An Analysis of Information Security Event Managers and the Data Extracted for Detecting Hidden Threats

Kutub Thakur, Sandra Kopecky, Moath Nuseir, Alecia Copeland, Nikhil Saxena, and Daniel Bivins
Seidenberg School of CSIS, Pace University, Pleasantville, NY

***Abstract*—The most effective security starts with real time visibility into all activity on all systems, networks, database and applications. The Security Event Manager is a system that detects tracks and identifies real time intrusion activities, whether the attackers use sniffer programs to access unauthorized resources; or the uses of eavesdroppers to intercept network traffic, or the intrusion of identity theft and invasion of malicious software. This paper focuses on structured data with some semi-structured and unstructured data also explored. Additionally, the paper will create awareness to present best solutions to contemporary security challenges whether the source is from network traffic, user activity, or application users, any variation from normal activity could indicate that a threat is imminent and that the data or infrastructure is at risk. In recent years, there has been a disturbing trend in which attackers are innovating much faster than the defenders. There has been a commercialization of malware with attack kits available through underground forums for those who want to perpetrate any variety of attacks. Large botnets are available for rent, allowing attackers to send spam or launch distributed denial-of-service attacks. Many attackers reuse malware and command and control and methods, adapting their products over time to keep ahead of the anti-malware industry and security professionals. This paper surveys Enterprise Security Managers and includes cyber-attack case studies.**

***Keywords*— Information Security, Security Information and Event Management, Cyber Security, Cyber Security Attack, Cyber Intelligence, Threat Analysis**

I. Introduction

Since the beginning of computer viruses along with other malicious software programs and the exploiting vulnerabilities of corporation networks, Cyber risk has grown from a relatively isolated data center problem to a top concern among senior executives in the corporate board rooms around the world. A worldwide survey by the Kaspersky Lab and B2B international indicated that 93% of the financial services organizations experienced various cyber threats in the last 12 month period between April 2013 and May 2014[1]. Early on, the financial world was the first target for cyber criminals. Today that cyber threat extends into not only public sectors but also private sectors worldwide. The cost, both monetary and time, of cybercrimes is increasing and additional there is also a growing systemic impact upon national and economic security. In this paper the Enterprise Security Manager (ESM) is examined as well as some case studies of various cyber-attacks.

Security Information and Event Management (SIEM) comprises of real-time monitoring, correlation of events, notifications, console views, analysis and reporting of log data from network and security devices. The term security information event management (SIEM), coined by Mark Nicolett and Amrit Williams of Gartner in 2005. [22] In this era of Big data and internet of things, the cyber security risk against an cyber attack has grown exponentially with larger volume, variety and velocity of data accessed. Continuous monitoring and analyzing large volumes of system generated log data defends the system and the resources against potential security threats.

“Big Data” describes data sets that are so large and complex that they are impractical to manage with traditional software tools. Big Data refers to the data creation, storage, retrieval and analysis in terms of volume, velocity and variety.

Security analytics fit this description of “Big Data” in that the amount of data that is collected in a short period of time, the variety of data that is collected, and the speed that this data is collected. Additionally, traditional software tools make the analysis of the data extremely difficult to sort through.

II. Case Study of an Enterprise Security Manager

Most organizations use some sort of security event management tools to gather and report on security data within their environments. There are organizations that have fallen through the cracks using traditional security methods which only lead to more being more vulnerable to security attacks. With the extent of the cyber threats today traditional log management tools are not enough and the need for more efficient and effective event intelligence as well as a deeper analysis of the activity within their environment with the use of, SIEM platforms. Organizations that have SIEM platforms will have the leverage in security event data. A Security Information and Event Management Survey in 2012 revealed that the majority of organizations are leveraging security event data for the following [3]:

- Detecting and tracking suspicious behavior
- Supporting forensic analysis and correlation
- Achieving/proving compliance with regulatory requirements

This case study noted that these are essentially the same use cases year after year, with a continued emphasis on saving time and making security operations as efficient as possible. As event data increases and cyber-attacks become more evolved the end goal is more and more complex.

A challenge that was found was the identification of key events from background activity – in other words, finding the needles in the haystack. Because the volume of day-to-day data increases detection any suspicious behavior is increasingly difficult even with SIEM tools.

