2013-09

Employing replay connectors for SIEM operator education

Wong, Wai Keat

Monterey, California: Naval Postgraduate School

http://hdl.handle.net/10945/37745

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EMPLOYING REPLAY CONNECTORS FOR SIEM OPERATOR EDUCATION

by

Wong Wai Keat

September 2013

Thesis Co-Advisors: John D. Fulp
John Krautheim

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
September 2013

3. REPORT TYPE AND DATES COVERED
Master's Thesis

4. TITLE AND SUBTITLE
EMPLOYING REPLAY CONNECTORS FOR SIEM OPERATOR EDUCATION

5. FUNDING NUMBERS

6. AUTHOR(S) Wong Wai Keat

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Security Information and Event Management (SIEM) solutions are a critical information systems security control for monitoring, assessing, and reacting to cyber threats in near real-time. A given SIEM solution, however, is not a simple plug-and-play, drop-in, security device. On the contrary, a successful implementation requires configuration tailored to the specifics of a target network, as well as operators who are very knowledgeable of both the SIEM's functionality and the characteristics of network/data-center events.

This thesis will lay the framework for SIEM operator education via use of pre-captured network/data-center events (i.e., network traffic and device log information). The desired outcome is a repeatable framework that can be utilized by organizations interested in deploying more technically savvy SIEM operators. The framework will be empirically demonstrated with a SIEM learning lab developed for HP's ArcSight SIEM.

14. SUBJECT TERMS
Security Information and Event Management, SIEM, Correlation, Rule, Filter, Aggregate

15. NUMBER OF PAGES
107

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

19. SECURITY CLASSIFICATION OF ABSTRACT
Unclassified

20. LIMITATION OF ABSTRACT
UU

THIS PAGE INTENTIONALLY LEFT BLANK

EMPLOYING REPLAY CONNECTORS FOR SIEM OPERATOR EDUCATION

Wong Wai Keat
Captain, Singapore Armed Forces
B.Eng., Nanyang Technological University, 2003

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
September 2013

Author: Wong Wai Keat

Approved by: John D. Fulp
Co-Advisor

John Krautheim
Co-Advisor

Peter J. Denning
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Security Information and Event Management (SIEM) solutions are a critical information systems security control for monitoring, assessing, and reacting to cyber threats in near real-time. A given SIEM solution, however, is not a simple plug-and-play, drop-in, security device. On the contrary, a successful implementation requires configuration tailored to the specifics of a target network, as well as operators who are very knowledgeable of both the SIEM's functionality and the characteristics of network/data-center events.

This thesis will lay the framework for SIEM operator education via use of pre-captured network/data-center events (i.e., network traffic and device log information). The desired outcome is a repeatable framework that can be utilized by organizations interested in deploying more technically savvy SIEM operators. The framework will be empirically demonstrated with a SIEM learning lab developed for HP's ArcSight SIEM.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CORR	Correlation Optimized Retention and Retrieval
CII	Critical Information Infrastructure
GLBA	Gramm-Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
PCI	Payment Card Industry
RDBMS	Relational Database Management System
ROI	Return of Investment
SEM	Security Event Management
SIEM	Security Information & Event Management
SIM	Security Information Management

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

During the development of this thesis, many individuals have provided me with great assistance and support. As such, I would like to take this opportunity to extend my heartfelt gratitude to them.

Firstly, I would like to thank my wife for giving her everything to support my decision in pursuing this master's degree program. Her unwavering love and care has been my emotional pillar throughout the period of writing this thesis. I truly appreciate her and my son's companion.

Secondly, I would like to offer my sincere gratitude to both my advisors, J.D. Fulp and Dr. John Krautheim. I thank them for their patience, guidance and time spent on advising me in this thesis write-up.

Lastly, I would like to thank my employer, the Singapore Armed Forces (SAF), for providing me with the chance to further my studies and broaden my horizons.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. THESIS STATEMENT

The purpose of this thesis is to develop a repeatable Security Information & Event Management (SIEM) educational framework that can be used to train and educate SIEM operators effectively. The framework will be empirically demonstrated with a scenario-based training lab that analyzes pre-captured replay events (e.g., network traffic and device log information) using HP ArcSight Enterprise Security Management (ESM) [1].[1] Through the lab sessions, operators will explore and understand the various functional components and operational processes of ArcSight, and work to develop a more optimal SIEM configuration solution for the target scenario represented by its pre-captured replay events.

To achieve the primary thesis objective, the research needs to answer the following questions:

1. What are the important learning elements that must be encapsulated within the SIEM educational framework so as to provide a cyber-forensic methodology for a SIEM operator?
2. What information within the pre-captured replay events is required for informative forensic analysis?
3. How does the correlation engine within ArcSight ESM perform to identify the threat relationships between events?
4. What is a more optimal SIEM configuration (e.g., rule filters and asset characterizations) that will result in the highest likelihood of threat detection?
5. How can the SIEM solution be generalized into an instructional methodology that can be demonstrated in a SIEM learning lab?

[1] ArcSight ESM is a comprehensive SIEM software solution that combines traditional security event monitoring with network intelligence, context correlation, anomaly detection, historical analysis tools and automated remediation.

B. THESIS SCOPE AND ORGANIZATION

This thesis will focus on three main areas:

1. Review Research on Currently Deployed SIEM solutions

The first phase will explain the role that SIEM solutions play in the overall, defense-in-depth, security posture of a well-defended data center. A short overview of worldwide deployment will provide some motivation regarding the growing adoption of these types of security controls for providing cyber situational awareness in data centers. In particular, we examine the significance of SIEM solutions in environments where the volume of events exceeds the ability of personnel to monitor or analyze these events manually.

2. Analysis of the Functional Components within ArcSight

The next phase will focus on studying the entire security event life cycle that starts with event collection and continues through event correlation and storage. This will involve the analysis of the functionality of the core components and workflow structure within ArcSight to understand its operational processes and how they combine to bring a valued-added solution to detection analysis in a security operations center (SOC).

3. Development of Training Scenarios Based on Pre-captured Replay Events

Pre-captured replay events are essentially a set of logged records of historic cyber activities which (by design) represent both normal (i.e., benign) and malicious actions. In this phase, a cyber-forensic methodology will be designed and incorporated within the training lab to edify SIEM operators regarding how configuration changes to a SIEM’s various settings result in a higher signal-to-noise ratio (S/N) regarding the identification of malicious events among the background noise of “normal” events.

This thesis consists of six chapters:

- The thesis objective and the procedural approach used in achieving the objective are described in Chapter I.
- The purpose of this thesis as it presents the impact of cyber-attacks, as well as the complexities and challenges in implementing a SIEM solution are highlighted in Chapter II. Also included in this chapter is an explanation of the need to derive an effective training methodology for SIEM operators. The fundamental principles of SIEM operation and its evolution are also examined.
- The system anatomy of ArcSight is described in Chapter III along with an overview of the functionalities of its core components. This will allow readers to understand the operational processes within ArcSight which serve to automate the detection, and optionally the reaction, to malicious actions taken against a data center.
- The strategy for deriving the SIEM training methodology and educational framework is discussed in Chapter IV. The tools, learning goals and method used in developing a scenario are also presented.
- The learning scenario is described in Chapter V by analyzing the replay events and subsequently deriving a more optimal SIEM solution. It includes a scenario brief to SIEM operators and expected results.
- A summary of the research is included in Chapter VI along with recommendations for future work

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

A. IMPACT OF CYBER-ATTACKS

In a network-centric modern society, the increasing operational “footprint” of computer-based systems, along with the rewards for subverting/exploiting the information they process, store, or transport, leads to a rising occurrence of cyber-attacks. Communication across vast distances is now quicker and easier with the advancement in mobile computing devices and more ubiquitous connectivity and bandwidth. As a result, more people and business organizations are connected virtually, which in turn increases the amount of sensitive and private information flowing in the virtual space. Based on statistical results from the Internet World Stats [1], a 566.4% growth in the number of Internet users around the world from 2000 to 2012 has been recorded. This explosive growth clearly indicates the pervasiveness of the Internet. In addition, the ever-growing reliance on Internet technology as the primary medium for our daily services (e.g., business operations, information sources, etc.), has further extended the damage that can be incurred by an individual or organization due to cyber-attacks. In an article compiled by Business Roundtable,[2] named “Growing Business Dependence on the Internet” [2], the economic consequences and adverse impact on the companies was highlighted, as they depend more on the Internet to help them conduct worldwide business operations. Within the article, the following is quoted:

> According to the World Economic Forum, a breakdown of the Critical Information Infrastructure (CII) is one of the core risks facing the international economy. The World Economic Forum estimates that there is a 10 to 20 percent probability of a CII breakdown in the next 10 years (Figure 1.), one of the highest likelihood estimates of the 23 global risks it examined in a recent report. The report estimates the global economic cost of the incident at approximately $250 billion, or more costly than two-thirds of the [all others included in the report] risks. [2]

[2] Business Roundtable (BRT) is an association of chief executive officers of leading U.S. companies with more than $7.3 trillion in annual revenues and nearly 16 million employees

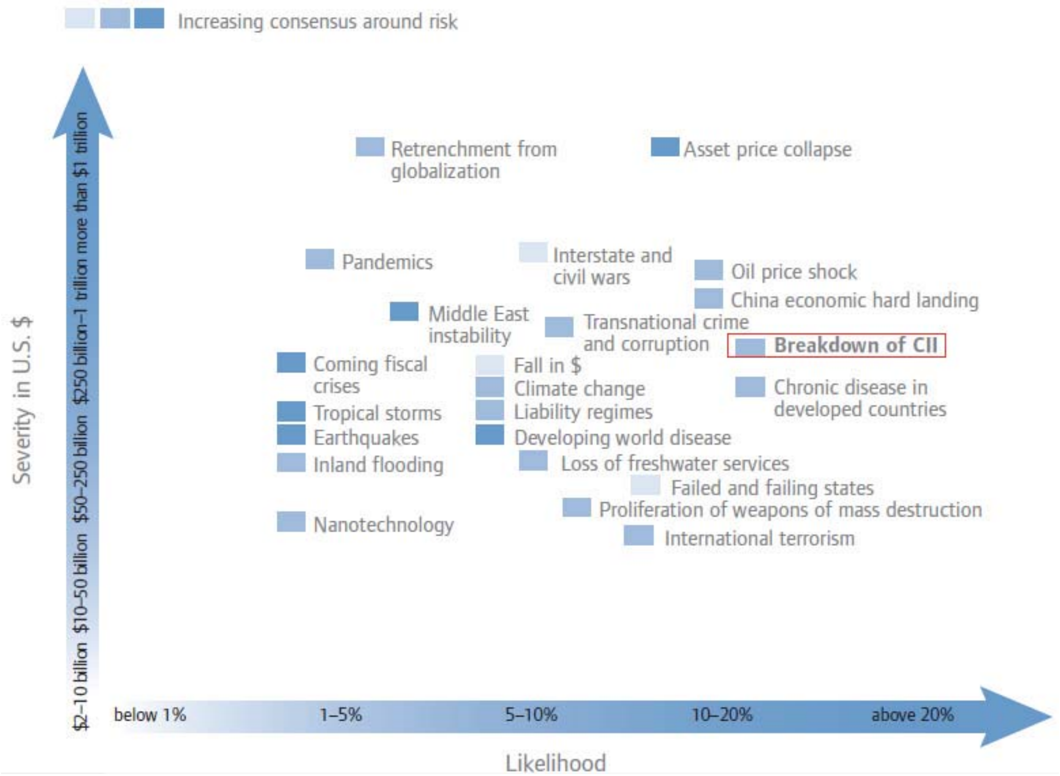


Figure 1. 23 Core global risks: Likelihood with severity by economic loss. From [2].

Based on the World Economic Forum’s estimate, it can be seen that the global economy relies heavily on CII, which is essentially the Internet. While natural disasters are also mentioned as a potential threat to the Internet, the article gave greater emphasis to cyber-attacks and highlighted them as the main threat behind various crisis scenarios. This emphasis is understandable given the increasing amount of cyber-attacks faced by many business organizations on a daily basis.

In the military domain, cyber-attacks have been treated with a more serious tone, being labeled as “cyber-warfare” or “cyber-terrorism.” Both terms explicitly describe the severe impact on the national security such attacks would have if they were to succeed. Many military intelligence agencies around the world have compared conventional warfare with cyber-warfare, revealing that the latter can inflict worse damage with much less effort. This is due in part to the increase in online (i.e., remote via the CII) control of critical national infrastructures such as power stations, transportation systems and oil refineries. Crippling such key installations can generate cascading effects that will not only disrupt daily activities, but also create mass damage that may result in catastrophic loss of life and destruction of property.

B. COUNTERING CYBER-ATTACKS WITH SIEM

Over the past decade, the aforementioned threats have forced cyber defenders to continuously invent protection mechanisms to mitigate cyber-attacks. A SIEM product is one such mitigation solution. Simply stated, a SIEM product is an information system security control employed for monitoring, assessing and reacting to cyber-attacks in real-time, or at least much more quickly than if any of the entailed processes were done manually.

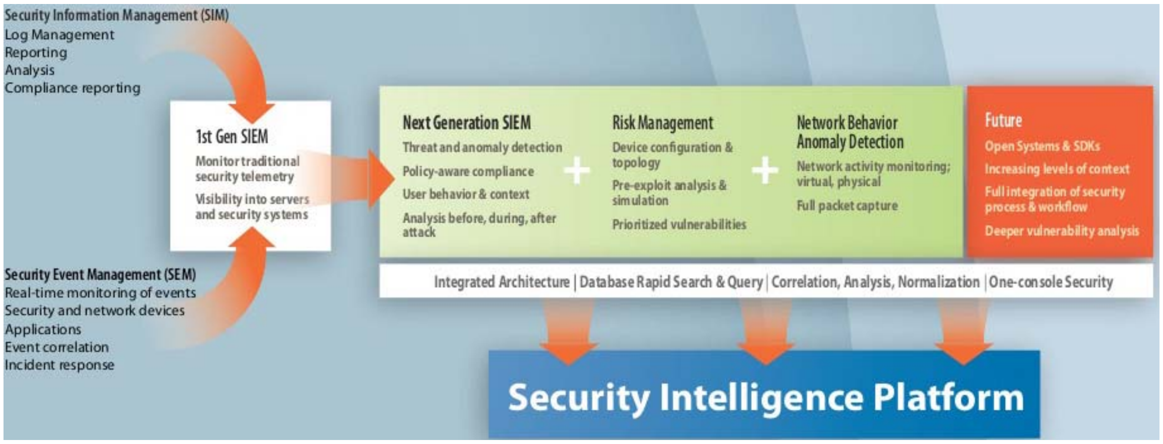

Security Information Management (SIM)
Log Management
Reporting
Analysis
Compliance reporting
1st Gen SIEM
Monitor traditional security telemetry
Visibility into servers and security systems
Security Event Management (SEM)
Real-time monitoring of events
Security and network devices
Applications
Event correlation
Incident response
Next Generation SIEM
Threat and anomaly detection
Policy-aware compliance
User behavior & context
Analysis before, during, after attack
Risk Management
Device configuration & topology
Pre-exploit analysis & simulation
Prioritized vulnerabilities
Network Behavior Anomaly Detection
Network activity monitoring; virtual, physical
Full packet capture
Future
Open Systems & SDKs
Increasing levels of context
Full integration of security process & workflow
Deeper vulnerability analysis
Integrated Architecture | Database Rapid Search & Query | Correlation, Analysis, Normalization | One-console Security
Security Intelligence Platform

Figure 2. Modern evolution of SIEM. From [3].

The current state of SIEM products has evolved from two formerly disparate product categories: SIM (Security Information Management) and SEM (Security Event Management) (Figure 2.). While SIM products were used primarily to gather and create reports from security logs, SEM products utilized event correlation and alerting functions to help with analysis and incident response. On the surface, both product classes possessed fundamental differences in their capabilities to manage a torrent of system events and enforce the desired security observations. However, in-depth analysis reveals various commonalities between these product classes, such as their workflow and reporting processes. Each product class provided security features that can be complemented by the other to provide a more holistic approach in countering cyber-attacks. As such, their functions were combined and integrated into a single security management system, known as a SIEM.

Most SIEM products work by deploying multiple collection agents and connecting them with end-users' devices, such as servers and firewalls, so as to gather many diverse security-related events. The collectors then normalize the events to a standard format before forwarding them to a centralized management console, which performs inspection and flags identified anomalies. By anomalies here, we mean any events that solely or in toto represent either a realized or pending threat to the protected system (network, data-center, etc.). The process of identifying anomalies is usually handled by either a rule-based or statistical correlation engine which establishes relationships between the event logs, infers the significance of those relationships and prioritizes them. Once flagged, the events will be monitored and inspected further to determine any potential or realized damage. Optionally, automated actions can be tied to such malicious event detections, thus providing not only *detection* capabilities but *reaction* capabilities as well.

C. COMPLEXITIES AND CHALLENGES IN IMPLEMENTING SIEM

The underlying principle of a SIEM product is that relevant system data about an organization's security is generated in multiple locations and collated into a single point of view, which makes it easier to spot the trends and patterns of a cyber-attack. This is supposed to make analysis and response easier for the security professionals. However, a SIEM product is not a simple plug-and-play, drop-in, security device. Based on a recent survey conducted by elQnetworks, a pioneer in simplified security, risk and compliance solutions; it was revealed that organizations are having difficulties with SIEM deployments [4].

The first challenge identified was the long deployment time required. The survey quoted 44% of the respondents reporting that it took a few weeks to more than a month to deploy their latest SIEM product. This reflects that the products require fine-tuning over time to get real security value (ROI) and can take months to obtain useful data.

The second challenge was attributed to the lack of trained personnel. It was found that the complexities involved in correlating security and configuration data across IT assets and deriving an adequate set of security controls could prove to be too technically complex for the typical IT operator. A successful implementation requires configuration tailored to the specifics of the target network, as well as operators who possess deep knowledge on both the SIEM's functionality and the characteristics of network events. This is a very broad domain of knowledge encompassing; among other things, operating systems, applications, log formatting, flows, authentication, protocol, and TCP/IP stack understanding.

The last challenge was associated with compliance issues. 35% of the respondents stated that compliance requirements were the primary driver behind the use of SIEM. Rather than focusing on the security deliverables offered by the SIEM product, some organizations are employing them only to satisfy compliance and regulatory requirements (e.g., PCI, HIPAA, and GLBA). As such, many SIEM products were reduced in functionality to being mere electronic organizers.

From the challenges and complexities stated, it is clear that the capabilities of many SIEM deployments have been marginalized and their full potential in providing a more secure cyber environment has yet to be realized. These are risk factors for organizations which have invested large amounts of money in SIEM products, only to receive sub-optimal protection returns on this investment. When configured, deployed, or operated incorrectly, SIEM products may even be counter-productive by introducing added complexity, confusion, and service disruption.

D. FRAMEWORK FOR SIEM OPERATOR EDUCATION

In truth, SIEM products remain a state-of-the-art technology that requires specialized and trained personnel to set up, configure and manage them. When an untrained IT operator is first tasked to utilize a SIEM product, he/she will likely be overwhelmed by the multitude of configurations, user-interfaces and processes he/she must understand prior to successful operation of the product. With lack of a systematic approach and detailed understanding of the workflow processes used by the core functionalities in a SIEM product, the IT operator will be set back for many weeks in his/her effort to implement the desired protection. To ensure that IT operators possess adequate knowledge and attain the required operational capability within a short time frame, it is important to derive an educational framework that can be used in a repeatable manner. This will provide the training foundation needed to increase the technical level of all operators in utilizing the SIEM product effectively to mitigate cyber-attacks.

III. ARCSIGHT ESM ANATOMY

In this chapter, the important learning elements required in implementing the ArcSight ESM are explained. Also highlighted are the various functional processes within a typical SIEM product.

Prior to utilizing ArcSight ESM, it is crucial to first identify and understand the functionalities of the various software/hardware components within the SIEM framework (Figure 3). These are the tools that are responsible for providing the cyber-forensic capabilities that will be used by SIEM operators to collect, analyze and detect the malicious events. They range from source devices (e.g., servers) that instantiate the events to ArcSight core components. The workflow structure throughout the ESM will then be explained to further enhance the reader's understanding of the operational processes required throughout the event life cycle.

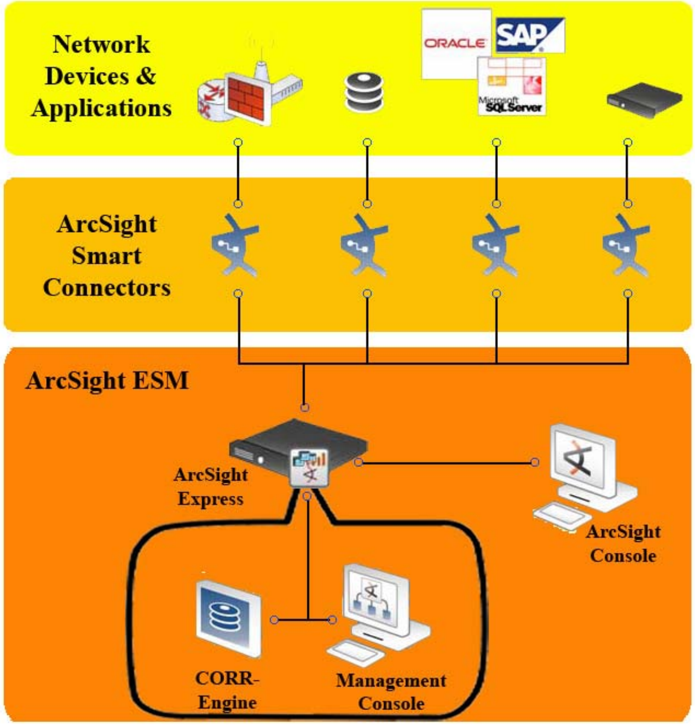


Figure 3. ArcSight ESM's connectivity diagram. After [5].

A. COMPONENT FUNCTIONALITIES

1. Network Devices and Applications

A network device is the source of events. It is a network node that has a physical processing location with a unique network address (e.g., IP address, MAC address) and possesses the capability to recognize, process and transmit to other nodes. The events output from the network device will be fed into the ArcSight SmartConnectors to generate correlation-relevant data on the network. The various types of network devices that are supported by ArcSight ESM are shown in Figure 4.

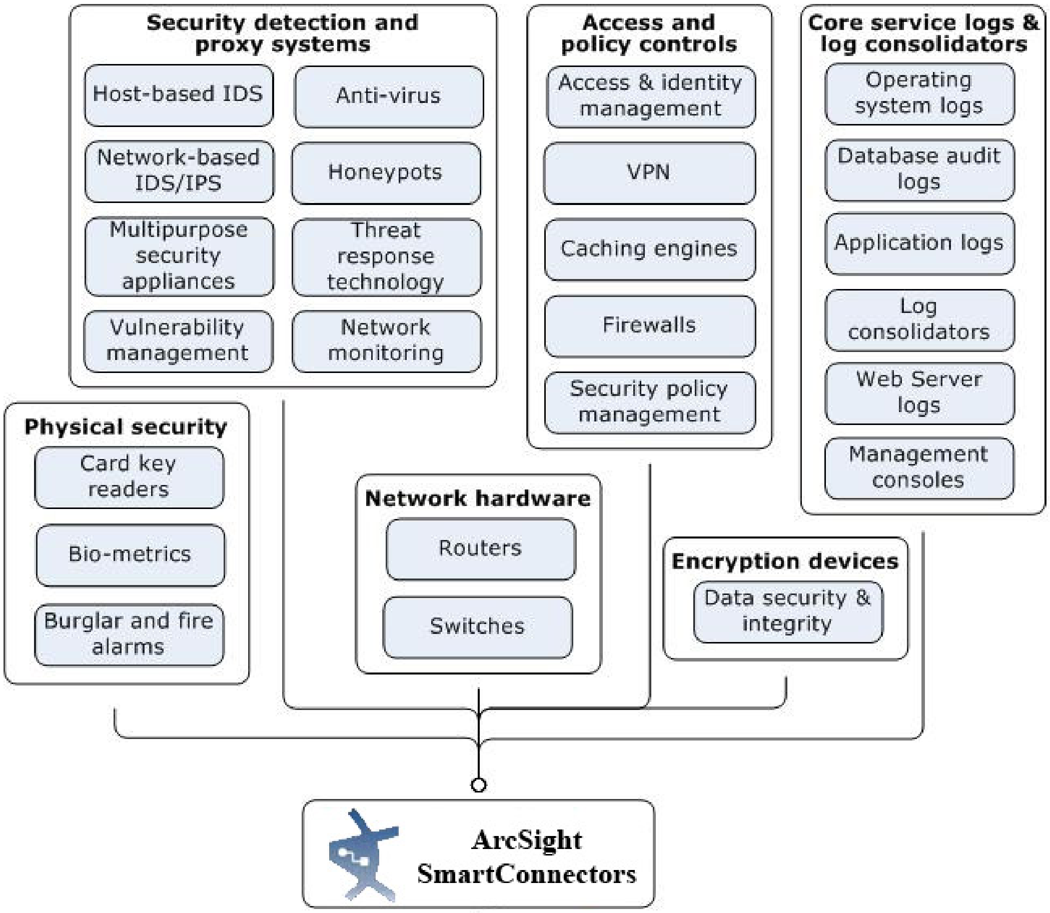


Figure 4. Network devices Supported by ArcSight ESM. From [5].

2. ArcSight SmartConnectors

SmartConnectors provide the interface between the network devices and the ArcSight Express. As different devices have varying logging formats and reporting mechanisms, it is difficult to extract information for querying without first normalizing the events. Henceforth, SmartConnectors are responsible for translating a multitude of device outputs into a normalized schema that becomes the starting point for the correlation process done by the ArcSight Express. After collecting the event data from the network devices, the SmartConnectors will normalize the data values and structures to a common schema. This will then allow SmartConnectors to filter events and reduce the volume of events sent to the ArcSight Express, which in turn increases its efficiency and accuracy while reducing event processing time.

3. ArcSight Express

ArcSight Express is the heart of the ESM framework. Commonly known as the Manager, it is a licensed hardware appliance that drives analysis, workflow and other security services. It writes events to the Correlation Optimized Retention and Retrieval Engine (CORR-Engine) as they stream into the system and simultaneously processes them through the correlation engine, which evaluates each event with network model and vulnerability information to develop real-time threat summaries. ArcSight Express is installed with a Management Console to provide the administrator interface for managing user accounts and events storage.

a. CORR-Engine Storage

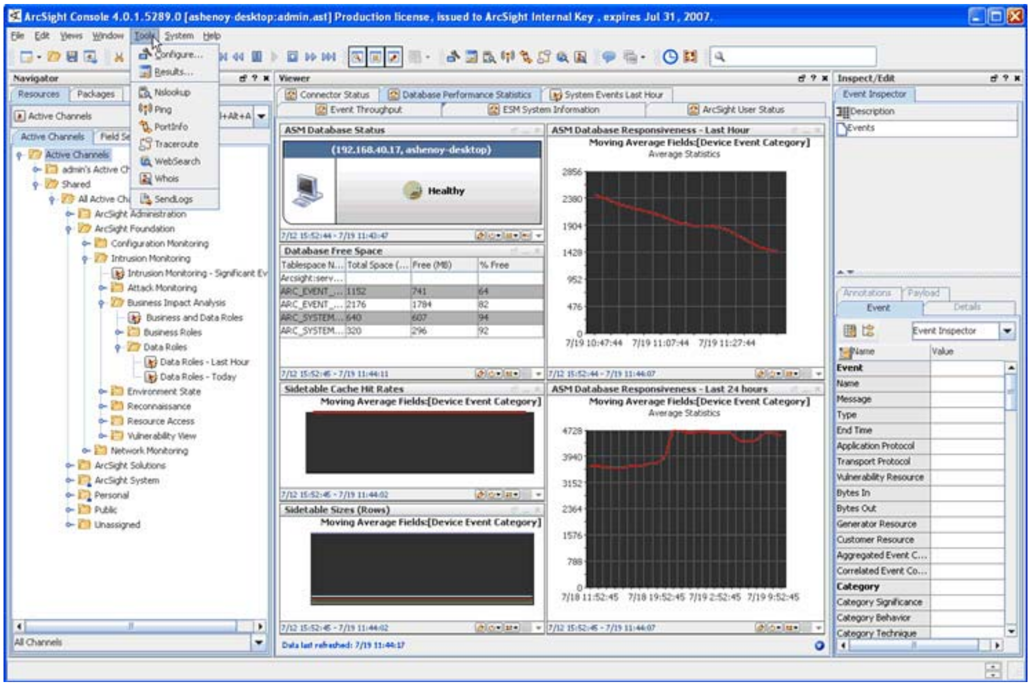
The CORR-Engine is a proprietary data storage and retrieval framework that receives and processes events at high rates and performs high-speed searches. Unlike traditional Relational Database Management System (RDBMS)-based storage that inhibits high-speed correlation [6], the CORR-Engine is able to access the vast amount of stored events at a greater speed, therefore allowing the correlation engine to process logged events at much higher rates for threat detection and security analysis.

b. Management Console

The Management Console is essentially an embedded web application that resides within the ArcSight Express to provide a streamlined interface for managing user accounts, monitoring events, configuring storage, updating licenses and managing component authentication (e.g., SmartConnectors' connection).

4. ArcSight Console

Unlike the Management Console that is used primarily for registration of users and connecting components, the ArcSight Console (Figure 5) is the main authoring tool for building filters, rules and security reports. It is a separate workstation that hosts an application interface intended for use by SIEM operators to build complex correlation rules within the correlation engine, as well as to perform routine administrative functions. In addition, the console also provides various graphical means (e.g., dashboards and line graphs) to present correlated events. Better visual representations of network status improve the situational awareness of the SIEM operator.



ArcSight Console 4.0.1.5289.0 [ashenoy-desktop:admin.ast] Production license, issued to ArcSight Internal Key , expires Jul 31, 2007.

Database Free Space

Tablespace N...	Total Space (...	Free (MB)	% Free
Arcsight:serv...			
ARC_EVENT_...	1152	741	64
ARC_EVENT_...	2176	1784	82
ARC_SYSTEM...	640	607	94
ARC_SYSTEM...	320	296	92

Data last refreshed: 7/19 11:44:17

Figure 5. ArcSight Console Interface. After [5].

B. WORKFLOW STRUCTURE

A well-defined workflow structure allows SIEM operators to understand the procedural approach in implementing ArcSight ESM. In addition, it also provides insight on the operational processes that will occur at each step. ArcSight ESM processes events in phases to identify and, optionally, act upon events of interest. An overview of the major steps in this event workflow is shown in Figure 6.

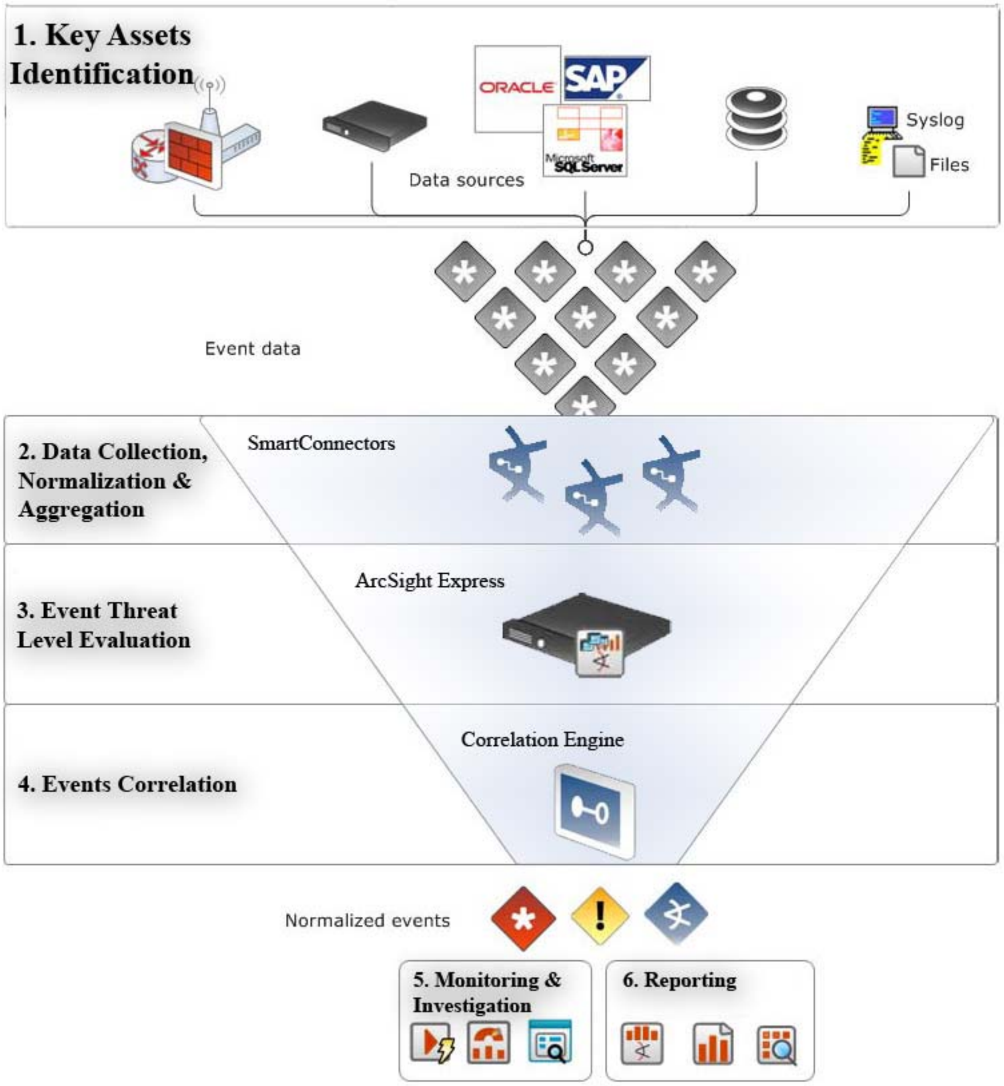


Figure 6. Life Cycle of ArcSight ESM. After [5].

