serious situations. The risk score value is comprehended in an interval established in advance: zero is the minimum score value and the maximum is a predefined value, set by the organisation.

In order to match EDP's needs, a dashboard to display all the results of the model was created. This dashboard shows the global risk of the company through a graph that presents the evolution of the last twelve months; has a page for each one of the layers described above and has also the capability to create a pdf report for the selected assets with its calculated risk.

In [20] we find a review of the risk assessment process previously used by the SIEM solutions adopted by the DiSIEM project.

The Micro Focus ArcSight uses a threat level prioritization process for each one of the events detected in order to detect the threats with the highest priority that target an organisation. The threat level formula process gives an indication to determine if an event should be investigated and is applied to every single event ingested into the ArcSight.

The priority formula is based on four distinct parameters: Relevance, Model Confidence, Severity, and Criticality. All these priority factor values fall within a range of 0 to 10, where 0 is low and 10 is a high-risk factor.

The Relevance factor depends on whether an event is relevant to an asset based on if the event contains ports and/or known vulnerabilities and its maximum value is 10. The Model Confidence variable is about the level of information available about the asset under assessment. The Severity factor works as a history function since it evaluates if the system has been attacked or compromised before and it is calculated through the parameter Severity Level. This parameter depends on five factors: Recognition, Suspicious, Compromised, Hostile and Infiltrators. Finally, the Asset Criticality factor concerns about the importance of the asset in the context of the organisation as it is defined in its network modelling process.

This document also presents a model to assess multi-level security risk. This model is a consolidation of the three models proposed in [2]. The model is divided hierarchically into three levels of decision making but it considers only one type of formulas to make the risk assessment process.

3.2.3 Discussion

As identified in the works presented in the previous sections, there is still no ideal way to assess risk while considering dependencies between assets. The existing works in the literature present some gaps, namely difficulties while identifying dependencies, lack of verification and evaluation of the results, and apart from that, there is also a lack of integration in a real environment. Although a model has already been conceptualized to aid in the risk management process of organisations in [2], it has not yet been integrated or tested in a real environment. Integrating the model within an organisational

environment is essential to prove its functionality and usefulness. There is also the necessity to integrate the model with the SIEM, given that this is one of the main objectives of the DiSIEM project.

Chapter 4

The Risk Assessment Model in DiSIEM

As stated in the Introduction, a model for multi-level risk assessment was already developed and implemented in the EDP context.

The main objective of this model was to help the SOC team making decisions as well as to facilitate the communication between the SOC team and the organisation top managers. By the possibility of assessing the amount of risk in the three different layers and the implementation in EDP environment, this objective should have been achieved.

Although this framework had been developed in the EDP context it had some flaws and was not integrated within the EDP environment, so there is a necessity to adapt it to meet the needs of the company. Even though the proposed framework is mainly focused around assets and organises them to allow the SOC to know which asset has the highest value in each one of the layers, it needed some improvement regarding reporting and risk communication mechanisms. Furthermore, there was no connection between the framework and the SIEM, which was essential for EDP.

With this starting point, our main objective was to integrate the framework in EDP environment and with the SIEM. This framework update should also make it easier for the SOC team to identify the applications that need special care, contributing to an improved security status of the organisation.

This chapter presents the general concepts of the model. We begin by introducing the structure of the model and then we explain all the formulas used in the risk calculation process.

4.1 Structure of the Model

The structure of the model presented in [2] is divided into three layers of decision making. The model divides the assets of the organisation into three types: services, applications, and hosts. It also considers dependencies between assets and the risk spreading between them.

As displayed in Figure 4.1, a bottom-up approach is used to assess risk, which means that to be able to know the risk of a service, it is required to first assess the risk of applications and hosts that support it.

The hosts layer works as the most operational layer of the decision-making process as it regards mostly technical or infrastructure details.

The middle layer, corresponding to the applications layer, is very similar to the previously mentioned one but there is an abstraction of the IT technical details and infrastructure. This allows us to start focusing on the business side.

The services layer improves the communication between security managers and C-Level managers. The C-Level managers set the company's strategy by making higher-stakes decisions, which means that they are more concerned with business instead of the technical issues. The risk assessment at the services level allows the C-Level managers to make their decisions based on the business-related information.

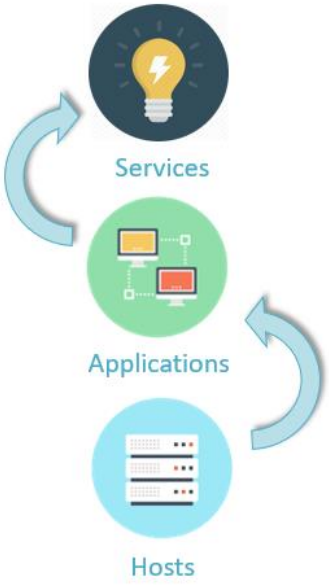

Figure 4.1 – Bottom-up approach

Although the model is organized in a three-layer structure it provides a risk score for each asset present in each layer, which provides the ability to determine which assets must be treated first, creating better and more efficient management process for the organisation.

An example of the three-layer structure in the specific environment of EDP is given in Figure 4.2. The hosts level corresponds to a set of physical assets, which means that these hosts can be servers, virtual machines, routers, switches or others. The applications level is where we find the assets that support the organisation. These assets are responsible for monitoring the network state and for maintenance management. Lastly, the services level is supported by the applications and hosts and this level is responsible for a business function, such as the country's electricity distribution service provided by the company.

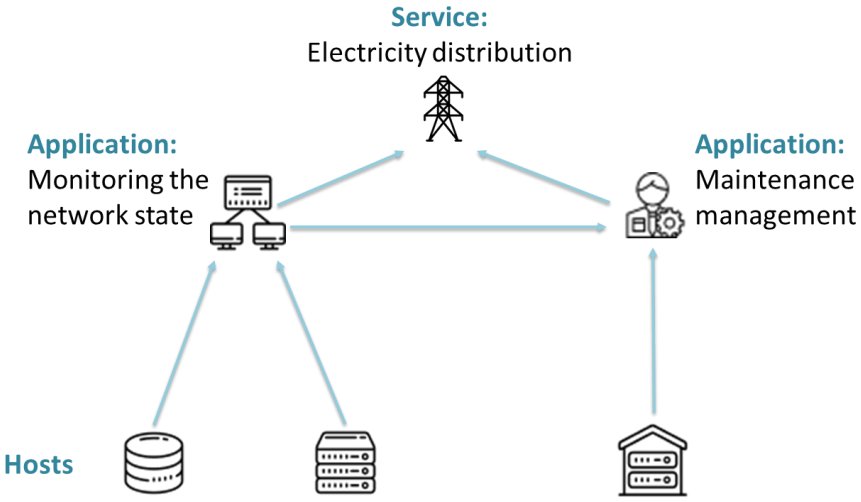

Figure 4.2 – Example of the three-layer structure in EDP's environment

For the model to work as expected, it is necessary to identify all the existing assets in the organisation. After identifying the assets, it is also necessary to identify the dependencies between them. While applications are supported by hosts and can depend on other applications, services typically work as a set of applications and do not have dependencies between them.

It is relevant to mention that this model considers two types of risk: the intrinsic risk which is relative to the asset itself, and the imported risk that is the risk inherited from all the dependencies. It is only after all the assets and dependencies are identified that the company's risk assessment process begins.

The multi-level risk scoring is made for each asset previously identified and it considers three elements: vulnerabilities, dependencies, and incidents.

4.2 Risk Evaluation

All the formulas present in this document are the ones in [20], with the exception of Equation (2). This formula was added to the risk calculation process to make it more complete and so that it considers historical data regarding the vulnerabilities variable.

The DiSIEM project adopts a quantitative approach to evaluate risk which allows a better differentiation of critical situations that occur in the assets under evaluation.

The risk of a generic asset j is calculated by the weighted sum of three components: the vulnerabilities variable, the dependencies variable, and the incidents variable. The risk score formula is present in Equation (1).

$$RiskScore_j = WeightedSum(VV_j, DV_j, IV_j) \quad (1)$$

Where,

- VV_j is the vulnerability variable score for the asset j,
- DV_j is the dependencies variable score for the asset j,
- IV_j is the incidents variable score for the asset j.

The risk score value of all the assessments is comprehended in a specific interval defined by the organisation, being 0 the minimum score and the maximum score is the value predefined e.g. 100. The function $WeightedSum$ indicates that each one of the variables has a specific weight attribute.

In a Service, the assessment only considers the dependencies variable score since a Service does not have vulnerabilities or incidents because usually, a service works as a set of applications. Otherwise, all the variables are considered.

4.2.1 Vulnerabilities Variable

The vulnerabilities variable represents the risk associated with the vulnerabilities present in the asset. This variable, represented by Equation (2), is obtained through the score of the vulnerabilities occurred in the present month and the history score of the past three months.

$$VV_j = WeightedSum\ (CurrentMonthScore_j, PreviousMonthScore_j) \quad (2)$$

This equation is not present in [20] since it is one of the improvements made to the model. It allows the risk assessment process to consider historic data regarding the vulnerabilities that affected the organisation in previous months. This allows the organisation to understand if the asset is susceptible to vulnerabilities since the asset may have few vulnerabilities in the current month but may have had many vulnerabilities in the previous ones, which indicates that the SOC team should be giving greater attention to this specific asset.

The equation used to assess the $CurrentMonthScore$ variable has into account the highest scored vulnerability and the sum of the score of all the other vulnerabilities present in the asset. This is based in the use of weights, so that the company can decide which variable values most, if the highest scored vulnerability, or the sum of all the others. It allows the users to focus only on the most severe vulnerability by setting the weight of

the highest vulnerability to one and the weight of the sum to zero, or vice versa. To give an equal importance to all the vulnerabilities, the weights should be set equal.

$$CurrentMonthScore_j = \frac{(wo*(\Sigma_{i\in Vulns(Assetj),i\neq h}\ VulnScoreij)+wh*VulnScorehj)}{MaxScoreV} * UL \qquad (3)$$

Where,

- $Vulns(Asset_j)$ is the set of indexes for open vulnerabilities in asset j,j$\in J$;
- $VulnScore_{ij}$ is the risk score of vulnerability i in asset j, $i\in Vulns(Asset_j)$, $j\in J$;
- h is the index of the highest scored vulnerability in $Vulns(Asset_j)$, $j\in J$;
- w_h and w_o are the weights for the highest scored vulnerability and for the sum scores of the others (that are not the highest)
- $MaxScoreV$ is the maximum total risk score of vulnerabilities on an asset; and
- UL is the upper limit of the risk scale interval.

The risk score of a vulnerability considers three elements: its severity score, the persistence of the vulnerability and the business value of the asset where the vulnerability exists. The persistence of the vulnerability has the objective to determine how much time the vulnerability remained open, which means that this factor can increase the risk score when a vulnerability is active for a long period of time. Therefore, an increased risk score on a vulnerability should alert managers to pay special attention to that vulnerability and to solve it as soon as possible. The persistence of a vulnerability is given by Equation (4). The $MaxNoD$ parameter considers the maximum amount of time the organisation conceives as acceptable to have an active vulnerability without resolution. This value is capped to one if a value greater than one is obtained.

$$VulnPersistence_{ij} = \min\left(\frac{NoD_{ij}}{MaxNoD}, 1\right) \qquad (4)$$

Where,

- NoD_{ij} is the number of days the vulnerability i is open in asset j, $NoDij \geq 1$, and
- $MaxNoD$ is the maximum number of days a vulnerability can remain open.

Equation (5) presents the calculation of the score of vulnerability i in asset j.

$$VulnScore_{ij} = VulnSeverity_i\,(1 + VulnPersistence_{ij}) * BusValue_j \quad (5)$$

The $VulnSeverity_i$ is the vulnerability severity score. The $VulnPersistence_{ij}$ is the persistence of the vulnerability i in the asset j and the $BusValue_j$ refers to the business value of the asset j in the system used for the asset evaluation by the organisation.

The vulnerability variable value also needs to be normalised to the common risk scale, so that it considers the maximum total risk score for vulnerabilities on an asset. This score corresponds to an extreme situation since the organisation must not tolerate risk beyond this value. The $MaxScoreV$ value is obtained from several of the criteria defined by the organisation:

- The maximum score value for which the organisation accepts to maintain a critical vulnerability without resolution;
- The maximum number of critical vulnerabilities that can exist simultaneously in an asset, without resolution;
- The maximum time the organisation tolerates the presence of a critical vulnerability without resolution (as a portion of one year), and
- The maximum value for assets valuation in a numerical representation of the upper limit of the scale.

$$MaxScoreV = MaxSV * 2 * MaxNV * MaxBVA \quad (6)$$

Where,

- $MaxSV$ is the maximum score value of a vulnerability that is kept without resolution;
- $MaxNV$ is the maximum number of open vulnerabilities with the score $MaxSV$ or higher;
- $MaxBVA$ is the maximum value for business valuation of assets.