SIEM tools just scratch the surface of being able to assist in detecting cyber threats to an organizations infrastructure because the amount and the complexity of attacks keep on rising and make the security protection to be vulnerable from attacks. On the other hand security teams must develop more sophisticated tools that can help them identify events quickly, distill large volumes of event data into simple timeframes for rapid analysis, and incorporate more types of data than ever before.

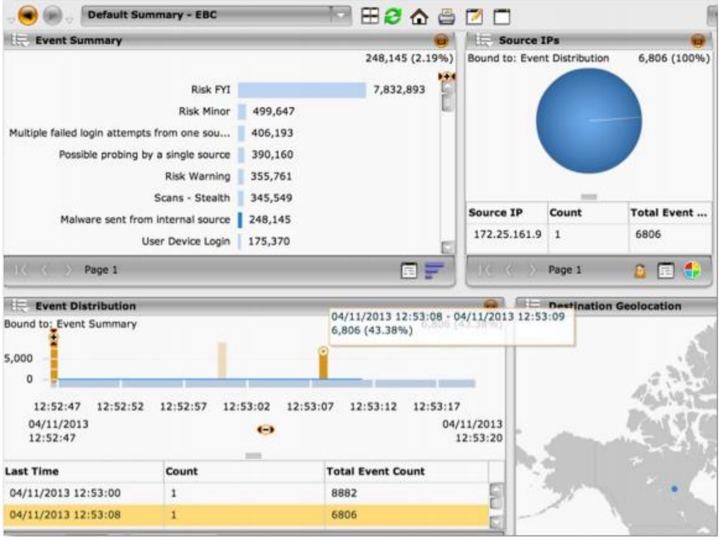
There were 43 million reported cyber-attacks reported this year [10]. This level of cyber-attacks has shifted organizations globally to develop and incorporate new sources of threat intelligence, with the hope of getting ahead of these threats. On top of this, analysts need tools they can implement with ease in a reasonable time period while quickly extracting meaning information from event stores. Data from a variety of correlated security information is useful as well.

This case study reviewed McAfee's ESM with a focus on fundamental SIEM features and capabilities.

A. *Rapid Event Analysis*

Given the amount of data many security teams are collecting today and the complexity of current threat scenarios, it is vital that the security teams be able to rapidly pinpoint events of interest and view granular details of events and network traffic. In breach and attack scenarios where seconds count, security teams will appreciate the ESM's ability to find what they're looking for quickly. It was found that the easiest way to get started was to find the specific information pane in the dashboard that we were interested in, highlight a data range or specific event type, and quickly "zoom" into this data for more in-depth searching and analysis.

After loading the various panes with specific event data to capture, the data was then drilled by highlighting a cross-section of the visible data. The process continued until an appropriate level of detail and granularity was reached. For example, successively smaller date ranges for events in the Event Distribution pane was selected until there were several thousand malware events within a several minute period on a single day. Highlighting any one of these events then updated the Source IP pane with the event's source IP address, as shown in Figure 1.



Default Summary - EBC

Event Summary

248,145 (2.19%)

Risk FYI	7,832,893
Risk Minor	499,647
Multiple failed login attempts from one sou...	406,193
Possible probing by a single source	390,160
Risk Warning	355,761
Scans - Stealth	345,549
Malware sent from internal source	248,145
User Device Login	175,370

Page 1

Source IPs

Bound to: Event Distribution 6,806 (100%)

Source IP	Count	Total Event ...
172.25.161.9	1	6806

Page 1

Event Distribution

Bound to: Event Summary

04/11/2013 12:53:08 - 04/11/2013 12:53:09
6,806 (43.38%)

Last Time	Count	Total Event Count
04/11/2013 12:53:00	1	8882
04/11/2013 12:53:08	1	6806