1. Phase 1 – Key Assets Identification

Identifying key assets within a network is the first major step required in the SIEM life cycle, as it will determine and directly influence the threat evaluation process associated with them. When an operator is required to set up the ArcSight ESM, he/she must clearly understand the network topology and distinguish the importance of the various subnets, network devices and end-points (e.g., workstations and servers). Those that are classified as sensitive shall then be identified as key assets and thus given greater emphasis during the processes of *Asset* and *Network Modeling*. Both processes are essential functional steps for ArcSight ESM to become "familiar" with the network environment that it is protecting and perform more informed, meaningful, event threat evaluation in a later phase.

a. Asset Modeling

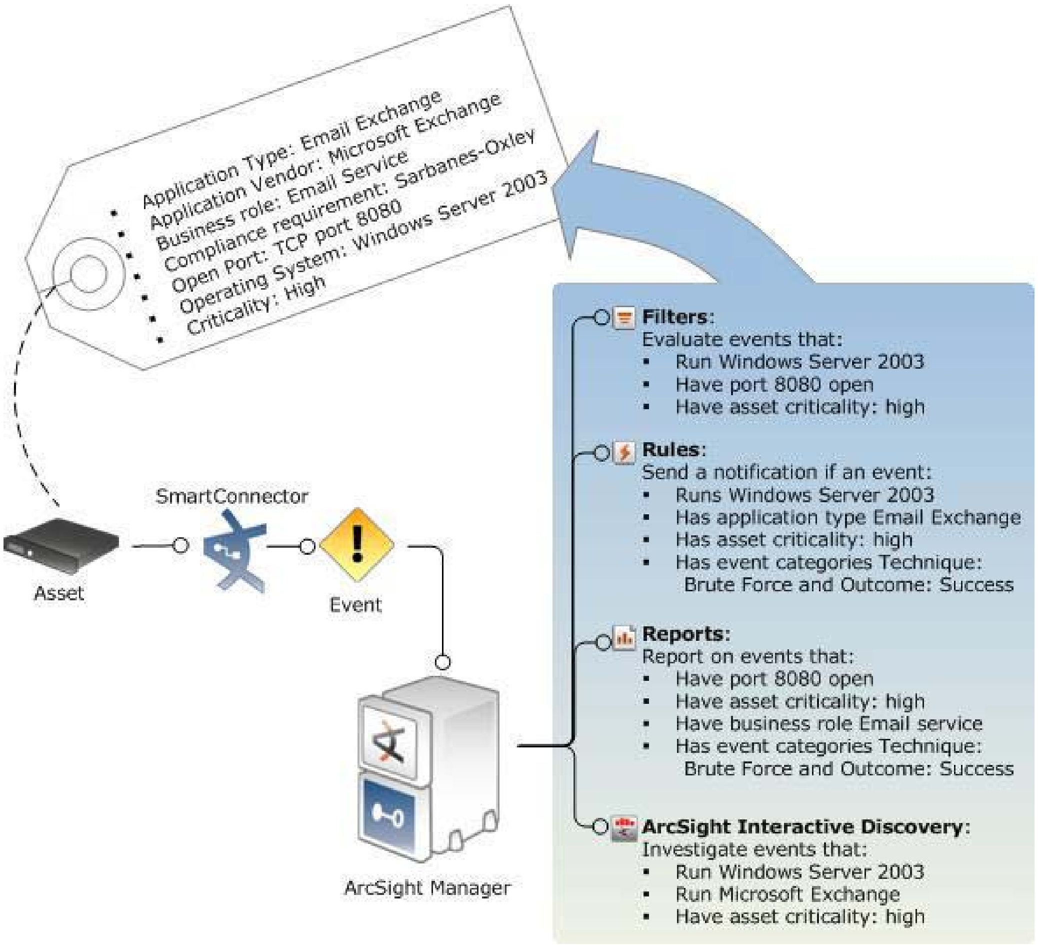
Modeling assets is a multi-step process that requires a SIEM operator to consider what types of information to track from various assets in the network and how those assets interrelate. The distinctions drawn in this process become factors for the filters, rules, data monitors and reports that will be used to correlate events generated.

In network architecture, an asset is any endpoint that is considered significant enough to be characterized with details that will make correlation and reporting more meaningful. The significance can be determined by the criticality of the information that is stored in the asset. They include servers and laptops. The following information is required to establish a unique identity of the asset that will be recognized by the ESM:

- Asset name (a name used to refer to the asset within ESM)
- Network IP address
- MAC address
- Full qualified domain name

Knowing the identity of an asset is not enough for ESM to perform evaluation on the events generated. To evaluate the threats or behaviors associated with the asset, it is crucial to include more information pertaining to each asset's configuration (Figure 7), particularly the following:

- Vulnerabilities – A vulnerability description is used to define the potential exploitation that exists in any hardware, firmware or software state. If an asset meets all of the requirements described in the vulnerability description, an event will be generated by ESM for subsequent evaluation.
- Open ports
- Operating system
- Key applications installed
- Roles of the asset within the enterprise



Application Type: Email Exchange
Application Vendor: Microsoft Exchange
Business role: Email Service
Compliance requirement: Sarbanes-Oxley
Open Port: TCP port 8080
Operating System: Windows Server 2003
Criticality: High
Asset
SmartConnector
Event
ArcSight Manager
Filters:
Evaluate events that:
Run Windows Server 2003
Have port 8080 open
Have asset criticality: high
Rules:
Send a notification if an event:
Runs Windows Server 2003
Has application type Email Exchange
Has asset criticality: high
Has event categories Technique: Brute Force and Outcome: Success
Reports:
Report on events that:
Have port 8080 open
Have asset criticality: high
Have business role Email service
Has event categories Technique: Brute Force and Outcome: Success
ArcSight Interactive Discovery:
Investigate events that:
Run Windows Server 2003
Run Microsoft Exchange
Have asset criticality: high

Figure 7. Asset attributes example. After [5].

b. Network Modeling

Network modeling is done to keep track of the asset traffic on the network that is being monitored. In this process, the physical network architecture is mapped and segregated into various functional zones. Every network device in the network is considered a separate asset. Examples of network-visible interfaces include routers, web servers or anything with an IP or MAC address.

A zone represents part of the network and is identified by a contiguous block of IP addresses. It usually represents a functional group within the network or a subnet, such as a wireless LAN, VPN or DMZ. Zones are also how ESM resolves private networks whose IP ranges may overlap with other existing IP ranges. SmartConnectors tag incoming events with zones. When the SmartConnector processes an event, it evaluates each of the IP addresses involved in the event and tries to locate the zone associated with that IP address among an ordered list of networks. Through this process, SIEM operators are be able to differentiate the events collected from the various assets in different zones.

2. Phase 2 – Data Collection, Normalization and Aggregation

The SmartConnector is the interface through which events arrive in ESM from devices. It performs the first layer of event tagging by applying normalization, filtering and event aggregation to reduce the volume of the event stream to make event processing faster and more efficient (Figure 8).

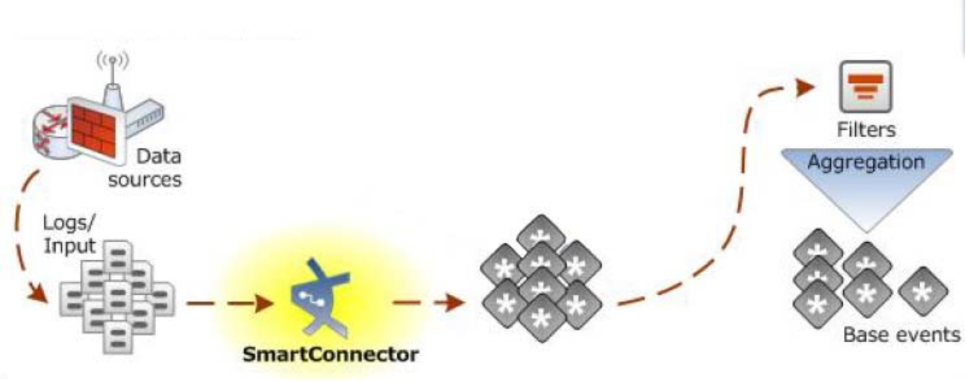


Figure 8. Data Collection, Normalization and Aggregation Process. After [5].

a. Data Collection

Once the key assets have been identified, the next process is to gather information from these assets. The data collected are essentially log data, where each log entry is translated into one event as interpreted by the SmartConnector.

b. Normalization

Normalization is the process of taking events from disparate devices that are presented in multiple formats and recasting them into a common schema (syntax and semantics). Because networks are heterogeneous environments, different devices will likely have dissimilar, vendor-specific, logging formats. This lack of standardization hinders event correlation, which requires that "apples be compared to apples." As such, the SmartConnector is responsible for normalizing the events gathered, into a conforming event schema. This is achieved through a parser which populates the native form values from the original event generator into the corresponding field in the normalized schema and reformats as may be necessary (e.g., *MMDDYY* date format may be recast into *DD-Month-YYYY* format). Once normalized, the raw (native form) event is now referred to as a *base* event.[3] A database, specifically the CORR-database, populated with these standardized base events allows for consistent reporting and forensic analysis to be performed on every event regardless of its original data source or format.

Other than inheriting the original values from the source device, the normalization process also converts certain values for the following event field:

- Event Severity – Some of the reporting devices to the SmartConnector offer initial threat evaluation that describes their interpretation of the danger posed by a particular event. For example, if a network IDS detects port scanning by a workstation with an external IP, the network IDS will flag this event as a high-priority exploit. To ArcSight ESM, this is known as *device severity*. Similar to the varying logging format, the scale of device severity also differs between security devices. For example, network Intrusion Detection System (IDS) A may use a security rating of 1–10 while network IDS B uses a scale of high, medium and low. In this case, the inherited device severity readings will be

[3] ArcSight refers to an event that has been processed by an ArcSight SmartConnector as a base event.

normalized by the ArcSight ESM into a single agent severity scale, called *agent severity*. Both *device severity* and *agent severity* are important data points that will be used to calculate the event's overall security priority.

- Timestamps – Another factor in normalization is to convert the varying timestamps to a common format. This is important for an enterprise network that stretches across continents with different time zones.

c. Aggregation

The purpose of aggregation is to streamline and group events with similar data information, thus reducing the volume of base events sent to the ArcSight ESM. It is common to see groups of events arriving at the SmartConnector with the same value in a specific set of fields. For example, a network device may submit multiple status log entries to the SmartConnector over a short period of time. In this case, the events will share the same source IP address and event name. SmartConnector aggregation will then merge these events with similar values into a single aggregated event that includes the earliest start time and latest end time. This will significantly reduce the computation burden on the ArcSight ESM, allowing processing to occur on smaller and more manageable data sets.

3. Phase 3 –Event Threat Level Evaluation

One of the main security functions of a SIEM product is to accurately identify a malicious event that is happening (or has happened) within the network to the SIEM operator so that security actions can be taken to counter or otherwise recover from the attack. This is only possible after the events have been evaluated to understand their potential threat to the network's overall security. Evaluated events will be categorized into different threat levels, where each level is associated with a series of security actions that can be invoked to reduce or eliminate the events' adverse impact.

In ArcSight ESM, once the base events have been processed to a common data set, a priority formula will then be used as the threat level metric to determine an event's relative importance to the network. This is an important function as it serves as an indicator to signal the SIEM operator on whether the evaluated event requires further investigation or action. A high priority factor generally means that an event is of high risk factor.

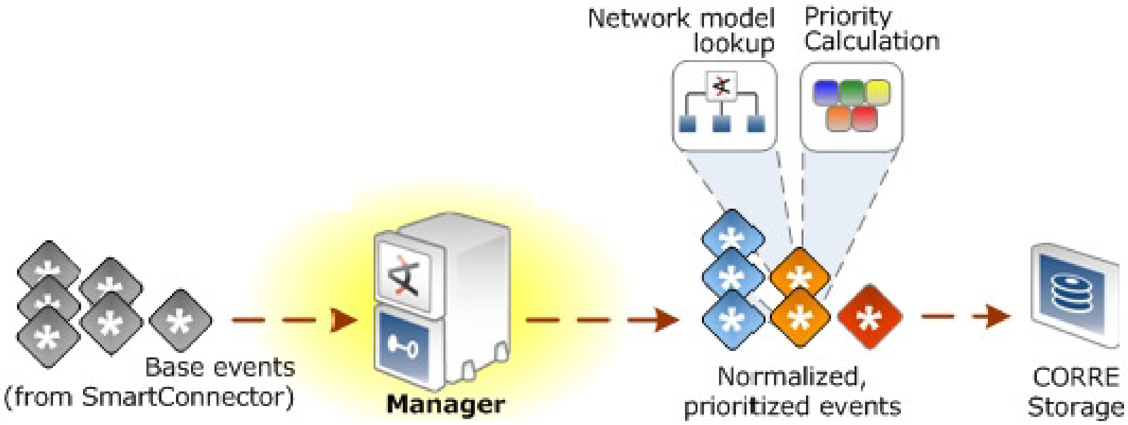

Network model lookup
Priority Calculation
Base events (from SmartConnector)
Manager
Normalized, prioritized events
CORRE Storage

Figure 9. Event Threat Level Evaluation. After [5].

The priority formula consists of four factors that combine with *agent severity* to generate an overall priority rating. Each of the criteria described in Table 1 contributes a numeric value to the priority formula, which are eventually averaged to provide the overall importance of an individual event.

S/N	PRIORITY FACTOR	DESCRIPTION
1	Model Confidence	Model confidence refers to whether or not the target asset has been modeled in ESM and to what degree. For assets that have not been modeled in ArcSight ESM, the associated event is regarded with lower model confidence, which in turn attributes to lower priority rating.
2	Relevance	As mentioned in Phase 1, attributing assets with additional configuration information allows in-depth threat evaluation to be performed. In this factor, relevance refers to the relevancy of an event to an asset and it looks at whether the event targets port and/or vulnerabilities of a particular modeled asset. If relevance is high, it means the target is vulnerable to the stated attack and/or the stated port is open.
3	Severity	Unlike *device* or *agent severity*, this parameter is used as a history function for the priority formula. It leverages on an ESM resource[4] called active list[5] to check on previous events on whether an associated asset has been listed as a target or attacker before. If the asset appears as an attacker in the active list, then severity will contribute to a higher priority rating.
4	Asset Criticality	This factor measures how important the target asset is in the context of the network when constructed during asset modeling. If an event reports on an asset which is categorized as higher criticality due to its access to confidential information, then this factor will reflect high priority rating.

Table 1. Factors contributing to Priority Formula. From [5].

The calculated priority is categorized into five different levels, namely *very low*, *low*, *medium*, *high* and *very high*. While the lowest level usually means a routine event that does not consist of threats, a high priority event may not necessarily mean a threat either. For example, if a critical asset fails due to internal hardware failure, the priority of events reporting it may be very high, but it does not represent a malicious attack. Therefore, it is always important for a SIEM operator to conduct further investigation

[4] ESM manages the logic used to process evens as objects called resources. A resource defines the properties, values and relationships to configure the functions ESM performs [5].

[5] Active Lists are used as like a bulletin board to specify fields of event data for correlation or monitoring purposes.

(e.g., a physical check on the reporting device) on events with high priority ratings so as to confirm the existence and characteristics of the threats. Once confirmed, a pre-determined series of security actions can then be carried out to mitigate the threats.

4. Phase 4 – Events Correlation

Events generated from multiple endpoints may contain a mixture of normal and malicious event information. While analyzing a single event in isolation is rarely enough to confirm its significance, the difficulty of event cross-referencing—correlation—increases with the volume of events. As such, automated event correlation becomes one of the most important value-added functions of a SIEM product. Event correlation is a process that discovers associations among different but related events, in order to provide a SIEM operator with a bigger, more accurate, picture than a single event would provide in isolation. Correlation links multiple events together to detect malicious behaviors that might have otherwise been missed in the background noise associated with a high volume of routine, non-malicious events and network traffic.

In ArcSight ESM, once events have been normalized, prioritized, and their endpoints identified within the asset and network model, they are processed by the correlation engine, which is where filters, rules and data monitors are used to find the events of interest (Figure 10.). ESM's correlation tools use statistical analysis, Boolean logic and aggregation to find events with particular characteristics as specified by the operator.

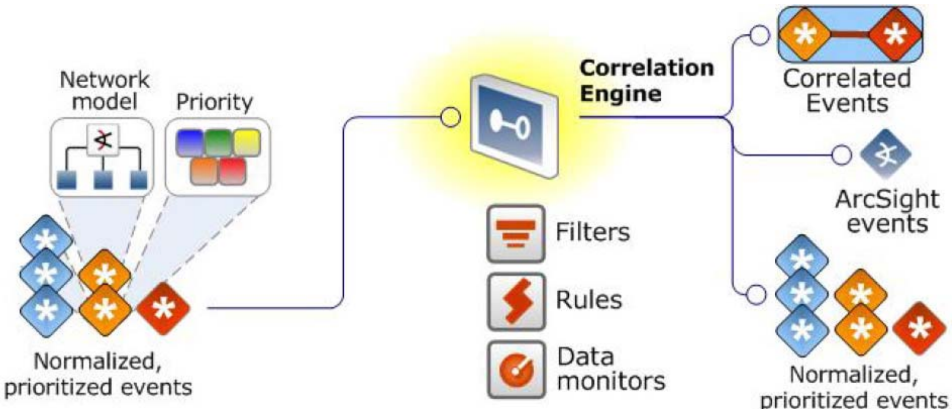
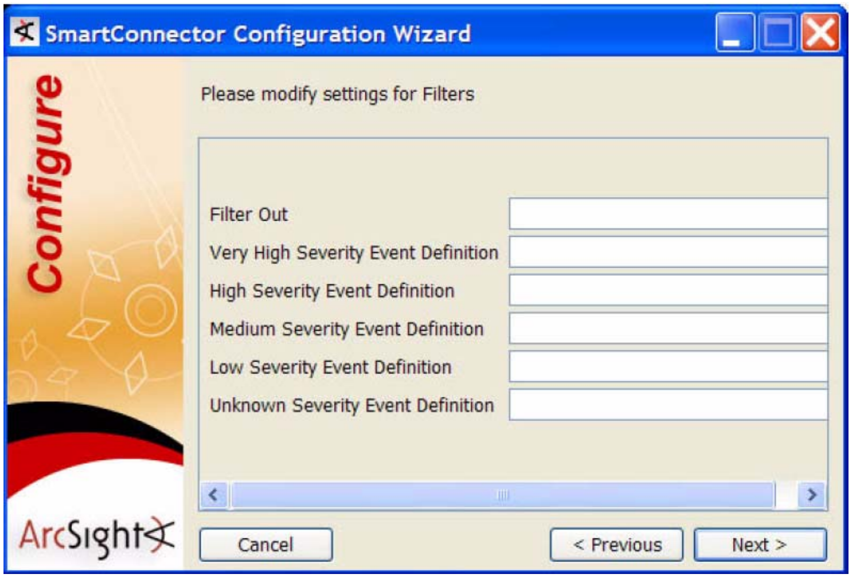


Figure 10. Events Correlation Process. After [5].

a. Filters

Filters are limiting gateways that help to separate events of interest from other “noisy events” and reduce the amount of events that are processed by the system. It uses a set of conditions that focus on particular event attributes to perform the separation.

Filters are applied in various stages of the event life cycle. During SmartConnector set up, the connector can be configured with filter conditions to focus the events passed to the ESM according to specific criteria (Figure 11). This first level of filtering prevents those events that do not meet the connector criteria from being forwarded to the ESM. Filters applied at the subsequent ESM level will then select which events it will process based on the conditions specified (Figure 12).


SmartConnector Configuration Wizard

Please modify settings for Filters

Filter Out

Very High Severity Event Definition

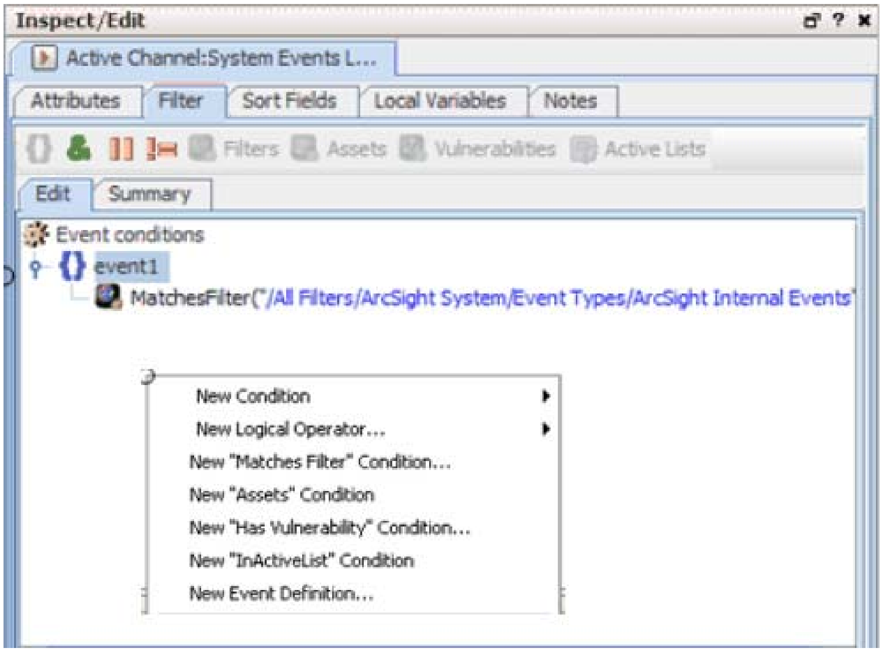
High Severity Event Definition

Medium Severity Event Definition

Low Severity Event Definition

Unknown Severity Event Definition

Figure 11. SmartConnector Filter Configuration. From [8].



MatchesFilter("/All Filters/ArcSight System/Event Types/ArcSight Internal Events'

Figure 12. ESM Filter Configuration. From [7].

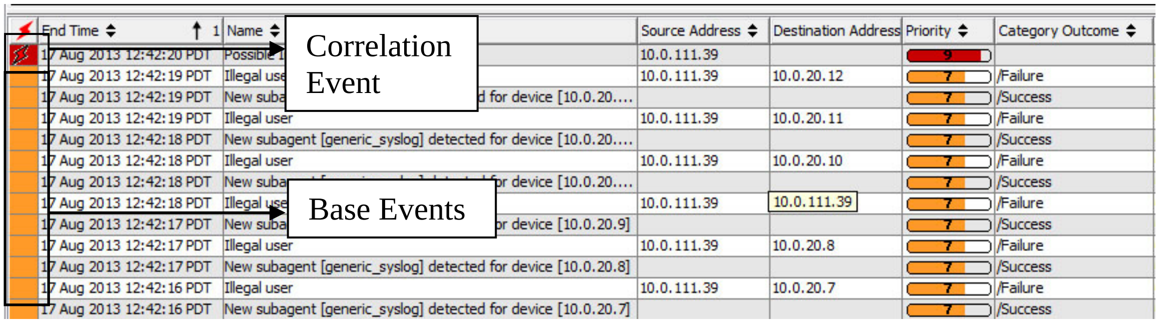
The main difference between both levels of filtering lies in their storage of rejected events. Only those rejected events from the ESM are stored in the CORR-engine storage. It is, therefore, important for the SIEM operator to decide where to apply the filter. While applying filters in the first level can significantly improve the signal-to-noise ratio, it must be carefully implemented with rigorous checking of the filter conditions. This verification ensures that useful events are not inadvertently left out. Rejected events that are stored in the ESM provide the SIEM operator with the flexibility to access those events later on if there is a change in investigative focus.

b. Rules

Rules are the core tool of the ESM correlation engine as they aid in revealing the broader *meaning* out of the steady stream of very narrow meaning individual events. A rule is a programmed procedure that evaluates incoming events for specific conditions and patterns. It leverages on the capability of filtering to first find matching base events and then provides initiate actions in response.

As events of interest may not stream into the Manager in a consecutive manner, the rules engine first looks for matches that fulfill the specified conditions and holds those matches in working memory. With more events streaming in, the stored events will be evaluated against the incoming events for aggregation and correlation. How long the matching events will be stored in the working memory depends on the rule threshold. The threshold is part of the rule that considers how many matching occurrences over a specified time frame must occur before the rule's criteria are considered to have been matched. Those partial matches and thresholds not met can be discarded from the working memory.

In ArcSight ESM, rules whose conditions have been met will generate an ESM event called a correlation event (Figure 13). Once generated, a correlation event will go through the event life cycle again, just as if it were a normalized base event reported by a SmartConnector.



End Time ↑ 1	Name	Source Address	Destination Address	Priority	Category Outcome
17 Aug 2013 12:42:20 PDT	Possible I	10.0.111.39		9	
17 Aug 2013 12:42:19 PDT	Illegal use	10.0.111.39	10.0.20.12	7	/Failure
17 Aug 2013 12:42:19 PDT	New suba d for device [10.0.20....			7	/Success
17 Aug 2013 12:42:19 PDT	Illegal user	10.0.111.39	10.0.20.11	7	/Failure
17 Aug 2013 12:42:18 PDT	New subagent [generic_syslog] detected for device [10.0.20....			7	/Success
17 Aug 2013 12:42:18 PDT	Illegal user	10.0.111.39	10.0.20.10	7	/Failure
17 Aug 2013 12:42:18 PDT	New suba r device [10.0.20....			7	/Success
17 Aug 2013 12:42:18 PDT	Illegal use	10.0.111.39	10.0.111.39	7	/Failure
17 Aug 2013 12:42:17 PDT	New suba r device [10.0.20.9]			7	/Success
17 Aug 2013 12:42:17 PDT	Illegal user	10.0.111.39	10.0.20.8	7	/Failure
17 Aug 2013 12:42:17 PDT	New subagent [generic_syslog] detected for device [10.0.20.8]			7	/Success
17 Aug 2013 12:42:16 PDT	Illegal user	10.0.111.39	10.0.20.7	7	/Failure
17 Aug 2013 12:42:16 PDT	New subagent [generic_syslog] detected for device [10.0.20.7]			7	/Success

Figure 13. Correlation and Base events on ArcSight Console. After [5].

When the correlation event passes through the correlation engine again, it is evaluated by other rules that are looking for correlation events with matching attributes. For this recursive correlation process to work most effectively, the rules leverage the following two ESM resources:

- Active Lists. These are configurable tables that act like a common access bulletin board where specified fields of event data are collected and retained during the first round of correlation process. The retained event data found in these lists can then be used as conditions evaluated by other rules in a subsequent correlation evaluation process. Active lists can be used by the operator to associate events happening in one area of the network with events happening in another area.

- Session Lists. Unlike active lists, session lists associate users with any events that are known to be associated with them. These lists are most typically used for identity correlation, such as to track user logins/logouts. For example, when a user logs in to a server, his/her user ID is added to the session list with a start time. When he/she logs out, an end time is appended to the same entry in the session list. This will allow later queries to the session list to check on the time interval over which a particular user was logged into a particular server. In terms of persistency of lists stored, session lists stay in the system longer and will require manual purging if removal from the list is desired. By contrast, active lists have a Time-To-Live (TTL) parameter that enables them to be automatically purged when the TTL expires.

SIEM operators should be familiar with the usage of both lists so that the malicious events within complex and varied scenarios can be tracked by the recursive correlation process.

5. Phase 5 – Monitoring and Investigation

ESM's normalization and correlation processes enable SOC personnel to have real-time situational awareness as events occur. After these backend processes (i.e., collection, normalization, filtering, and rule-evaluation) have completed their tasks, the next phase will be to present derived information to the operator. This can be achieved by using the various monitoring and investigation resources within ESM (Figure 14).

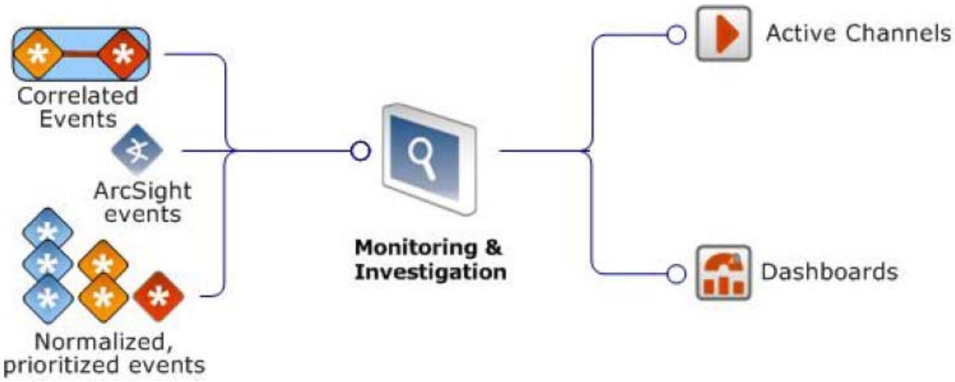
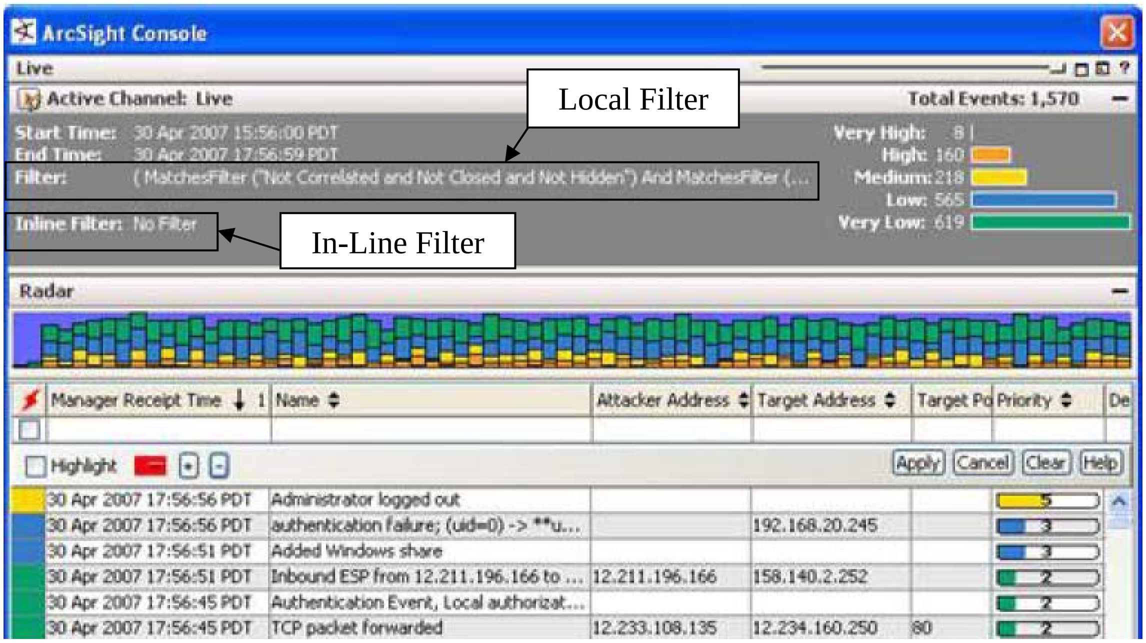


Figure 14. Monitoring and Investigation Process. After [5].

a. Active Channels

Similar to a channel tuned to a certain frequency on a television set, an active channel displays a stream of information defined by parameters set in the active channel editor. As mentioned previously, filters are used across the event life cycle stages. A local filter condition in the active channel helps to filter the stream of normalized base events, status events, and correlation events flowing through the ESM and to display only those that are of interest to the operators. In addition, an in-line filter can be configured within an active channel to further refine the conditions already set by the local filter. Unlike the local filter that allows manipulation of different event attributes, an in-line filter only works on one event attribute (i.e., schema column) at a time and uses the logical AND operator to perform the condition refinement. The in-line filter offers a quick and flexible way for the SIEM operator to further examine filtered events that works on the base conditions.



Active Channel: Live

Total Events: 1,570

Start Time: 30 Apr 2007 15:56:00 PDT
End Time: 30 Apr 2007 17:56:59 PDT
Filter: (MatchesFilter ("Not Correlated and Not Closed and Not Hidden") And MatchesFilter (...
Inline Filter: No Filter

Very High: 8
High: 160
Medium: 218
Low: 565
Very Low: 619

Manager Receipt Time ↓ 1	Name	Attacker Address	Target Address	Target Po	Priority	De
30 Apr 2007 17:56:56 PDT	Administrator logged out				5	
30 Apr 2007 17:56:56 PDT	authentication failure; (uid=0) -> **u...		192.168.20.245		3	
30 Apr 2007 17:56:51 PDT	Added Windows share				3	
30 Apr 2007 17:56:51 PDT	Inbound ESP from 12.211.196.166 to ...	12.211.196.166	158.140.2.252		2	
30 Apr 2007 17:56:45 PDT	Authentication Event, Local authorizat...				2	
30 Apr 2007 17:56:45 PDT	TCP packet forwarded	12.233.108.135	12.234.160.250	80	2	

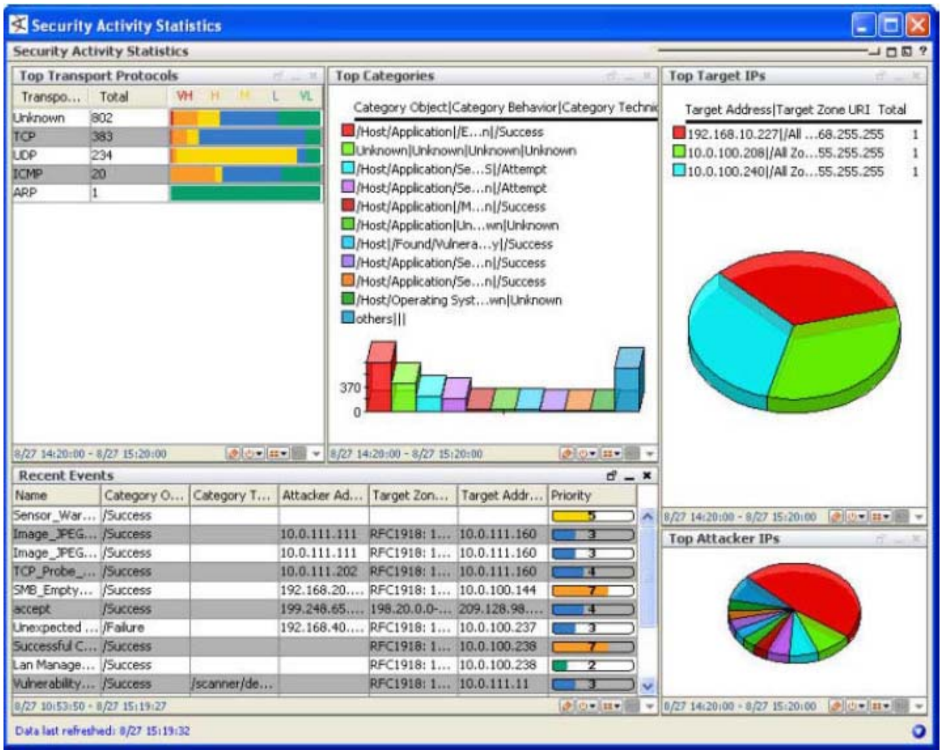
Figure 15. Active channel local and in-line filters. After [5].

The following two types of active channel are used extensively for monitoring and investigation:

- Live Channel – This channel displays real-time events and reflects any changes at its next refresh cycle, such as new base events arriving from SmartConnectors or when a user annotates an existing event with an investigation.
- Rules Channel – During situations whereby suspicious behavior are observed and new rules are required to draw on different fields of event data for correlation purposes, this channel allows SIEM operators to test newly-created rules on a fixed time window with historical events. The advantage of this channel is that rules can be tested and adjusted accordingly without conflicting with the ongoing rules that are being actively applied to the real-time events. Once the rules are proven to work as expected, they can then be linked to the Real-Time Rules folder, which holds all the rules that act on the real-time events.

b. Dashboard

ESM also uses another resource type called a dashboard, which is used to present events in various user-chosen formats. Instead of using the typical matrix table as shown in the active channels, dashboards are capable of showing events in a variety of graphical and tabular formats that summarize selected collections of events. Within a single dashboard, there can be multiple data monitors that provide different graphical event presentations. For example, if a SIEM operator wants to have a continuous update on the overall state of an enterprise's network security, he/she can create the various data monitors as shown in Figure 16.