The number 2 in Equation (6) represents the maximum factor for persistence.

The historical component $PreviousMonthsScore$ assesses the impact of previous existing vulnerabilities and depends on the risk score of vulnerabilities on the previous three months, as represented in Equation (7).

$$PreviousMonthsScore_j = WeightedSum\ (FMScore_j, SMScore_j, TMScore_j) \quad (7)$$

Where,

- $FMScore_j$ is the incidents risk score for asset j in the previous month, i.e., the value of IV_j one month ago;
- $SMScore_j$ is the incidents risk score for asset j two months ago, i.e., the value of IV_j two months ago; and
- $TMScore_j$ is the incidents risk score for asset j three months ago, i.e., the value of IV_j three months ago.

Example of Application:

Consider that an organisation classifies the severity of its vulnerabilities and the business values of its assets as represented in Table 2 and Table 3, respectively.

Qualitative Value	Quantitative Value
Critical	10
High	5
Medium	3
Low	1

Table 2 – Vulnerability severity

Qualitative Value	Quantitative Value
Diamond	4
Gold	3
Silver	2
Bronze	1

Table 3 – Business value of assets

This classification is defined by the organisation. If the organisation wishes to classify vulnerabilities through the use of the Common Vulnerability Scoring System

(CVSS) [21], these values can be updated to the average values of the respective intervals, where:

Severity	Base Score Ratings
Critical	9.0 – 10.0
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9

Table 4 – CVSS 3.0 Ratings

Now consider that this organisation has an open vulnerability for the last 4 months in an asset with the highest business value possible, named Asset1, that in this organisation is scored with the value 4.

The organisation established that the maximum number of days a vulnerability may be open is 365 days. With this, we are now able to calculate the vulnerability persistence, where $VulnPersistence = \min\left(\frac{122}{365}, 1\right) = 0{,}33$. Since the vulnerability is a critical one, its severity value is 10. With this information, we are now able to calculate the vulnerability score, where $VulnScore = 10 * (1 + 0{,}33) * 4 = 53{,}2$. This organisation only tolerates 3 vulnerabilities with the highest score open in the current month, which means that to normalize the variable to the common risk scale, the $MaxScore$ will be:

$MaxScore = 10 * 2 * 3 * 4 = 240$. Let's now consider that the Asset1 does not have any other vulnerabilities open in the current month, which makes this specific vulnerability the highest one. Let us assume that the risk scale is comprehended between 0 and 100.

With this, and considering that the organisation gives a weight of 0,75 to the highest scored vulnerability and a weight of 0,25 to the sum of the other ones, we get the

$CurrentMonthScore$ of the vulnerabilities present in this asset:

$$CurrentMonthScore = \frac{0{,}75 * 53{,}2 + 0{,}25 * 0}{240} * 100 = 16{,}63 \quad (8)$$

Now, let's consider that the $PreviousMonthsScore$ of Asset1 is zero, which means that this asset had no vulnerabilities in the last three months. The organisation gives an importance of 0,8 to the current month vulnerabilities and an importance of 0,2 to the ones identified in the previous months. We can now calculate the vulnerabilities score of this asset, where $VV = 0{,}8 * 16{,}63 + 0{,}2 * 0 = 13{,}04$.

4.2.2 Dependencies Variable

The dependencies variable DV_j is described by Equation (9). This variable considers the risk that is inherited from other assets due to the dependency on them and the risk of the asset itself.

$$DV_j = w_h * RiskScore_h + w_a * \sum_{i \in Deps(Asset_j) j \neq h} RiskScore_i \quad (9)$$

Where,

- $RiskScore_i$ is the risk score of the asset i computed by Equation (1);
- h is the index of the asset with the highest risk score in the asset set of dependencies;
- w_a and w_h are the weights for the sum scores of all the assets that are not the highest and the highest scored one, respectively, with $w_a, w_h \geq 0$ and $w_a + w_h = 1$.

Example of Application:

If an organisation gives an importance of 0,75 to the highest scored asset and an importance of 0,25 to the other ones, and Asset1 is supported by 3 assets with the risks scores 10, 30 and 60, the risk score of Asset 1 is $DV_j = 0{,}25 * (30 + 10) + 0{,}75 * 60 = 55$.

4.2.3 Incidents Variable

Such as the vulnerabilities variable, the incidents variable also considers the risk score from the three previous months and the current month. This variable represents the risk existent in an asset given its incidents.

$$IV_j = WeightedSum\ (CurrentMonthScore_j, PreviousMonthsScore_j) \quad (10)$$

An asset that suffers several incidents is either vulnerable or it is an attractive asset for attackers, which means that it will have a certain amount of risk that should be considered by the assets that depend on it. The equation used to assess the $CurrentMonthScore$ variable is the sum of the scores of the incidents that occurred in the current month, in $asset_j$. The process is similar to the computation of the variable vulnerabilities.

$$CurrentMonthScore_j = \frac{\left(w_o * \sum_{i \in Incs\left(Asset_j\right), i \neq h} IncScore_{ij} + w_h * IncScore_{hj}\right)}{MaxScoreI} * UL \quad (11)$$

Where,

- $Incs(Asset_j)$ is the set of incidents in asset j, in the current month, $j \in J$;
- $IncScore_{ij}$ is the risk score of incident i in asset j, $i \in Incs(Asset_j)$, $j \in J$;
- h is the index of the highest scored incident in $Incs(Asset_j)$, $j \in J$;
- w_h and w_o are the weights for the highest scored incident and for the sum scores of the others, respectively; with $w_h, w_o \geq 0$ and $w_h + w_o = 1$;
- $MaxScore$ is the maximum total risk score of incidents occurring in an asset in a month period, and
- UL is the upper limit of the risk scale interval.

Again, by considering different weights for the incident with the highest score and for the others, it allows the organisation to give more importance to the most severe incident.

The assessment of incidents can be done using different scoring systems since each organisation can adopt its own system. We score an incident by using the multiplication of the properties given by the SIEM used by EDP. These properties are presented in Table 5 .

$$IncScore = OpImpact * ConsSeverity * SecClassification \quad (12)$$

Where,

Property	Values
Operational Impact	0 - No Impact 1 - No Immediate Impact 2 - Low Priority Impact 3 - High Priority Impact 4 - Immediate Impact
Consequence Severity	0 - None 1 - Insignificant 2 - Marginal 3 - Critical 4 - Catastrophic
Security Classification	1 - Unclassified 2 - Confidential 3 - Secret 4 - Top Secret

Table 5 – Properties for classifying incidents according to ArcSight

A conversion of scale using the intended scale and the maximum risk that an asset can have regarding incidents is also applied to the sum of the scores. This conversion is represented by the $MaxScoreI$ component. The $MaxScoreI$ represents the maximum risk for incidents in a month and it depends on the highest score value of an incident in the incident scoring system used by the organisation; and the maximum number of incidents with the highest score that can occur in a month.

$$MaxScoreI = MaxSI * MaxNI \quad (13)$$

Where

- $MaxSI$ is the maximum score value of an incident in the incidents scoring system;
- $MaxNI$ is the maximum acceptable number of incidents with the score $MaxSI$ in any given month.

The component $PreviousMonthsScore_j$ evaluates the impact of incidents that occurred in the previous months, and it has into account the risk score of those incidents in the past. This is represented in Equation (14).

$$PreviousMonthsScore_j = WeightedSum\ (FMScore_j, SMScore_j, TMScore_j) \quad (14)$$

Where,

- $FMScore_j$ is the incidents risk score for asset j in the previous month, i.e., the value of IV_j one month ago;
- $SMScore_j$ is the incidents risk score for asset j two months ago, i.e., the value of IV_j two months ago; and
- $TMScore_j$ is the incidents risk score for asset j three months ago, i.e., the value of IV_j three months ago.

Example of Application:

Consider an organisation that uses the incidents scoring system present in Table 5. Consider that Asset1 has an incident scored with an Operational Impact of 3, Consequence Severity scored as 3 and Security Classification scored as 2. This means

that $IncScore = 3 * 3 * 2 = 18$. The $MaxScoreI$ component, given that the organisation can only tolerate 3 incidents with the highest score open in one month, is given by $MaxScoreI = 3 * 64 = 192$. Let's again consider that Asset1 does not have any other incidents open in the current month, which makes this incident the highest one. With this, and considering that the organisation gives a weight of 0,75 to the highest scored incident and a weight of 0,25 to the sum of the other ones, we get the $CurrentMonthScore$ of the incidents present in this asset:

$$CurrentMonthScore = \frac{0,25*0+0,75*18}{192} * 100 = 7,03 \quad (15)$$

Now, let's consider that the $PreviousMonthsScore$ of the Asset1 is zero, which means that this asset had no incidents in the last three months. The organisation gives an importance of 0,7 to the current month incidents and an importance of 0,3 to the ones identified in the previous months, and we can now calculate the incidents score of this asset, where $IV = 0,7 * 7,03 + 0,3 * 0 = 4,92$.

Risk Score of Asset1:

Let's consider that this organisation cares more about vulnerabilities than incidents and that gives the weights 0.40, 0.35 and 0.25 to the vulnerabilities, incidents, and dependencies respectively.

Given the results obtained in the previous three examples, we can now conclude that Asset1 has a risk score of 20,69/100 as displayed in Figure 4.3.

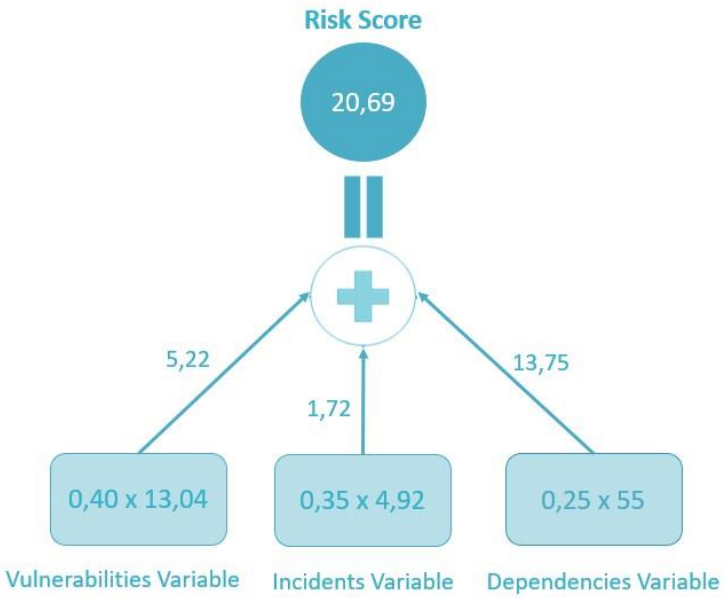

Figure 4.3 – Risk score of Asset 1

Chapter 5

Implementation

In this chapter, we describe the implementation of the tool for risk assessment in EDP's SOC environment.

The chapter starts with our solution architecture, describing how the data flow process works, as well as the connection between the model database with the dashboard and the SIEM. The structure of the developed database is explained as well as the dashboard that allows to visualise the information present in the database and to perform risk analytics.

Lastly, we explain how the integration with the SIEM is done.

5.1 Architecture

Figure 5.1 displays a representation of the tool's components, as well as their interaction. Our model is centred around a database and it is through it that everything intertwines and functions. This database is fed by several sources of information coming from EDP, and from a risk assessment application, based on the model described in Chapter 4.

While the list of assets consists of data coming from EDP's Configuration Management Database (CMDB), the list of vulnerabilities comes from two different sources as it will be further explained in this chapter, and the list of incidents comes from ArcSight events.

The Nessus applications script is responsible to add the vulnerabilities detected in the Nessus scan to our database. Since the SIEM is connected to Nessus and the vulnerabilities are collected and processed by it, our script uses the processed information present in the SIEM. These vulnerabilities are crossed with the assets already present in the database. This process allows a greater knowledge about what is happening in this asset since the final value of the risk will be influenced by the presence of new vulnerabilities.

The risk assessment application populates the database with updated information about the risk score of each asset, using data from the vulnerabilities and incidents present in the database. This application goes further than assessing events since it allows the calculation of the risk of the asset beyond applications and hosts: it considers dependencies and the business value of assets of the organisation.