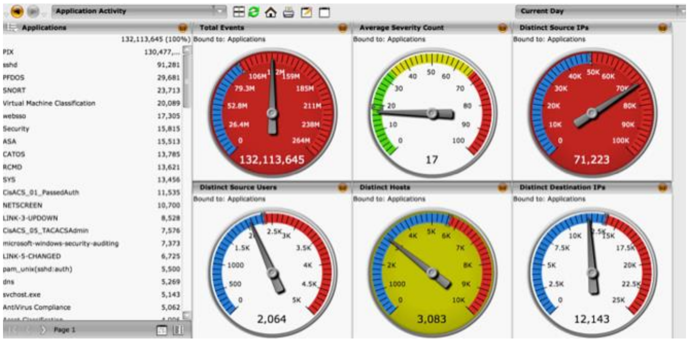
Destination Geolocation

Figure 1: Source IP pane with event source IP address

As for speed and efficiency, this level of fine-grained detail was reached in only a few seconds. Different dashboard panes and views were also explored.

1) *Application Activity:*

This view shows specific applications and services communicating in the environment. It was quick to discern the top traffic related to different services, in terms of hosts, source and destination users and IP addresses, and total events and severity of the events detected. Figure 2 shows this dashboard.



Application Activity

Current Day

Applications

132,113,645 (100%)

PIX	130,477,...
sshd	91,281
PFDOS	29,681
SNORT	23,713
Virtual Machine Classification	20,089
websso	17,305
Security	15,815
ASA	15,513
CATOS	13,785
RCMD	13,621
SYS	13,456
CisACS_01_PassedAuth	11,535
NETSCREEN	10,700
LINK-3-UPDOWN	8,528
CisACS_05_TACACSAdmin	7,576
microsoft-windows-security-auditing	7,373
LINK-5-CHANGED	6,725
pam_unix(sshd:auth)	5,500
dns	5,269
svchost.exe	5,143
AntiVirus Compliance	5,062

Page 1

Total Events — Bound to: Applications — 132,113,645

Average Severity Count — Bound to: Applications — 17

Distinct Source IPs — Bound to: Applications — 71,223

Distinct Source Users — Bound to: Applications — 2,064

Distinct Hosts — Bound to: Applications — 3,083

Distinct Destination IPs — Bound to: Applications — 12,143

Figure 2: Application Activity Dashboard

2) *Incidents:*

This dashboard showed us the correlated events over a given period, with source and destination IP addresses, events and event distribution over time, severity, and network flows between source and destination as shown in Figure 3, after some simple tuning and investigation.

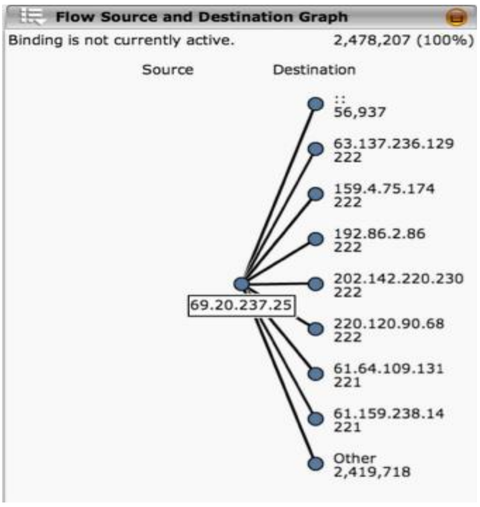


Figure 3: Network Flows Between Source and Destination

3) Flow—Packets by Destination and Source:

This is another useful gauge of network flows that has a quick display of source and destination IPs with the number of flows by packet count displayed as shown in Figure 4.

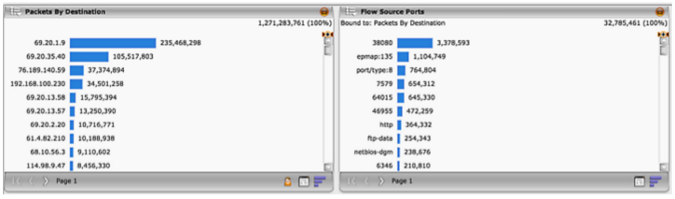


Figure 4: Number of Packets by Destination and Source

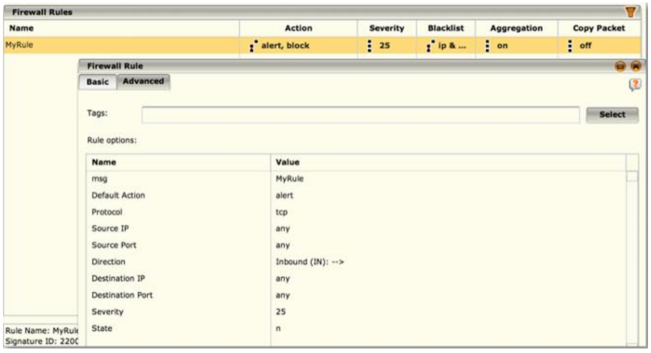
B. *Polices and the advanced correlation Engine*