Transpo...	Total	VH H M L VL
Unknown	802	
TCP	383	
UDP	234	
ICMP	20	
ARP	1	

Category Object|Category Behavior|Category Techni

- 🟥 /Host/Application|/E...n|/Success
- 🟩 Unknown|Unknown|Unknown|Unknown
- 🟦 /Host/Application/Se...S|/Attempt
- 🟪 /Host/Application/Se...n|/Attempt
- 🟥 /Host/Application|/M...n|/Success
- 🟩 /Host/Application|Un...wn|Unknown
- 🟦 /Host|/Found/Vulnera...y|/Success
- 🟪 /Host/Application/Se...n|/Success
- 🟧 /Host/Application/Se...n|/Success
- 🟩 /Host/Operating Syst...wn|Unknown
- 🟦 others|||

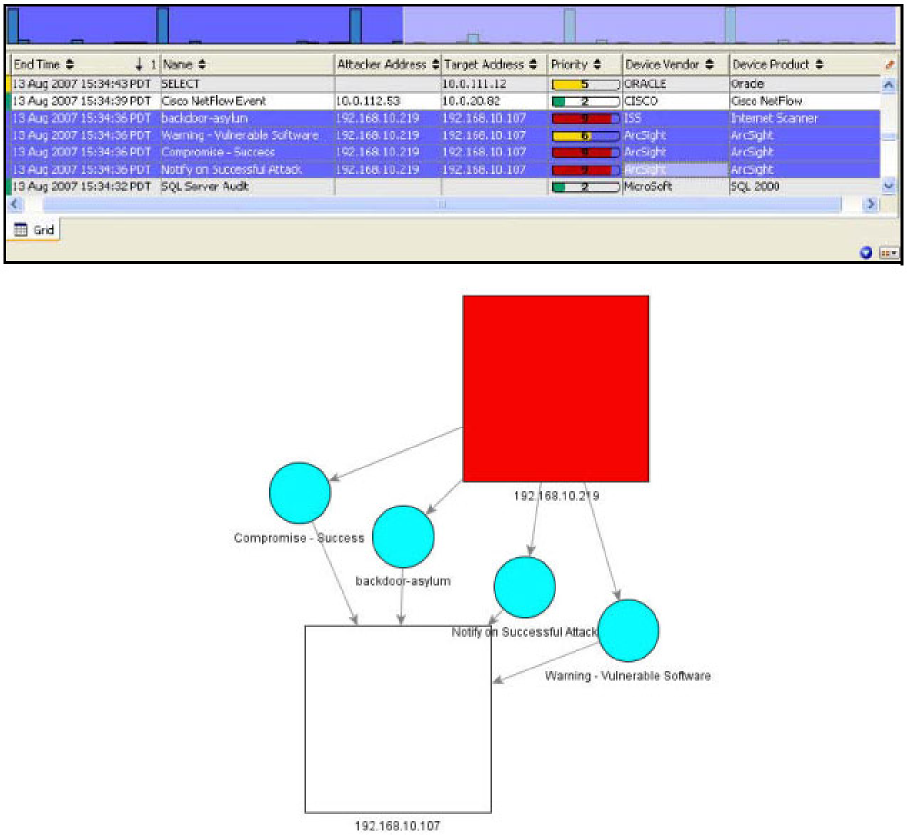
Target Address|Target Zone URI	Total
🟥 192.168.10.227|/All ...68.255.255	1
🟩 10.0.100.208|/All Zo...55.255.255	1
🟦 10.0.100.240|/All Zo...55.255.255	1

Name	Category O...	Category T...	Attacker Ad...	Target Zon...	Target Addr...	Priority
Sensor_War...	/Success					5
Image_JPEG...	/Success		10.0.111.111	RFC1918: 1...	10.0.111.160	3
Image_JPEG...	/Success		10.0.111.111	RFC1918: 1...	10.0.111.160	3
TCP_Probe_...	/Success		10.0.111.202	RFC1918: 1...	10.0.111.160	4
SMB_Empty...	/Success		192.168.20....	RFC1918: 1...	10.0.100.144	7
accept	/Success		199.248.65....	198.20.0.0-...	209.128.98....	4
Unexpected ...	/Failure		192.168.40....	RFC1918: 1...	10.0.100.237	3
Successful C...	/Success			RFC1918: 1...	10.0.100.238	7
Lan Manage...	/Success			RFC1918: 1...	10.0.100.238	2
Vulnerability...	/Success	/scanner/de...		RFC1918: 1...	10.0.111.11	3

Figure 16. Security Activity Statistics Dashboard. From [5].

Data monitors work essentially the same as rules in that they evaluate the event stream and aggregate events with common elements. Rules focus on inferring meaning from certain event conditions and combinations to enhance interpretation and, optionally, to specify certain actions. Data monitors, on the other hand, focus on summarizing event data and presenting them graphically. They cannot be used to trigger actions like rules. As such, data monitors provide another type of analysis, such as calculating statistics and moving data averages.

The benefit of having a composite dashboard is that it offers an "all-in-one-glance" panel that summarizes multi-node enterprise security data. This makes it easier to visualize attack patterns among nodes on the network. In certain situations, a causal relationship between events can also be discovered. For example, an attacker has been attempting to hack into an asset through various means. By selecting those events together and investigating them with the ESM graphical tools, a causal relationship between the attacker and the asset can be more easily seen (Figure 17).



End Time ↓ 1	Name	Attacker Address	Target Address	Priority	Device Vendor	Device Product
13 Aug 2007 15:34:43 PDT	SELECT		10.0.111.12	5	ORACLE	Oracle
13 Aug 2007 15:34:39 PDT	Cisco NetFlow Event	10.0.112.53	10.0.20.82	2	CISCO	Cisco NetFlow
13 Aug 2007 15:34:36 PDT	backdoor-asylum	192.168.10.219	192.168.10.107	[illegible]	ISS	Internet Scanner
13 Aug 2007 15:34:36 PDT	Warning - Vulnerable Software	192.168.10.219	192.168.10.107	6	ArcSight	ArcSight
13 Aug 2007 15:34:36 PDT	Compromise - Success	192.168.10.219	192.168.10.107	[illegible]	ArcSight	ArcSight
13 Aug 2007 15:34:36 PDT	Notify on Successful Attack	192.168.10.219	192.168.10.107	[illegible]	ArcSight	ArcSight
13 Aug 2007 15:34:32 PDT	SQL Server Audit			2	MicroSoft	SQL 2000

Figure 17. Causal relationship between attacker and asset. From [5].

6. Phase 6 - Reporting

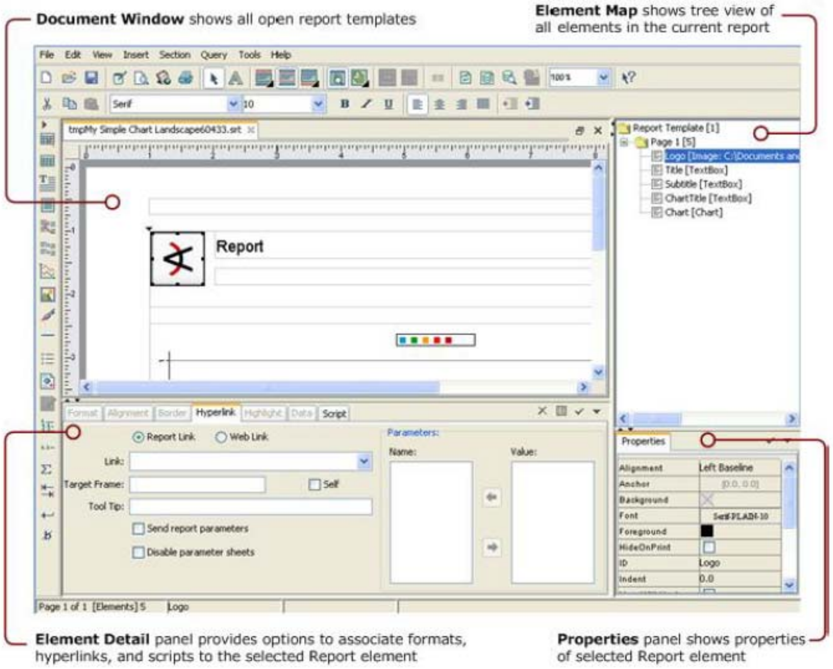
With all the events processed and stored in the CORR-Engine storage, the next logical step is to produce reports that can be archived and/or provided in support of accreditation or other established security procedures. In the ESM, a summarized collection of information pertaining to any particular incident is known as a report. Reports are generated either manually or via a pre-defined rule action. Two ESM resources utilized in the report creation process are the Query and Template resources.

a. Query Resource

A query is a request action to a data source that reports events to ESM. Based on the query statement, certain parameters of the data can then be gathered. Some of the data sources are CORR-Engine storage and data stored in active lists or session lists.

b. Template Resource

Templates are another form of resource that defines the structure in which data results from the report are presented. The layout specification can be tailored by the SIEM operator to suit an enterprise's desired reporting format and can enforce the necessary standardization.



Document Window shows all open report templates

Element Map shows tree view of all elements in the current report

Element Detail panel provides options to associate formats, hyperlinks, and scripts to the selected Report element

Properties panel shows properties of selected Report element

● Report Link ○ Web Link

Link:

Target Frame: □ Self

Tool Tip:

□ Send report parameters

□ Disable parameter sheets

Parameters:

Name: Value:

Alignment	Left Baseline
Anchor	[0.0, 0.0]
Background	
Font	Serif-PLAIN-10
Foreground	■
HideOnPrint	□
ID	Logo
Indent	0.0

Figure 18. Customer Template Design. From [5].

The procedural approach in implementing ArcSight ESM has been explained in this chapter, with specific emphasis on how the SIEM operator can effectively utilize the various tools and resources to conduct the forensic activities. Certain resources of ArcSight ESM are deliberately left out of the explanation as they either: a) require additional licensing modules (e.g., Pattern discovery & Interactive discovery) which are not available in the standard package or b) will not be utilized in the training scenarios. Despite this, the chapter has covered the core functional processes that are essential to the operation of a typical SIEM product, and this should facilitate the basic understanding required to follow the material presented in subsequent chapters.

IV. TRAINING STRATEGY

As part of the thesis objectives, a repeatable educational framework has to be created in order to facilitate the SIEM training. This chapter outlines the training strategy that will be used to achieve the aforementioned objective. It will include the tools, learning goals and method used to develop the scenario-based training lab for SIEM operators.

A. REPLAY TOOLS

Traffic replay is one of the key features of a SIEM product. The ability to replay pre-captured events is particularly useful for the following purposes:

- Testing – This allows stress testing to be conducted for the ArcSight configuration and deployment, while identifying possible loopholes and vulnerabilities.
- Training – For ease of demonstration and training for new cadres of SIEM operators.

In ArcSight, the replay events and connectors are the replay tools. Similar to the SmartConnectors, the *replay* connectors are used primarily to feed the ArcSight Express with base events. However, there is a difference in the timestamp of the events provided.

The SmartConnectors lie in between the network devices and ArcSight Express. Real-time raw events generated from the network devices stream through the SmartConnectors and undergo filtering, aggregation, normalization and categorization prior to arriving at the ArcSight Express. In contrast, the replay connectors are standalone modules that are not associated with any network devices (Figure 19). Rather than "live" streaming, the replay connectors provide the replay of pre-captured (historical) events saved from past activities.

Despite the difference in the timestamp, ArcSight Express handles every base event received in the same manner. When the events arrive, ArcSight Express subjects the events to the real-time rules for filtering and correlation purposes.

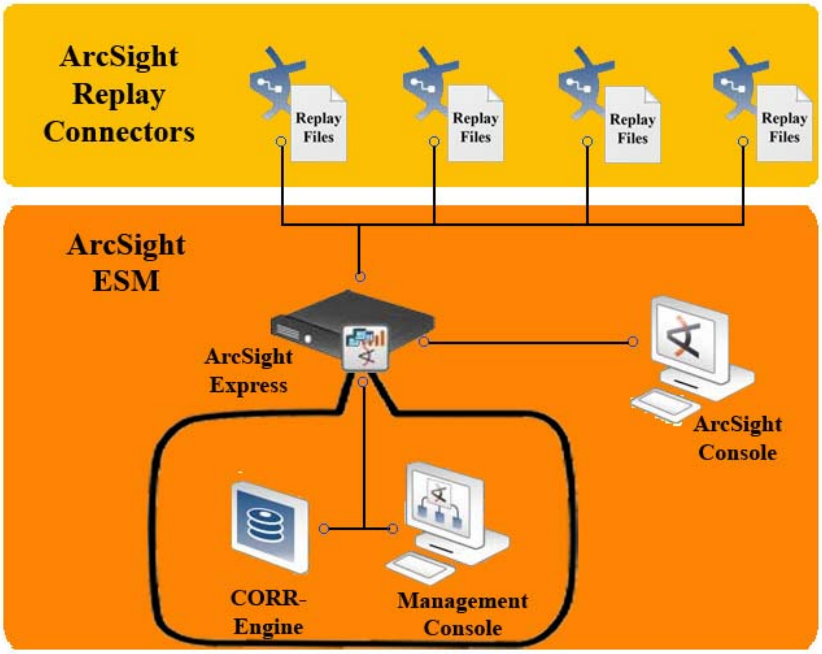


Figure 19. ArcSight replay connectors' connectivity. After [5].

B. LEARNING GOALS

The learning goals are stated to guide the construction of the method, content and structure for the learning lab. The learning goals include the steps to create the lab environment and the important concepts and skills that will be taught to the SIEM operators.

1. Understand the Behavior of a Cyber Threat

Without a clear understanding on the behavior of the cyber threat, SIEM operators will experience great difficulties in conducting cyber forensic analysis. Therefore, it is important to study the behavior of the cyber threat as it will build the knowledge foundation in searching for malicious indicators among the myriad events interspersed within the seemingly normal cyber activities. An understanding of the interrelation between a given cyber threat and its associative event-based indicators will also allow SIEM operators to utilize the ArcSight resources for various core processes more effectively.

In the realm of computer networks, many cyber threats exist. Considering the non-distinctive behaviors that can be exhibited by the various threats, it is practically impossible to create a single use case or rule that will reliably detect all threats. As such, the learning lab will only focus on a particular cyber threat. In this way, the complexities involved in rules configuration will be significantly reduced, and hence allow the SIEM operators to concentrate on learning the concepts and skills required for cyber forensic analysis.

2. Set up Lab Environment

Before a SIEM operator can embark on the learning process, the lab environment must be set up correctly. The environment will require a collection of replay events that can demonstrate the behavior of a particular cyber threat. Then the replay connector will be leveraged as the events generator to provide a steady stream of events to the ArcSight Express.

3. Construct Network Topology through "Reverse-Engineering" Method

The main purpose of the "reverse-engineering" method is to allow the construction of the network topology using the information within the base events. During the research phase of this thesis, it was realized that the replay events obtained were not accompanied by notes regarding the topology of the network from which the replay events were collected. As previously mentioned, the network topology aids in network and asset modeling and is a crucial step required in the workflow process to properly characterize and prioritize information gleaned from the raw events provided by the reporting devices. While this situation of an "unfamiliar" network is unlikely in a real-world operational environment, it is necessary to deal with this in the context of this thesis: owing to the goal of being able to utilize replay events that have been collected from various networks, yet process them as though they were from one's own—familiar—operational network.

4. Associate Threat Behavior

All the ArcSight core processes depend on the parameters of the event schema to perform their functions. For example, during the aggregation process, the rules may use the "Source IP address" parameter to combine the network traffic, while in the correlation process the "Agent Hostname" parameter can be used to recognize this common association between events. With an understanding of a given cyber threat's behavior, SIEM operators will be better able to correlate collected events to indications of that threat.

5. Configure Rules

Rule writing is an important skill for SIEM operators since a SIEM product is a passive system. As such, it requires rules to provide the logical relationships that are deemed likely indicators of threats or exploited system behavior. Identified threat characteristics are the conditional parameters for the structuring of rules. With an understanding of these characteristics, SIEM operators can intelligently modify, or even create, rules.

6. Present and Report Detected Threats

ArcSight offers various graphical resources to represent network activities and detected threats. Many are of these graphical resources are rather intuitive, permitting the SIEM operator to quickly understand the current situation. The lab will introduce some of the primary graphical resources that can be used to represent the network activity of interest and detected threats. Subsequently, the ArcSight *report* resource will be utilized to create a summary of detected threat indications that can be saved and/or printed out for archiving purposes.

C. METHOD

Scenario-based training will be adopted as the methodology in the learning lab to educate the SIEM operators. The scenario will closely mimic a "real-world" situation so that the learning experience is practical and can be applicable to other similar situations.

1. Scenario Overview

A computer worm is a form of cyber threat that is encountered by many networked systems. A worm is malware that does not rely on human intervention to execute and is capable of replicating itself and spreading within and across computer networks. A worm targets certain security vulnerabilities and often causes harm to the network, such as consuming bandwidth capacity, thus making services unavailable to legitimate users and applications.

As a simple demonstration, the model scenario used in this thesis is based on a computer worm that does not carry malicious payload. Recall that a SIEM product is used to analyze events *reported by* network devices rather than (itself) analyzing the semantics of the "raw" stimuli that elicited the various events from the monitored network devices. The replay events for this model scenario will consist of thousands of entries that will simulate a worm outbreak situation where the worm spreads within and across multiple networks. This behavior of the typical computer worm will serve as the model threat for inexperienced SIEM operators to conduct analysis.

The "storyboard" of the scenario will revolve around a fictional organization that is hosting an online Web portal called "SporeFusion.com." According to our exercise story, in recent months this fictional organization has been facing an increasing number of cyber-attacks and has suffered financial loss during some of the more pernicious attacks. Seeing the need to protect their business, the organization has decided to purchase ArcSight ESM as a detective security control against these threats. The IT employees within the organization are tasked with the mission of utilizing ArcSight ESM to detect, report, and recover from threats as quickly as possible.

2. Training Phases

The learning goals stated will form the structure of the lab, with each goal translated to a phase. In most of the phases, the SIEM operators are required to interact with the ArcSight ESM. The different phases are intended for progressive learning in which the operators will obtain the necessary knowledge and skillset from the earlier phases, which are necessary to complete tasks required in later phases.

The first phase will require the SIEM operators to study the behavior of computer worms and, in particular, understand their “self-replicating” and “spreading” traits. The second phase will then focus on the installation of the replay connector on the host machine and configuration of the replay events to generate the event flow to ArcSight Express. The third phase will demonstrate a way to infer the network topology of the capture environment using ArcSight graphical resources. The fourth phase will expose SIEM operators to many of the most prominent worm attack indicators that can be used to associate to the parameters of the event schema. The fifth and sixth phases are the highlights of the learning lab; where the SIEM operators will step through the workflow process, construct a set of logical worm detection rules (the fifth phase), and ultimately present their worm-detection analysis as an incident report (the sixth phase). These last two phases will require more time than the previous four phases due to the trial-and-error nature of getting the best rules to elicit the desired response (a high confidence detection alert) from the base events involved.

D. SUMMARY

This chapter has presented the general approach for the design of a worm outbreak scenario that models a realistic cyber-attack issue faced by many Internet-facing enterprises nowadays. The activities and tasks associated with the six phases will cover the learning objectives stated in Chapter I. The next chapter will provide more detail on the phases and how various ArcSight resources can be utilized to achieve the objectives.

V. TRAINING SCENARIO

This chapter will elaborate on the training methodology applied for the worm-outbreak scenario. The content will be categorized into six training phases and will include the expected results.

A. SCENARIO BRIEFING

The purpose of this scenario briefing is to provide SIEM operators with the background context for their cyber-forensic analysis. The scenario describes a cyber-threat (computer worm) faced by a fictional organization that is hosting an online Web portal called “SporeFusion.com” and is summarized as follows:

> “SporeFusion.com” belongs to a company that provides personal photo service for subscribed customers to customize their digital photos with the company’s online photo editing tools. It also allows the customers to print their personalized photos on an array of products (e.g., mugs, shirts). The company maintains its own IT infrastructure. The infrastructure supports two networks: an external network to provide their online services to the customers and an internal network to maintain their proprietary company information (e.g., sales, orders and inventory).
>
> Over the years, the organization has been suffering from periodic cyber-attacks, some of which have resulted in financial loss due to lost customer satisfaction or added service costs. The most serious attack rendered the online portal unavailable for five days, resulting in great financial loss during that period. A preliminary investigation by the company’s own IT employees discovered it to be a denial-of-service attack caused by a computer worm. Despite this discovery, the company was unable to trace the source of the attack or determine the extent of infected hosts within their network.
>
> To improve this situation and improve their overall IT security posture, the company has decided to purchase ArcSight ESM as a detective security control against these threats. The IT employees within the organization are tasked with the mission of utilizing ArcSight ESM to detect and recover from threats as quickly as possible.

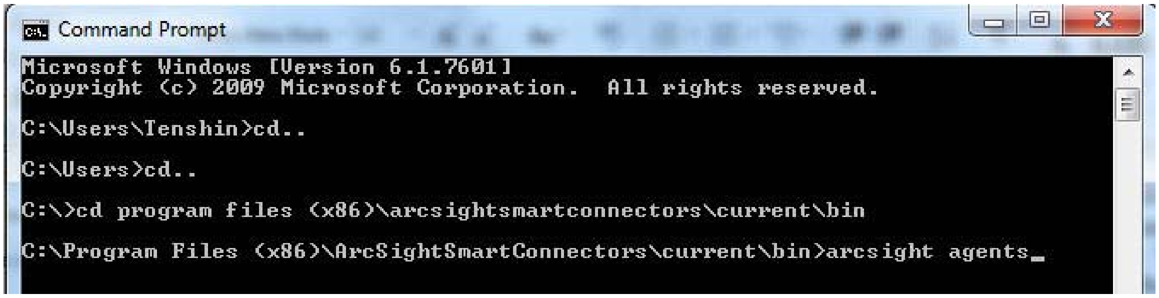
B. PHASE 1 – UNDERSTAND THE BEHAVIOR OF A COMPUTER WORM

The first phase will require SIEM operators to conduct a study on the behavior of a computer worm. Through this study, the SIEM operators will learn and understand the worm's associative traits, which will then become the target of analysis. The following highlights some of the fundamental information pertaining to the computer worm that must be understood by the SIEM operators during their study:

- The worm usually originates from a single host.
- The worm has the ability to self-replicate. This means that once it infects a host, the worm will understand what network it is on and will attempt to find nearby host(s) (likely to be a host with the same vulnerability and lies within the same network) and attempt connections to the host(s) through various sockets/ports. Thereafter, these newly spread worms will repeat the same actions on their newly infected hosts.

C. PHASE 2 – SET UP REPLAY ENVIRONMENT

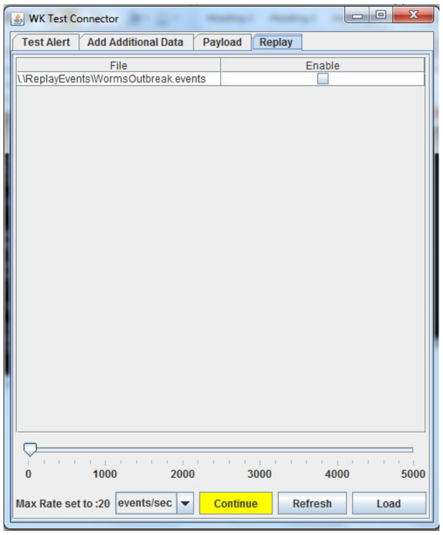
The next phase is to install the replay events and connector for continuous testing and analysis on a set of pre-captured events. (Refer to the Appendix for the installation guide.) After successful installation, the replay graphical user interface (GUI) can be activated through the command prompt in administrator mode.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Tenshin>cd..

C:\Users>cd..