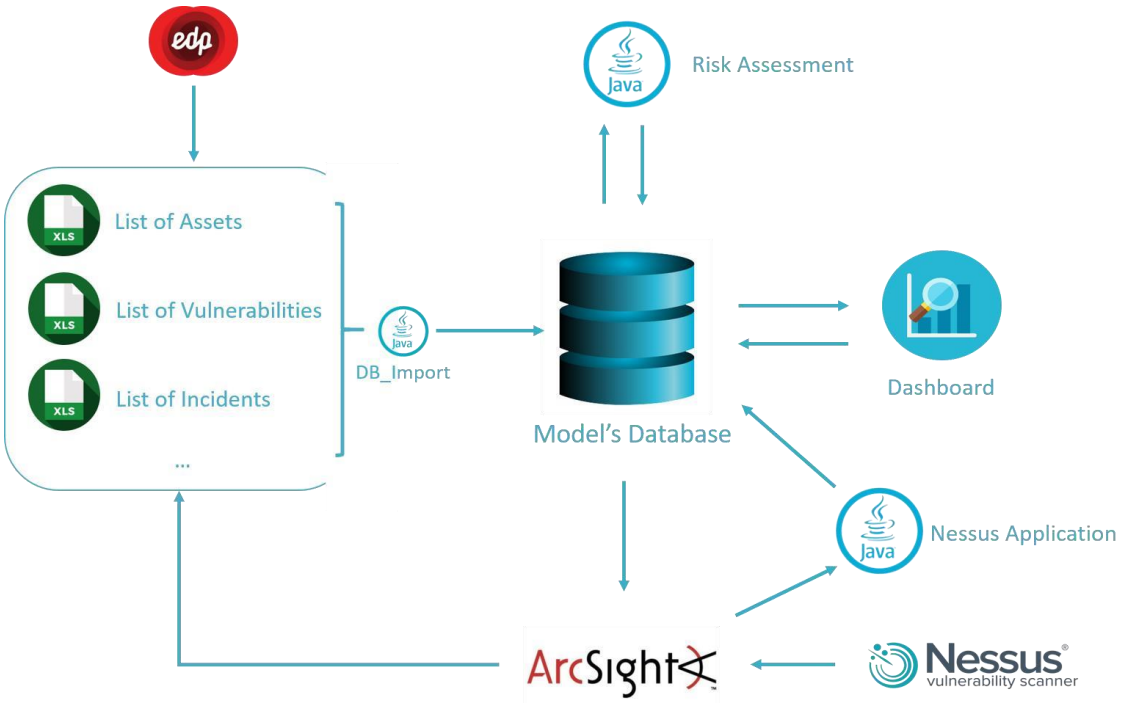

Figure 5.1 – Risk Assessment tool architecture

After our database is populated with the risk score for each existent asset, all the information considered relevant will be fed into the SIEM in order to improve the SOC team decision-making process. By feeding this information to the SIEM, the SOC will be able to prioritize incidents in assets with the highest levels of risk, instead of treating incidents in the order of arrival. This feeding mechanism is achieved through the existence of a *SmartConnector*, which collects raw events from the database and processes them into the SIEM.

As an addition, to allow the SOC to visualize all the relevant details that were used for the risk assessment, the database also feeds the EDP dashboard with the calculated risk score for each asset. The dashboard allows the company managers to analyse the assets with greater risk through the possibility of extracting reports with graphs of the risk evolution in a chosen period. This helps the decision-making process and managers are more aware of the full range of actions that they can take to reduce or cope with systems or applications risk.

5.2 Database Structure

To implement our model, it is essential to allow an easy way to access, manage and update all the information provided. For this reason, all the data were collected in a MariaDB database [22] which was the database already in use in the EDP environment. The data model is represented in Figure 5.2, and it was developed with the purpose to improve the one implemented in [2].

Our database model uses an Enhanced Entity-Relationship model (EER) [23], which is used frequently to model databases and works as a high-level entity-relationship model, since it incorporates some extensions, like the concepts of subclass and superclass.

Although all the tables are relevant for the model, we can see from Figure 5.2 that the Asset table is the one that has more relevance in the model, being central for the database as it is the table with more connections.

The *Asset* table represents each asset of the organisation. It has the following essential attributes:

- *Asset_ID*, used as a unique identifier for each one of the assets in the database;
- *Name*, which is the real name of the asset used by the organisation;
- *Owner*, the collaborator responsible for the respective asset and its management;
- *Business_Value*, value of the asset to the organisation. This value is previously set by a Business Impact Analysis (BIA);
- *Type_Of_Asset* refers to one of the three types of assets that we can have: Service, Application or Host;
- *Application_Block* that matches each application with a service. Do note that this attribute was required by EDP, but formally it should be represented as a dependency.

It is relevant to mention that not all the attributes are mandatory. We only consider some attributes to be relevant for the risk assessment process, leaving the presence of the remaining ones to the organisation discretion. The ones that aren't marked in Figure 5.2 with a blue diamond are the optional attributes that are relevant in the EDP context, but that may not be relevant for other companies.

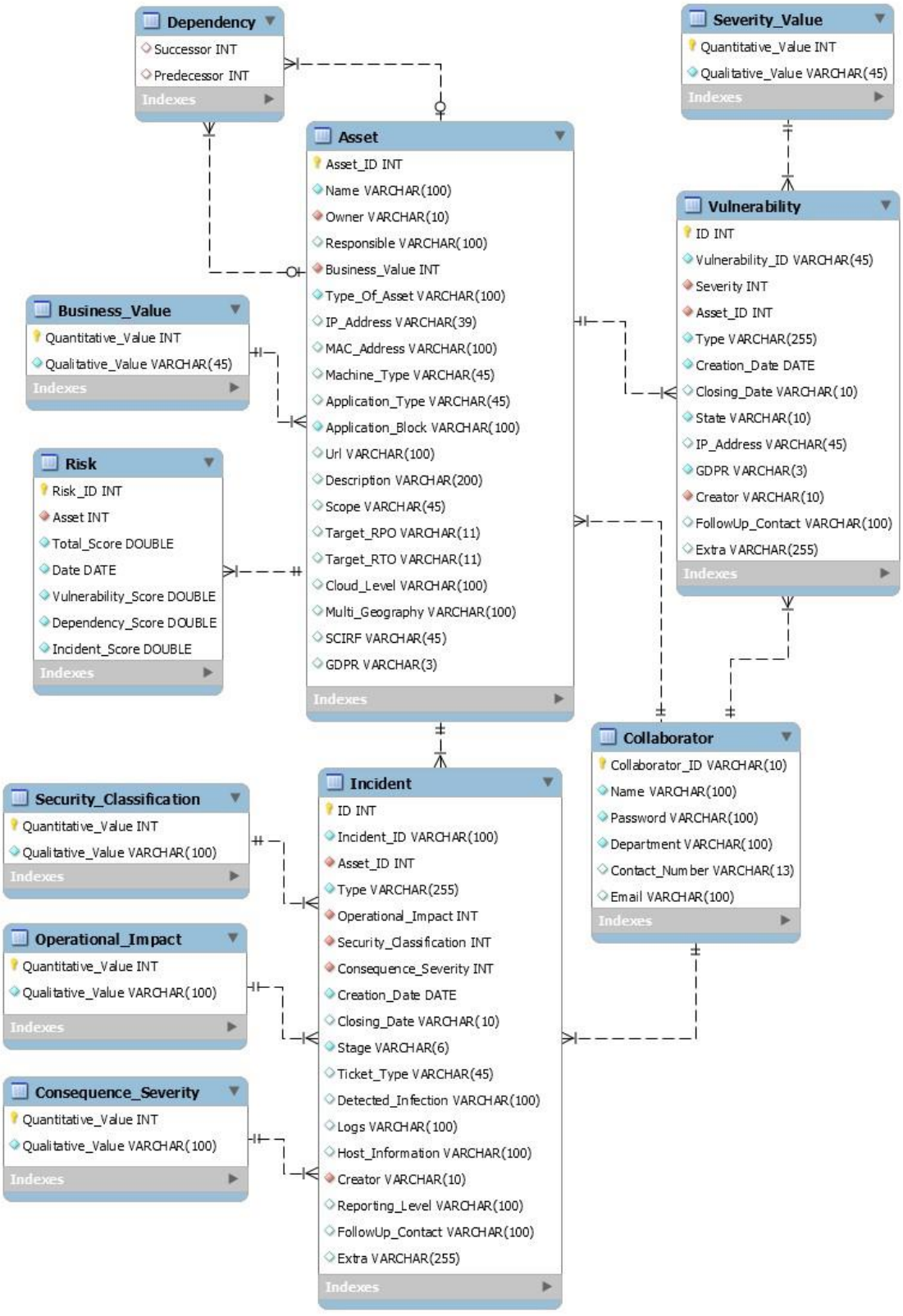

Figure 5.2 – Model's Database

The *Business_Value* table holds all the values used to classify assets, i.e. the value of the asset to the organisation. The values used by EDP in their environment to make a classification of the assets are: Bronze, Silver, Gold, and Diamond. This table has two

attributes, one is the qualitative value and the second one is the quantitative value. The quantitative value exists because the risk calculation is quantitative, so we had to establish a relationship between the qualitative value and the quantitative value. This also happens for every attribute of these tables: $Severity\_Value$, $Security\_Classification$, $Operational\_Impact$, and $Consequence\_Severity$.

The $Dependency$ table is very simple and establishes a relationship between two assets. It has two attributes, the $Predecessor$, and the $Successor$, where the successor asset depends on the predecessor.

As described above, every asset has an assigned owner. This owner belongs to the $Collaborator$ table. Ideally this table would be linked with the application responsible for managing entities in the company, therefore not being necessary in this database model. However, it was not possible to link the database with this application, so the table $Collaborator$ is responsible for representing the employees of the company. This table has a:

- $Collaborator\_ID$ that works as a unique identifier for each one of the collaborators, for example 'e73727';
- $Name$ attribute that refers to the name of the collaborator;
- $Password$. This attribute is only used for the login available in the dashboard provided;
- $Department$ that identifies the department where the collaborator belongs in the organisation.

The $Vulnerability$ table is also connected with the $Asset$ table and holds all the vulnerabilities identified. It is based in nine essential attributes:

- ID is the identifier generated by the database;
- $Vulnerability\_ID$ is the identifier used by the organisation for that vulnerability, for example 'VULN#088';
- $Severity$ is the attribute that classificates the vulnerability and is connected to the $Severity\_Value$ table;
- $Asset\_ID$ refers to the asset where the vulnerability is hosted;
- $Type$ is the type of vulnerability;
- $Creation\_Date$ is the day, month and year when the vulnerability was opened;
- $State$ defines if the vulnerability is either opened or closed;
- $GDPR$ is a reference to the General Data Protection Regulation (GDPR) [24], therefore, this attribute defines if a vulnerability can affect the protection of data;

- $Creator$ is the id of the collaborator who created the vulnerability.

The table $Severity\_Value$ classifies the severity of each vulnerability. EDP classifies its vulnerabilities accordingly to the following values: Low, Medium, High, and Critical.

The $Incident$ table has ten essential attributes and represents each incident that occurred on an asset.

- ID is the identifier generated by the database;
- $Incident\_ID$ is the ID provided by the organisation to the incident;
- $Asset\_ID$ is the ID of the asset where the incident occurred;
- $Type$ refers to the type of incident and is organisational dependant;
- $Creation\_Date$ is the date when the incident was opened;
- $Stage$ defines if the incident is still open or if it is already closed;
- $Creator$ is the ID of the collaborator that was responsible for creating that incident;
- $Security\_Classification$, $Operational\_Impact$, and $Consequence\_Severity$ attributes that refer to three other tables.

The $Security\_Classification$ table measures the impact of an incident regarding the importance of the information that was compromised or exposed. Its values range between one and four and correspond to Unclassified, Confidential, Secret and TopSecret respectively for the EDP context.

The $Operational\_Impact$ table represents the impact an incident has on the operation of the IT infrastructure and the company. In the current implementation, at EDP, it's characterized by the following values: 0 – No Impact, 1 – No Immediate Impact, 2 – Low Priority Impact, 3 – High Priority Impact and 4 – Immediate Impact.

The $Consequence\_Severity$ table measures the severity of the consequences an incident can have on the IT infrastructure of an organisation. Its values range between zero and four and correspond to None, Insignificant, Marginal, Critical and Catastrophic respectively for the EDP context.

To store the scores of each variable of the proposed model, a $Risk$ table was created. This table is only connected with the Asset table since each one of the scores stored belongs to a unique asset.