Another area of focus is the policy and correlation rule engine within the ESM, which can be one of the most complex aspects of a SIEM system. Security teams need a relatively simple interface, coupled with a flexible and powerful rule engine. Most security teams spend a fair amount of time creating and tuning rules, so this process needs to be as easy to use as possible.

Using the policy editor, variables can first be evaluated or newly created. These variables are useful for defining network details and other data for use within rules and help clarify the purpose of the rules and simplify their creation. Many different rule types can be created in several major categories.

The first rule category is "IPS". This type focuses on intrusion detection and prevention capabilities. IPS preprocessor rules are anomaly detection and packet inspection rules and include fragmented packet analysis and reconstruction, port scan analyzers, HTTP traffic normalization and more.

Rules in the "Firewall" category cover basic packet analysis and traffic control; source and destination ports and IP addresses can be monitored and blocked, alerts can be sent, and other actions initiated. In addition, rules can be used to generate a blacklist of addresses and/or ports automatically, consolidate the blacklists into a unified view and take further steps. Figure 5 depicts firewall rule creation.



Firewall Rules

Name	Action	Severity	Blacklist	Aggregation	Copy Packet
MyRule	alert, block	25	ip & ...	on	off

Firewall Rule

Basic | Advanced

Tags: Select

Rule options:

Name	Value
msg	MyRule
Default Action	alert
Protocol	tcp
Source IP	any
Source Port	any
Direction	Inbound (IN): -->
Destination IP	any
Destination Port	any
Severity	25
State	n

Rule Name: MyRul
Signature ID: 220

Figure 5: Firewall Rule Creation

Deep Packet Inspection rules enable more advanced IPS rule customization and application through the use of rule attributes and options.

Another main rules category is the set of "Receiver" rules. These rules pertain to the McAfee Event Receiver, which can accept numerous event types, including firewalls, routers, and flow data, IDS/IPS, among others. Instantiating this class of rules is simple, enabling the user to define specific actions to be taken when the Event Receiver detects specific data types. "Application Data Monitor (ADM)" rules enable more complex and deeper analysis of application behavior profiles and traffic. "Database Event Monitor (DEM)" rules can monitor database transactions for a variety of events.

C. *Promoting Situational Awareness:*

Knowing what's taking place inside the network perimeter is only the beginning of what McAfee ESM can do when it comes to providing threat intelligence and early warning. An interesting feature is the Global Threat Intelligence (GTI) service, which centralizes and correlates threat and attack data from around the world and incorporates McAfee's own security research and analysis. This feature enables the delivery of reputation-based, relevant intelligence to numerous McAfee security platforms in a manner that facilitates real-time event correlation and threat identification. First, GTI creates automatic watch lists from globally noted malicious and suspicious IP addresses, which can be integrated into filters, rules and dashboard views to quickly see what GTI is now reporting. Figure 6 shows a sample dashboard display of GTI sources and events.