C:\>cd program files (x86)\arcsightsmartconnectors\current\bin

C:\Program Files (x86)\ArcSightSmartConnectors\current\bin>arcsight agents_
```

Figure 20. Replay connector activation.

The replay GUI is the main control mechanism that initiates the events transmission to ArcSight ESM. Once the replay files have been placed in the correct folder as stated in the Appendix, the replay GUI will automatically load all the stored events and allow SIEM operators to select the desired set of events to be streamed into ArcSight ESM (Figure 21). The GUI also provides a time slider and events transmission rate option (e.g., events/sec or events/min) to manipulate the rate of events being transmitted.

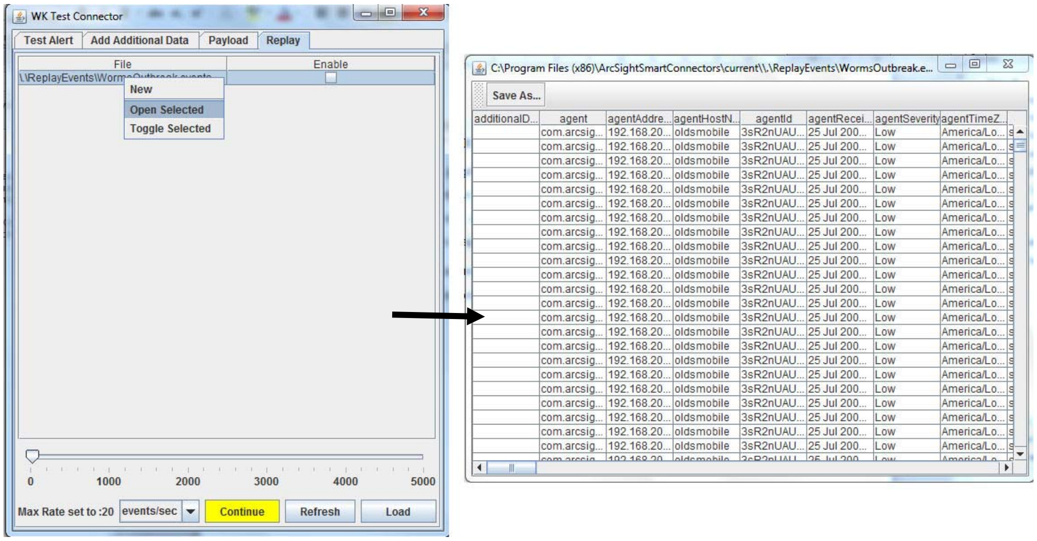


File	Enable
\.\ReplayEvents\WormsOutbreak.events	□

Max Rate set to :20 events/sec

Figure 21. Replay connector GUI.

The base events stored within the file can be accessed by "right-clicking" on the selected file and choosing "Open Selected." A new screen will appear with all the base event entries as shown in Figure 22.

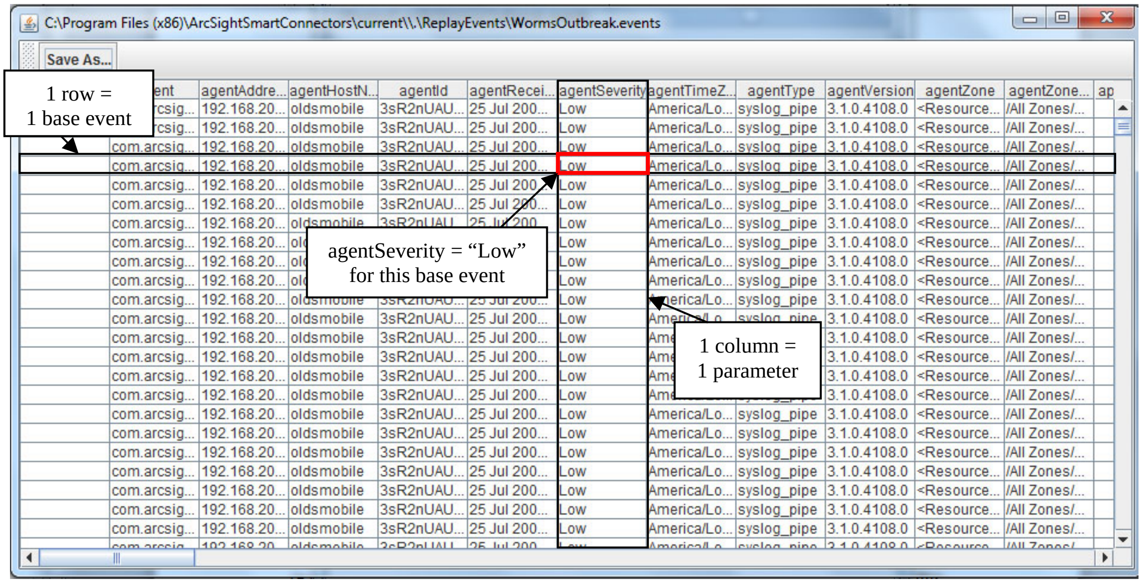


C:\Program Files (x86)\ArcSightSmartConnectors\current\.\ReplayEvents\WormsOutbreak.e...

additionalD...	agent	agentAddre...	agentHostN...	agentId	agentRecei...	agentSeverity	agentTimeZ...
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...

Figure 22. Access base event entries.

For this test scenario, the “WormOutbreak.events” file is selected. As seen in Figure 23, each row represents one base event, while each column represents a parameter of the ArcSight event schema. The cell holds the value of the parameter associated with that particular base event.



C:\Program Files (x86)\ArcSightSmartConnectors\current\\.\ReplayEvents\WormsOutbreak.events

	ent	agentAddre...	agentHostN...	agentId	agentRecei...	agentSeverity	agentTimeZ...	agentType	agentVersion	agentZone	agentZone...	ap
	rcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...	syslog_pipe	3.1.0.4108.0	<Resource...	/All Zones/...	
	rcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...	syslog_pipe	3.1.0.4108.0	<Resource...	/All Zones/...	
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...	syslog_pipe	3.1.0.4108.0	<Resource...	/All Zones/...	
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...	syslog_pipe	3.1.0.4108.0	<Resource...	/All Zones/...	
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...	syslog_pipe	3.1.0.4108.0	<Resource...	/All Zones/...	
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...	syslog_pipe	3.1.0.4108.0	<Resource...	/All Zones/...	
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU	25 Jul 200	Low	America/Lo...	syslog_pipe	3.1.0.4108.0	<Resource...	/All Zones/...	
	com.arcsig...	192.168.20...	ol	[illegible]	[illegible]	Low	America/Lo...	syslog_pipe	3.1.0.4108.0	<Resource...	/All Zones/...	
	com.arcsig...	192.168.20...	ol	[illegible]	[illegible]	Low	America/Lo...	syslog_pipe	3.1.0.4108.0	<Resource...	/All Zones/...	
	com.arcsig...	192.168.20...	ol	[illegible]	[illegible]	Low	America/Lo...	syslog_pipe	3.1.0.4108.0	<Resource...	/All Zones/...	
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...	syslog_pipe	3.1.0.4108.0	<Resource...	/All Zones/...	
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...	syslog_pipe	3.1.0.4108.0	<Resource...	/All Zones/...	
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	Ame	[illegible]	3.1.0.4108.0	<Resource...	/All Zones/...	
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	Ame	[illegible]	3.1.0.4108.0	<Resource...	/All Zones/...	
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	Ame	[illegible]	3.1.0.4108.0	<Resource...	/All Zones/...	
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	Ame	[illegible]	3.1.0.4108.0	<Resource...	/All Zones/...	
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...	syslog_pipe	3.1.0.4108.0	<Resource...	/All Zones/...	
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...	syslog_pipe	3.1.0.4108.0	<Resource...	/All Zones/...	
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...	syslog_pipe	3.1.0.4108.0	<Resource...	/All Zones/...	
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...	syslog_pipe	3.1.0.4108.0	<Resource...	/All Zones/...	
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...	syslog_pipe	3.1.0.4108.0	<Resource...	/All Zones/...	
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...	syslog_pipe	3.1.0.4108.0	<Resource...	/All Zones/...	
	com.arcsig...	192.168.20...	oldsmobile	3sR2nUAU...	25 Jul 200...	Low	America/Lo...	syslog_pipe	3.1.0.4108.0	<Resource...	/All Zones/...	

1 row =
1 base event

agentSeverity = “Low”
for this base event

1 column =
1 parameter

Figure 23. Event Entries in “WormOutbreak.events” file.

D. PHASE 3 – CONSTRUCT NETWORK TOPOLOGY THROUGH “REVERSE-ENGINEERING” METHOD

ArcSight graphical resources are particularly useful in analyzing the traffic flow within a set of replay events. The resources work by leveraging the parameters within the event schema (e.g., source and destination IP addresses, device vendor name and zone) to map out the networks, associated network devices and the communication flow between these devices. With a basic understanding on IP networking (e.g. RFC1918[6] private networks), it is therefore possible for SIEM operators to utilize the graphical resources to “reconstruct” the network topology from a set of replay events.

In normal circumstances, the reconstruction method must be applied to all the events in the replay file so as to obtain the full network topology, which may consist of

[6] RFC1918 are standards that define the private IP address space.

many sub-networks. For the ease of illustration, the following example will focus on a small subset of the events within the replay files. This is done because the particular replay file used in our example was collected from a rather large volume of IP space; and viewing *all* of this space using the SIEM's graphical utilities would result in a very "crowded" topological depiction. By limiting the demonstration to a smaller subset of the entire IP space (by selecting a subset of the collected events), the resulting graph will be easier to see via the below screen captures.

Prior to viewing the base events in ArcSight Console, the SIEM operators must first create an active channel. Periodically, ArcSight ESM will generate internal system events that report its current status (e.g. user log-in). To prevent such events from clustering with the events of interest, the SIEM operators will use the active channel editor to filter out the internal system events. In addition, a customized grid field object will be created to limit the number of viewable events' parameters. In our training scenario, both the "Agent Type" and "Severity" parameters will be set to "syslog_pipe" and ">= 3," respectively (with an OR condition), in the active channel editor to display the base and correlation events pertaining to the worm outbreak scenario.

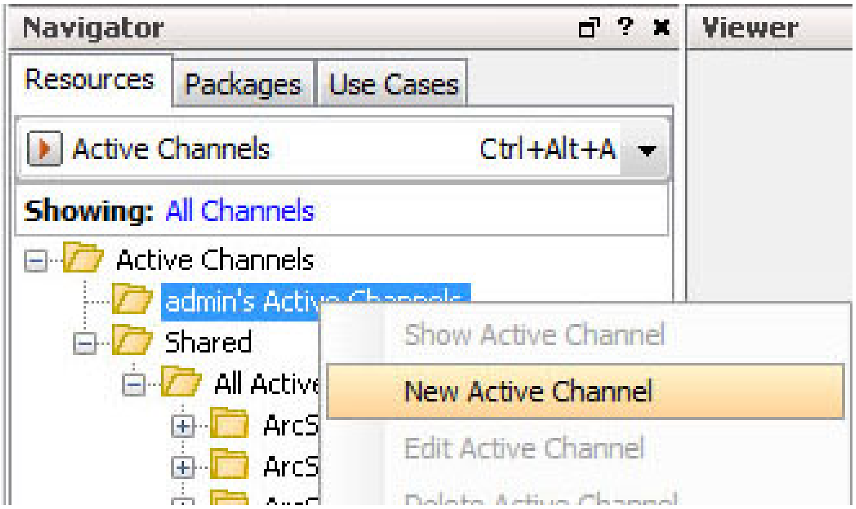
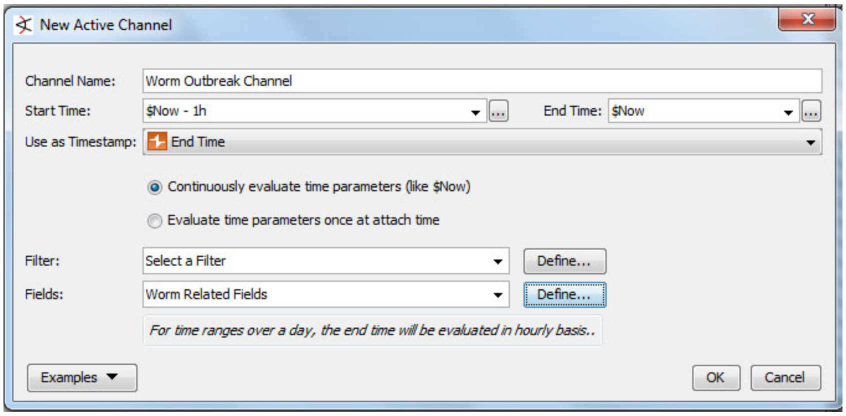


Figure 24. Create Active Channel in Navigator Panel.


New Active Channel

Channel Name: Worm Outbreak Channel

Start Time: $Now - 1h

End Time: $Now

Use as Timestamp: End Time

● Continuously evaluate time parameters (like $Now)

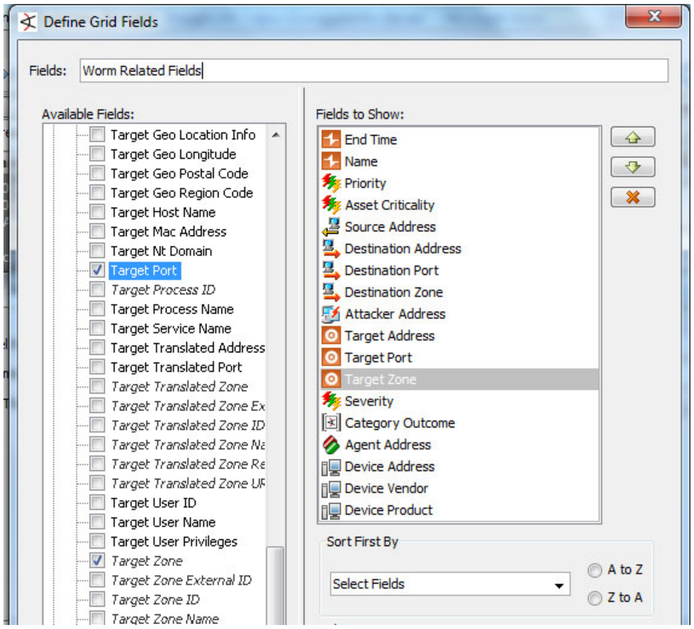
○ Evaluate time parameters once at attach time

Filter: Select a Filter

Fields: Worm Related Fields

For time ranges over a day, the end time will be evaluated in hourly basis..

Figure 25. Customize Active Channel.


Define Grid Fields

Fields: Worm Related Fields

Available Fields:

- □ Target Geo Location Info
- □ Target Geo Longitude
- □ Target Geo Postal Code
- □ Target Geo Region Code
- □ Target Host Name
- □ Target Mac Address
- □ Target Nt Domain
- ☑ Target Port
- □ *Target Process ID*
- □ Target Process Name
- □ Target Service Name
- □ Target Translated Address
- □ Target Translated Port
- □ *Target Translated Zone*
- □ *Target Translated Zone Ex*
- □ *Target Translated Zone ID*
- □ *Target Translated Zone Na*
- □ *Target Translated Zone Re*
- □ *Target Translated Zone UF*
- □ Target User ID
- □ Target User Name
- □ Target User Privileges
- ☑ *Target Zone*
- □ *Target Zone External ID*
- □ *Target Zone ID*
- □ *Target Zone Name*

Fields to Show:

- End Time
- Name
- Priority
- Asset Criticality
- Source Address
- Destination Address
- Destination Port
- Destination Zone
- Attacker Address
- Target Address
- Target Port
- Target Zone
- Severity
- Category Outcome
- Agent Address
- Device Address
- Device Vendor
- Device Product

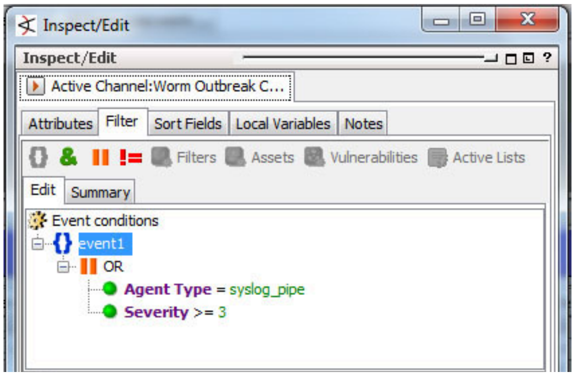
Sort First By

Select Fields

○ A to Z

○ Z to A

Figure 26. Customize Grid Fields.

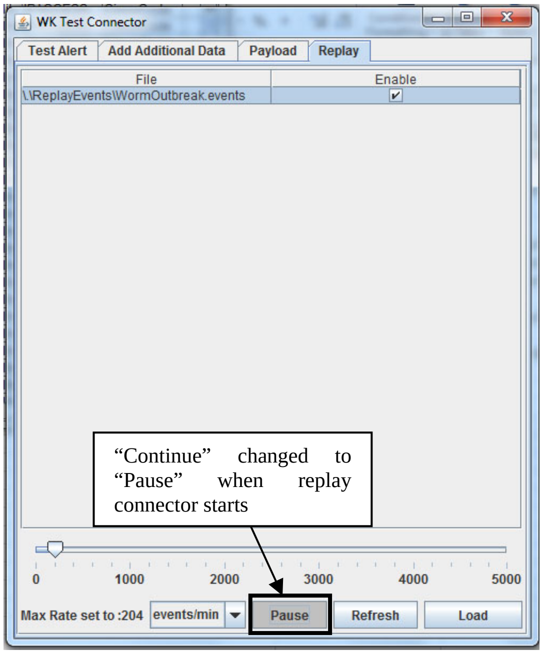

Inspect/Edit

Active Channel:Worm Outbreak C...

Event conditions
- event1
  - OR
    - **Agent Type** = syslog_pipe
    - **Severity** >= 3

Figure 27. Create filter in Active Channel Editor.

Next, start the replay connector to allow the base events to flow into ArcSight Express.



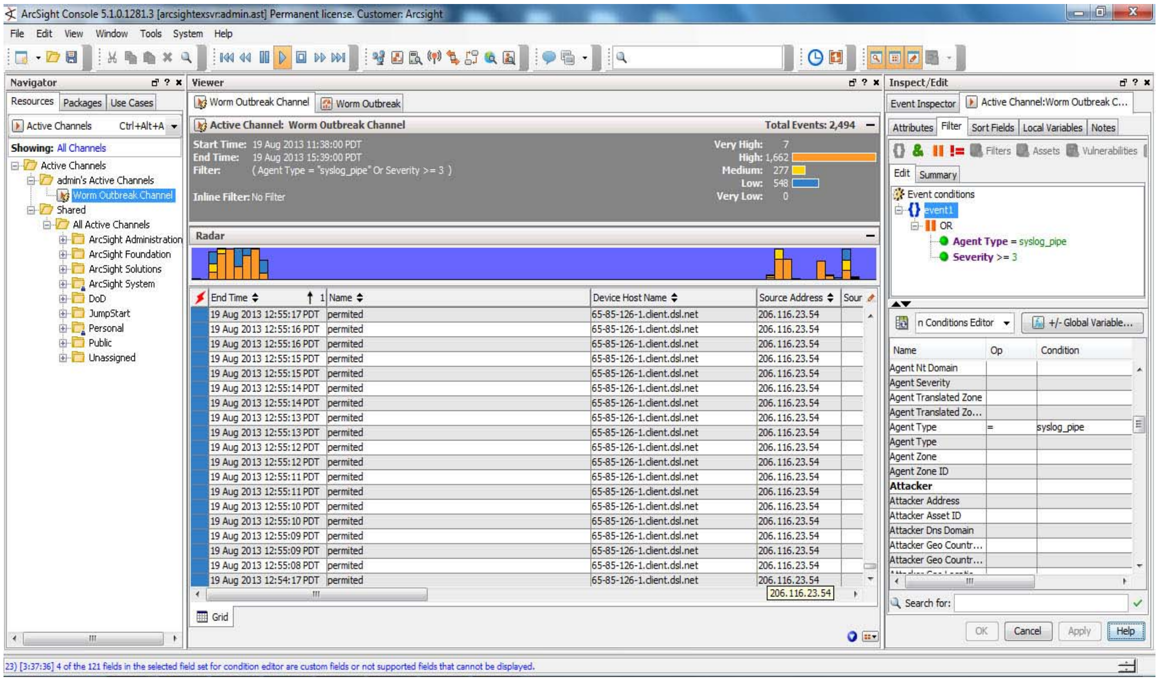
File	Enable
\.\ReplayEvents\WormOutbreak.events	☑

Max Rate set to :204 events/min

Pause

“Continue” changed to “Pause” when replay connector starts

Figure 28. Start replay connector.



Active Channel: Worm Outbreak Channel

Total Events: 2,494

Start Time: 19 Aug 2013 11:38:00 PDT
End Time: 19 Aug 2013 15:39:00 PDT
Filter: (Agent Type = "syslog_pipe" Or Severity >= 3)

Inline Filter: No Filter

Very High: 7
High: 1,662
Medium: 277
Low: 548
Very Low: 0

End Time	Name	Device Host Name	Source Address	Sour
19 Aug 2013 12:55:17 PDT	permited	65-85-126-1.client.dsl.net	206.116.23.54	
19 Aug 2013 12:55:16 PDT	permited	65-85-126-1.client.dsl.net	206.116.23.54	
19 Aug 2013 12:55:16 PDT	permited	65-85-126-1.client.dsl.net	206.116.23.54	
19 Aug 2013 12:55:15 PDT	permited	65-85-126-1.client.dsl.net	206.116.23.54	
19 Aug 2013 12:55:15 PDT	permited	65-85-126-1.client.dsl.net	206.116.23.54	
19 Aug 2013 12:55:14 PDT	permited	65-85-126-1.client.dsl.net	206.116.23.54	
19 Aug 2013 12:55:14 PDT	permited	65-85-126-1.client.dsl.net	206.116.23.54	
19 Aug 2013 12:55:13 PDT	permited	65-85-126-1.client.dsl.net	206.116.23.54	
19 Aug 2013 12:55:13 PDT	permited	65-85-126-1.client.dsl.net	206.116.23.54	
19 Aug 2013 12:55:12 PDT	permited	65-85-126-1.client.dsl.net	206.116.23.54	
19 Aug 2013 12:55:12 PDT	permited	65-85-126-1.client.dsl.net	206.116.23.54	
19 Aug 2013 12:55:11 PDT	permited	65-85-126-1.client.dsl.net	206.116.23.54	
19 Aug 2013 12:55:11 PDT	permited	65-85-126-1.client.dsl.net	206.116.23.54	
19 Aug 2013 12:55:10 PDT	permited	65-85-126-1.client.dsl.net	206.116.23.54	
19 Aug 2013 12:55:10 PDT	permited	65-85-126-1.client.dsl.net	206.116.23.54	
19 Aug 2013 12:55:09 PDT	permited	65-85-126-1.client.dsl.net	206.116.23.54	
19 Aug 2013 12:55:09 PDT	permited	65-85-126-1.client.dsl.net	206.116.23.54	
19 Aug 2013 12:55:08 PDT	permited	65-85-126-1.client.dsl.net	206.116.23.54	
19 Aug 2013 12:54:17 PDT	permited	65-85-126-1.client.dsl.net	206.116.23.54	

206.116.23.54

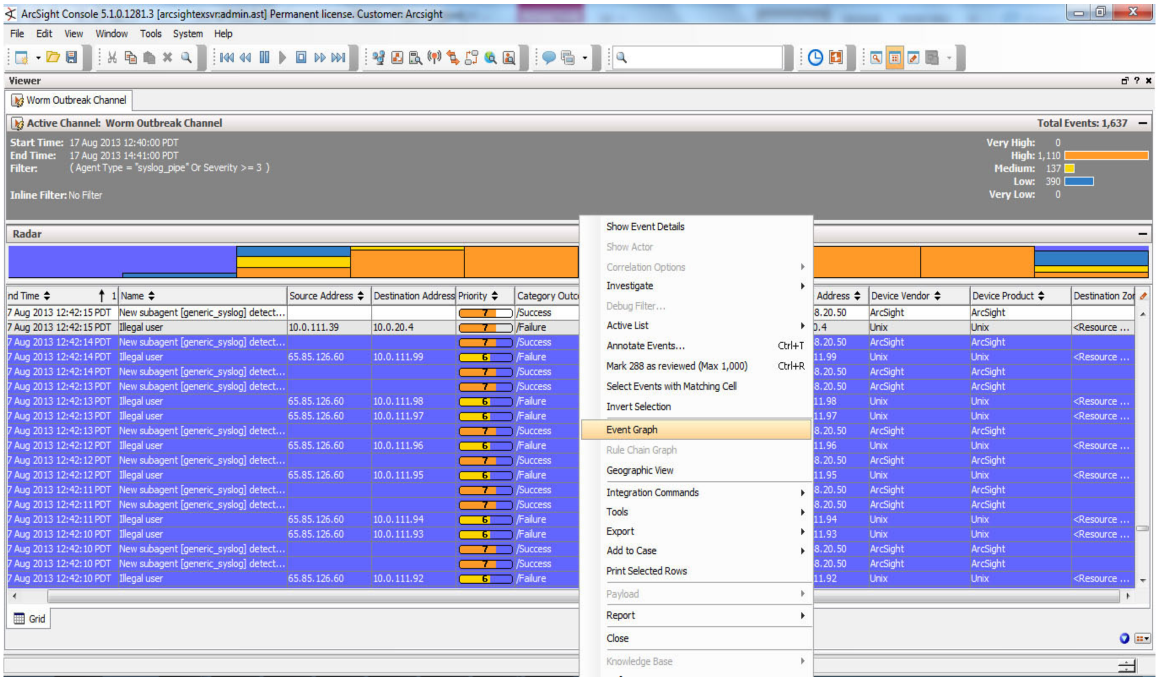
Event conditions
event1
OR
Agent Type = syslog_pipe
Severity >= 3

Name	Op	Condition
Agent Nt Domain		
Agent Severity		
Agent Translated Zone		
Agent Translated Zo...		
Agent Type	=	syslog_pipe
Agent Type		
Agent Zone		
Agent Zone ID		
Attacker		
Attacker Address		
Attacker Asset ID		
Attacker Dns Domain		
Attacker Geo Countr...		
Attacker Geo Countr...		

23] [3:37:36] 4 of the 121 fields in the selected field set for condition editor are custom fields or not supported fields that cannot be displayed.

Figure 29. “WormOutbreak” Base events in ArcSight Console.

Once all the base events have been received, ArcSight Console will be able to process the encapsulated information and display the inter-connecting network devices through its graphical resources.



Active Channel: Worm Outbreak Channel

Total Events: 1,637

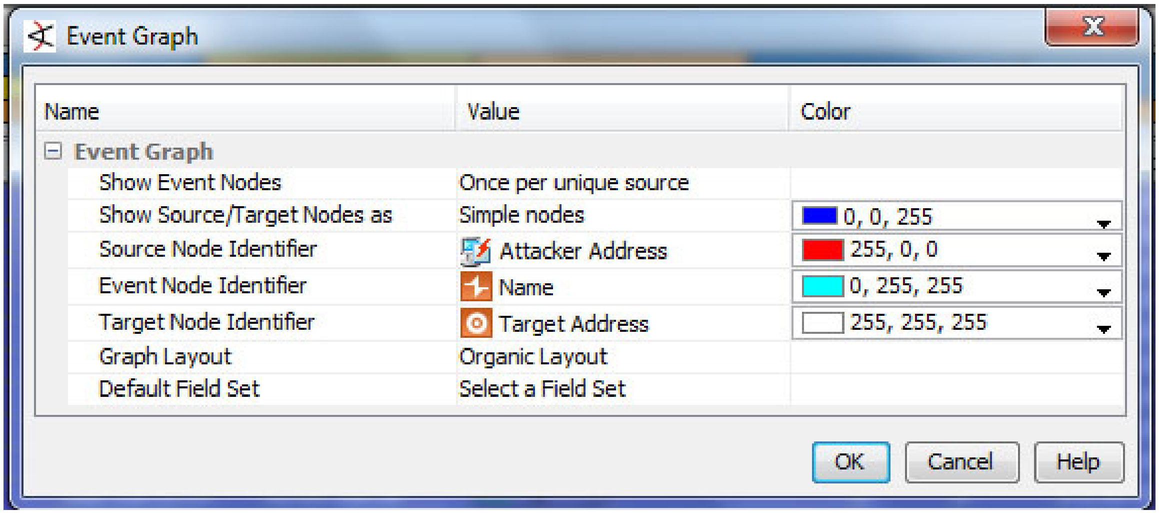
Start Time: 17 Aug 2013 12:40:00 PDT
End Time: 17 Aug 2013 14:41:00 PDT
Filter: (Agent Type = "syslog_pipe" Or Severity >= 3)

Inline Filter: No Filter

Very High: 0
High: 1,110
Medium: 137
Low: 390
Very Low: 0

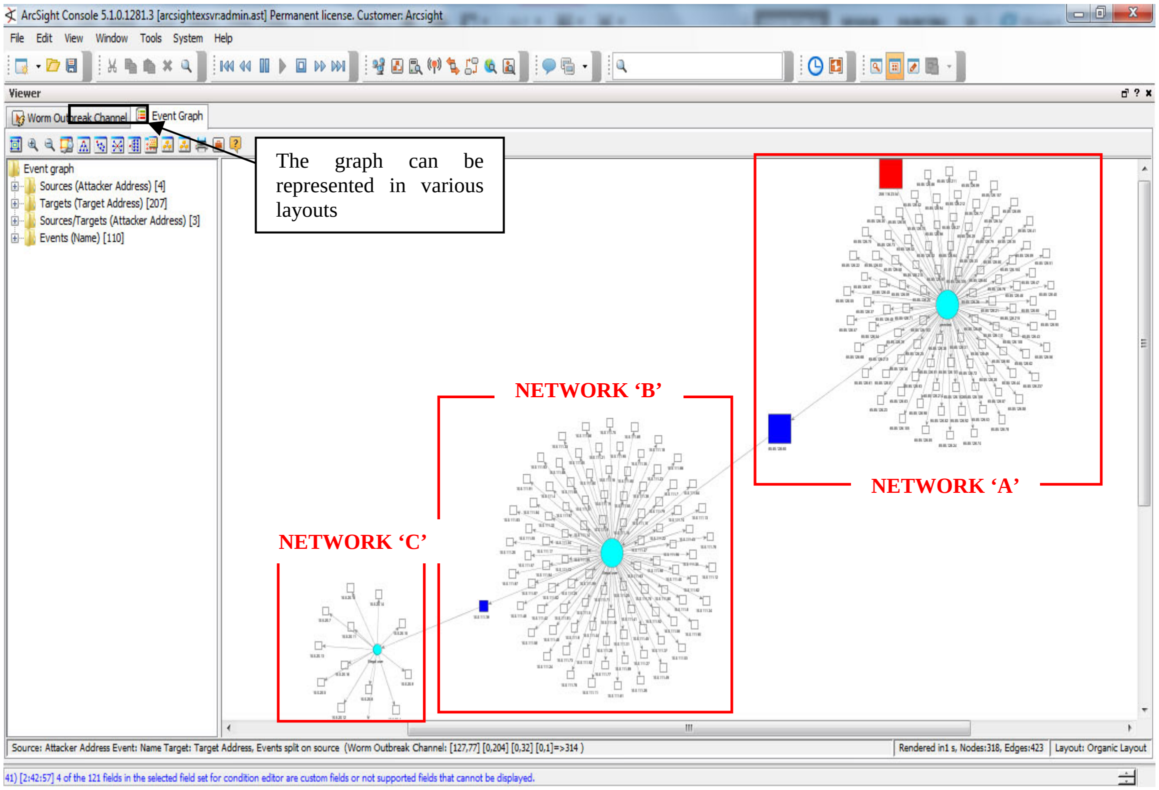
nd Time	Name	Source Address	Destination Address	Priority	Category Outc	Address	Device Vendor	Device Product	Destination Zor
7 Aug 2013 12:42:15 PDT	New subagent [generic_syslog] detect...			7	/Success	8.20.50	ArcSight	ArcSight	
7 Aug 2013 12:42:15 PDT	Illegal user	10.0.111.39	10.0.20.4	7	/Failure	0.4	Unix	Unix	<Resource ...
7 Aug 2013 12:42:14 PDT	New subagent [generic_syslog] detect...			7	/Success	8.20.50	ArcSight	ArcSight	
7 Aug 2013 12:42:14 PDT	Illegal user	65.85.126.60	10.0.111.99	6	/Failure	11.99	Unix	Unix	<Resource ...
7 Aug 2013 12:42:14 PDT	New subagent [generic_syslog] detect...			7	/Success	8.20.50	ArcSight	ArcSight	
7 Aug 2013 12:42:13 PDT	New subagent [generic_syslog] detect...			7	/Success	8.20.50	ArcSight	ArcSight	
7 Aug 2013 12:42:13 PDT	Illegal user	65.85.126.60	10.0.111.98	6	/Failure	11.98	Unix	Unix	<Resource ...
7 Aug 2013 12:42:13 PDT	Illegal user	65.85.126.60	10.0.111.97	6	/Failure	11.97	Unix	Unix	<Resource ...
7 Aug 2013 12:42:13 PDT	New subagent [generic_syslog] detect...			7	/Success	8.20.50	ArcSight	ArcSight	
7 Aug 2013 12:42:12 PDT	Illegal user	65.85.126.60	10.0.111.96	6	/Failure	11.96	Unix	Unix	<Resource ...
7 Aug 2013 12:42:12 PDT	New subagent [generic_syslog] detect...			7	/Success	8.20.50	ArcSight	ArcSight	
7 Aug 2013 12:42:12 PDT	Illegal user	65.85.126.60	10.0.111.95	6	/Failure	11.95	Unix	Unix	<Resource ...
7 Aug 2013 12:42:11 PDT	New subagent [generic_syslog] detect...			7	/Success	8.20.50	ArcSight	ArcSight	
7 Aug 2013 12:42:11 PDT	New subagent [generic_syslog] detect...			7	/Success	8.20.50	ArcSight	ArcSight	
7 Aug 2013 12:42:11 PDT	Illegal user	65.85.126.60	10.0.111.94	6	/Failure	11.94	Unix	Unix	<Resource ...
7 Aug 2013 12:42:10 PDT	Illegal user	65.85.126.60	10.0.111.93	6	/Failure	11.93	Unix	Unix	<Resource ...
7 Aug 2013 12:42:10 PDT	New subagent [generic_syslog] detect...			7	/Success	8.20.50	ArcSight	ArcSight	
7 Aug 2013 12:42:10 PDT	New subagent [generic_syslog] detect...			7	/Success	8.20.50	ArcSight	ArcSight	
7 Aug 2013 12:42:10 PDT	Illegal user	65.85.126.60	10.0.111.92	6	/Failure	11.92	Unix	Unix	<Resource ...

Figure 30. Select a subset of events and choose “Event Graph.”



Name	Value	Color
⊟ Event Graph		
Show Event Nodes	Once per unique source	
Show Source/Target Nodes as	Simple nodes	0, 0, 255
Source Node Identifier	Attacker Address	255, 0, 0
Event Node Identifier	Name	0, 255, 255
Target Node Identifier	Target Address	255, 255, 255
Graph Layout	Organic Layout	
Default Field Set	Select a Field Set	

Figure 31. Choose color code for different nodes.


ArcSight Console 5.1.0.1281.3 [arcsightexsvr:admin.ast] Permanent license. Customer: Arcsight
File Edit View Window Tools System Help
Viewer
Worm Outbreak Channel
Event Graph
Event graph
Sources (Attacker Address) [4]
Targets (Target Address) [207]
Sources/Targets (Attacker Address) [3]
Events (Name) [110]
The graph can be represented in various layouts
NETWORK 'B'
NETWORK 'A'
NETWORK 'C'

Source: Attacker Address Event: Name Target: Target Address, Events split on source (Worm Outbreak Channel: [127,77] [0,204] [0,32] [0,1]=>314)

Rendered in1 s, Nodes:318, Edges:423

Layout: Organic Layout

41) [2:42:57] 4 of the 121 fields in the selected field set for condition editor are custom fields or not supported fields that cannot be displayed.

Figure 32. Overall graph view using organic layout.

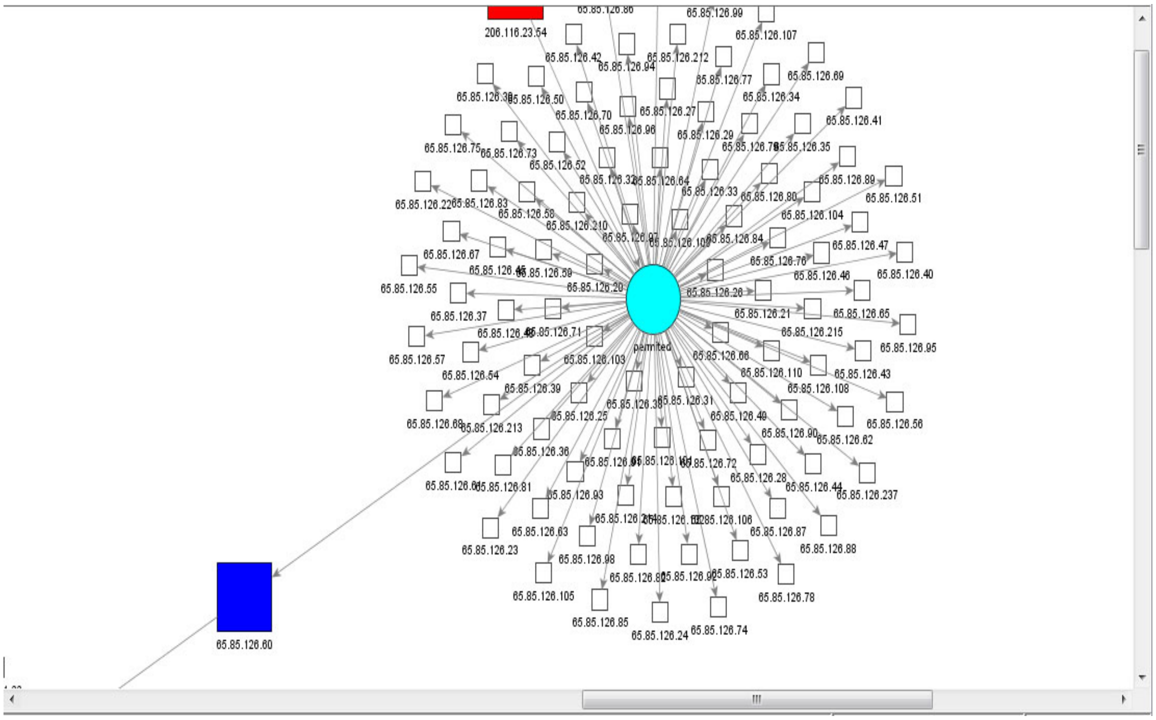


Figure 33. Zoomed in view of Network 'A.'

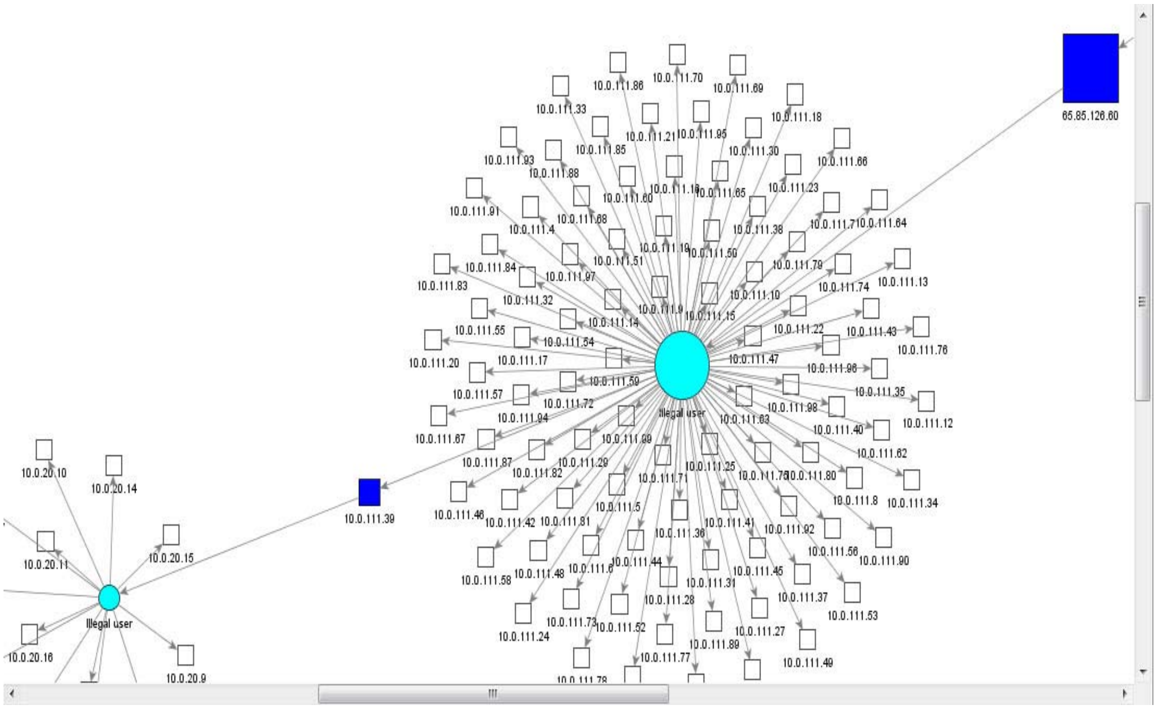
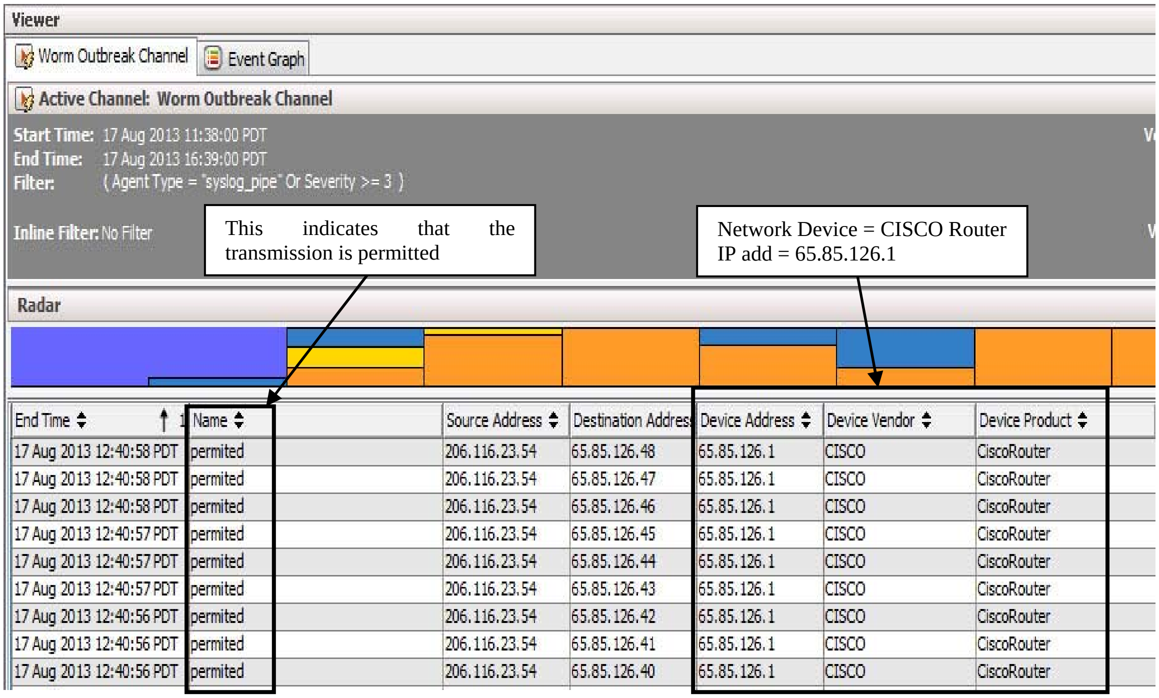


Figure 34. Zoomed in view of Network 'B' and 'C.'



Active Channel: Worm Outbreak Channel

Start Time: 17 Aug 2013 11:38:00 PDT
End Time: 17 Aug 2013 16:39:00 PDT
Filter: (Agent Type = "syslog_pipe" Or Severity >= 3)

Inline Filter: No Filter

This indicates that the transmission is permitted

Network Device = CISCO Router
IP add = 65.85.126.1

End Time	Name	Source Address	Destination Address	Device Address	Device Vendor	Device Product
17 Aug 2013 12:40:58 PDT	permited	206.116.23.54	65.85.126.48	65.85.126.1	CISCO	CiscoRouter
17 Aug 2013 12:40:58 PDT	permited	206.116.23.54	65.85.126.47	65.85.126.1	CISCO	CiscoRouter
17 Aug 2013 12:40:58 PDT	permited	206.116.23.54	65.85.126.46	65.85.126.1	CISCO	CiscoRouter
17 Aug 2013 12:40:57 PDT	permited	206.116.23.54	65.85.126.45	65.85.126.1	CISCO	CiscoRouter
17 Aug 2013 12:40:57 PDT	permited	206.116.23.54	65.85.126.44	65.85.126.1	CISCO	CiscoRouter
17 Aug 2013 12:40:57 PDT	permited	206.116.23.54	65.85.126.43	65.85.126.1	CISCO	CiscoRouter
17 Aug 2013 12:40:56 PDT	permited	206.116.23.54	65.85.126.42	65.85.126.1	CISCO	CiscoRouter
17 Aug 2013 12:40:56 PDT	permited	206.116.23.54	65.85.126.41	65.85.126.1	CISCO	CiscoRouter
17 Aug 2013 12:40:56 PDT	permited	206.116.23.54	65.85.126.40	65.85.126.1	CISCO	CiscoRouter

Figure 35. IP address of network device.

Figures 32, 33, and 34 show the inter-connecting networks. The white, blue and red boxes represent the hosts, while the arrow lines indicate the transmission flow direction between the hosts. From the figures, you can see that a series of transmissions have been initiated by different hosts in the following order:

- Public host (IP address = 206.116.23.54) to public hosts in Network ‘A’ (65.85.126.x). Transmission is permitted as indicated in Figure 35.
- Public host in Network ‘A’ (IP address = 65.85.126.60) to private hosts in Network ‘B’ (10.0.111.0).
- Private host in Network ‘B’ (IP address = 10.0.111.39) to private hosts in Network ‘C’ (10.0.20.x).

Network ‘B’ and Network ‘C’ are private networks because they contain IP addresses that belong to the private address space as defined in RFC1918. With this analysis, the above transmission trend can be interpreted as a typical traffic flow that usually happens when an external host attempts to communicate with an internal host that is secured within a DMZ. For this case, the situation can be translated to the training scenario as such:

- A “foreign” (not part of SporeFusion) host on the Internet (IP address = 206.116.23.54) has sent an email containing a computer worm to an email relay server (IP address = 65.85.126.60) hosted by “SporeFusion.com.” This email relay server lies in SporeFusion’s DMZ zone, Network ‘A’, and is responsible for relaying emails from external networks to internal networks and vice versa.
- The computer worm infected the email relay server, causing the mass sending of emails to other hosts within SporeFusion’s internal (in relation to the DMZ) network, Network ‘B’ (10.0.111.x).
- One of the hosts (IP address = 10.0.111.39) is infected by the computer worm and in turn forwards the mail to the hosts within another internal network, Network ‘C.’
- From Figure 35, the Cisco router (IP address = 65.85.126.1) is the firewall that implements the DMZ and separates the internal and external networks.

Using the above information, the network topology of the subset events can then be constructed as shown in Figure 36. .

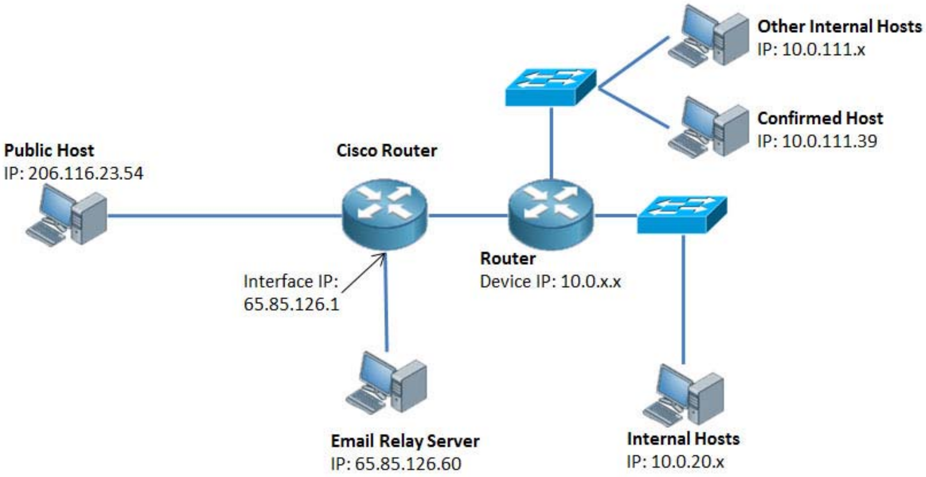
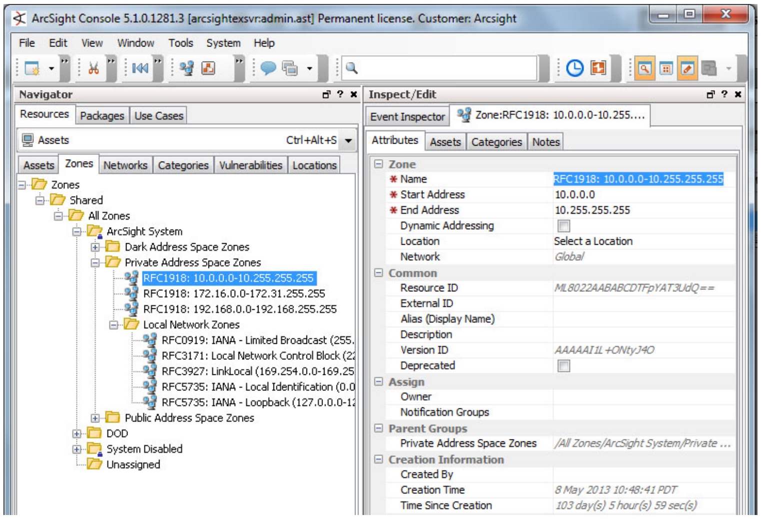


Figure 36. Simplified Network Topology.

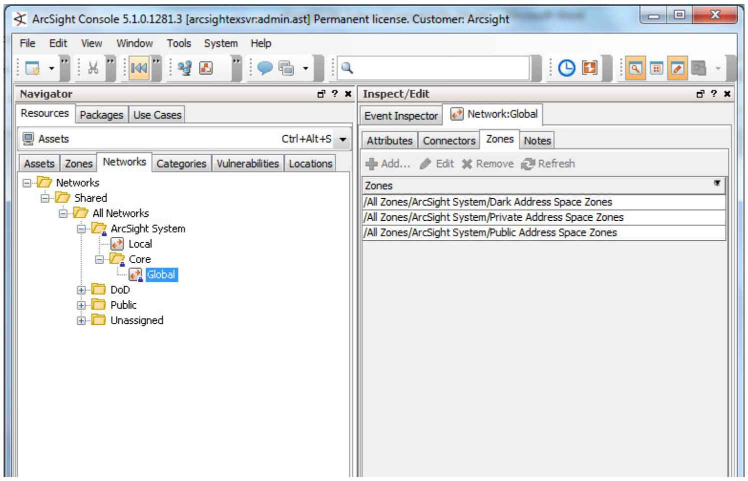
SIEM operators can now begin to follow through the workflow structure as described in Chapter III by starting with key asset identification. Supposedly, the finance manager of the "SporeFusion.com" organization is given a personal computer (IP address = 10.0.111.39) to carry out his/her work routine. The computer contains a lot of confidential information pertaining to the financial health of the organization and is therefore identified as a key asset. ArcSight has preemptively modeled the private network space (IP address = 10.x.x.x) into the Zone and Network models using the globalized Internet standards (e.g., RFC1918), as shown in the following figures:


ArcSight Console 5.1.0.1281.3 [arcsightexsvr:admin.ast] Permanent license. Customer: Arcsight
File Edit View Window Tools System Help
Navigator
Resources Packages Use Cases
Assets Ctrl+Alt+S
Assets Zones Networks Categories Vulnerabilities Locations
Inspect/Edit
Event Inspector Zone:RFC1918: 10.0.0.0-10.255....
Attributes Assets Categories Notes