- $Risk\_ID$ is the attribute referent to the primary key;
- $Asset$ is the attribute that corresponds to the ID of the respective asset;

- *Total_Score* is the total risk score of the asset and it depends on the other three attributes: the *Vulnerability_Score*, the *Dependency_Score*, and the *Incident_Score*, which correspond to the values of the variables vulnerabilities, dependencies and incidents respectively;
- *Date* is the date of the last time the risk values were assessed.

Finally, there is a table that is not connected to any of the previous ones: the Parameters table (Figure 5.3). This table is essential to the model since it is responsible to store all the parameterized weights, maximum values accepted and the scale upper limit, that are defined by the organisation and that are used in the risk assessment process. All its attributes are presented and described in the Appendix A – Risk Assessment Model Parameters.

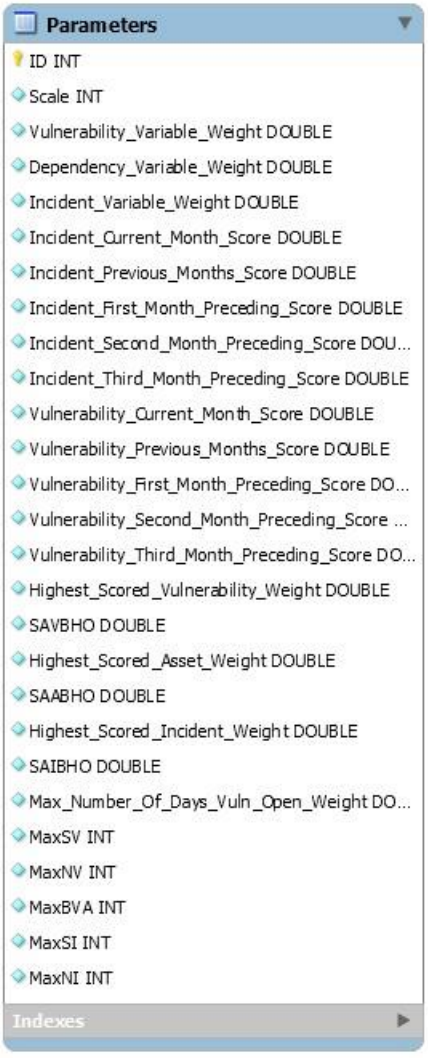

Figure 5.3 – Parameters table

5.3 Identification of Assets and Dependencies

The information about the assets that populate our model's database comes from EDP's CMDB. The CMDB is a repository that ideally holds all information regarding all the hardware and software components of an organisation, as well as their relationships.

The identification of assets started off with an extraction from the CMDB. This extraction contained data about the different types of servers (application, infrastructure, database, and virtualization), the databases and all the virtual machine instances. Since this process gave us a lot of unstructured information about all the company assets, the process of consolidating the information was very time consuming and complicated, but it was necessary to place all the relevant data in the structure needed before it was imported into the database.

To facilitate the process of structuring information, we chose to cross the data with other sources of information from EDP, such as the vulnerabilities and the incidents list.

After crossing all the data and obtaining the relevant information of assets, for the risk assessment process, i.e. assets that contained vulnerabilities or incidents, we collected all the necessary information to populate our database. In total, 1047 assets were added in the desired format to a .xls document that was ready to be imported into the database.

After the identification of all the assets, it was necessary to identify all the dependencies between them. Although some of the dependencies were identified on the extraction from the CMDB, some of them had to be identified through other information sources provided by EDP, such as websites, files, and people.

Lastly, all this was imported to our database using a script in Java that connects our list of assets and our list of dependencies to the database, the DatabaseImport.jar.

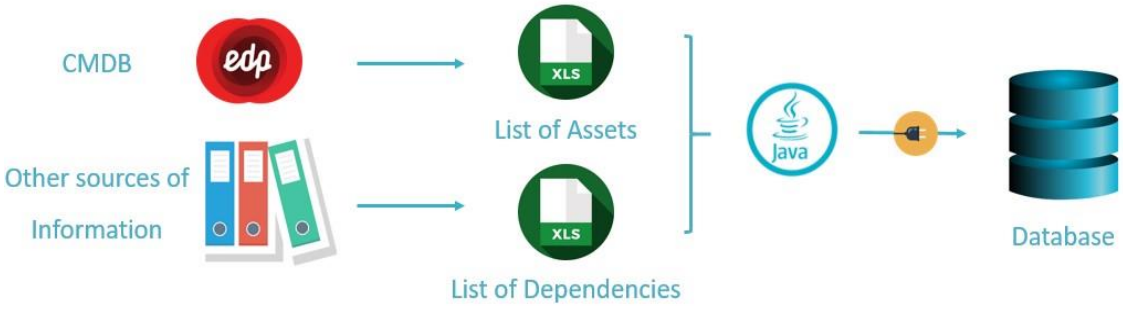

Figure 5.4 – Asset identification process

5.4 Identification of Incidents

Although EDP already has a list with all the incidents that are reported to the SOC team (namely phishing incidents) or detected as part of the continuous security monitoring service, it was still necessary to identify the incidents we were going to use in our model.

After analysing all the types of incidents collected by EDP, we concluded that only a small subset of existing applications in the EDP universe had associated security incidents. One of the applications with a higher number of security incidents is the one responsible for the management of digital identities within the company and its incidents are mostly regarding the inappropriate use of resources. Although EDP has other types of incidents, the most common incident is the malicious code attack, which usually occurs in workstations. Given that only server hosts were considered in our database and that the number of security incidents associated with applications is very limited, the impact of the incidents in this company context becomes minimal.

After the identification of the incidents collected by EDP, the incidents were placed in a .xls document. This document is structured accordingly with the attributes of the Incidents table present in the database. This allows the data to be ready to be imported into the database, similarly to what happened with assets and dependencies.

5.5 Identification of Vulnerabilities

The process of identifying vulnerabilities was divided into two distinct parts. First, all the software vulnerabilities already present in the EDP universe were considered. This service is provided by a third-party company that is responsible for testing EDP applications through persistent penetration testing. This company provides the test results through an online platform that allows the SOC team to view, analyse and follow up all the vulnerabilities. After this, we added the infrastructure vulnerabilities detected by Nessus to our model. Although this vulnerability scanner was already present in the EDP universe, these vulnerabilities weren't used to make any sort of incident prevention.

5.5.1 Software Vulnerabilities

To obtain all the vulnerabilities detected by the EDP's *pen-testing* service provider, it was necessary to extract all the existing data from the provider's platform. The third-party company does penetration tests in the entire EDP universe that includes other countries such as Brazil and Spain. However, EDP's CMDB only contains assets belonging to the

Portuguese and Spain infrastructures, therefore we only chose to extract the results corresponding to these countries.

After the extraction was made, there was the need to cross the information about the vulnerabilities identified in the *pen-testing* with the assets gathered before. While crossing the assets affected by vulnerabilities with the ones extracted from the CMDB, it was possible to notice that not all the assets names matched. This gave us the need to try to understand which asset of the CMDB the vulnerability matched, after leading to a process of data normalization.

After the matching process, all the data were added to a .xls file, in the structure required to fit our database.

5.5.2 Infrastructure Vulnerabilities

As represented in Figure 5.5, the results from the Nessus scan are imported to the SIEM before they are added to our list of vulnerabilities. This happens because this report contains a huge amount of other information that is difficult to understand and process. When imported into the SIEM, the information is processed by the connector and normalized, after which it can be gathered in the required format and interpreted in a much easier and faster way.

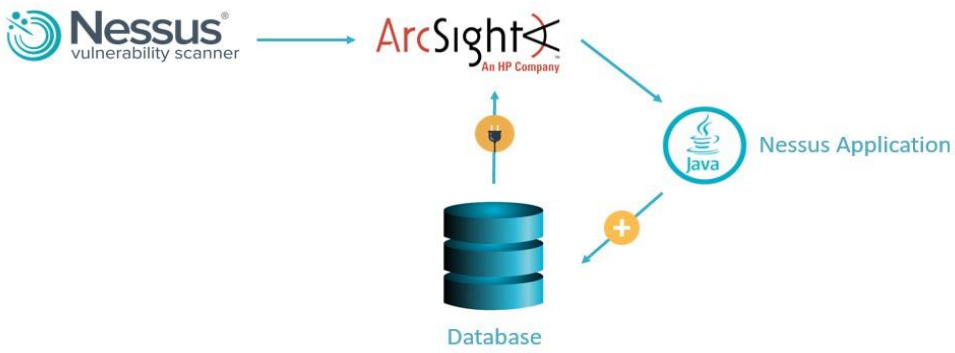

Figure 5.5 – Nessus scan data flow

To interpret all the data coming from SIEM, a script was written in Java. This script deals with all the data coming from the Nessus scan and intersects it with the one contained in the database. All the IP addresses and the Host Names detected in the scan had to be validated against the assets that were present in the database. Again, this took a considerable amount of time and unfortunately it was not possible to match all the scanned

IP addresses with the identified assets since not all the assets from EDP's CMDB have an associated IP address. Since it is crucial to link the identified vulnerabilities with the respective assets to have a sense of risk, we chose to add the unidentified IPs as assets to our list of assets, allowing us to take those vulnerabilities into consideration in the risk assessment process.

After obtaining the assets, the scanned vulnerabilities were added directly to the database. Given that EDP generates Nessus reports monthly, all our data needs to be updated in the same frequency of the report generation. In every report, new vulnerabilities are identified but, unlike what happens with the external service provider, old vulnerabilities are not closed. This requires closing all the vulnerabilities that are no longer in the new report because if the scan was not able to identify them, they are no longer a threat to their respective asset. Given this, if the old vulnerabilities are not identified in the new report, they are closed with the date of the new report. Therefore, these vulnerabilities are no longer considered with the same weight in the risk assessment process.

In the database, a new service was created to encapsulate all the new assets identified by Nessus that were not in the CMDB, correspondent to the vulnerabilities. With this, EDP can identify specifically the risk associated with infrastructural vulnerabilities by assessing the risk of the 'Infrastructure' service.

5.6 Dashboard

Although a dashboard was already developed in a previous phase of the project, some improvements had to be made to match the needs of EDP. The old dashboard presented a graph with the evolution of the global risk in the last twelve months and a table with some relevant metrics. Instead of having only the graph with the evolution of risk, a gauge with the global risk was inserted to provide more immediate information and to match the design of other panes used by the SOC at EDP. We kept the table with the metrics on the right side of the page, making only a few colour changes regarding the risk score.

It is important to know that the buttons Global Metrics, Infrastructure 1 Incidents, Infrastructure 2 Incidents, and Vulnerabilities do not have a specific function in the dashboard since they come from the EDP SOC environment.

The dashboard is composed of seven PHP pages: Global Risk, Services, Applications, Hosts, Parameters, Reports, and a Login page.

Figure 5.6 displays our Global Risk age that has three mains areas: the gauge with the current risk of the organisation, the risk evolution in the last months and on the right side of the page there is a table with metrics.

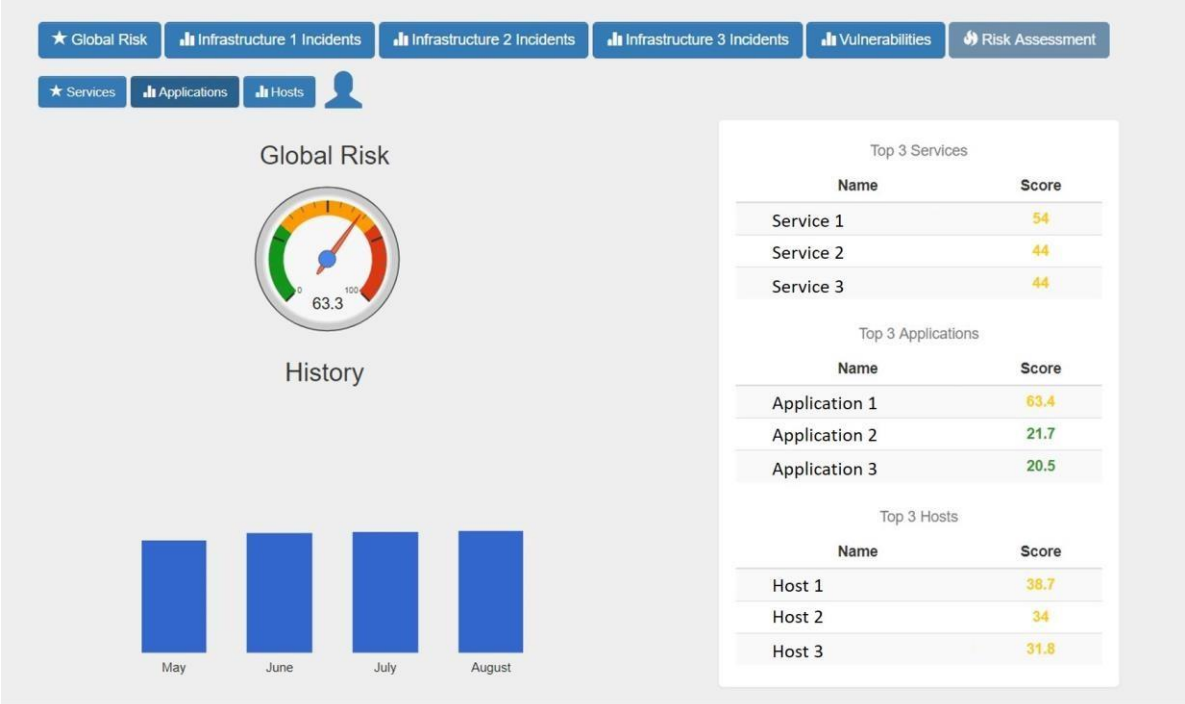

Figure 5.6 – Global Risk page

The global risk value present in the gauge corresponds to an asset that relates all the services by depending on them, giving the organisation a global view of the state of all services. The risk evolution histogram has a bar for each one of the months where a risk assessment occurred. Each one of the bars represents the average risk score based on daily values and the graph is scaled accordingly to the scale defined in the Parameters table of the model. The metrics displayed correspond to the three highest scored assets of each one of the layers, offering a better insight into which assets risk needs to be taken care of first.