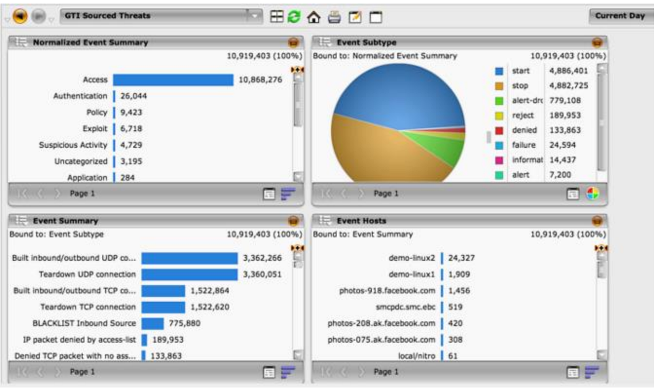


Figure 6: Global Threat Intelligence Dashboard

D. Reporting:

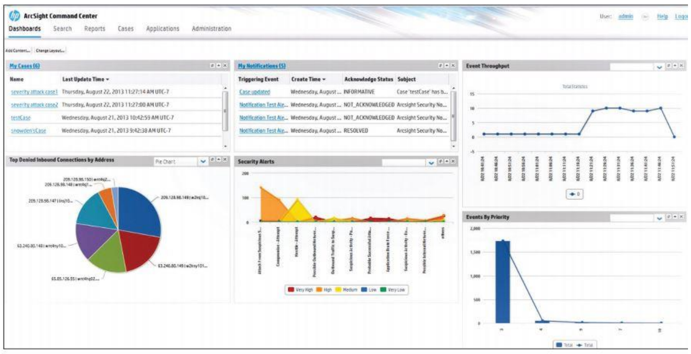
A variety of ESM reports, from high-level executive reports to more detailed ones focusing on event and correlation data was evaluated. The reports can be easily customized by using drag-and-drop design, storing them locally, and sending them to a defined remote location or e-mail them to users and/or groups.

With today's rapidly evolving threat landscape, the need to more quickly analyze an increasing amount of security event data over an expanding timeframe is evident. Security teams need the ability to assess and correlate data easily, track events for investigations, and report on security controls within the environment.[2]

III. HP ARCSIGHT ENTERPRISE SECURITY MANAGER

Today with a huge volume of data are available and the increasing number of cyber criminals which are getting more sophisticated, the security teams in the organizations needs software to help minimize these attacks on the organization system also it's not about minimizing and detecting the threats, but they need to protecting the system in timely manner by quickly detect and respond to breaking. In order for organizations to defend their important data and their infrastructure, they need quick and efficient software to detect and react to any attack. One of best software which we will review it in this paper is HP ArcSight ESM. Since the organization could have a multiple of types of devices, systems and networks, HP ArcSight ESM gives an essential point for analysis of everyday business process.

Lastly, HP ArcSight ESM has capabilities of visualization and reporting; the different kind of team members could schedule the reports and work on personalized dashboard. Figure 7 shows a sample of HP ArcSight dashboard.



My Cases (6)

Name	Last Update Time
severity attack case1	Thursday, August 22, 2013 11:27:14 AM UTC-7
severity attack case2	Thursday, August 22, 2013 11:27:00 AM UTC-7
testCase	Wednesday, August 21, 2013 10:42:59 AM UTC-7
snowden'sCase	Wednesday, August 21, 2013 9:42:38 AM UTC-7

My Notifications (5)

Triggering Event	Create Time	Acknowledge Status	Subject
Case updated	Wednesday, August ...	INFORMATIVE	Case 'testCase' has b...
Notification Test Ale...	Wednesday, August ...	NOT_ACKNOWLEDGED	Arcsight Security No...
Notification Test Ale...	Wednesday, August ...	NOT_ACKNOWLEDGED	Arcsight Security No...
Notification Test Ale...	Wednesday, August ...	RESOLVED	Arcsight Security No...

Figure 7: HP ArcSight Dashboard

A. Intuitive dashboards, robust reporting

Another feature could HP ArcSight ESM with Risk insight give it to us, it is a complete operational and technical report and that makes the management level of business to reporting different kind of reports, standard or customizable reports. Also the framework gives users opportunity to generate new report and template for ad hoc and scheduled reporting.

Figure 8 shows what we can get from the dashboard.