```
Zones
  Shared
    All Zones
      ArcSight System
        Dark Address Space Zones
        Private Address Space Zones
          RFC1918: 10.0.0.0-10.255.255.255
          RFC1918: 172.16.0.0-172.31.255.255
          RFC1918: 192.168.0.0-192.168.255.255
          Local Network Zones
            RFC0919: IANA - Limited Broadcast (255.
            RFC3171: Local Network Control Block (2
            RFC3927: LinkLocal (169.254.0.0-169.25
            RFC5735: IANA - Local Identification (0.0
            RFC5735: IANA - Loopback (127.0.0.0-1
        Public Address Space Zones
      DOD
      System Disabled
      Unassigned
```

Zone	
* Name	RFC1918: 10.0.0.0-10.255.255.255
* Start Address	10.0.0.0
* End Address	10.255.255.255
Dynamic Addressing	□
Location	Select a Location
Network	Global
Common	
Resource ID	ML8022AABABCDTFpYAT3UdQ==
External ID	
Alias (Display Name)	
Description	
Version ID	AAAAAI1L+ONtyJ4O
Deprecated	□
Assign	
Owner	
Notification Groups	
Parent Groups	
Private Address Space Zones	/All Zones/ArcSight System/Private ...
Creation Information	
Created By	
Creation Time	8 May 2013 10:48:41 PDT
Time Since Creation	103 day(s) 5 hour(s) 59 sec(s)

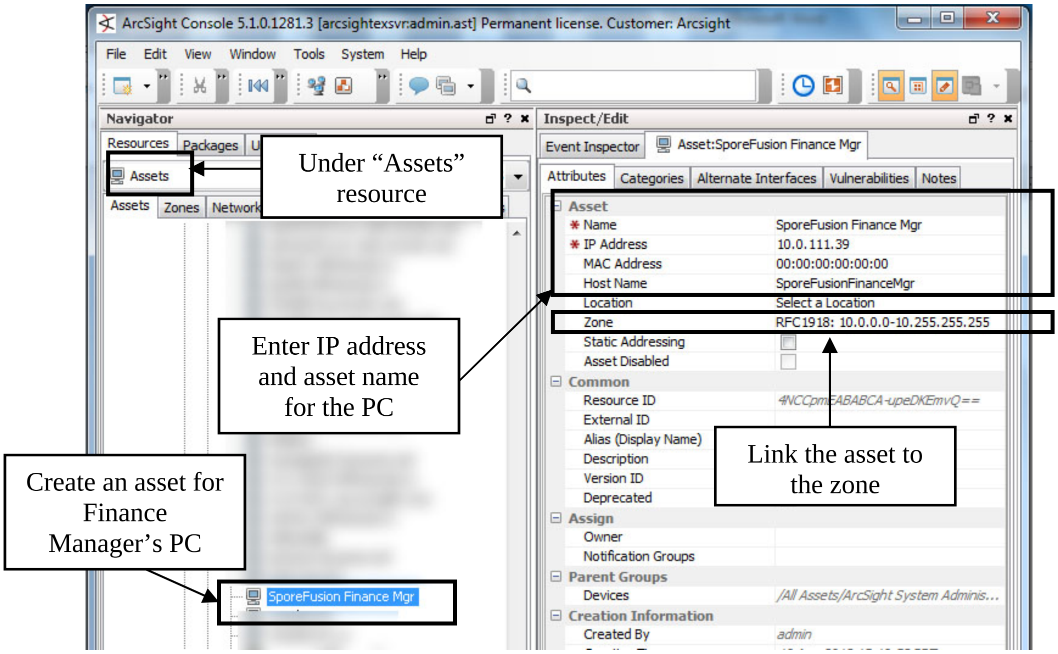
Figure 37. Zone Model.


ArcSight Console 5.1.0.1281.3 [arcsightexsvr:admin.ast] Permanent license. Customer: Arcsight
File Edit View Window Tools System Help
Navigator
Resources Packages Use Cases
Assets Ctrl+Alt+S
Assets Zones Networks Categories Vulnerabilities Locations
Networks
Shared
All Networks
ArcSight System
Local
Core
Global
DoD
Public
Unassigned
Inspect/Edit
Event Inspector
Network:Global
Attributes Connectors Zones Notes
Add... Edit Remove Refresh

Zones
/All Zones/ArcSight System/Dark Address Space Zones
/All Zones/ArcSight System/Private Address Space Zones
/All Zones/ArcSight System/Public Address Space Zones

Figure 38. Network Model.

With the network models already available (as per the original networks from which the replay traffic was collected), the SIEM operators will only have to create the asset model for the personal computer that belongs to the Finance Manager and link it to the zone. ArcSight has provided a "System Asset Category" that helps to define the importance of the asset in the perspective of the organization. Since the personal computer is a key asset to the organization, it will be tagged with "very high" criticality.


ArcSight Console 5.1.0.1281.3 [arcsightexsvr:admin.ast] Permanent license. Customer: Arcsight
File Edit View Window Tools System Help
Navigator
Resources Packages U
Assets
Assets Zones Network
SporeFusion Finance Mgr
Inspect/Edit
Event Inspector
Asset:SporeFusion Finance Mgr
Attributes Categories Alternate Interfaces Vulnerabilities Notes

Asset	
* Name	SporeFusion Finance Mgr
* IP Address	10.0.111.39
MAC Address	00:00:00:00:00:00
Host Name	SporeFusionFinanceMgr
Location	Select a Location
Zone	RFC1918: 10.0.0.0-10.255.255.255
Static Addressing	□
Asset Disabled	□
Common	
Resource ID	4NCCpmEABABCA-upeDKEmvQ==
External ID	
Alias (Display Name)	
Description	
Version ID	
Deprecated	
Assign	
Owner	
Notification Groups	
Parent Groups	
Devices	/All Assets/ArcSight System Adminis...
Creation Information	
Created By	admin

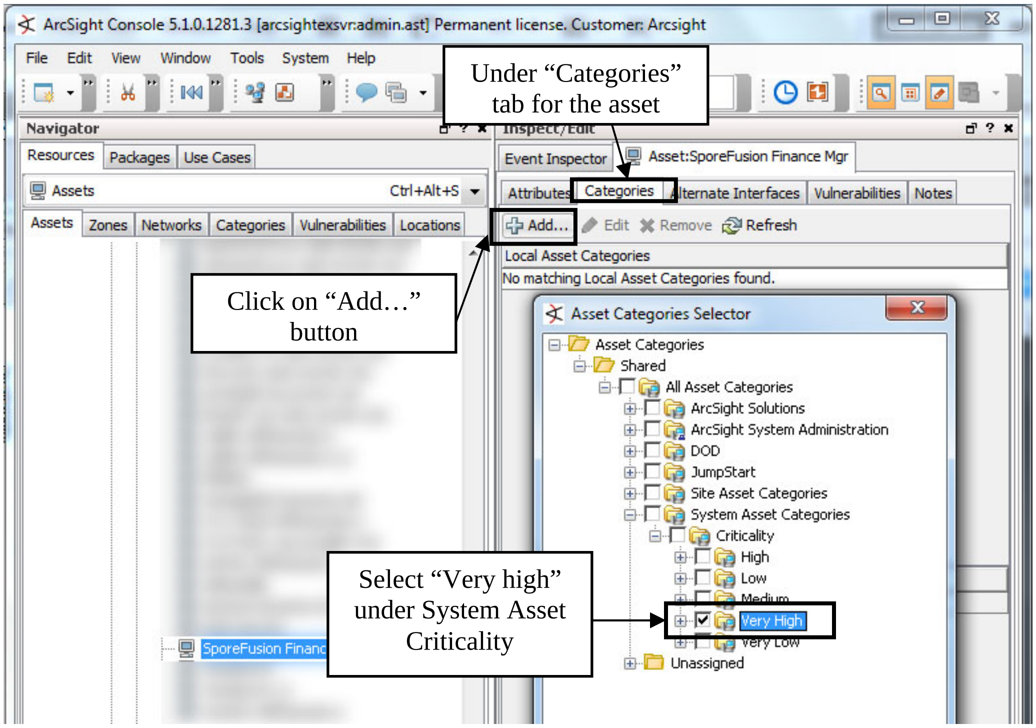
Under "Assets" resource

Enter IP address and asset name for the PC

Link the asset to the zone

Create an asset for Finance Manager's PC

Figure 39. Create asset model step 1.



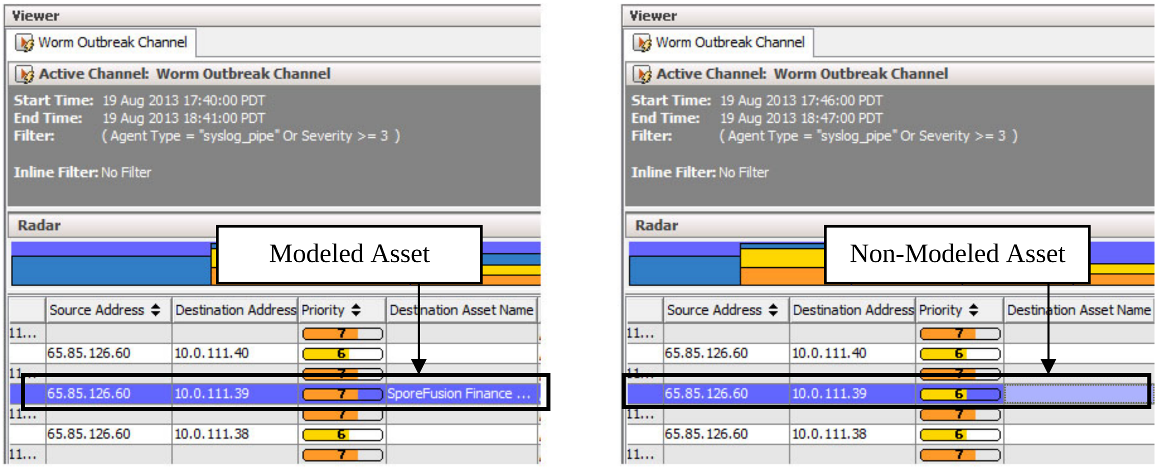
Under "Categories" tab for the asset

Click on "Add…" button

Select "Very high" under System Asset Criticality

Figure 40. Create asset model step 2.

By creating an asset model for the personal computer, ArcSight Express will now be able to analyze the asset with greater detail and provide a better threat level evaluation, which contributes to event priority determination. Figure 41 illustrates how this added asset characterization contributes to the situational awareness of the operator.



Active Channel: Worm Outbreak Channel
Start Time: 19 Aug 2013 17:40:00 PDT
End Time: 19 Aug 2013 18:41:00 PDT
Filter: (Agent Type = "syslog_pipe" Or Severity >= 3)

Inline Filter: No Filter

Modeled Asset

	Source Address	Destination Address	Priority	Destination Asset Name
11...			7	
	65.85.126.60	10.0.111.40	6	
11...			7	
	65.85.126.60	10.0.111.39	7	SporeFusion Finance ...
11...			7	
	65.85.126.60	10.0.111.38	6	
11...			7	

Active Channel: Worm Outbreak Channel
Start Time: 19 Aug 2013 17:46:00 PDT
End Time: 19 Aug 2013 18:47:00 PDT
Filter: (Agent Type = "syslog_pipe" Or Severity >= 3)

Inline Filter: No Filter

Non-Modeled Asset

	Source Address	Destination Address	Priority	Destination Asset Name
11...			7	
	65.85.126.60	10.0.111.40	6	
11...			7	
	65.85.126.60	10.0.111.39	6	
11...			7	
	65.85.126.60	10.0.111.38	6	
11...			7	

Figure 41. Priority level difference for modeled and non-modeled asset.

E. PHASE 4 - ASSOCIATE WORM BEHAVIOR

With the fundamental information gathered in Phase 1, Phase 4 will focus on associating the following:

- The worm’s behavior with the parameters of the event schema.
- The communication pattern of a worm outbreak.

Computer worms usually originate from a single host and attempt to spread to other hosts in the same network. Based on this, the “Source IP address,” “Destination IP address,” “Port” and “Zone Name” serve as good candidate cueing parameters to track the spreading effect. Other than those IP addresses, the ArcSight ESM also introduced two more virtual parameters, “Attack IP Address” and “Target IP address,” that can be used to identify a worm’s infected source and target destination. The reason for introducing the additional parameters can be explained as such: A Network Intrusion Detection System (NIDS) has reported attacks from A (e.g., hacker) to B (e.g., server). In this normal case, the “Source” and “Attacker” will hold the same value, while the “Destination” will correspond to “Target.” However, if information were to flow from the server to the hacker (e.g., password file is downloaded by the hacker from the server), the base event will report this case as “Source” = “Attacker” = B, and “Destination” = “Target” = A. This means that the server has become the “Attacker” while the hacker has become the “Target,” which is obviously not true. To rectify such situations, the “Originator” parameter within the event schema can be configured accordingly to ensure that “Attacker” and “Target” are pointing to the correct hacker and server, respectively. As explained, both the “Attacker” and “Target” parameters provide better clarity in threat identification. Henceforth, the rules-writing covered in the next phase will cue on these two parameters rather than using the “Source” and “Destination” parameters.

In addition, the worm’s transmission pattern also suggests a “one-to-many” communication pattern, which can be translated to the possibility of a network sweep occurrence, whereby an infected host will attempt to communicate with multiple, perhaps consecutive IP addresses, hosts within the same network. This pattern provides another threat behavior that ArcSight can be configured (via a correlation rule) to cue off of.

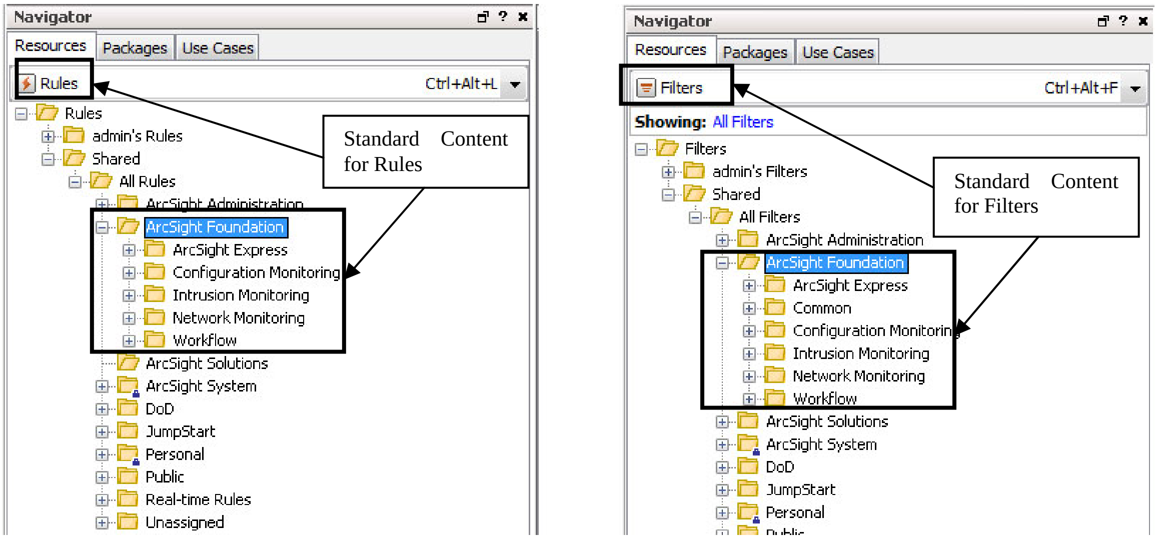
With the above assumptions, the association result is summarized in Table 2.

S/N	WORM INFORMATION	ASSOCIATED PARAMETERS	ASSOCIATED PATTERNS
1	It usually originates from a single host.	- “Attacker” & “Target” IP Addresses, Port and Zone - “Attacker” & “Target” Port - “Attacker” & “Target” Zone	-
2	It has the ability to self-replicate.	-	- Internal network sweep - Outbound network sweep

Table 2. Worm association table.

F. PHASE 5 – CONFIGURE RULES

Prior to writing new rules for the worm outbreak scenario, it is important to know that ArcSight ESM provides a Standard Content package that comes pre-installed within the ArcSight Console (Figure 42). There are a series of “out-of-the-box” resources (e.g., filters, rules and dashboards) that address common security and management tasks and that are designed to help new users quickly deploy ArcSight [10].



Standard Content for Rules

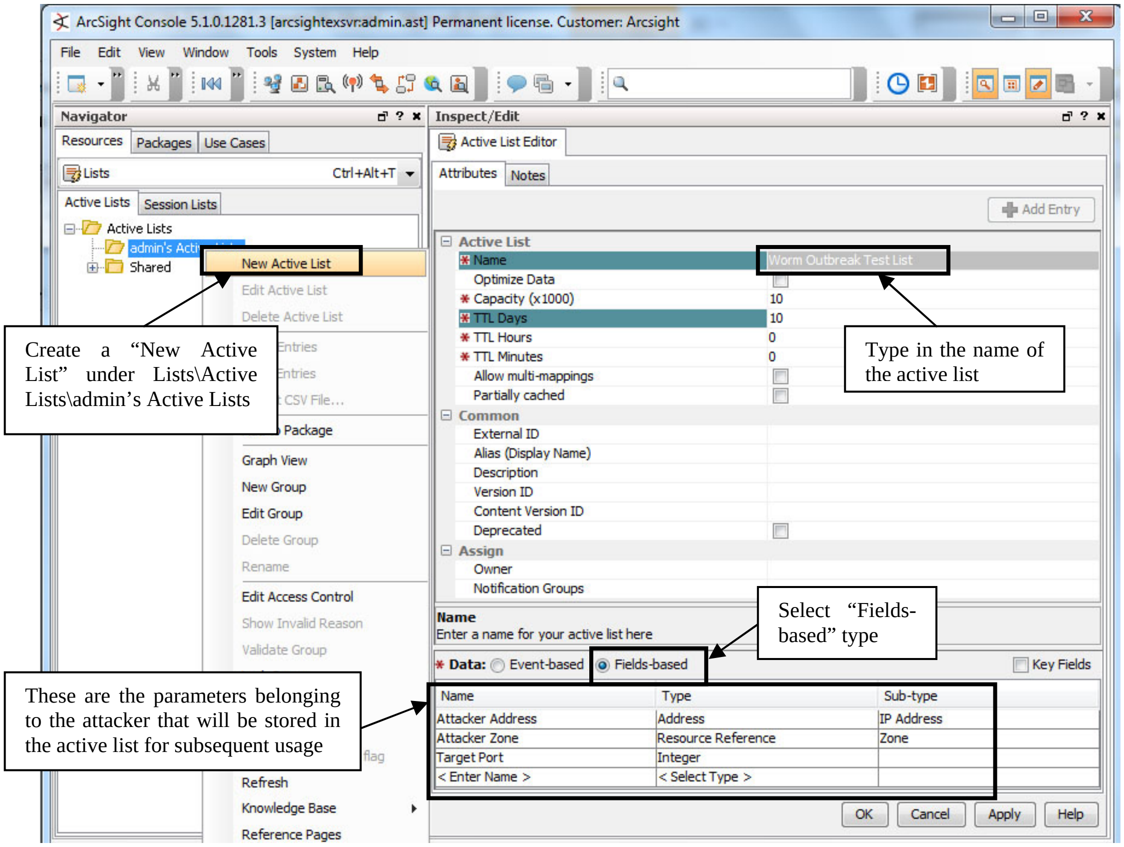
Standard Content for Filters

Figure 42. Standard Content for rules and filters.

In this phase, some of the resources in the Standard Content will be utilized and explained. With an understanding on how these resources perform, SIEM operators will be able to leverage the given resources to either *modify* (improve) existing rules or create *new* rules that may be much better tailored to the operator’s own network/system environment. The following sections illustrate the steps to create a rule.

1. Step 1 – Create “Worm Outbreak Test List” Active List

As mentioned earlier, an active list can be used as a kind of ad hoc “bulletin board” to specify fields of event data for correlation or monitoring purposes. For this scenario, an active list called “Worm Outbreak Test List” (Figure 43) will be created to hold the information of the internal infected hosts once the worm outbreak detection rules have been triggered. This active list will be useful for the next phase.



ArcSight Console 5.1.0.1281.3 [arcsightexsvr:admin.ast] Permanent license. Customer: Arcsight

Active List	
* Name	Worm Outbreak Test List
Optimize Data	□
* Capacity (x1000)	10
* TTL Days	10
* TTL Hours	0
* TTL Minutes	0
Allow multi-mappings	□
Partially cached	□
Common	
External ID	
Alias (Display Name)	
Description	
Version ID	
Content Version ID	
Deprecated	□
Assign	
Owner	
Notification Groups	

Name
Enter a name for your active list here

* **Data:** ○ Event-based ● Fields-based □ Key Fields

Name	Type	Sub-type
Attacker Address	Address	IP Address
Attacker Zone	Resource Reference	Zone
Target Port	Integer	
< Enter Name >	< Select Type >	

Create a “New Active List” under Lists\Active Lists\admin’s Active Lists

Type in the name of the active list

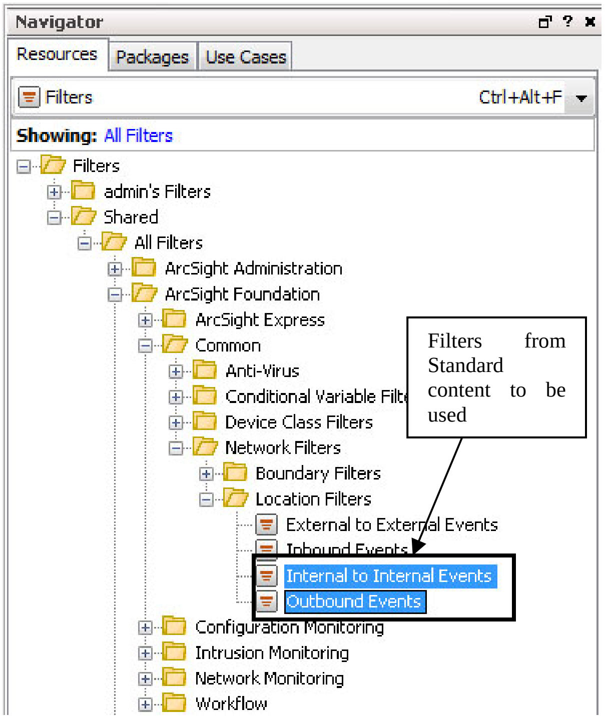
Select “Fields-based” type

These are the parameters belonging to the attacker that will be stored in the active list for subsequent usage

Figure 43. Create “Worm Outbreak Test List” Active List.

2. Step 2 – Create “Worm Outbreak Test Rule”

This is the main rule that will be responsible for correlating the base events and detecting the presence of any worm-infected hosts. SIEM operators would create the rule using the associated parameters identified previously. For ease of configuration, the existing filters “Internal to Internal Events” and “Outbound Events” (Figure 44) from the Standard Content will be utilized to identify the associated patterns in this rule. Both filters are meant to track events that flow from a private network (e.g., 10.0.x.x) to another private network or external (and non-private) network.



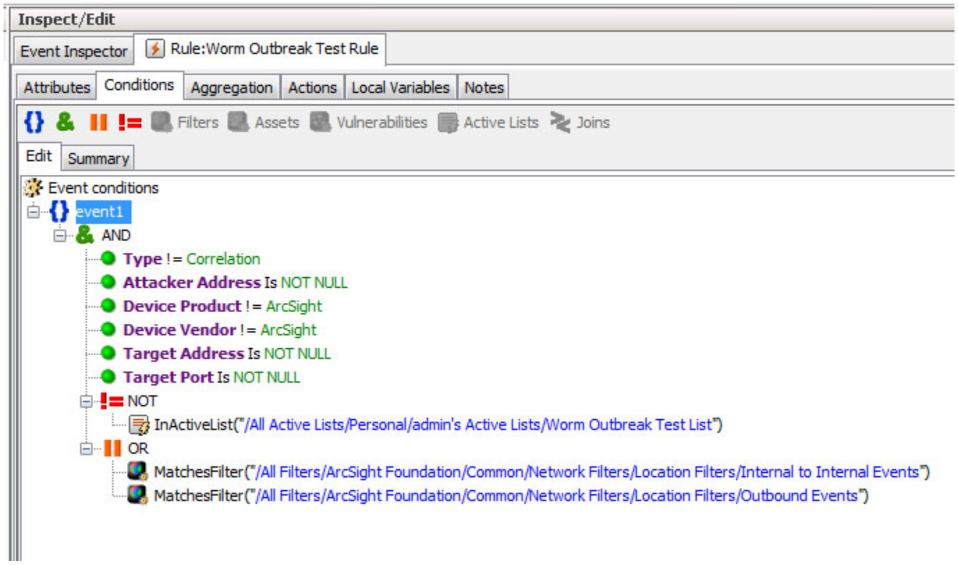
Filters from Standard content to be used

Figure 44. Filters from Standard content.

The detection rule will be created to look for a single host trying to communicate with at least 10 other hosts on the same target port within a given network within one minute. To achieve this, the logical configuration to correlate the base events is as such:

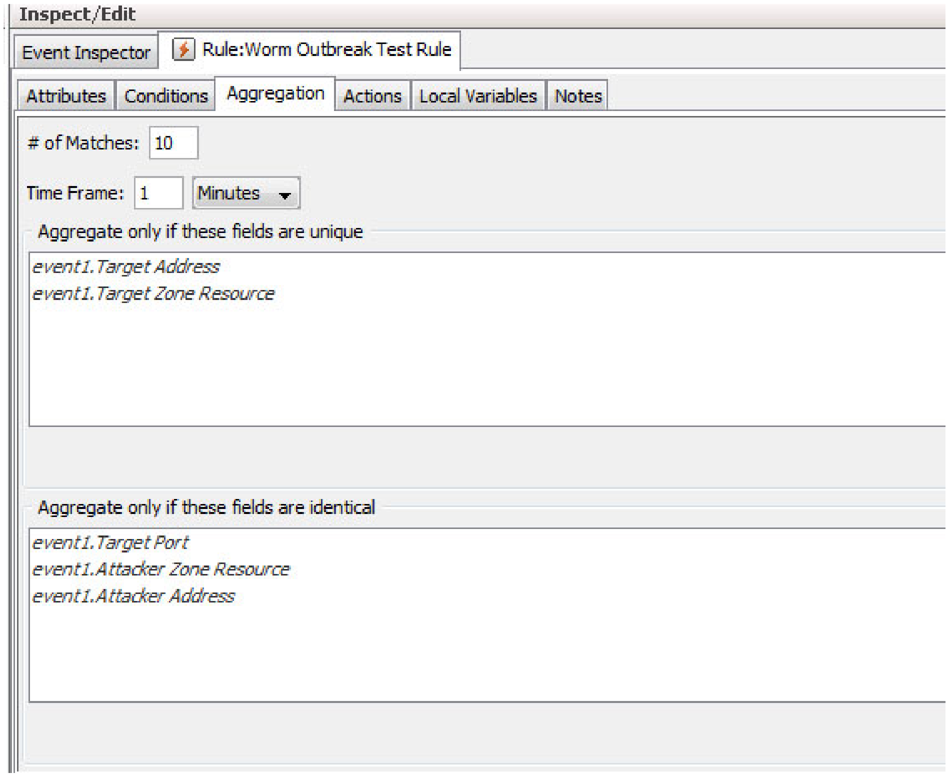
LOGICAL CONFIGURATION	COMPARISON & ACTIONS
Conditions (Figure 45.)	Every base event shall be checked and ensured that: • the associated parameters contain a certain value(s) for comparison, and… • the correlated event does not already exist in the active list, and… • the traffic mimics a network sweep pattern (e.g., Internal to Internal or outbound network sweep).
Aggregation (Figure 46.)	Correlate 10 base events if its: • “Attacker” IP address and zone and “Target” port remains the same, or… • “Target” IP address and zone is unique.
Actions (Figure 47.)	If the conditions are met, and the aggregation minimum is reached, the applicable base events will be considered “correlated” to worm attack behavior, and these actions will be taken: • Add the “Attacker” IP address and zone and “Target” port to the active list (if not already in the list). • Set the “Priority” to 10. • Set the “Category” parameters to be worm-related.

Table 3. Logical Configuration for “Worm Outbreak Detection Test Rule.”