Along with every page, there are buttons in the upper left corner that allow the user to easily navigate through the dashboard, giving him the possibility to access the different layers of the model and to access the global risk page at any point.

Next, to the far-right button, there is a login option. An authenticated user has different accesses and privileges. One can access the list of vulnerabilities of each asset, can add new incidents or vulnerabilities, can close incidents or vulnerabilities, can configure some of the parameters of the models as well as generate risk reports. None of these tasks can be performed by a non-authenticated user. The authentication process is

done by matching the Collaborator_ID and Password attributes from the Collaborator table with the inputs given in the login page.

In this page, it is also possible to add new vulnerabilities and incidents to the model (Figure 5.7), by selecting the plus next to the “Hosts” button. This was one of the improvements to the dashboard since it allows EDP to stop using excel files to deal with vulnerabilities and incidents. These new functionalities also allow EDP to have all its information centralized in a database, enabling the creation of new security metrics based on all the available information. This functionality has all the attributes considered relevant to this specific environment and it contemplates the attributes essential to the vulnerabilities and incidents table existent in our database.

The main value of these new functionalities is the possibility of stop using excel files to save data and events that exist in the EDP environment. will no longer use files to record data and events, so you can have all the information centralized in a database.

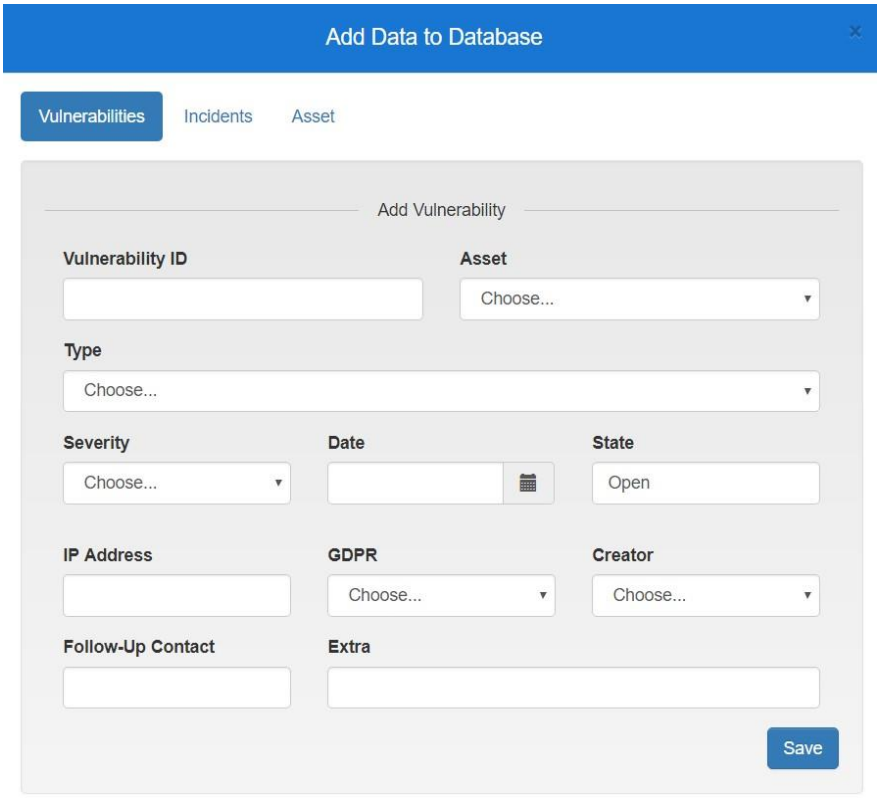

Figure 5.7 – Functionality to add a vulnerability

The Services, Applications and Hosts pages all have the same structure. Each of these pages displays a table where every line corresponds to a different asset, and the columns match the most relevant attributes of the corresponding type of asset (Figure 5.9). In the far left of each line, a button is displayed. This button controls the display of the asset’s

dependencies if they are available. Additionally, in case the user is logged in, the asset's vulnerabilities and its incidents are also displayed (Figure 5.8).

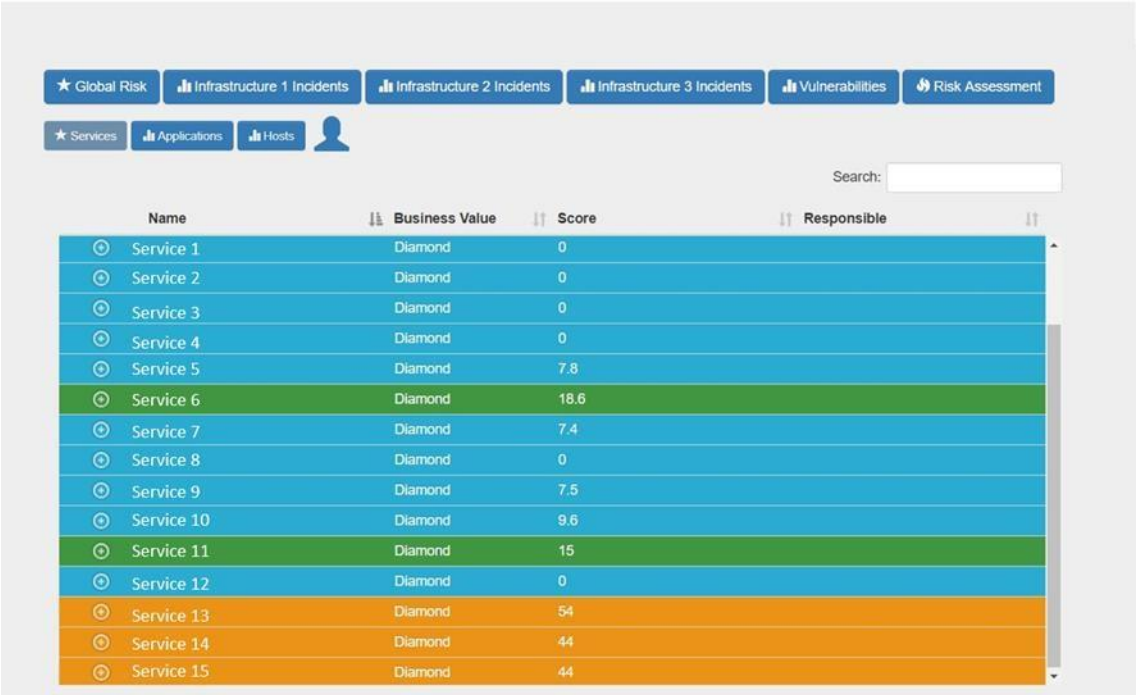

Figure 5.9 – Services page

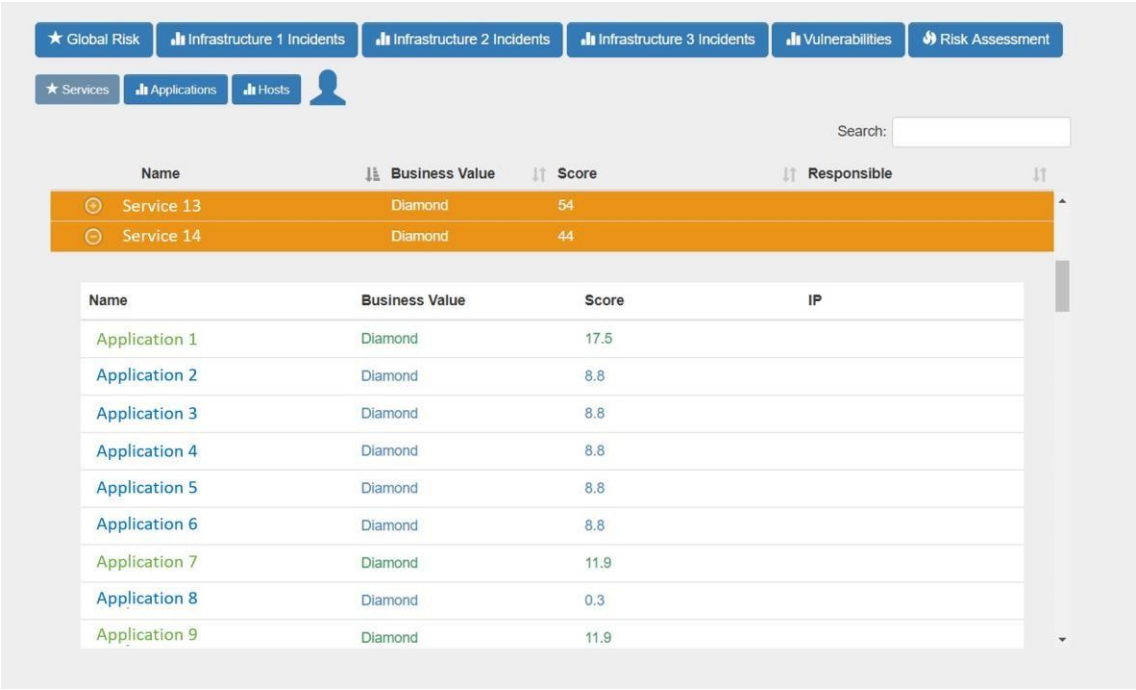

Figure 5.8 – Applications supporting Service 14

By selecting the button ‘Applications’ when the user is authenticated, the page with the risk scores of each application is presented as well as the list of its vulnerabilities and incidents (Figure 5.10). If needed, the user can also close a vulnerability through the ‘Close’ button. This functionality is also available for the ‘Hosts’ page.

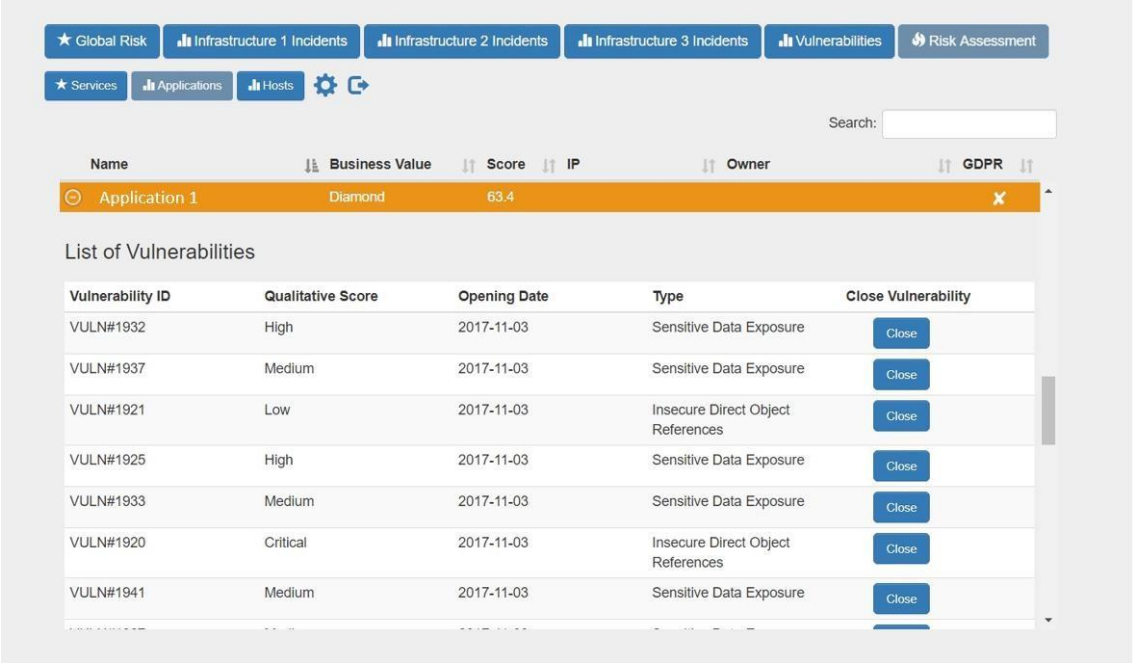

Figure 5.10 – Applications page with button to close vulnerabilities

The Parameters page, accessible only when the user is logged in, has the objective to configure some of the parameters of the database Parameter’s table. Unlike the previously developed dashboard, this page only allows the team to change four parameters used in the process of risk calculation, namely:

- the maximum value of the risk scale – risk will be scored in the interval [0; Risk Scale];
- the weights of the variables Vulnerabilities, Incidents, and Dependencies – these weights represent the relative importance of each of these variables in the model, the weights values should be between zero (if the variable should not be considered) and one (if the model should only consider that variable), and the sum of the weights should be one.