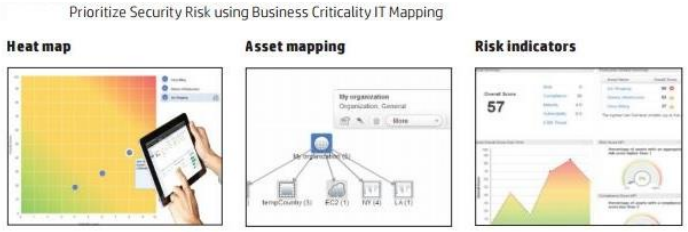

Prioritize Security Risk using Business Criticality IT Mapping
Heat map
Asset mapping
Risk indicators
57

Figure 8: HP ArcSight Dashboard Capabilities

In order for security team to catch the areas of risk and work on it to solve it and quickly answer key business questions, that needs framework merges the association information in the best way into fully views. When we have events and we need to check their impact in specific period of time then we should use Trend reporting because it allows us to track the event over time, another use for trend reporting when we change the policy in the organization and we would like to see what is the impact of changing the policy, the trend reporting used to simulate "what if" scenarios. Figure 9 shows the area of risk.

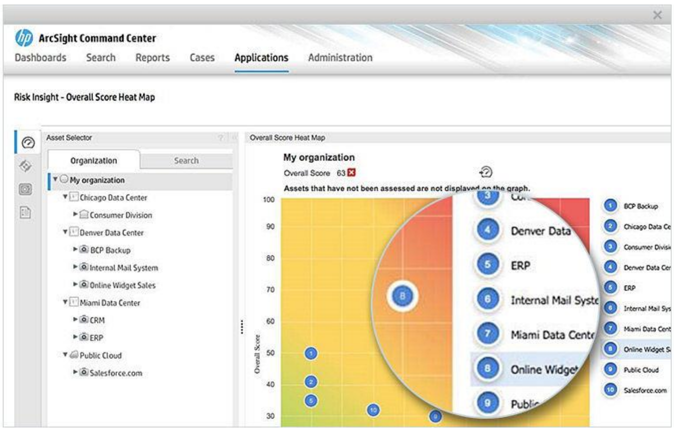


Figure 9: HP ArcSight Areas of Risk

B. Stop threats at the application layer

The HP ArcSight Application view can be used when we have the security problem because of inappropriate user access and handling of applications. In addition the application view can capture the real events directly from the application, without any change the application itself. The data what we had captured is associated with the HP ArcSight platform which help the security team to get current application security event intelligence without any customization.

The intelligence allows quick analysis of database retrieval, error messages, and other application-related attacks that can guide to loss of secret information

C. Automated intelligence and response

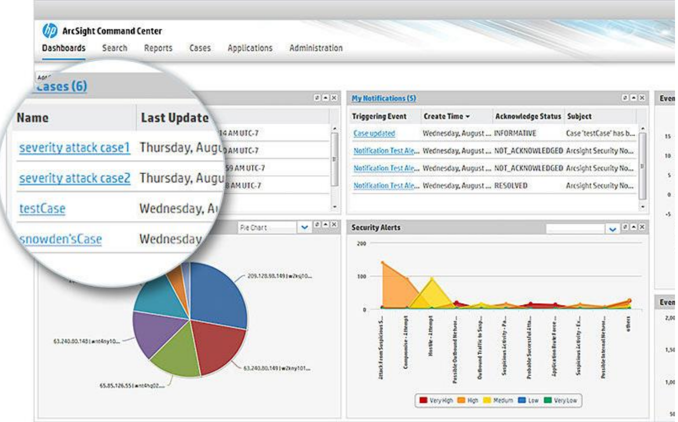
In order to make better capabilities of HP ArcSight ESM platform, we should use HP ArcSight Reputation Security Monitor (RepSM) by arranging attacks intelligence through the network flow analysis to separate out connection with malicious networks. The HP ArcSight Reputation Security Monitor (RepSM) works on different scenarios for detection and defending the threats at every stage. It could catch the threats before happing also after the threats occurs, the HP ArcSight Reputation Security Monitor (RepSM) could know which the areas affected by the threats. The organization can keep their intellectual assets safe by catching these threats quickly.

D. ArcSight Threat Detector

As we know detecting threats it's one of the main objectives of ESM and security teams responsibilities in any organization. So, HP ArcSight ESM has a hundreds of pre-built rules and alerts which are helping to detect the advanced threats. Threat detector has many activities to perform. Firstly, it will make the correlation engine of ArcSight to maintain historical activities which in turn will detect new patterns. As a result, the engine will use these patterns to automatically devise new rules. These rules have the ability to detect new threats likewise zero-day worms and misconfigurations of network devices, systems, and applications.