```
Event conditions
event1
  AND
    Type != Correlation
    Attacker Address Is NOT NULL
    Device Product != ArcSight
    Device Vendor != ArcSight
    Target Address Is NOT NULL
    Target Port Is NOT NULL
    NOT
      InActiveList("/All Active Lists/Personal/admin's Active Lists/Worm Outbreak Test List")
    OR
      MatchesFilter("/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/Internal to Internal Events")
      MatchesFilter("/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/Outbound Events")
```

Figure 45. Worm outbreak detection conditions.



# of Matches: 10

Time Frame: 1 Minutes

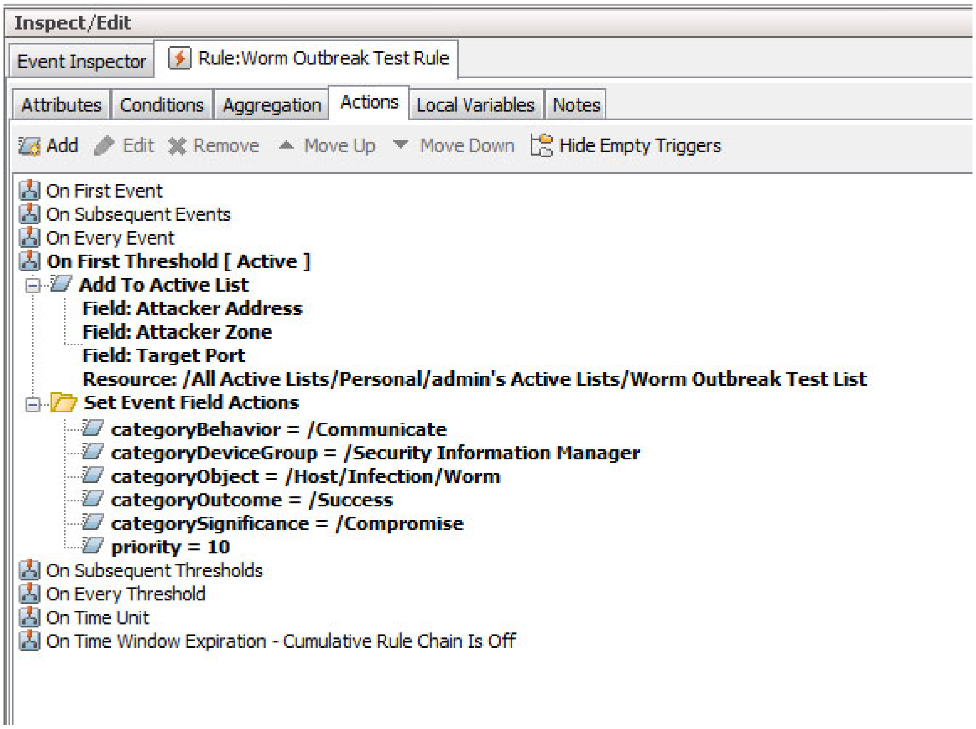
Aggregate only if these fields are unique

event1.Target Address
event1.Target Zone Resource

Aggregate only if these fields are identical

event1.Target Port
event1.Attacker Zone Resource
event1.Attacker Address

Figure 46. Worm outbreak detection aggregation.

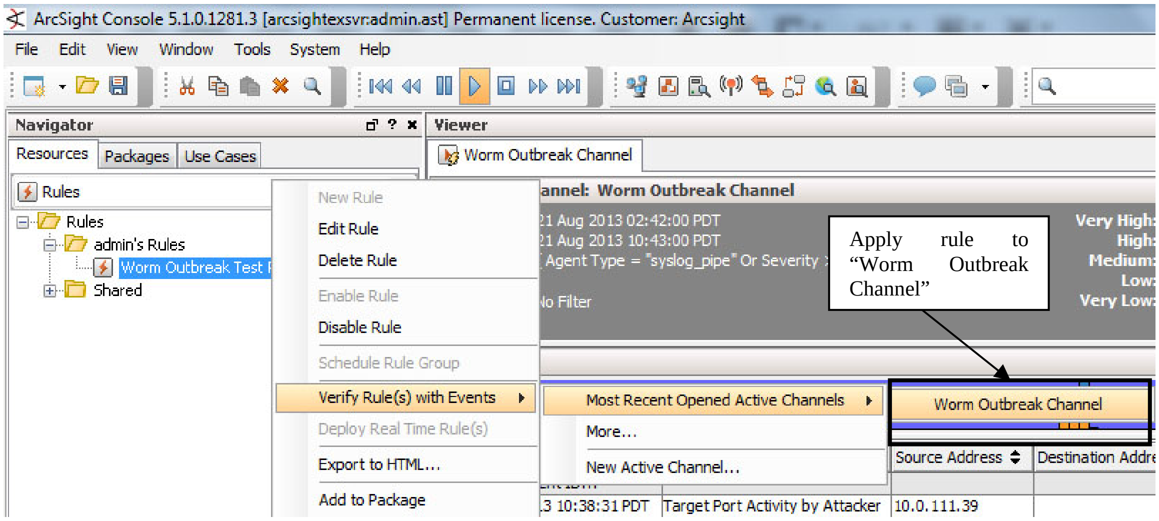


- On First Event
- On Subsequent Events
- On Every Event
- **On First Threshold [Active]**
  - **Add To Active List**
    - **Field: Attacker Address**
    - **Field: Attacker Zone**
    - **Field: Target Port**
    - **Resource: /All Active Lists/Personal/admin's Active Lists/Worm Outbreak Test List**
  - **Set Event Field Actions**
    - **categoryBehavior = /Communicate**
    - **categoryDeviceGroup = /Security Information Manager**
    - **categoryObject = /Host/Infection/Worm**
    - **categoryOutcome = /Success**
    - **categorySignificance = /Compromise**
    - **priority = 10**
- On Subsequent Thresholds
- On Every Threshold
- On Time Unit
- On Time Window Expiration - Cumulative Rule Chain Is Off

Figure 47. Worm outbreak detection actions.

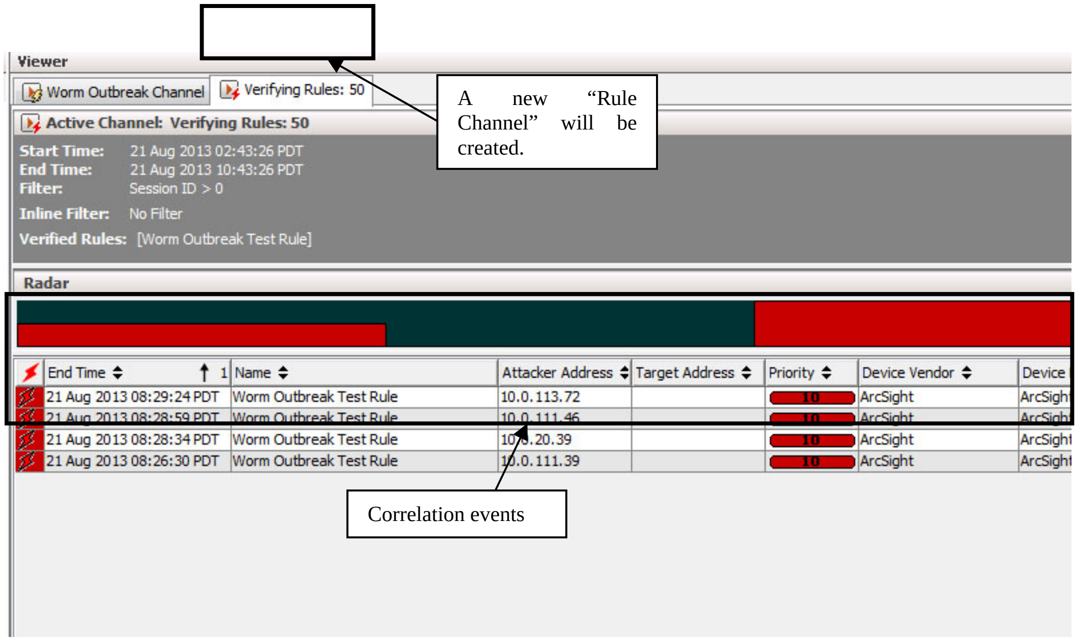
3. Step 3 – Test rule in "Rules Channel"

After the rule has been created, the SIEM operator can test the rule using the "Rules Channel." This channel allows the rules to be imposed on a fixed time window with historical events and prevents any conflicts made to the real-time rules deployed for the "Live Channel." A SIEM operator will usually undergo a few iterations of trial-and-error in steps 2 and 3 prior to obtaining the desired result. The following shows the expected (desired) result:



Apply rule to "Worm Outbreak Channel"

Figure 48. Verify newly created rule.



Start Time: 21 Aug 2013 02:43:26 PDT
End Time: 21 Aug 2013 10:43:26 PDT
Filter: Session ID > 0
Inline Filter: No Filter
Verified Rules: [Worm Outbreak Test Rule]

	End Time	Name	Attacker Address	Target Address	Priority	Device Vendor	Device
	21 Aug 2013 08:29:24 PDT	Worm Outbreak Test Rule	10.0.113.72		10	ArcSight	ArcSigh
	21 Aug 2013 08:28:59 PDT	Worm Outbreak Test Rule	10.0.111.46		10	ArcSight	ArcSigh
	21 Aug 2013 08:28:34 PDT	Worm Outbreak Test Rule	10.0.20.39		10	ArcSight	ArcSigh
	21 Aug 2013 08:26:30 PDT	Worm Outbreak Test Rule	10.0.111.39		10	ArcSight	ArcSigh

A new "Rule Channel" will be created.

Correlation events

Figure 49. Correlation events from rule.

4. Step 4 – Apply rule to "Live Channel"

Once the rule has been verified to be working, the next step will be to apply the rule to the "Live Channel" as follows (Figures 50 and 51).

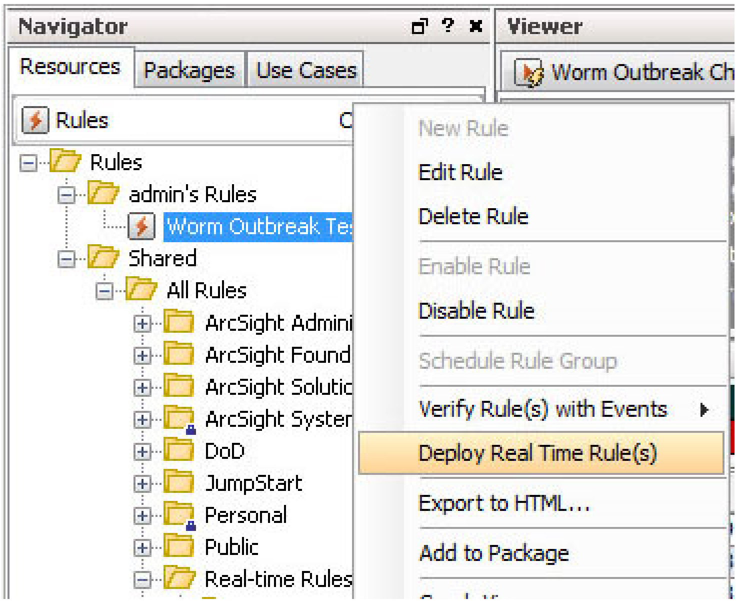


Figure 50. Deploy Real-time rule.

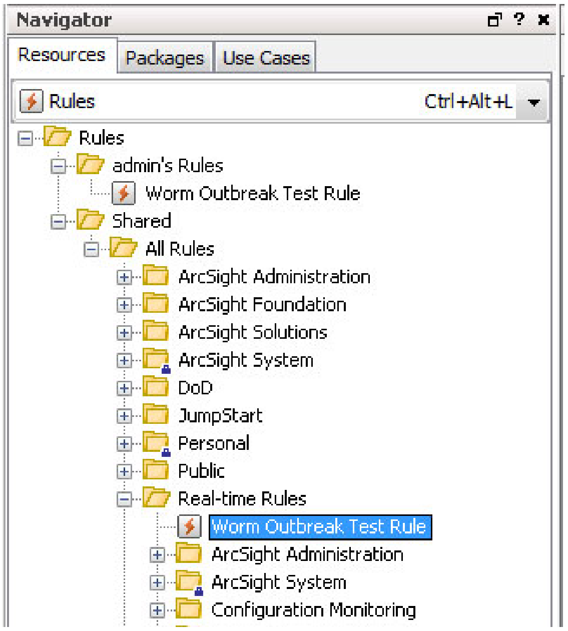
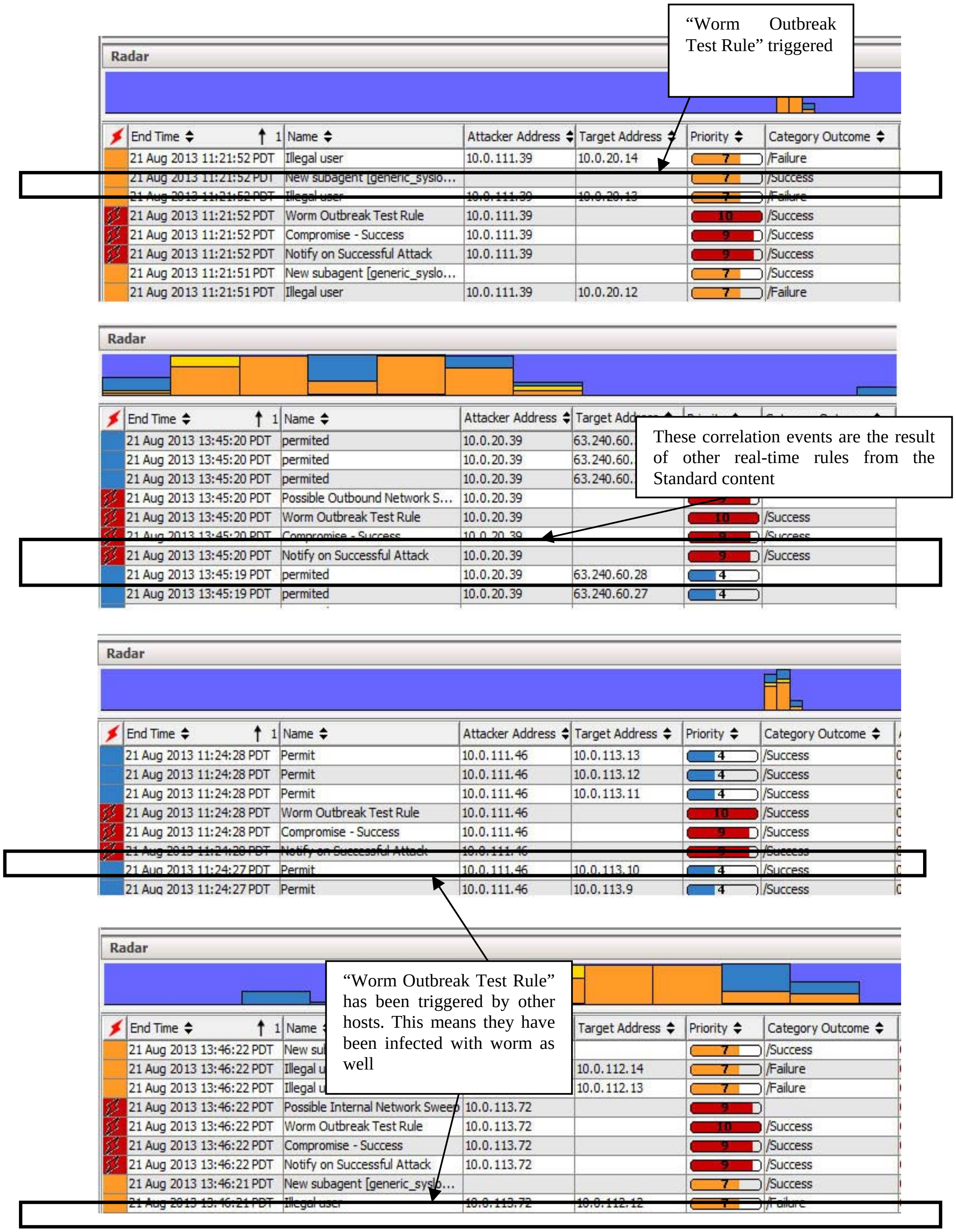


Figure 51. "Worm Outbreak Test Rule" in "Real-time Rules" folder.

With the rule deployed to the "Real-time Rules" folder, all the replay events from the replay connector will now be examined to detect the presence of internal worm-infected hosts. The expected results are as such:



"Worm Outbreak Test Rule" triggered

	End Time	Name	Attacker Address	Target Address	Priority	Category Outcome
	21 Aug 2013 11:21:52 PDT	Illegal user	10.0.111.39	10.0.20.14	7	/Failure
	21 Aug 2013 11:21:52 PDT	New subagent [generic_syslo...			7	/Success
	21 Aug 2013 11:21:52 PDT	Illegal user	10.0.111.39	10.0.20.13	7	/Failure
	21 Aug 2013 11:21:52 PDT	Worm Outbreak Test Rule	10.0.111.39		10	/Success
	21 Aug 2013 11:21:52 PDT	Compromise - Success	10.0.111.39		9	/Success
	21 Aug 2013 11:21:52 PDT	Notify on Successful Attack	10.0.111.39		9	/Success
	21 Aug 2013 11:21:51 PDT	New subagent [generic_syslo...			7	/Success
	21 Aug 2013 11:21:51 PDT	Illegal user	10.0.111.39	10.0.20.12	7	/Failure

These correlation events are the result of other real-time rules from the Standard content

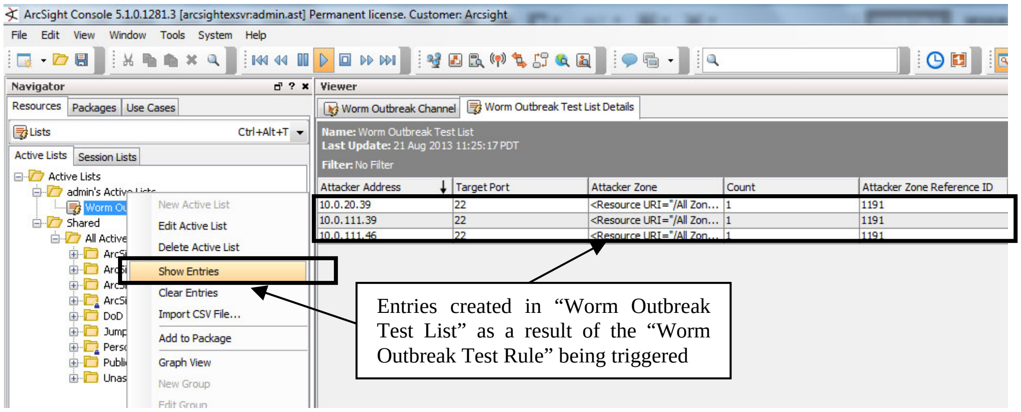
	End Time	Name	Attacker Address	Target Add		
	21 Aug 2013 13:45:20 PDT	permited	10.0.20.39	63.240.60.		
	21 Aug 2013 13:45:20 PDT	permited	10.0.20.39	63.240.60.		
	21 Aug 2013 13:45:20 PDT	permited	10.0.20.39	63.240.60.		
	21 Aug 2013 13:45:20 PDT	Possible Outbound Network S...	10.0.20.39			
	21 Aug 2013 13:45:20 PDT	Worm Outbreak Test Rule	10.0.20.39		10	/Success
	21 Aug 2013 13:45:20 PDT	Compromise - Success	10.0.20.39		9	/Success
	21 Aug 2013 13:45:20 PDT	Notify on Successful Attack	10.0.20.39		9	/Success
	21 Aug 2013 13:45:19 PDT	permited	10.0.20.39	63.240.60.28	4	
	21 Aug 2013 13:45:19 PDT	permited	10.0.20.39	63.240.60.27	4	

	End Time	Name	Attacker Address	Target Address	Priority	Category Outcome
	21 Aug 2013 11:24:28 PDT	Permit	10.0.111.46	10.0.113.13	4	/Success
	21 Aug 2013 11:24:28 PDT	Permit	10.0.111.46	10.0.113.12	4	/Success
	21 Aug 2013 11:24:28 PDT	Permit	10.0.111.46	10.0.113.11	4	/Success
	21 Aug 2013 11:24:28 PDT	Worm Outbreak Test Rule	10.0.111.46		10	/Success
	21 Aug 2013 11:24:28 PDT	Compromise - Success	10.0.111.46		9	/Success
	21 Aug 2013 11:24:28 PDT	Notify on Successful Attack	10.0.111.46		9	/Success
	21 Aug 2013 11:24:27 PDT	Permit	10.0.111.46	10.0.113.10	4	/Success
	21 Aug 2013 11:24:27 PDT	Permit	10.0.111.46	10.0.113.9	4	/Success

"Worm Outbreak Test Rule" has been triggered by other hosts. This means they have been infected with worm as well

	End Time	Name		Target Address	Priority	Category Outcome
	21 Aug 2013 13:46:22 PDT	New su			7	/Success
	21 Aug 2013 13:46:22 PDT	Illegal u		10.0.112.14	7	/Failure
	21 Aug 2013 13:46:22 PDT	Illegal u		10.0.112.13	7	/Failure
	21 Aug 2013 13:46:22 PDT	Possible Internal Network Sweep	10.0.113.72		9	
	21 Aug 2013 13:46:22 PDT	Worm Outbreak Test Rule	10.0.113.72		10	/Success
	21 Aug 2013 13:46:22 PDT	Compromise - Success	10.0.113.72		9	/Success
	21 Aug 2013 13:46:22 PDT	Notify on Successful Attack	10.0.113.72		9	/Success
	21 Aug 2013 13:46:21 PDT	New subagent [generic_syslo...			7	/Success
	21 Aug 2013 13:46:21 PDT	Illegal user	10.0.113.72	10.0.112.12	7	/Failure

Figure 52. Infected hosts detected in "Worm Outbreak Channel."



Name: Worm Outbreak Test List
Last Update: 21 Aug 2013 11:25:17 PDT
Filter: No Filter

Attacker Address	Target Port	Attacker Zone	Count	Attacker Zone Reference ID
10.0.20.39	22	<Resource URI="/All Zon...	1	1191
10.0.111.39	22	<Resource URI="/All Zon...	1	1191
10.0.111.46	22	<Resource URI="/All Zon...	1	1191

Entries created in "Worm Outbreak Test List" as a result of the "Worm Outbreak Test Rule" being triggered

Figure 53. Infected hosts information in "Worm Outbreak Test List."

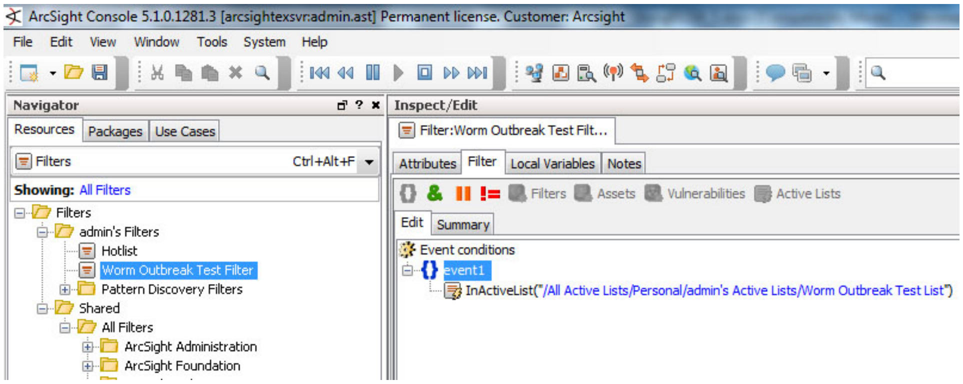
G. PHASE 6 – LIST INFECTED HOSTS

This phase will focus on using the graphical resources, in particular the dashboard, to list the infected hosts once they have been detected by the rule. The dashboard will consist of several data monitors that are supplemented by a filter. The filter is responsible for eliciting and displaying the events of interest. An incident report will be created to provide summaries of the data pertaining to the infected hosts. The steps are as follows:

1. Create "Worm Outbreak Filter List."
2. Create "Worm Infected Test Monitor."
3. Create "Worm Propagation by Host Test Monitor."
4. Create "Worm Propagation by Zone Test Monitor."
5. Create "Worm Outbreak Test Dashboard."
6. Create "Worm Outbreak Test Report."

1. Step 1 – Create "Worm Outbreak Filter List"

The reason for creating the "Worm Outbreak Test List" in the previous phase was to provide the information of the worm-infected hosts as a rule *input* to yet another rule. This other rule will be used by the data monitors to create a list of all infected hosts.


ArcSight Console 5.1.0.1281.3 [arcsightexsvr:admin.ast] Permanent license. Customer: Arcsight
File Edit View Window Tools System Help
Navigator
Resources Packages Use Cases
Filters Ctrl+Alt+F
Inspect/Edit
Filter:Worm Outbreak Test Filt...
Attributes Filter Local Variables Notes
Filters Assets Vulnerabilities Active Lists
Edit Summary

Showing: All Filters

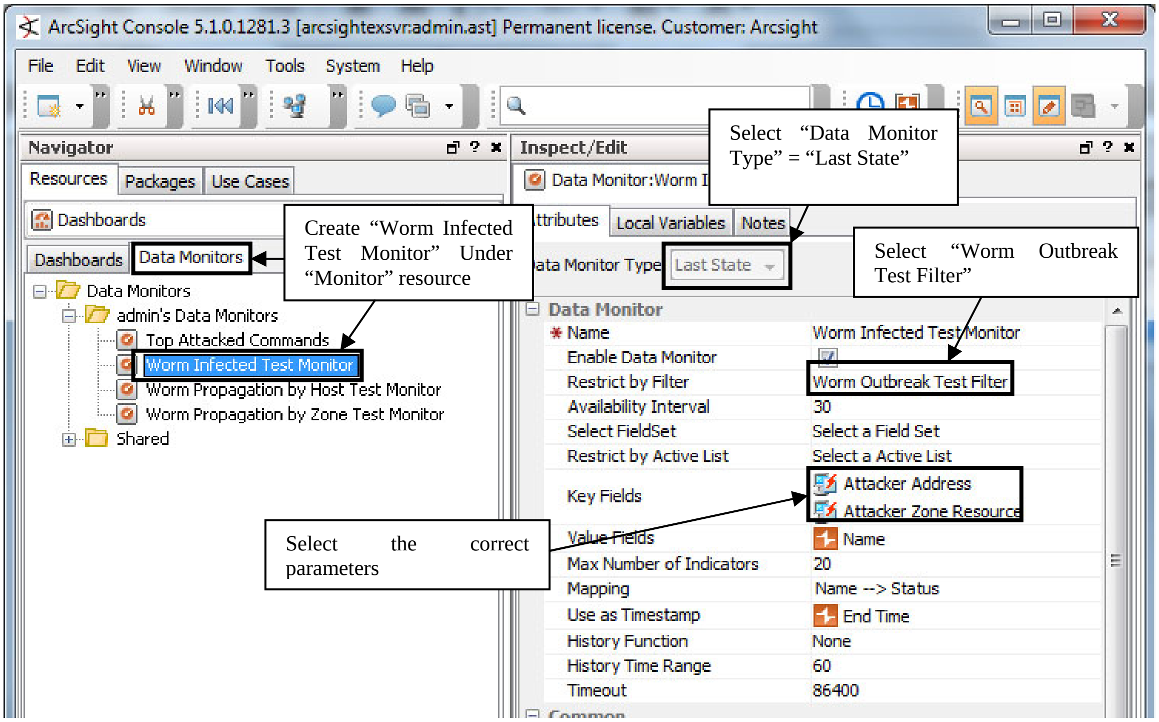
- Filters
  - admin's Filters
    - Hotlist
    - Worm Outbreak Test Filter
    - Pattern Discovery Filters
  - Shared
    - All Filters
      - ArcSight Administration
      - ArcSight Foundation

Event conditions
- event1
  - InActiveList("/All Active Lists/Personal/admin's Active Lists/Worm Outbreak Test List")

Figure 54. “Worm Outbreak Test Filter” configuration

2. Step 2 – Create “Worm Infected Test Monitor”

This data monitor displays the number of hosts that have been infected in the course of a worm outbreak.


ArcSight Console 5.1.0.1281.3 [arcsightexsvr:admin.ast] Permanent license. Customer: Arcsight
File Edit View Window Tools System Help
Navigator
Resources Packages Use Cases
Dashboards
Dashboards Data Monitors
Inspect/Edit
Data Monitor:Worm I
ttributes Local Variables Notes

- Data Monitors
  - admin's Data Monitors
    - Top Attacked Commands
    - Worm Infected Test Monitor
    - Worm Propagation by Host Test Monitor
    - Worm Propagation by Zone Test Monitor
  - Shared

ata Monitor Type: Last State

Data Monitor

* Name	Worm Infected Test Monitor
Enable Data Monitor	☑
Restrict by Filter	Worm Outbreak Test Filter
Availability Interval	30
Select FieldSet	Select a Field Set
Restrict by Active List	Select a Active List
Key Fields	Attacker Address Attacker Zone Resource
Value Fields	Name
Max Number of Indicators	20
Mapping	Name --> Status
Use as Timestamp	End Time
History Function	None
History Time Range	60
Timeout	86400

Common

Select “Data Monitor Type” = “Last State”

Create “Worm Infected Test Monitor” Under “Monitor” resource

Select “Worm Outbreak Test Filter”

Select the correct parameters

Figure 55. “Worm Infected Test Monitor” configuration.

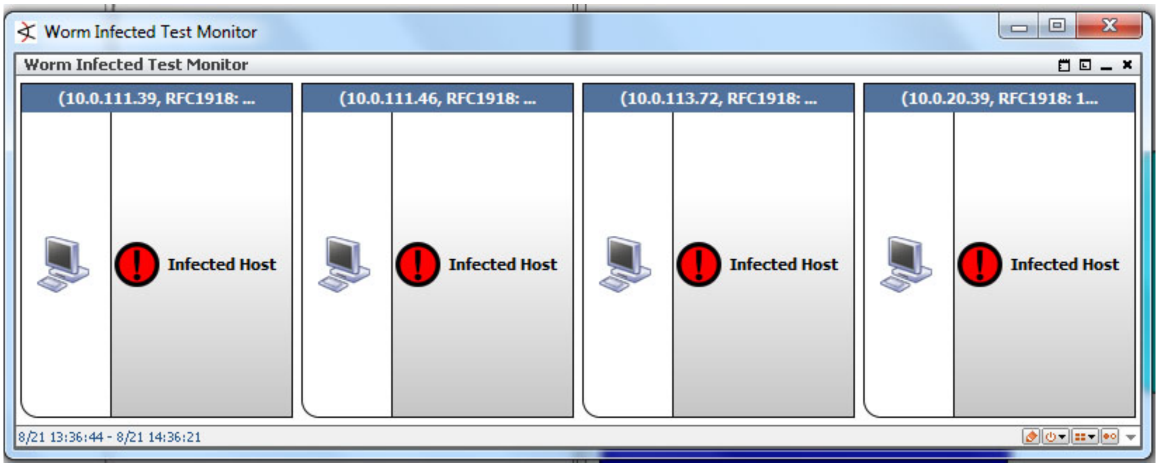
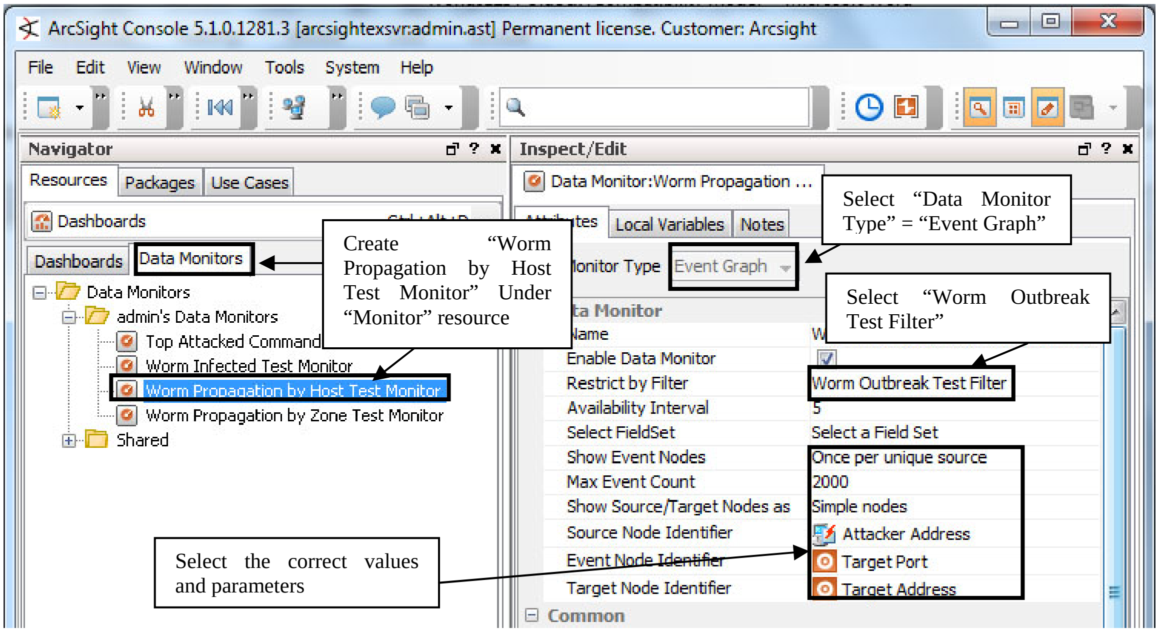

Worm Infected Test Monitor
Worm Infected Test Monitor
(10.0.111.39, RFC1918: ...
(10.0.111.46, RFC1918: ...
(10.0.113.72, RFC1918: ...
(10.0.20.39, RFC1918: 1...
Infected Host
Infected Host
Infected Host
Infected Host
8/21 13:36:44 - 8/21 14:36:21

Figure 56. “Worm Infected Test Monitor” expected display.

3. Step 3 - Create “Worm Propagation by Host Test Monitor”

This data monitor shows the spread of worm activity throughout the network.


ArcSight Console 5.1.0.1281.3 [arcsightexsvr:admin.ast] Permanent license. Customer: Arcsight
File Edit View Window Tools System Help
Navigator
Resources Packages Use Cases
Dashboards
Dashboards Data Monitors
Data Monitors
admin's Data Monitors
Top Attacked Command
Worm Infected Test Monitor
Worm Propagation by Host Test Monitor
Worm Propagation by Zone Test Monitor
Shared
Inspect/Edit
Data Monitor:Worm Propagation ...
Attributes Local Variables Notes
Common

Monitor Type: Event Graph

Data Monitor

Name	W
Enable Data Monitor	☑
Restrict by Filter	Worm Outbreak Test Filter
Availability Interval	5
Select FieldSet	Select a Field Set
Show Event Nodes	Once per unique source
Max Event Count	2000
Show Source/Target Nodes as	Simple nodes
Source Node Identifier	Attacker Address
Event Node Identifier	Target Port
Target Node Identifier	Target Address

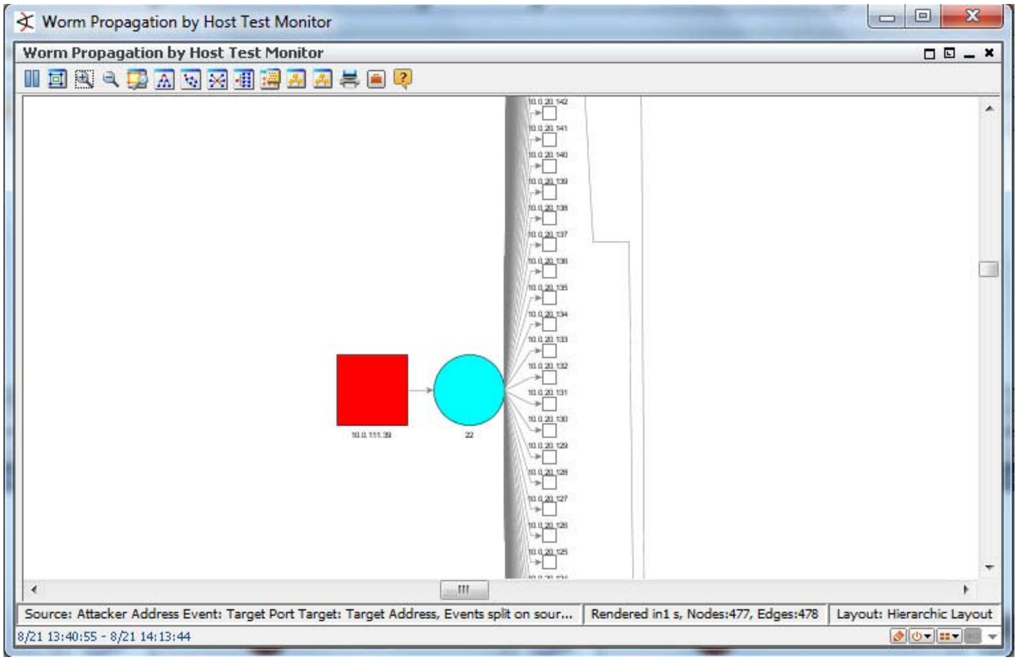
Create “Worm Propagation by Host Test Monitor” Under “Monitor” resource

Select “Data Monitor Type” = “Event Graph”

Select “Worm Outbreak Test Filter”

Select the correct values and parameters

Figure 57. “Worm Propagation by Host Test Monitor” configuration.



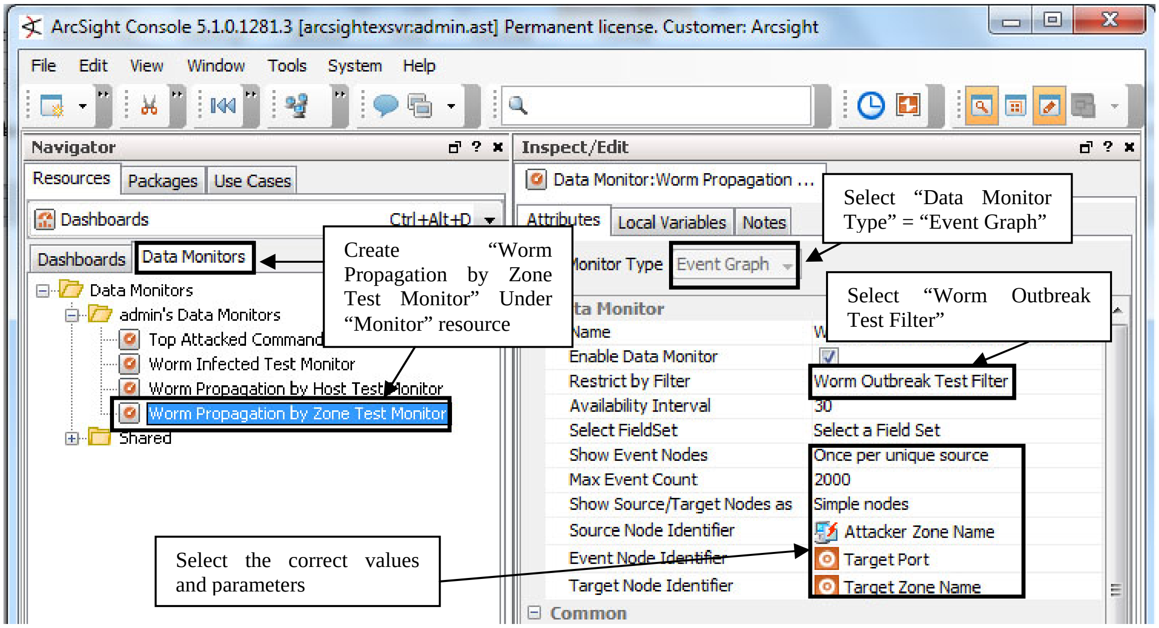
Source: Attacker Address Event: Target Port Target: Target Address, Events split on sour... | Rendered in1 s, Nodes:477, Edges:478 | Layout: Hierarchic Layout

8/21 13:40:55 - 8/21 14:13:44

Figure 58. “Worm Propagation by Host Test Monitor” expected display.

4. Step 4 – Create “Worm Propagation by Zone Test Monitor”

This data monitor shows the spread of worms across network zones.



Create “Worm Propagation by Zone Test Monitor” Under “Monitor” resource

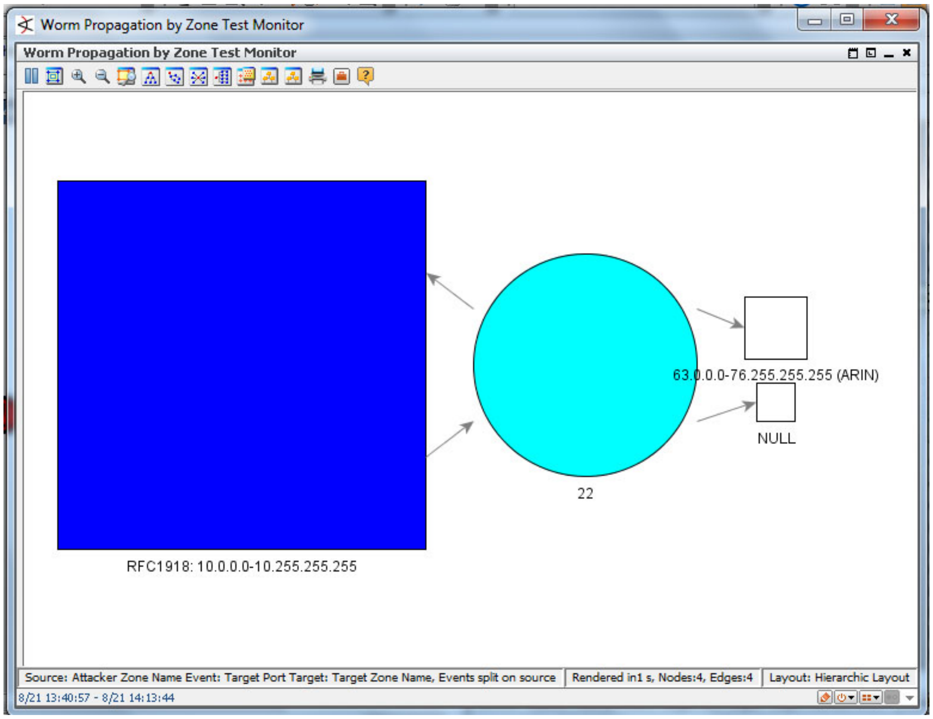
Select “Data Monitor Type” = “Event Graph”

Select “Worm Outbreak Test Filter”

Select the correct values and parameters

Monitor Type	Event Graph
Name	W
Enable Data Monitor	☑
Restrict by Filter	Worm Outbreak Test Filter
Availability Interval	30
Select FieldSet	Select a Field Set
Show Event Nodes	Once per unique source
Max Event Count	2000
Show Source/Target Nodes as	Simple nodes
Source Node Identifier	Attacker Zone Name
Event Node Identifier	Target Port
Target Node Identifier	Target Zone Name

Figure 59. “Worm Propagation by Zone Test Monitor” configuration.


Worm Propagation by Zone Test Monitor
Worm Propagation by Zone Test Monitor
RFC1918: 10.0.0.0-10.255.255.255
22
63.0.0.0-76.255.255.255 (ARIN)
NULL

Source: Attacker Zone Name Event: Target Port Target: Target Zone Name, Events split on source | Rendered in1 s, Nodes:4, Edges:4 | Layout: Hierarchic Layout

8/21 13:40:57 - 8/21 14:13:44

Figure 60. “Worm Propagation by Zone Test Monitor” expected display.

5. Step 5 – Create “Worm Outbreak Test Dashboard”

Prior to displaying the content, the data monitors must be attached to the dashboard.

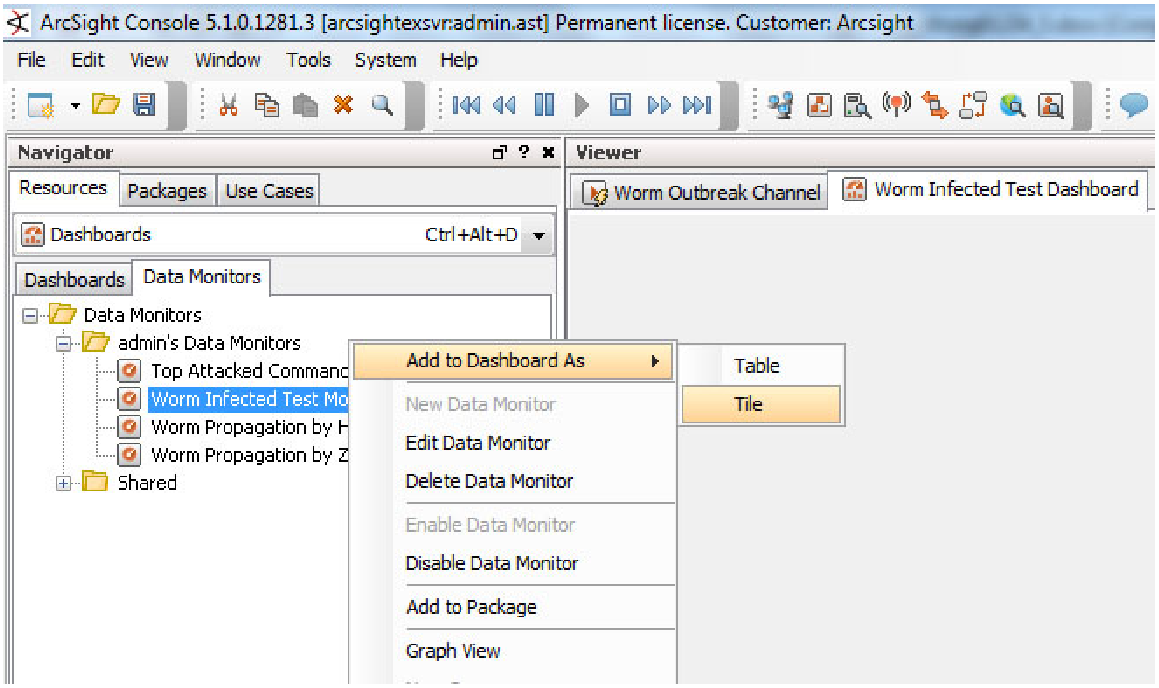


Figure 61. Attach data monitors to dashboard.

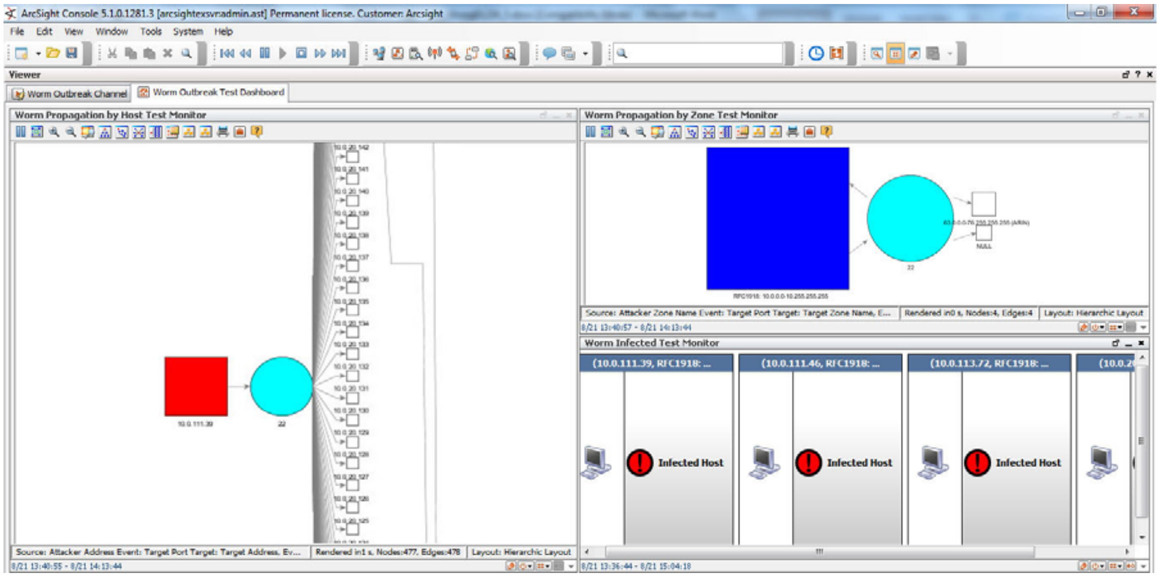
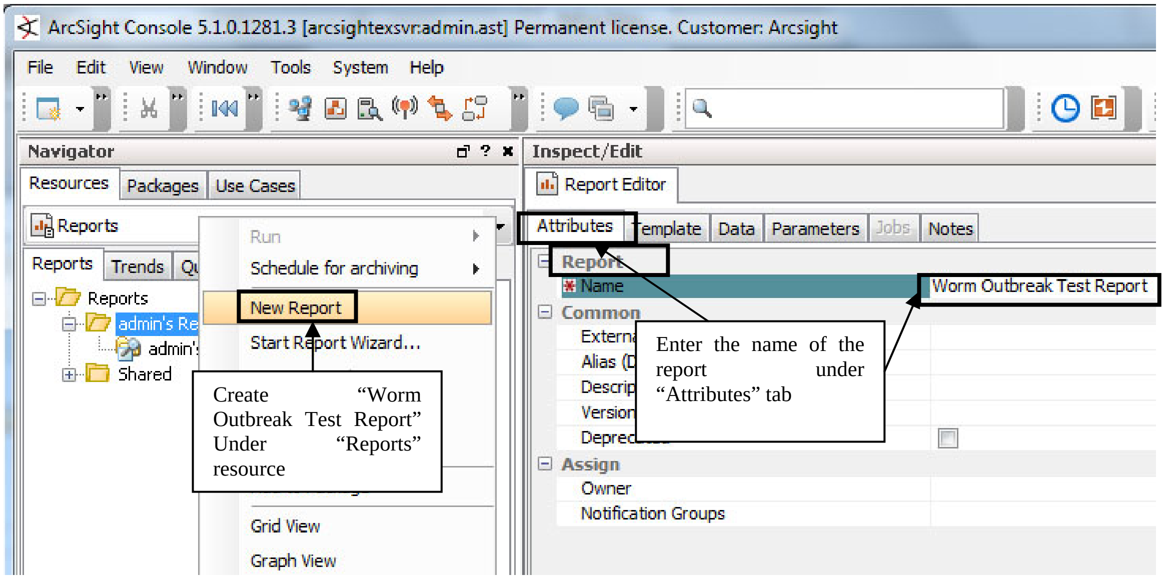

ArcSight Console 5.1.0.1281.3 [arcsightexsvr:admin.ast] Permanent license. Customer: Arcsight
File Edit View Window Tools System Help
Viewer
Worm Outbreak Channel
Worm Outbreak Test Dashboard
Worm Propagation by Host Test Monitor
Worm Propagation by Zone Test Monitor
Source: Attacker Address Event: Target Port Target: Target Address, Ev...
Rendered in1 s, Nodes:477, Edges:478
Layout: Hierarchic Layout
Source: Attacker Zone Name Event: Target Port Target: Target Zone Name, E...
Rendered in0 s, Nodes:4, Edges:4
Layout: Hierarchic Layout
Worm Infected Test Monitor
(10.0.111.39, RFC1918: ...
(10.0.111.46, RFC1918: ...
(10.0.113.72, RFC1918: ...
Infected Host
Infected Host
Infected Host

Figure 62. “Worm Outbreak Test Dashboard” expected display.

6. Step 6 – Create “Worm Outbreak Test Report”

Similar to the data monitors, a pdf report will be generated based on the information captured in the “Worm Outbreak Test List.” The report will consist of a table that provides the information of the infected host and a chart that shows the number of times the infected hosts have been detected (i.e., matched against the Worm Outbreak Test Rule).

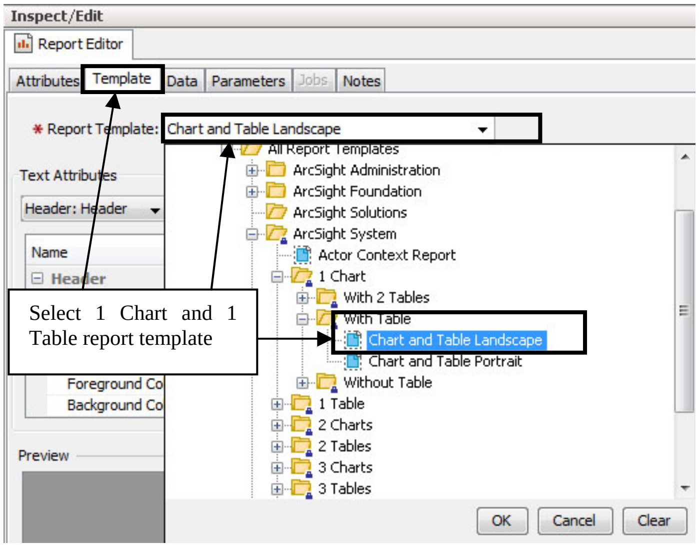


Create “Worm Outbreak Test Report” Under “Reports” resource

Enter the name of the report under “Attributes” tab

Name: Worm Outbreak Test Report

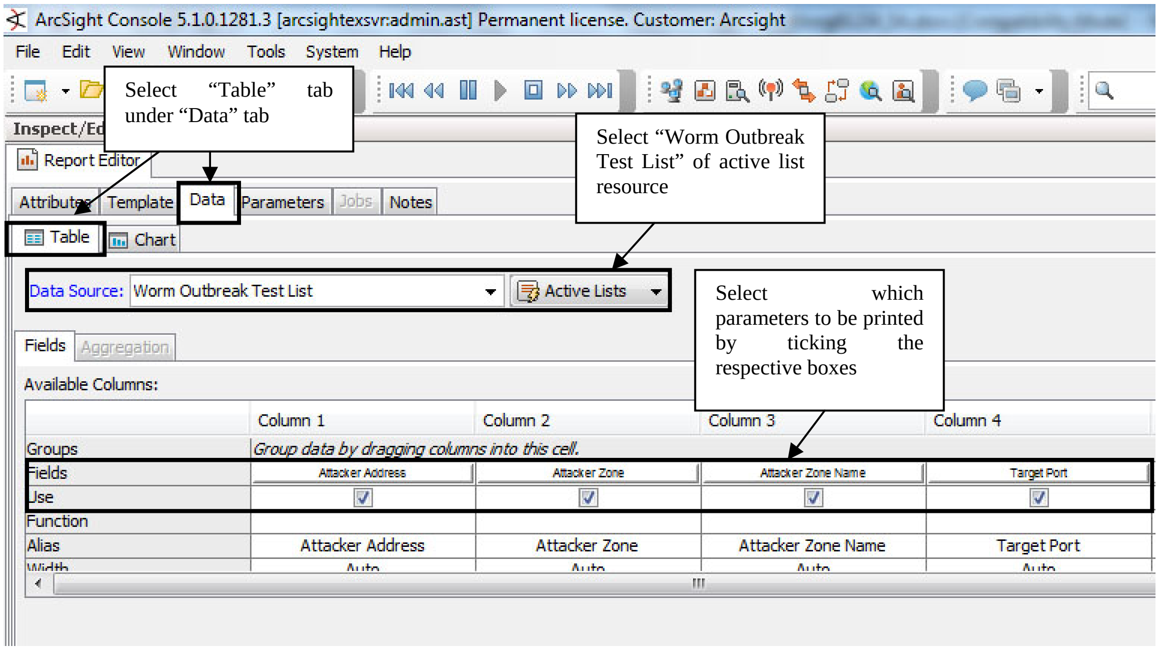
Figure 63. “Worm Outbreak Test Report” attributes configuration.



Select 1 Chart and 1 Table report template

Report Template: Chart and Table Landscape

Figure 64. “Worm Outbreak Test Report” template configuration.


ArcSight Console 5.1.0.1281.3 [arcsightexsvr:admin.ast] Permanent license. Customer: Arcsight
File Edit View Window Tools System Help
Inspect/Ed
Report Editor
Attributes Template Data Parameters Jobs Notes
Table Chart
Fields Aggregation

Select “Table” tab under “Data” tab

Select “Worm Outbreak Test List” of active list resource

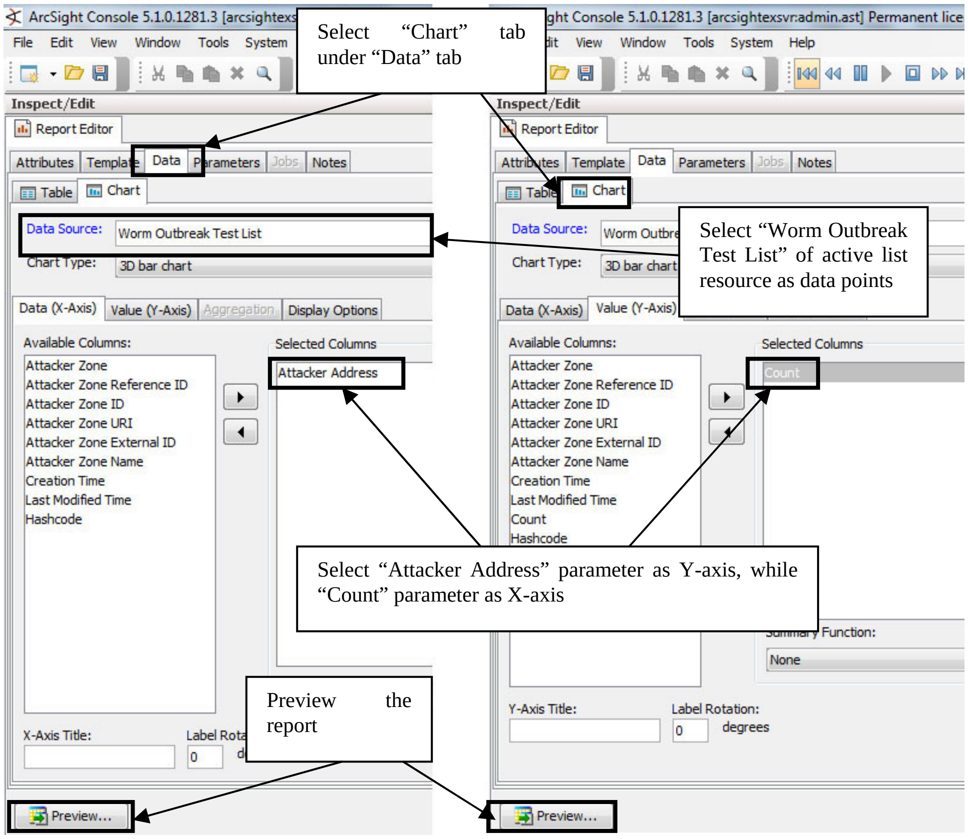
Select which parameters to be printed by ticking the respective boxes

Data Source: Worm Outbreak Test List | Active Lists

Available Columns:

	Column 1	Column 2	Column 3	Column 4
Groups	*Group data by dragging columns into this cell.*			
Fields	Attacker Address	Attacker Zone	Attacker Zone Name	Target Port
Use	☑	☑	☑	☑
Function				
Alias	Attacker Address	Attacker Zone	Attacker Zone Name	Target Port
Width	Auto	Auto	Auto	Auto

Figure 65. “Worm Outbreak Test Report” table data configuration.


ArcSight Console 5.1.0.1281.3 [arcsightexs
ght Console 5.1.0.1281.3 [arcsightexsvr:admin.ast] Permanent lice
File Edit View Window Tools System Help
Inspect/Edit
Report Editor
Attributes Template Data Parameters Jobs Notes
Table Chart
Data (X-Axis) Value (Y-Axis) Aggregation Display Options
Preview...
Preview...

Select “Chart” tab under “Data” tab

Select “Worm Outbreak Test List” of active list resource as data points

Select “Attacker Address” parameter as Y-axis, while “Count” parameter as X-axis

Preview the report

Data Source: Worm Outbreak Test List

Chart Type: 3D bar chart

Available Columns:

- Attacker Zone
- Attacker Zone Reference ID