As an addition to the previously developed dashboard, a functionality to generate reports was added. This functionality allows the SOC to generate a report of the results present in the model, by selecting a period of time of their interest.

The functionality creates a pdf file with data corresponding to the period selected. It creates four distinct graphs: one with the evolution of risk over the selected period and

the other three graphs carry the information regarding the ten higher risk services, applications, and hosts. The user can choose to obtain information from any of the three levels of our model.

The reports, along with the dashboard, were designed to promote and improve the communication of risk from the IT technicians to the top-level managers.

Appendix B – Dashboard presents examples illustrating the remaining features of the dashboard and an example of a report.

5.7 SIEM Integration

The integration of the results obtained in the risk assessment process with the SIEM is fundamental for the SOC operation and for using the component at its fullest.

When utilized as a stand-alone component, without feeding the SIEM but receiving information concerning incidents and vulnerabilities, the component delivers risk assessment capabilities. In real life utilization, integrated with the SIEM, the component offers both risk assessment and risk management capabilities, because the SIEM can take advantage of the knowledge about assets' risk scores to differentiate the security alerts. This way, enhanced information is given to the SOC operators to improve risk mitigation.

By sending the results obtained in the risk assessment process to the SIEM the EDP SOC can have a better context of risk in specific assets so that the most relevant events can be prioritized and analysed first.

The integration with the SIEM works in a bidirectional way (Figure 5.11). The SIEM feeds the developed database with the information about incidents and vulnerabilities identified by Nessus, while the SIEM fetches the results of the risk assessment process.

In the case of EDP, it was necessary to add other data sources to the component since the organisation's asset model was not linked to SIEM. However, in organisations that have everything centralized in the SIEM, specifically the assets model and the vulnerabilities, the tool can enjoy the integration without external interfaces.

The integration of the database that has all the risk information with the SIEM is achieved through an SQL query to the database. The integration can be done in two different ways: through a .csv file or, in the case of a SIEM through the creation of a connector.

By using a .csv file an automated export to a folder can be made and the SIEM can consume the information directly from there. This can automate the process of data

consumption by SIEM and it also allows the integration of the model with the various SIEMs in the market.

Figure 5.11 – SIEM Integration

Creating the connector requires to select a connector available from the manufacturer (in the ArcSight case is the *SmartConnector*), then it is necessary to define the query to the database. A connector allows for an automatic integration with the SIEM without other external manual procedures to import information regarding assets risk.

A rule was created in the SIEM that is triggered whenever an event is identified on assets with a risk score above a predefined threshold. This way, the SOC team is able to prioritize the treatment of events on assets with a higher risk score.

Chapter 6

Evaluation of the Preliminary Component Integration

The following sections present the results of the risk assessment process using the model presented in Chapter 4 and the implementation described in Chapter 5.

We begin by describing the experiment, starting with the parameters that we found adequate for the model to work as expected. Then there is an explanation of how the risk assessment is done in the EDP context and how the dashboard was integrated and used by the EDP SOC team, as well as the results obtained due to this integration.

Finally, we conduct an analysis of the integration with the SIEM and evaluate the new features for opening and closing vulnerabilities.

The results presented in this chapter were obtained over a three-month period.

6.1 Description of the Experiment

Our objectives with the experiment were to:

- Evaluate the efficiency of the new features for opening and closing vulnerabilities directly in the dashboard.
- Assess the efficacy of our component when integrated with the SIEM;

Before we started the risk assessment process, it was necessary to configure all the parameters. This configuration must always be made before the risk assessment process, and it should consider the context of the organisation in which it is made. Do note that the values of all the parameters can be changed later, directly in the database, by an expert, and some of the values can be changed while using the dashboard.

The values chosen for the implementation of the model in the EDP context are present in Appendix A – Risk Assessment Model Parameters.

The choice of these values for the parameters was made considering the EDP universe. Since that in EDP, the number of applications affected by incidents is very reduced, our parameters are influenced by this scenario. Given this, we chose to give a

lower value to the incidents parameter, given that very few are identified. Therefore, the parameter that has a greater impact on the calculation of the risk is the parameter corresponding to the weight of the vulnerabilities, followed by the incidents and dependencies weight that take the same value.

Given that the model considers the vulnerabilities and the incidents that occurred in the last three months, weights were given to the variables corresponding to the current month and the previous months. In this case, we considered that vulnerabilities and incidents opened in the present month are more relevant than the ones that happened in the previous ones. In relation to the previous month's variable weight, as the months go by we consider that the importance of incidents and vulnerabilities decreases, i.e., the most recent past month is the most relevant one and the third month is the one that has the least relevance on the risk score.

EDP considers that any vulnerability must be solved within 365 days, which means that if a vulnerability is open for more than one year, the risk score of the asset is the maximum value in the scale. The maximum number of open vulnerabilities with a maximum score in an asset tolerated by EDP is three vulnerabilities, while the maximum number of incidents with the highest score that may occur in a month in an asset is two. Therefore, the corresponding parameters were set with these values.

All values of the other parameters were associated with the assigned values to the fields used to assess the severity of the vulnerabilities as well as the operational impact, consequence severity, and security classification of the incidents.

After defining the parameters and identifying all the assets, dependencies, incidents and vulnerabilities, everything was ready for the risk assessment application.

To ensure that the risk is calculated daily without human intervention, a rule was created in the task scheduler of the server, that allows to enforce the risk assessment application to run every day at 11:55 pm. This process saves time from the SOC team that does not have to run the application manually.

Every time the risk assessment process is run, and the risk scores are calculated, the database is updated with the values obtained. After this process, all the information is loaded automatically in the dashboard described in Implementation.

6.2 Evaluation of the New Functionalities

After the values are displayed in the dashboard it is then possible to analyse the risk value associated with each host, application, and service. During the trial period of three months, it was also possible to test the new features of closing and opening vulnerabilities as well as incidents.

These two new features were used by the SOC operators who are responsible for opening and closing both vulnerabilities and incidents. Over the course of three months, 47 vulnerabilities and 8 incidents were opened, and 87 vulnerabilities and 7 incidents were closed.

Using the previous manual procedure before the integration, the SOC operator had to access a local file and update it every time a vulnerability was opened or closed. Using the dashboard, the SOC operator always started to use it as a non-authenticated user. This required him to log in before being able to open vulnerabilities or search for them in order to close them (by using the search box available in the dashboard) because these features are only available for logged in users.

An analysis was made to evaluate if the implementation of the new functionalities had any improvement in the operation of the SOC. These new features have replaced the need to use an excel file to keep track of open and closed vulnerabilities or incidents. With the analysis made, it was possible to conclude that when using the functionality to open vulnerabilities, the opening time while using the dashboard was superior to the one while using the file, as it is mentioned in Table 6.

Vulnerability ID	Document Insertion	Dashboard Insertion
2253	01:06.17	01:00.00
2254	00:55.42	01:02.14
2255	00:59.55	01:10.88
2256	01:03.15	01:08.50
2257	00:58.20	01:05.10
Total AVG	**01:00.42**	**01:05.32**

Table 6 – Vulnerabilities opening time in minutes while using the document and the dashboard

This happens because while using the implemented functionality it is necessary to create each vulnerability individually, regardless of whether there are multiple vulnerabilities for the same asset. When creating vulnerabilities directly in the file, it is possible to copy the data from previous rows, which allows to save some time. However, copying data from previous rows is more likely to cause errors. Therefore, with the new functionality, we can assure that an existing asset is chosen, while making the cross-referencing of vulnerabilities with the assets name. Given this, the functionality to insert vulnerabilities or incidents increases the quality of the information collected and can reduce some errors.

Concerning the closing vulnerabilities and incidents functionality there was an improvement in the execution time of the task. Closing vulnerabilities in the dashboard is relatively faster than in the file and simultaneously allows to reduce the error rate in the introduction of closing dates. The button to close vulnerabilities also allows the team to save some time when dealing with the dashboard, otherwise, the team would have to edit the file correspondent to either vulnerabilities or incidents, edit the respective vulnerability or incident closing date, and then re-import the file into the database to make the changes.

Vulnerability ID	Document Closing Time	Dashboard Closing Time
1237	01:15.88	00:39.36
1238	00:59.80	00:19.05
1339	01:08.17	00:28.15
1342	00:58.14	00:24.01
1343	00:49.90	00:23.15
Total AVG	**01:02.32**	**00:26.50**

Table 7 – Vulnerabilities closing time in minutes while using the document and the dashboard

6.3 Evaluation of the Integration with SIEM

The results of the risk assessment were later introduced in the SIEM. Regardless of the insertion mode chosen, a query to the database is made. This query obtains the risk score of the assets that have an IP address associated, for the last day that the risk assessment process was made. The typical result of the query is illustrated in Figure 6.1.

As displayed in Figure 6.1, the results of the query were ordered by risk score and not all the IP addresses have an associated hostname. These results fit into the risk categories presented in 2.1 . Ideally, in an organisation with higher risk scores, we would only care about the ones that correspond for example to high and critical levels of risk, depending on the scale used. However, in the EDP context, given that we did not obtain many assets with high-risk levels, we chose to use all the query results.

This query allowed us to insert the results into the SIEM and the fact that the insertion considers the risk value, it allows us to quickly identify the events associated with assets with higher risks. In the SIEM, the results of the query are crossed with the events detected through a correlation rule that was programmed in the SIEM. Whenever the rule is triggered, the SIEM creates an alert to warn about the corresponding event. These events are also ordered by its assigned priority value given by ArcSight, and in this analysis, we considered events with a very high and high priority.

Date	HostName	IPAddress	Score
2018-08-05	Hostname 1	IP Address 1	63.4
2018-08-05		IP Address 2	38.7
2018-08-05	Hostname 2	IP Address 3	34
2018-08-05	Hostname 3	IP Address 4	31.8
2018-08-05		IP Address 5	30
2018-08-05	Hostname 4	IP Address 6	28.5
2018-08-05	Hostname 5	IP Address 7	26.7
2018-08-05		IP Address 8	26.3
2018-08-05	Hostname 6	IP Address 9	25.4
2018-08-05	Hostname 7	IP Address 10	25.4
2018-08-05	Hostname 8	IP Address 11	25.4
2018-08-05		IP Address 12	24.9
2018-08-05	Hostname 9	IP Address 13	21.7
2018-08-05		IP Address 14	19.4
2018-08-05	Hostname 10	IP Address 15	19
2018-08-05		IP Address 16	19
2018-08-05	Hostname 11	IP Address 17	18.6
2018-08-05		IP Address 18	18
2018-08-05	Hostname 12	IP Address 19	17.6
2018-08-05	Hostname 13	IP Address 20	17.6
2018-08-05	Hostname 14	IP Address 21	17.6
2018-08-05		IP Address 22	17.5
2018-08-05	Hostname 15	IP Address 23	17.5
2018-08-05		IP Address 24	17.2
2018-08-05		IP Address 25	16.8
2018-08-05		IP Address 26	16.1
2018-08-05		IP Address 27	15.7

Figure 6.1 – Example of the query results

After these events are detected by the SIEM, the SOC is responsible for assessing the situation and for analysing the respective event. Consequently, if the event is confirmed to be relevant then an incident is created for the respective asset.

During the three-month period, it was possible to identify one incident that would have gone unnoticed if the framework was not in use. Considering that in that period only

eight incidents occurred, this corresponds to an improvement of 14,3% in the detection of incidents.