- Attacker Zone ID
- Attacker Zone URI
- Attacker Zone External ID
- Attacker Zone Name
- Creation Time
- Last Modified Time
- Hashcode

Selected Columns: Attacker Address

X-Axis Title:

Label Rota

Available Columns:

- Attacker Zone
- Attacker Zone Reference ID
- Attacker Zone ID
- Attacker Zone URI
- Attacker Zone External ID
- Attacker Zone Name
- Creation Time
- Last Modified Time
- Count
- Hashcode

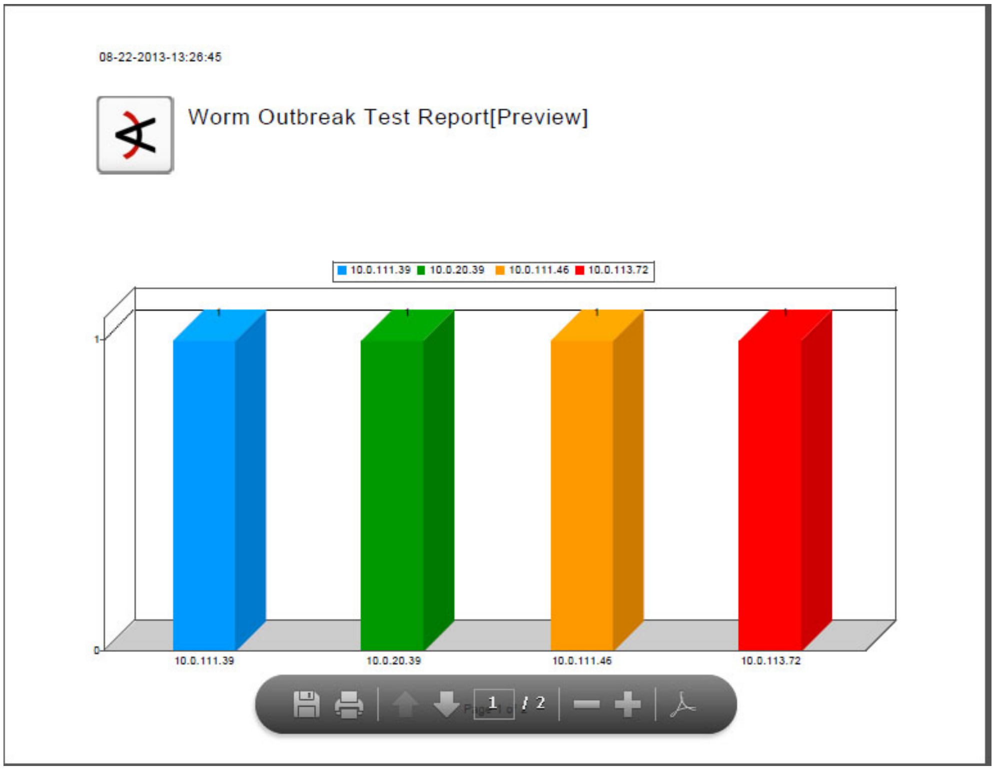
Selected Columns: Count

Summary Function: None

Y-Axis Title:

Label Rotation: 0 degrees

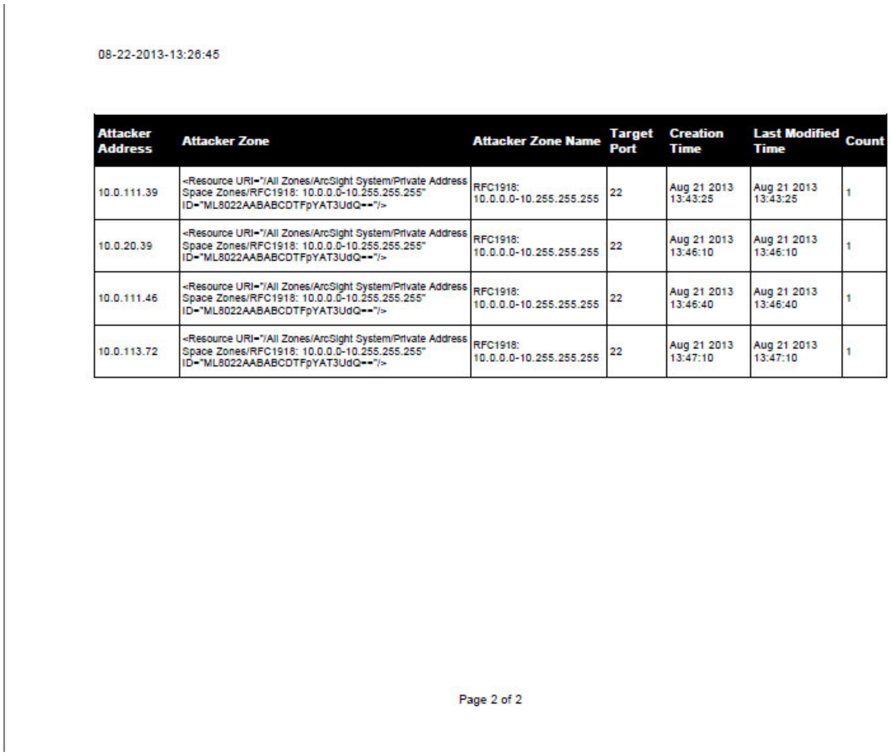
Figure 66. “Worm Outbreak Test Report” chart data configuration.



08-22-2013-13:26:45

Worm Outbreak Test Report[Preview]

Figure 67. “Worm Outbreak Test Report” expected display page 1.



08-22-2013-13:26:45

Attacker Address	Attacker Zone	Attacker Zone Name	Target Port	Creation Time	Last Modified Time	Count
10.0.111.39	<Resource URI="/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255" ID="ML8022AABABCDTFpYAT3UdQ=="/>	RFC1918: 10.0.0.0-10.255.255.255	22	Aug 21 2013 13:43:25	Aug 21 2013 13:43:25	1
10.0.20.39	<Resource URI="/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255" ID="ML8022AABABCDTFpYAT3UdQ=="/>	RFC1918: 10.0.0.0-10.255.255.255	22	Aug 21 2013 13:46:10	Aug 21 2013 13:46:10	1
10.0.111.46	<Resource URI="/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255" ID="ML8022AABABCDTFpYAT3UdQ=="/>	RFC1918: 10.0.0.0-10.255.255.255	22	Aug 21 2013 13:46:40	Aug 21 2013 13:46:40	1
10.0.113.72	<Resource URI="/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255" ID="ML8022AABABCDTFpYAT3UdQ=="/>	RFC1918: 10.0.0.0-10.255.255.255	22	Aug 21 2013 13:47:10	Aug 21 2013 13:47:10	1

Page 2 of 2

Figure 68. “Worm Outbreak Test Report” expected display page 2.

H. SUMMARY

This chapter has elaborated on the training methodology and provided details on how to utilize the comprehensive resources within ArcSight to detect the occurrence of a worm outbreak threat situation. The structural approach has been categorized into procedural phases and is summarized as such:

- Scenario briefing – Provide the background context of the training scenario.
- Phase 1 – Conduct a study on the computer worm and understand its behavior.
- Phase 2 – Set up the replay connector with the worm outbreak replay file.
- Phase 3 – Construct a network topology using the parameters from the events provided by the worm outbreak replay file.
- Phase 4 – Associate worm behavior to the parameters of the events.
- Phase 5 – Configure rules and filters to detect and elicit information about the infected hosts.
- Phase 6 – Present the information of the infected hosts using monitors and dashboard and create a summarized report of the incident.

In addition to the explanation, the expected results (e.g., screenshots) are also included to enhance the understanding. The next, and final, chapter will conclude this thesis by presenting the findings and proposing additional areas for future research.

VI. CONCLUSION

A. FINDINGS

1. Importance of Source Events

SIEM products are passive systems that do not possess the capability of detecting or analyzing malicious payload. The products rely on information culled from the various log reports collected from the various reporting devices. The reported information may be highly specific if, for example, the reporting device is a security system (e.g., a host-based IPS) that "intelligently" analyzes traffic and/or end-device events. The reported information may, on the other hand, provide only a "hint" about a threat (e.g., a failed connection attempt) and require clever correlative rules writing on the SIEM itself in order to deduce an actual threat. Threats (e.g., virus) that only harm the infected host (e.g., deletion of system files) and do not display any distinctive network traits may be able to sneak past the watchful SIEM products if no device reporting to the SIEM provides any tell-tale log information related to that threat. As such, it is important for SIEM operators to understand this causal relationship and emphasize the proper configurations at the source devices.

2. "Reverse-Engineering" Inadequacy

As demonstrated in Chapter IV, a simplified network topology can be constructed using the steps mentioned. However, it is crucial to know that the "reverse-engineering" method is non-intuitive and will require certain assumptions to justify the sequence of transmission flow. In addition, the reconstruction method is not "perfect" due to the following:

S/N	INADEQUACY	EXAMPLE
1	Events captured in the replay file may not reveal the entire configuration of the reporting device.	A router with 4 used interfaces will typically have 4 IP addresses. However, if the replay file only contains transmission records involving 2 of these interfaces, the IP addresses of the other 2 would never be reported.
2	The actual number of network devices and hosts identified may differ from the actual topology.	When a base event shows that a transmission occurs between two hosts, it does not necessarily mean that the destination host is physically available. The base event can only ascertain the existence of a source host that attempts to communicate with the destination host.
3	The replay file may not contain events that report existing devices in the actual topology.	A host connected to the reporting device may not have any transmission with other devices. As a result, the replay file will not contain any events that will provide information on the presence of the host.

Table 4. Reconstruction method inadequacies

Despite this, the "reverse-engineering" method is still important in the absence of the actual network topology for the context of this thesis.

B. ADDITIONAL AREAS FOR FUTURE RESEARCH

1. Create more Scenarios with Different Threats

This thesis has illustrated only the structural approach in tackling one cyber-threat. There are many other cyber threats that could be "captured" as replay files, some of which could be quite complex, and thus requiring more effort in tailoring the specific rules and filters to attain some desired level of student learning. By working on other training scenarios, SIEM operators would be able to gain further insights on the commonalities amongst various threats and better understand the utilization of the resources provided by ArcSight ESM in deriving a more optimal solution.

2. Explore Other ArcSight Resources

In addition to the resources mentioned, ArcSight also provides other resources that are useful in profiling the entities within the network. For example, the “Actor” resource can be used to model the user and administer his/her associated security classification; which is useful for detecting insider threats. The “Use Case” resource provides a way to view, configure, and transport specially developed sets of related resources that address specific security issues and business requirements. When used effectively, this resource can be translated into different scenarios for multi-level training purposes.

C. CONCLUSION

Computer threats have constantly evolved over the years and security practitioners are finding it harder to keep in pace with this worrying trend. As explained in Chapter II, issues exacerbating the situation can be attributed to the lengthy time required in training qualified and competent SIEM operators, as well as the complexity of the tools that can be used to detect the presence of such threats.

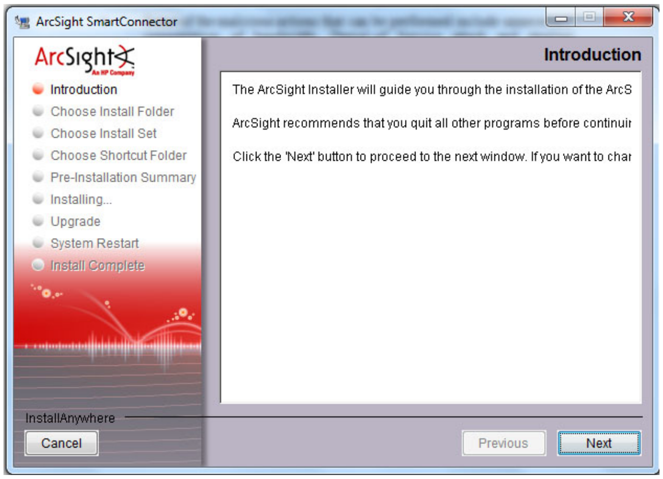
In the face of such problems, this thesis has focused on developing a cyber-forensics training methodology that aims to educate SIEM operators on the effective approach to monitoring and reacting to cyber threats. It incorporates a repeatable SIEM educational framework and highlights the structural approach in utilizing ArcSight ESM to collect, analyze and detect malicious events. The framework has been empirically demonstrated with a worm outbreak lab scenario, where the captured results illustrate the feasibility of the proposed approach. Through the methodology presented, it is hoped that the rate of training competent SIEM operators might be increased so as to keep up with the growing risks of operating in cyber space.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX. REPLAY CONNECTOR INSTALLATION GUIDE

This installation guide illustrates some of the parameters to be configured and provides screenshots to aid the installation process. Two files are required in this setup: “WormOutbreak.events” and “ArcSight_Connector_Installer.exe.”

First, install “ArcSight_Connector_Installer.exe” on a host. For ease of management, you can install the connector on the same host that contains the ArcSight Console. The following figures show screenshots of the installation process.



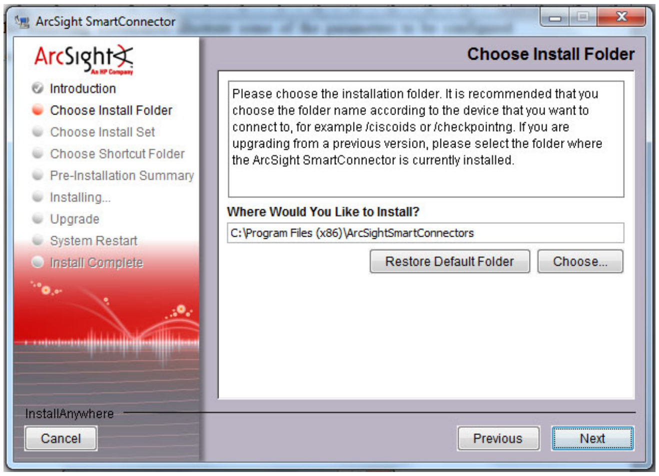
Introduction

The ArcSight Installer will guide you through the installation of the ArcS

ArcSight recommends that you quit all other programs before continuir

Click the 'Next' button to proceed to the next window. If you want to char

Figure 69. ArcSight Connector Installer screenshot.



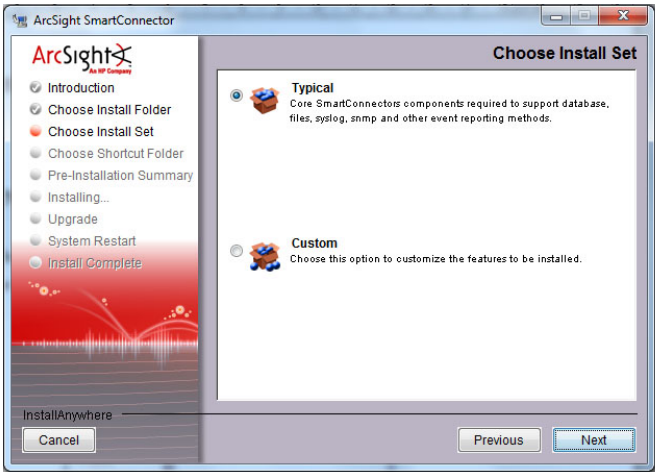
Choose Install Folder

Please choose the installation folder. It is recommended that you choose the folder name according to the device that you want to connect to, for example /ciscoids or /checkpointng. If you are upgrading from a previous version, please select the folder where the ArcSight SmartConnector is currently installed.

Where Would You Like to Install?

C:\Program Files (x86)\ArcSightSmartConnectors

Figure 70. “Choose Install Folder” screenshot.

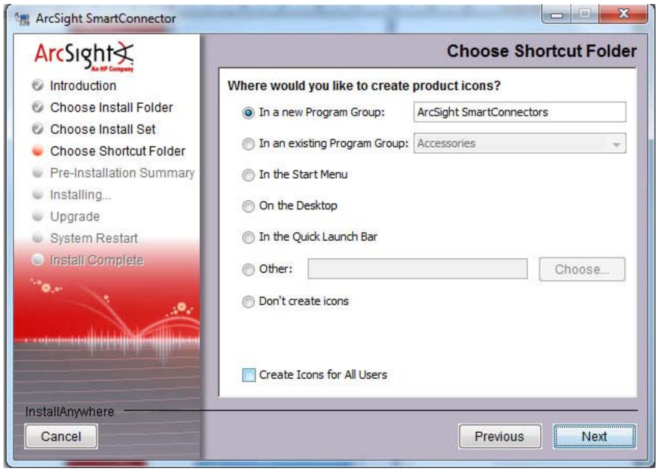


Choose Install Set

● **Typical**
Core SmartConnectors components required to support database, files, syslog, snmp and other event reporting methods.

○ **Custom**
Choose this option to customize the features to be installed.

Figure 71. “Choose Install Set” screenshot.



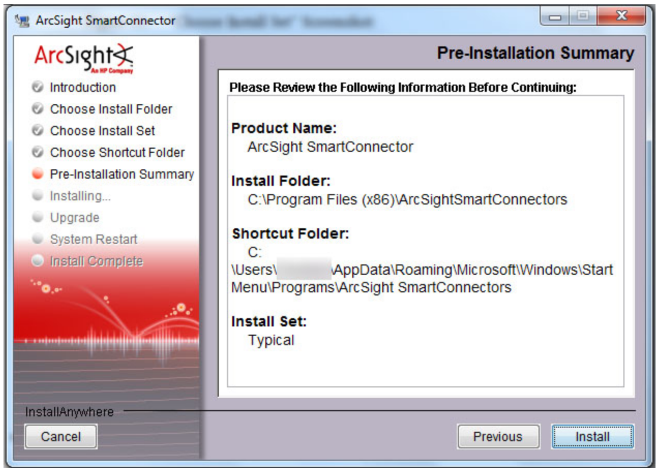
Choose Shortcut Folder

Where would you like to create product icons?

● In a new Program Group: ArcSight SmartConnectors
○ In an existing Program Group: Accessories
○ In the Start Menu
○ On the Desktop
○ In the Quick Launch Bar
○ Other: Choose...
○ Don't create icons

□ Create Icons for All Users

Figure 72. “Choose Shortcut Folder” screenshot.



Pre-Installation Summary

Please Review the Following Information Before Continuing:

Product Name:
ArcSight SmartConnector

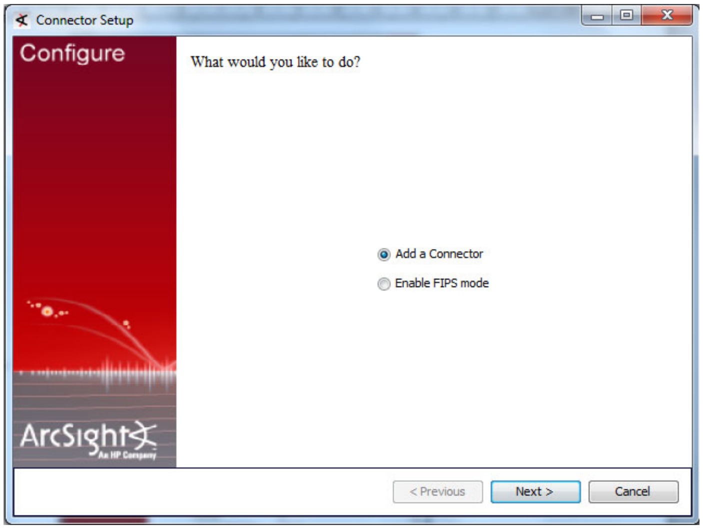
Install Folder:
C:\Program Files (x86)\ArcSightSmartConnectors

Shortcut Folder:
C:
\Users\[redacted]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\ArcSight SmartConnectors

Install Set:
Typical

Figure 73. “Pre-Installation Summary” screenshot.

After the installer has copied all the working files to the selected folders, a separate “Connector Setup” screen will appear. Select “Add a Connector” and continue to the next screen.



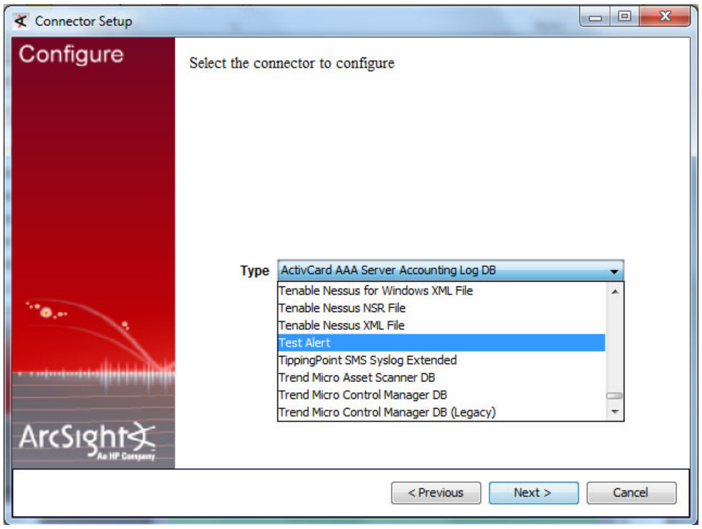
What would you like to do?

● Add a Connector

○ Enable FIPS mode

Figure 74. “Add a Connector” screenshot.

In this screen, you must select the “Test Alert” option from the list of ArcSight SmartConnectors“Connector details” (Figure 75.).



Select the connector to configure

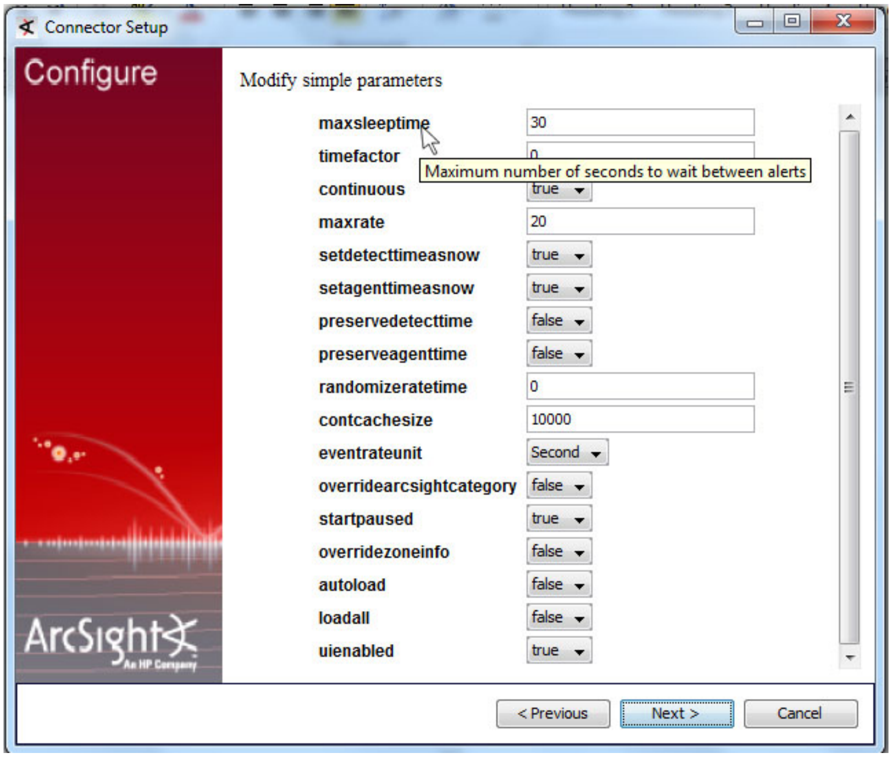
Type: ActivCard AAA Server Accounting Log DB

- Tenable Nessus for Windows XML File
- Tenable Nessus NSR File
- Tenable Nessus XML File
- Test Alert
- TippingPoint SMS Syslog Extended
- Trend Micro Asset Scanner DB
- Trend Micro Control Manager DB
- Trend Micro Control Manager DB (Legacy)

Figure 75. “Connector options” screenshot.

Figure 76 shows the parameters that control the events flow to the ArcSight Express. Their definition can be seen by mousing over their text label (Figure 76). Some of the more important parameters to take note are as follows:

- maxrate & eventrateunit – These two parameters control the maximum rate at which events will be sent to ArcSight ESM. For initial learning purpose, the rate shall be slow so that it allows ample time for analysis.
- setdetecttimeasnow & setagenttimeasnow – These two parameters shall be set to "true" so that the timestamp of the base events can be synchronized with ArcSight Console.
- randomizeratetime – This parameter introduces randomness to the base events received. It shall be set to "0" to prevent the confusion during the analysis of the base events.
- Uienabled – This parameter must be set to "true" for the replay GUI to appear.

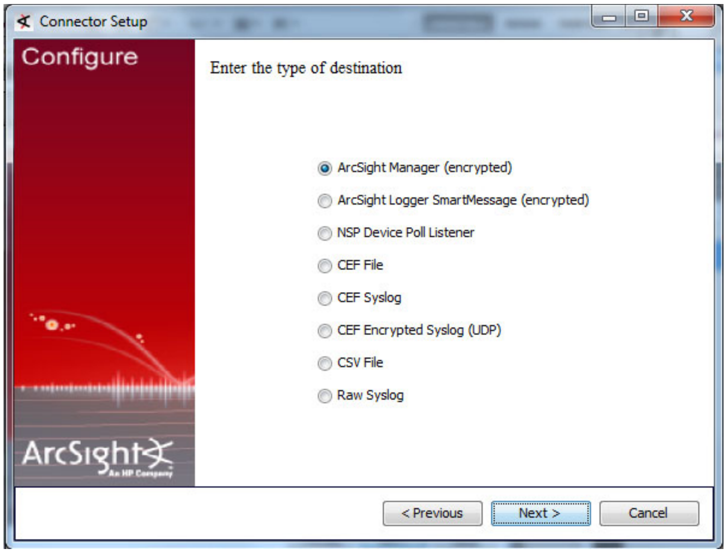


Modify simple parameters

maxsleeptime 30
timefactor 0
Maximum number of seconds to wait between alerts
continuous true
maxrate 20
setdetecttimeasnow true
setagenttimeasnow true
preservedetecttime false
preserveagenttime false
randomizeratetime 0
contcachesize 10000
eventrateunit Second
overridearcsightcategory false
startpaused true
overridezoneinfo false
autoload false
loadall false
uienabled true

Figure 76. "Connector details" screenshot.

Since the base events must be sent to ArcSight Manager for analysis, the "ArcSight Manager (encrypted)" option shall be selected as the destination.

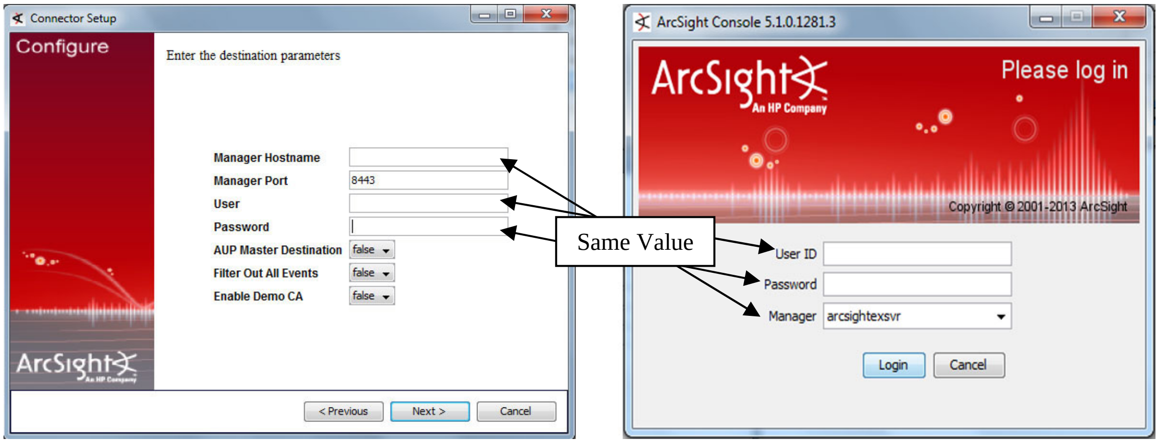


Enter the type of destination

- ● ArcSight Manager (encrypted)
- ○ ArcSight Logger SmartMessage (encrypted)
- ○ NSP Device Poll Listener
- ○ CEF File
- ○ CEF Syslog
- ○ CEF Encrypted Syslog (UDP)
- ○ CSV File
- ○ Raw Syslog

Figure 77. “Select destination” screenshot.

Depending on how the ArcSight Console has been configured, the “Manager Hostname,” “User” and “Password” fields will be filled with the respective values that are used to log into the ArcSight Console. The rest of the parameters shall be set to false.



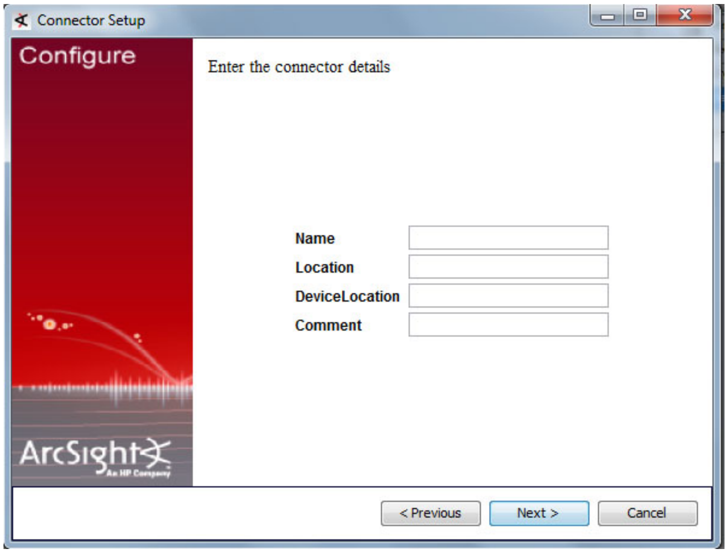
Enter the destination parameters

Manager Hostname	
Manager Port	8443
User	
Password	
AUP Master Destination	false
Filter Out All Events	false
Enable Demo CA	false

User ID	
Password	
Manager	arcsightexsvr

Figure 78. “Destination parameters” screenshot.

The respective values will be used to uniquely identify the connector.



Enter the connector details

Name

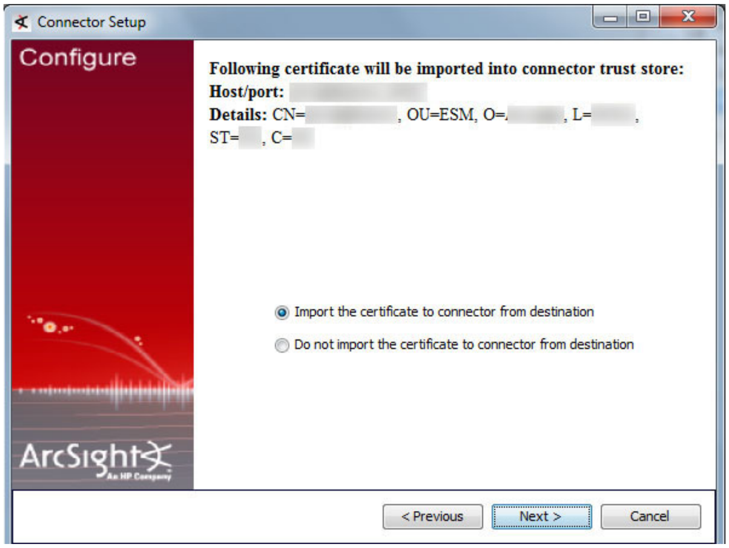
Location

DeviceLocation

Comment

Figure 79. “Connector details” screenshot.

If the values in Figure 78 have been entered correctly, the connector setup will attempt to import the certificate from the ArcSight Manager.

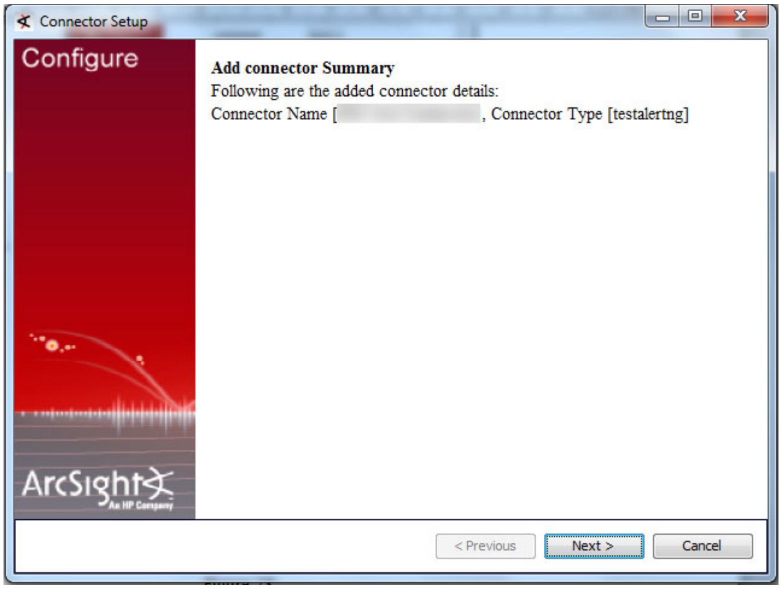


Following certificate will be imported into connector trust store:
Host/port: [redacted]
Details: CN=[redacted], OU=ESM, O=[redacted], L=[redacted], ST=[redacted], C=[redacted]

● Import the certificate to connector from destination

○ Do not import the certificate to connector from destination

Figure 80. “Import Certificate” screenshot.

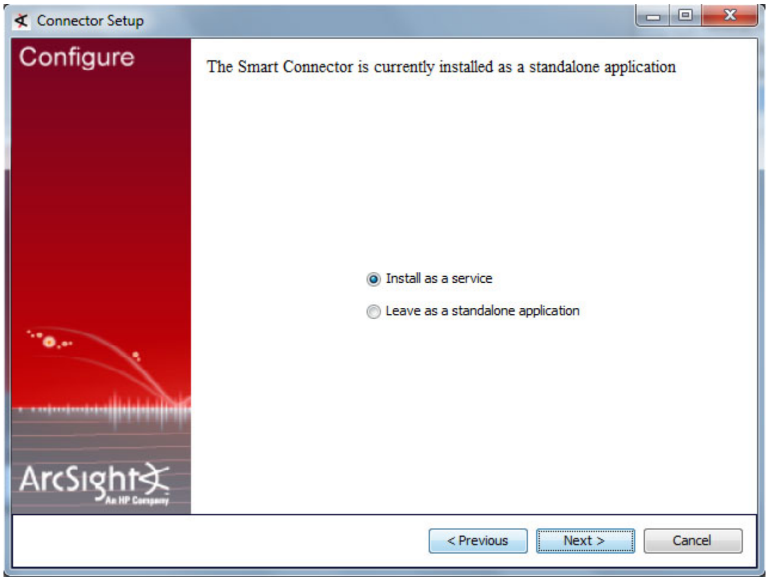


Add connector Summary

Following are the added connector details:

Connector Name [[redacted], Connector Type [testalertng]

Figure 81. “Add connector Summary” screenshot.

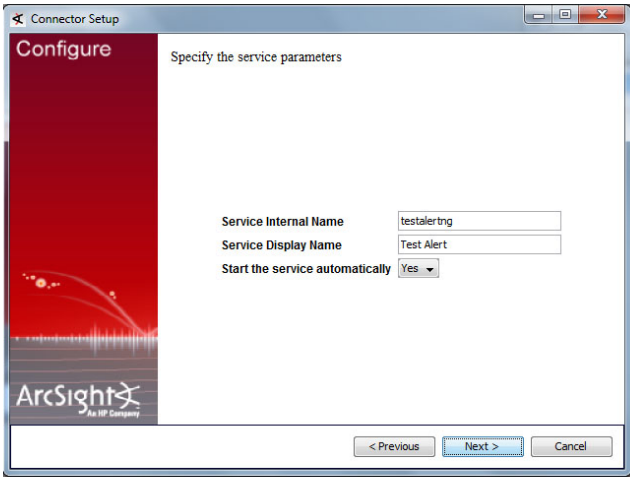


The Smart Connector is currently installed as a standalone application

● Install as a service

○ Leave as a standalone application

Figure 82. “Install as a service” screenshot.



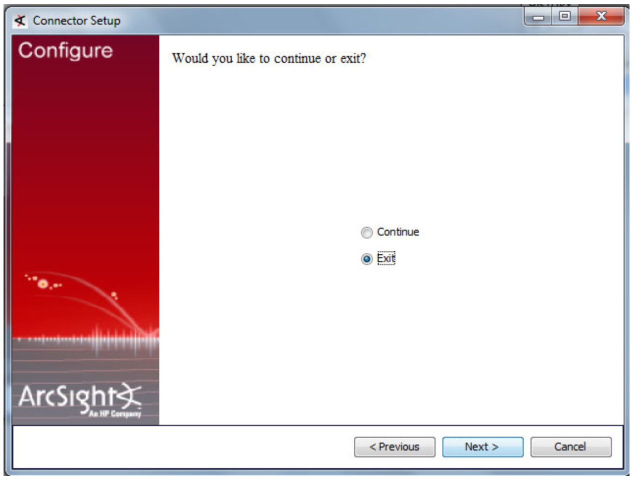
Specify the service parameters

Service Internal Name: testalertng

Service Display Name: Test Alert

Start the service automatically: Yes

Figure 83. “Service parameters” screenshot.

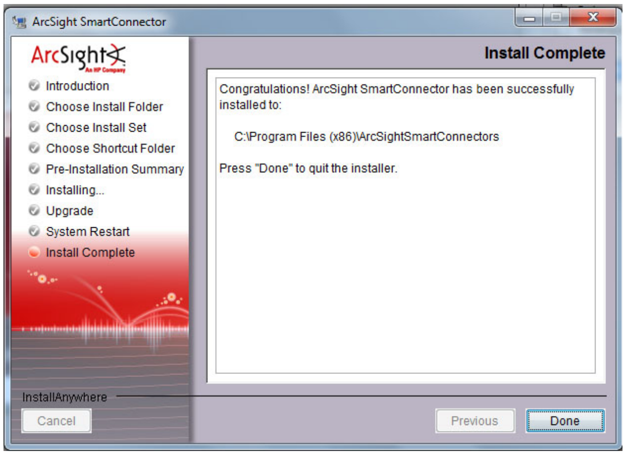


Would you like to continue or exit?

○ Continue

● Exit

Figure 84. “Exit” screenshot.



Install Complete

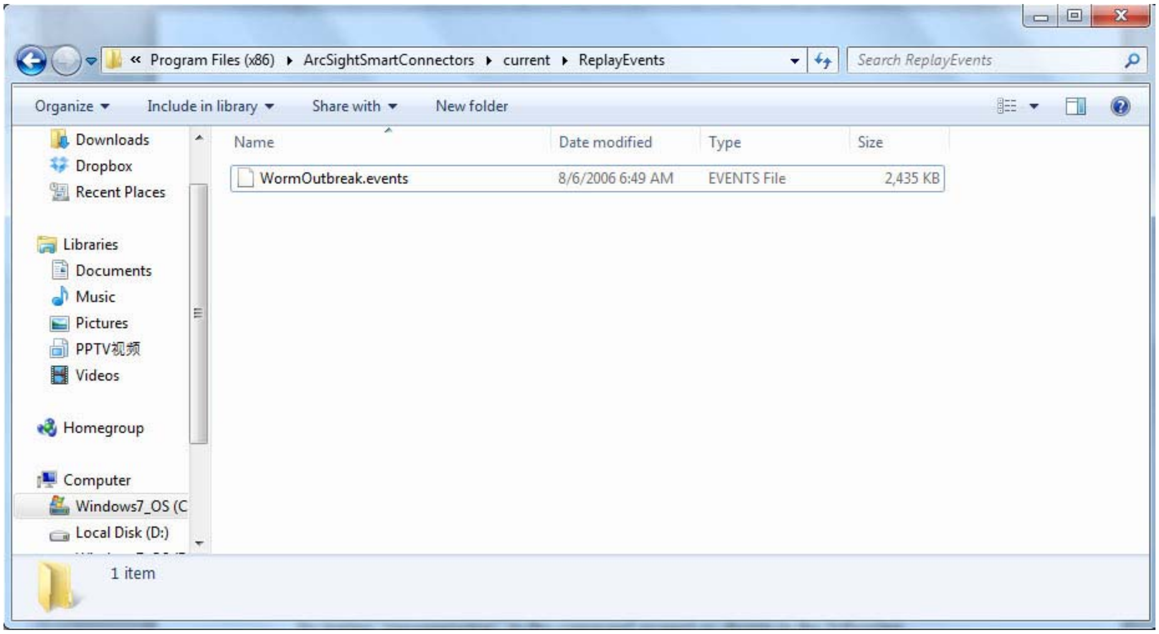
Congratulations! ArcSight SmartConnector has been successfully installed to:

C:\Program Files (x86)\ArcSightSmartConnectors

Press "Done" to quit the installer.

Figure 85. “Install complete” screenshot.

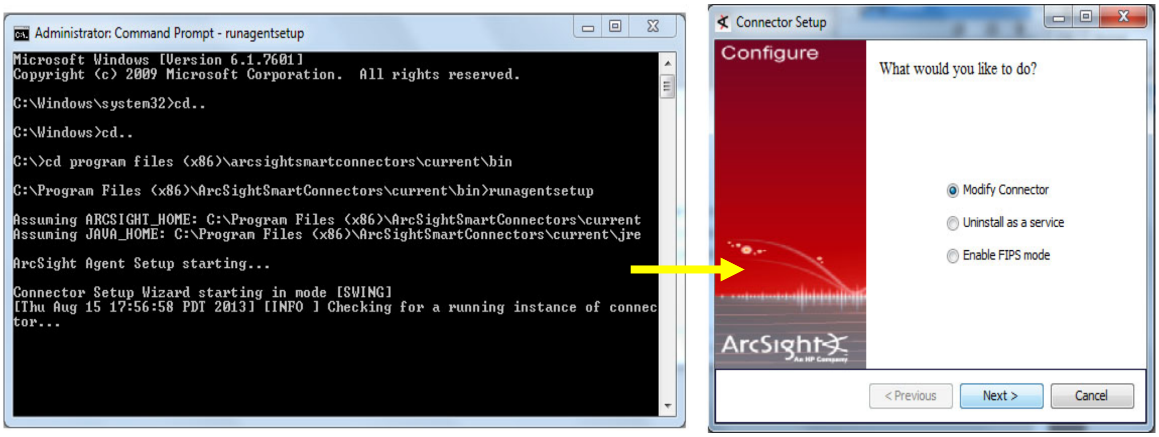
Once the replay connector has been installed successfully, create a ‘ReplayEvents” folder within the ArcSight SmartConnector folder, and copy the “WormOutbreak.events” file into it.



Name	Date modified	Type	Size
WormOutbreak.events	8/6/2006 6:49 AM	EVENTS File	2,435 KB

Figure 86. “ReplayEvents” folder screenshot.

The parameters of the replay connector (Figure 76) can be modified subsequently by typing “runagentsetup” in the command prompt as shown in the following:



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd..

C:\Windows>cd..

C:\>cd program files (x86)\arcsightsmartconnectors\current\bin

C:\Program Files (x86)\ArcSightSmartConnectors\current\bin>runagentsetup

Assuming ARCSIGHT_HOME: C:\Program Files (x86)\ArcSightSmartConnectors\current
Assuming JAVA_HOME: C:\Program Files (x86)\ArcSightSmartConnectors\current\jre

ArcSight Agent Setup starting...

Connector Setup Wizard starting in mode [SWING]
[Thu Aug 15 17:56:58 PDT 2013] [INFO ] Checking for a running instance of connec
tor...
```

What would you like to do?

● Modify Connector
○ Uninstall as a service
○ Enable FIPS mode

Figure 87. Modify replay connector’s configuration.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] Internet World Stats, “Internet World stats,” 30 June 2012. [Online]. Available: http://www.internetworldstats.com/stats.htm. [Accessed 6 May 2013].

[2] Business Rountable, “Growing Business Dependence on the Internet,” September 2007. [Online]. Available: http://businessroundtable.org/uploads/news-center/downloads/200709_Growing_Business_Dependence_on_the_Internet.pdf. [Accessed 6 May 2013].

[3] H. Howland, “Evolution of the Modern SIEM (Infographic),” 26 September 2011. [Online]. Available: http://blog.q1labs.com/2011/09/26/evolution-of-the-modern-siem-infographic/. [Accessed 13 May 2013].

[4] elQnetworks, “Organizations are suffering from SIEM deployments,” elQnetworks, 6 March 2013. [Online]. Available: http://www.eiqnetworks.com/press-release/eiqnetworks-survey-reveals-organizations-are-suffering-from-siem-deployments. [Accessed 12 May 2013].

[5] HP ArcSight, “Concepts for ArcSight Express v3.0,” Aug 2011. [Online]. Available: https://protect724.arcsight.com/servlet/JiveServlet/previewBody/2174-102-1-2721/ESM_101_AE_v3.0.pdf. [Accessed 04 Jun 2013].

[6] HP ArcSight, “Security Intelligence for a faster world,” May 2012. [Online]. Available: http://static.knowledgevision.com/account/idgenterprise/assets/attachment/WP_SFW_with_ArcSight_Express_rebranded.pdf. [Accessed 31 May 2013].

[7] HP ArcSight, “ArcSight Console User's Guide,” 21 Feb 2013. [Online]. Available: https://protect724.arcsight.com/docs/DOC-3151/AE_ArcSightConsoleGuide_4.0.pdf. [Accessed 04 Jun 2013].

[8] HP ArcSight, “SmartConnector User's Guide,” 24 Feb 2010. [Online]. Available: https://protect724.arcsight.com/servlet/JiveServlet/previewBody/1534-102-1-1761/SmartConnectorUsersGuide.pdf. [Accessed 17 Jun 2013].

[9] HP ArcSight, “Intrusion Monitoring Standard Content Guide,” 6 July 2012. [Online]. Available: https://protect724.arcsight.com/docs/DOC-2885. [Accessed 20 August 2013].

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California