Chapter 7

Conclusion and Future Work

The objective of this work was to improve an already existing model in order to satisfy the requirements of the European project DiSIEM and put it into operation in one of the companies involved in this same project, EDP.

The work began by performing an improvement of the database developed in the previous iteration of the model. This change allowed the database to be more suited to the context of EDP since its structure is now more comprehensive.

The risk assessment proposal of the model was also simplified to include only one way of assessing risk rather than the previous three, and it was also added the possibility for organisations to consider a history of vulnerabilities when calculating the risk of the asset.

Throughout the development of this work, we also introduced new components, namely the insertion of a new type of vulnerabilities, the infrastructural. This new component is based on the use of the Nessus Professional software and these vulnerabilities are introduced into the database through a Java application that crosses the detected vulnerabilities with the assets identified in the organisation. The application is also responsible for closing infrastructure vulnerabilities that happened in previous months that do not appear in the latest scan.

The implemented dashboard has also been improved to meet the needs of EDP. The dashboard now allows the insertion of new vulnerabilities, incidents, and assets, which saves some time for the SOC operators. Its appearance was also refined and a feature to generate reports was added. This feature allows the SOC to create a pdf with the evolution of risk and all the information concerning the highest scored assets in a certain period.

In addition, the tool was also integrated with SIEM, therefore allowing the results of the risk calculation to be used in the detection of possible events that would once go unnoticed. This integration allows the SOC team to pay more attention to the assets with a higher level of risk, giving them the opportunity to act first on the events that arise related to the highly scored assets.

At the end of the integration in the EDP universe, we also evaluated the performance of the tool and its use during a three-month experimental period. Given the obtained results we concluded that the tool improved the performance of the SOC by reducing the time spent interacting with the opening and closing of vulnerabilities or incidents and by increasing the quality of the collected data since it decreased the probability of occurrence of errors when inserting new data. The integration with the SIEM also allowed detecting events that, without the existence of the component, would go unnoticed, therefore proving the effectiveness of the model.

With the integration of this work in the EDP universe we could contribute to an improvement in the performance of the SOC team, not only because they can now detect the assets that should be treated first, but also because it was the first step to avoid using Excel files to register relevant security events in the EDP universe. EDP has now a database that contains a lot of centralized information and can adopt it, in the future, to record all the information considered relevant. The organisation can also connect its entire dashboard with the database developed, also being able to easily create new metrics to evaluate their performance while dealing with events.

This component is also ready to be integrated in other organisations if necessary. To do that, it is necessary to identify all the relevant data to populate the database so that the risk assessment process can be applied and then the integration with the SIEM should be made, through specially developed connectors. If the organisation has all the information centralised and organised, this process is simplified, since one of the main difficulties was the identification and normalization of all the data needed for the risk assessment process.

Even though the component integration contributed to an improvement of the functioning of the SOC, the model has the potential to become more accurate, efficient and effective in the EDP context. To have a more effective risk assessment process, a direct integration with the CMDB is essential since this will allow the asset model to always be up-to-date, consequently avoiding the need to add new assets directly in the dashboard. Another way to increase the quality of the model in the EDP context involves using the incidents that were not considered so far: the ones that occur in collaborators computers. Most of the events detected by the Micro Focus ArcSight at EDP are related to incidents that occur on collaborators' computers.

Although that when including these incidents, it would also be necessary to include the assets corresponding to the employees of the company (which would substantially increase the complexity of the model), this would be a way of adding a new layer of knowledge regarding the behaviour and attitudes of employees which also influences the overall risk of the organisation.

As future work, we also need to include the generated charts into the reports developed by the SOC team. This functionality also needs to be evaluated regarding the new ways of communicating risk. Therefore, it is still required to evaluate the results of the multi-level risk assessment by the C-Levels of EDP and the usefulness of the assessment provided for the different services.

References

[1] DiSIEM, "D2.1 In-depth analysis of SIEMs extensibility," 2017. [Online]. Available: http://disiem-project.eu/wp-content/uploads/2017/03/D2.1.pdf.

[2] L. M. Ferreira, "A Multi-Level Model for Risk Assessment in SIEM, Master Thesis Dissertation," *FCUL*, 2017.

[3] "Nessus Professional™ Vulnerability Scanner." [Online]. Available: https://www.tenable.com/products/nessus/nessus-professional. [Accessed: 13-Dec-2017].

[4] "DiSIEM Project." [Online]. Available: http://disiem-project.eu/. [Accessed: 20-Nov-2017].

[5] "EDP - Energias de Portugal." [Online]. Available: https://www.edp.com/en. [Accessed: 20-Nov-2017].

[6] "ArcSight Enterprise Security Manager (ESM)." [Online]. Available: https://software.microfocus.com/en-us/products/siem-security-information-event-management/overview. [Accessed: 10-Dec-2017].

[7] G. Scott, "Putting the Top 10 SIEM Best Practices to Work Processes, Metrics, Technologies," 2010.

[8] DiSIEM, "D2.2 Reference Architecture and Integration Plan," 2017. [Online]. Available: http://disiem-project.eu/wp-content/uploads/2018/06/D2.2v2.pdf.

[9] "National Institute of Standards and Technology | NIST." [Online]. Available: https://www.nist.gov/. [Accessed: 12-Dec-2017].

[10] "ISO - International Organization for Standardization." [Online]. Available: https://www.iso.org/home.html. [Accessed: 12-Dec-2017].

[11] ISO/IEC, "ISO/IEC 27005:2011 - Information Security Risk Management," *Int. Organ. Stand. Int. Electrotech. Comm.*, 2011.

[12] ISO/IEC, "ISO 31000:2009 Risk management - Principles and guidelines," *Int. Organ. Stand. Int. Electrotech. Comm.*, 2009.

[13] T. W. Kwan and H. K. N. Leung, "A Risk Management Methodology for Project Risk Dependencies," *Ieee Trans. Softw. Eng.*, vol. 37, no. 5, pp. 635–648, 2011.

[14] L. Tang, K. Jing, J. He, and H. E. Stanley, "Robustness of assembly supply chain networks by considering risk propagation and cascading failure," *Phys. A Stat. Mech. its Appl.*, vol. 459, pp. 129–139, 2016.

[15] Y. Zhang, "Selecting risk response strategies considering project risk interdependence," *Int. J. Proj. Manag.*, vol. 34, no. 5, pp. 819–830, 2016.

[16] N. Kheir, H. Debar, F. Cuppens, N. Cuppens-Boulahia, and J. Viinikka, "A service dependency modeling framework for policy-based response enforcement," in *U. Flegel D. Bruschi DIMVA 2009, 5587 LNCS*, pp. 176–195, 2009. Springer-Verlag Berlin Heidelberg 2009.

[17] E. Condon and M. Cukier, "Using Approximate Bayesian Computation to Empirically Test Email Malware Propagation Models Relevant to Common Intervention Actions," *Proc. - Int. Symp. Softw. Reliab. Eng. ISSRE*, pp. 287–297, 2016.

[18] A. Kotenko, Igor and Chechulin, "Attack modeling and security evaluating in SIEM systems," *Int. Trans. Syst. Sci. Appl.*, vol. 8, no. December, pp. 129–147, 2012.

[19] Z. Xinlan, H. Zhifang, W. Guangfu, and Z. Xin, “Information Security Risk Assessment Methodology Research: Group Decision Making and Analytic Hierarchy Process,” *2010 Second World Congr. Softw. Eng.*, vol. 2, no. 2, pp. 157–160, 2010.

[20] DiSIEM, “D3.1 Security Metrics and Measurements,” 2017. [Online]. Available: http://disiem-project.eu/wp-content/uploads/2018/02/D3.1.pdf.

[21] “Common Vulnerability Scoring System (CVSS).” [Online]. Available: https://www.first.org/cvss/. [Accessed: 13-Sep-2018].

[22] “MariaDB.org - Supporting continuity and open collaboration.” [Online]. Available: https://mariadb.org/. [Accessed: 03-Jun-2018].

[23] R. Elmasri, *Fundamentals of Database Systems*, 6th ed. 2011.

[24] “General Data Protection Regulation (GDPR) – Final text neatly arranged.” [Online]. Available: https://gdpr-info.eu/. [Accessed: 28-Apr-2018].

Appendix A – Risk Assessment Model

Parameters

Attribute	Description	Score
Scale	The upper limit of the risk scale interval.	100
Vulnerability_Variable	The weight used for the vulnerabilities ponderation.	0.70
Dependency_Variable	The weight used for the dependencies ponderation.	0.15
Incident_Variable	The weight used for the incidents ponderation.	0.15
Incident_Current_Month	The weight of the incidents that happened in the current month.	0.80
Incident_Previous_Month	The weight of the incidents that happened in the previous months.	0.20
Incident_First_Month_Preceding	The weight of the incidents risk score from one month ago.	0.60
Incident_Second_Month_Preceding	The weight of the incidents risk score from two months ago.	0.25
Incident_Third_Month_Preceding	The weight of the incidents risk score from three months ago.	0.15
Vulnerabilities_Current_Month	The weight of the vulnerabilities that happened in the current month.	0.80
Vulnerabilities_Previous_Month	The weight of the vulnerabilities that happened in the previous months.	0.20
Vulnerabilities_First_Month_Preceding	The weight of the vulnerabilities risk score from one month ago.	0.60
Vulnerabilities_Second_Month_Preceding	The weight of the vulnerabilities risk score from two months ago.	0.25
Incident_Third_Month_Preceding	The weight of the vulnerabilities risk score from three months ago.	0.15
Highest_Scored_Vulnerability	The weight of the vulnerability with the highest score.	0.75
SAVBHO	The weight of the sum of all vulnerabilities but the highest one.	0.25
Highest_Scored_Asset	The weight of the asset with the highest score.	0.75

SAABHO	The weight of the sum of all assets score but the highest one.	0.25
Highest_Scored_Incident	The weight of the incident with the highest score.	0.75
SAIBHO	The weight of the sum of all incidents score but the highest one.	0.25
Max_Number_Of_Days_Vulnerability_Open	A maximum number of days a vulnerability can remain open.	365
MaxSV	Maximum severity value a vulnerability can have.	9
MaxNV	A maximum number of open vulnerabilities with maximum score an asset can have.	3
MaxBVA	Maximum Business_Value admitted for assets.	4
MaxSI	A maximum score value of an incident in the incidents scoring system.	64
MaxNI	A maximum number of incidents with the maximum score that can happen in a single month.	2

Appendix B – Dashboard

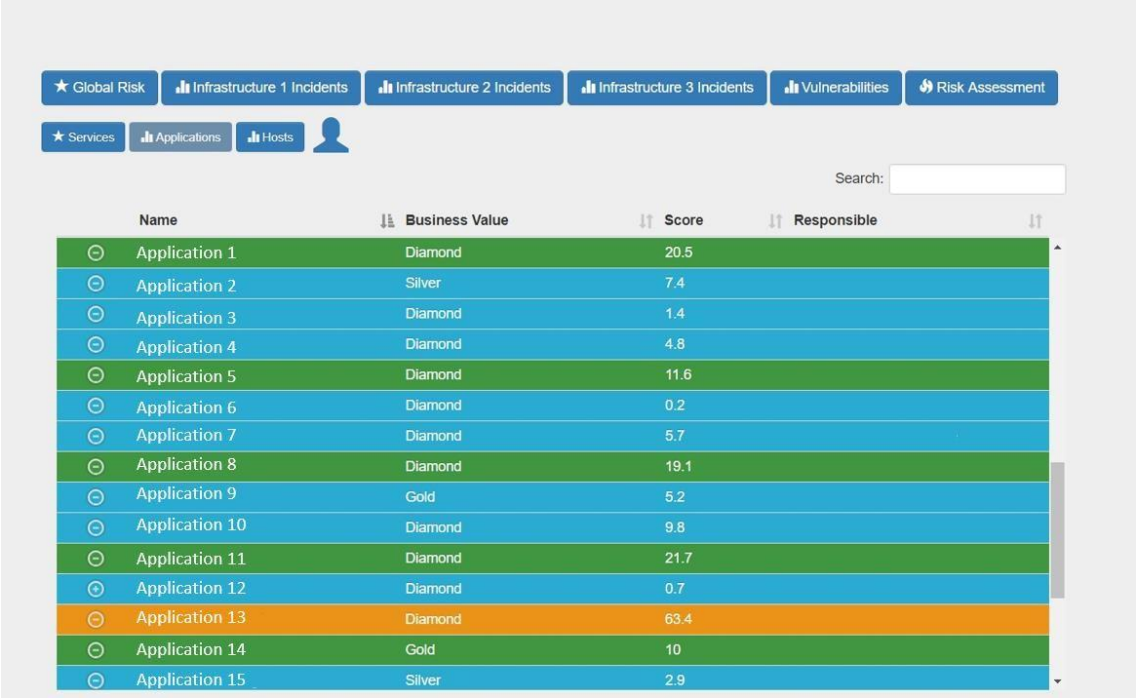

Figure 0.1 – Applications page

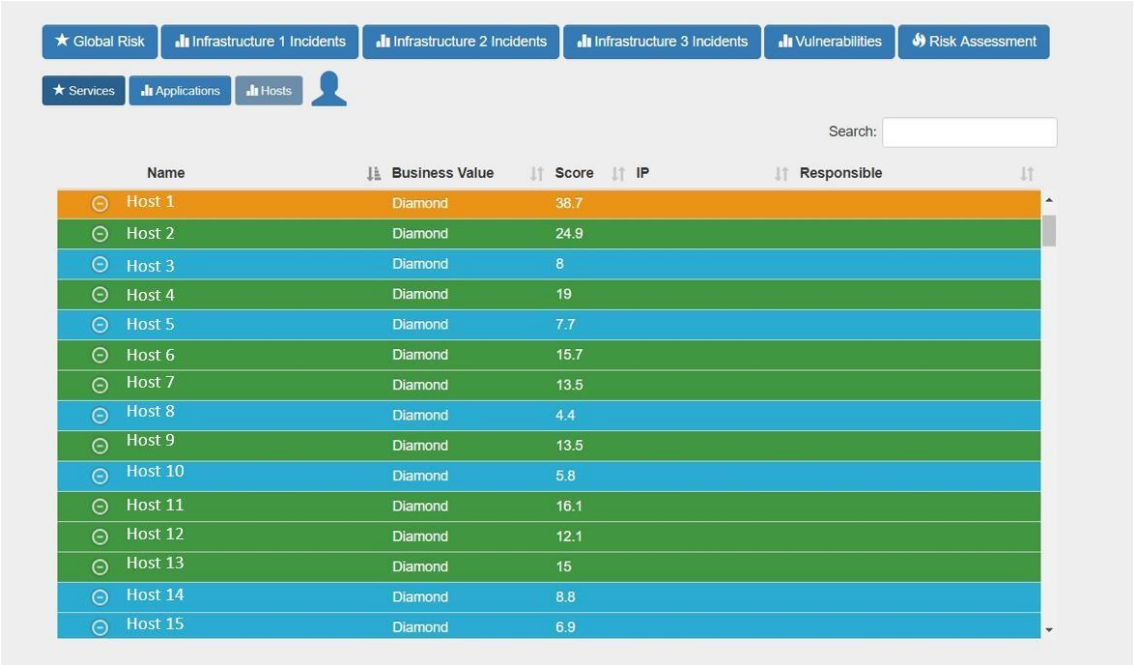

Figure 0.2 – Hosts page

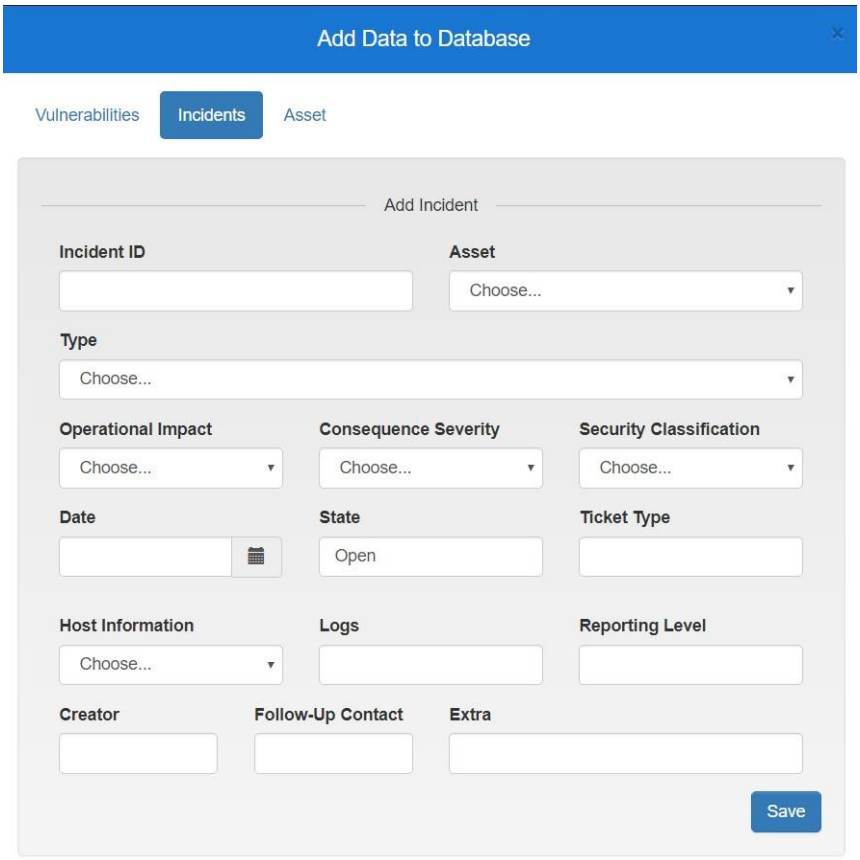

Figure 0.3 - Page to add an incident

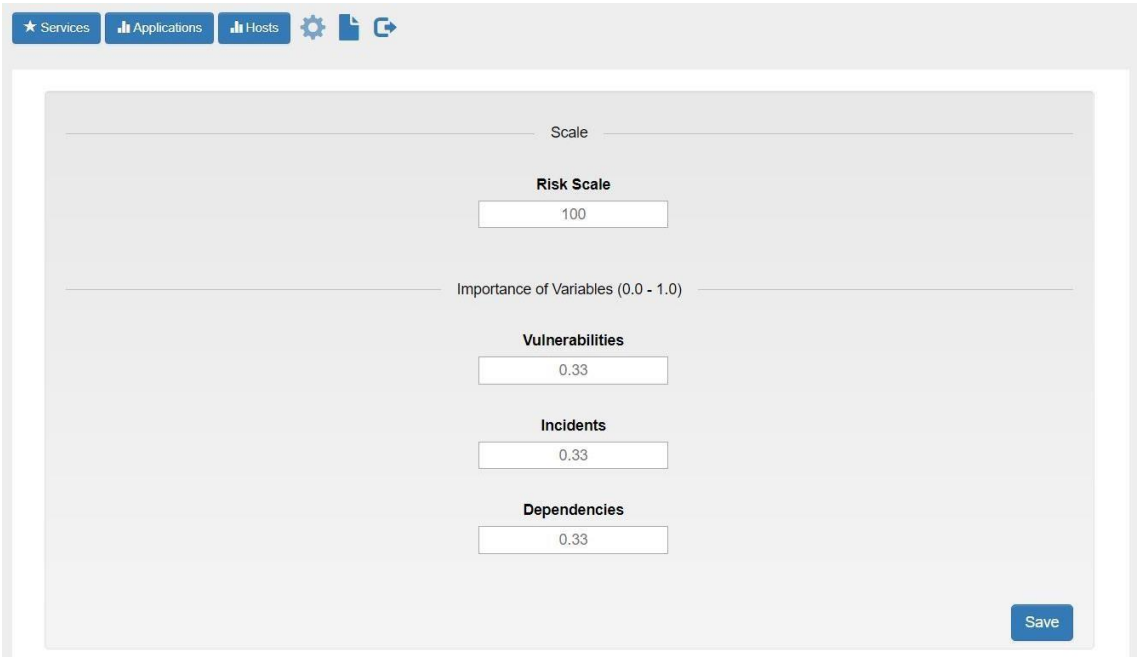

Figure 0.4 – Parameters page

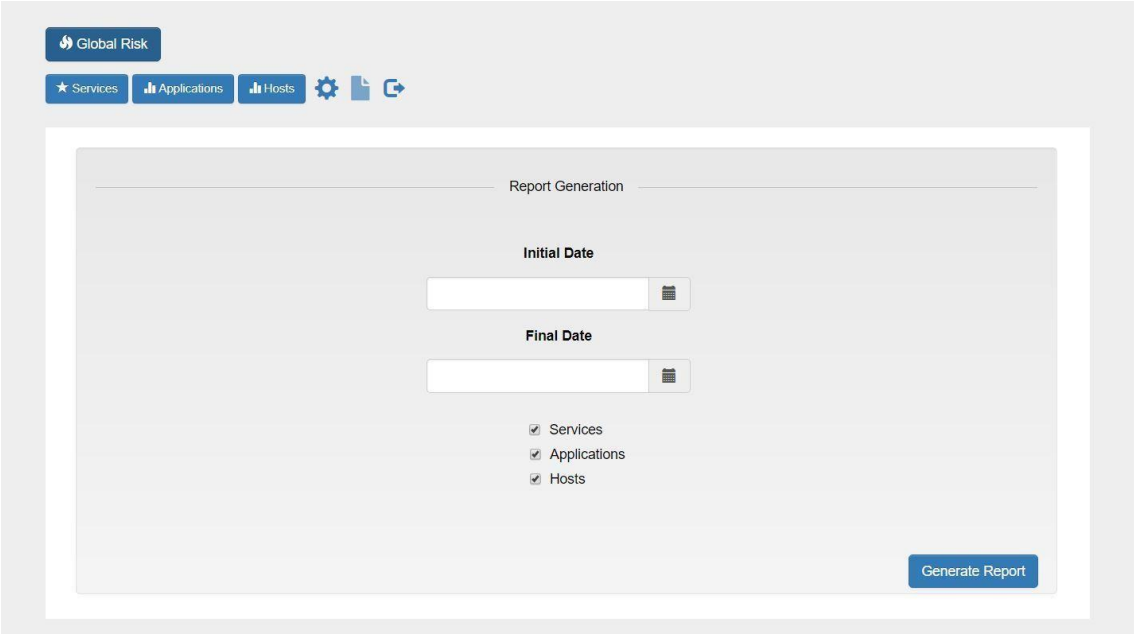

Figure 0.5 – Report generation page

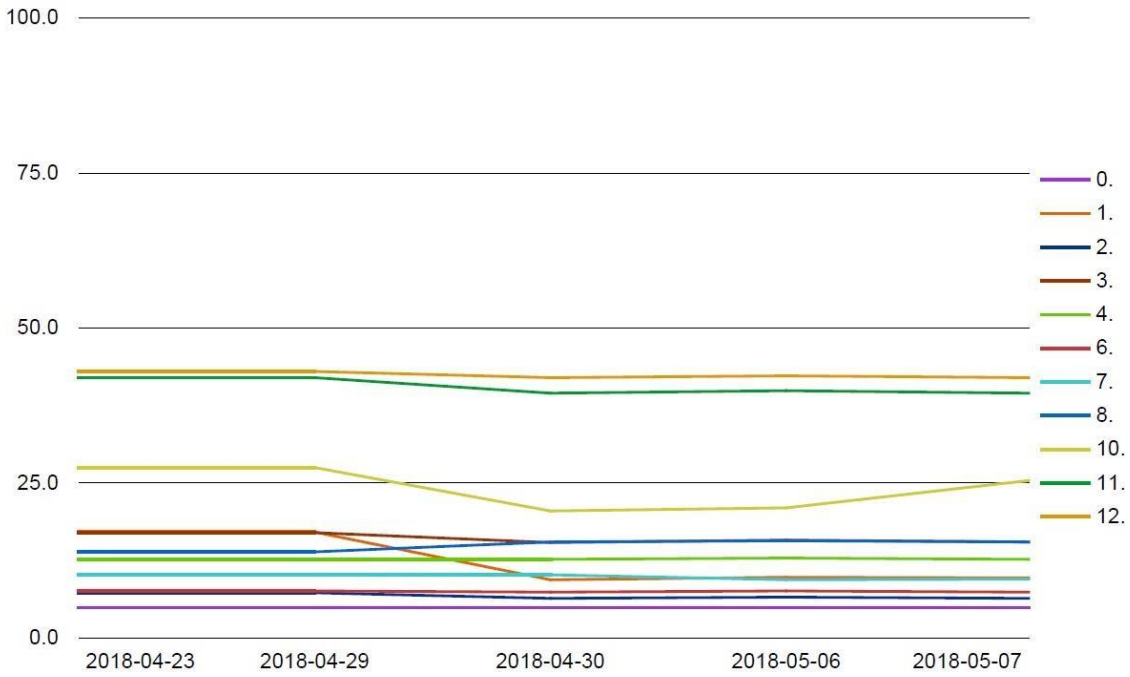

Figure 0.6 – Report result

Figure 0.7 – Graph in a report example for services risk score