Secondly, analysts conducted a tool by the threat detector to differentiate the suspicious events were happened to your network from any other events. Consequently, many benefits are shown; ESM became specific to use-cases, and security operation resources were reduced.

Thirdly, the threat detector is able to find the insider attack or a compromised account. Finally, using such patterns will help the threat detector to restate the rules in order to capture the future activities where the managers can address early. Figure 10 shows the threats on the system.



ArcSight Command Center
Dashboards
Search
Reports
Cases
Applications
Administration
Cases (6)
My Notifications (5)
Pie Chart
Security Alerts
209.128.98.149 | w2ksj10...
63.240.80.148 | wnt4ny10...
63.240.80.149 | w2kny101...
65.85.126.55 | wnt4hq02...
200
100
0
Attack From Suspicious S...
Compromise - Attempt
Hostile - Attempt
Possible Outbound Networ...
Outbound Traffic to Susp...
Suspicious Activity - Pa...
Probable Successful Atta...
Application Brute Force ...
Suspicious Activity - Ex...
Possible Internal Networ...
others
🟥 Very High
🟧 High
🟨 Medium
🟦 Low
🟩 Very Low
Even

Name	Last Update
severity attack case1	Thursday, Augu
severity attack case2	Thursday, Augu
testCase	Wednesday, A
snowden'sCase	Wednesday

Triggering Event	Create Time	Acknowledge Status	Subject
Case updated	Wednesday, August ...	INFORMATIVE	Case 'testCase' has b...
Notification Test Ale...	Wednesday, August ...	NOT_ACKNOWLEDGED	Arcsight Security No...
Notification Test Ale...	Wednesday, August ...	NOT_ACKNOWLEDGED	Arcsight Security No...
Notification Test Ale...	Wednesday, August ...	RESOLVED	Arcsight Security No...

Figure 10: HP ArcSight Command Center – Attack Monitoring

E. HP ArcSight Threat Response Manager

Finally after the threats are recognized, we need to remove these threats. And the Threat Response Manager (TRM) gives you the opportunity to automate and reduce the time needed to remove these threats. By shortening the reaction times, you can deal with the business hazard in a more proactive style, permitting to lessen expenses and expand adaptability in the way you convey the frameworks to meet the company remarkable needs. [11]

IV. Symantec Enterprise Security Manager

Corporations handle large amounts of information in complex computer environments with multiple platforms and integrated networks. The client or the server system solves the challenge of accessing this information quickly and easily. However, client or the server computers can leave sensitive data vulnerable to unauthorized access or modification. Organizations need to secure their data against unauthorized use while still providing easy access to authorized users on multiple platforms. They need a way to apply security policies, then monitor and enforce compliance throughout the enterprise network. Symantec provides the solution to security policy management with the Symantec Enterprise Security Manager (ESM).

The primary functions of Symantec ESM are as follows:

1) Manage security policies

2) Detect changes to security settings or files

3) Evaluate and report computer conformance with security policies

A. Components of Symantec Enterprise Security Manager

Symantec ESM has the following components:

A. Console

B. Manager

C. Agent

B. Symantec Enterprise Security Manager Functions

1) Perform policy runs: Policy runs audit the computers to find potential areas of vulnerability. When you perform policy runs, Symantec ESM reports security problems and their severity. You initiate policy runs from either the graphical user interface or the command-line interface. Symantec ESM uses agents to perform the policy runs. Policy runs are host-based. Symantec ESM provides a module that lets you perform network-based scans of computers without installing an agent on each computer.

2) Customize policies: Symantec ESM lets you create your own custom policies and apply the policies that are tailored to your needs. You can implement the policies that are specific to your industry, or you can implement the policies that ensure compliance with a government mandate.

3) Create reports: Symantec ESM has a powerful reporting tool that lets you dynamically create reports. You can report on any aspect of your Symantec ESM application. You can create reports on managers, agents, user accounts, or any other item that you choose. The reports can be broad and show only security states of managers or domains. They can also be detailed enough to show a specific security check on a few selected computers.

C. How Symantec Enterprise Security Manager works

Symantec ESM uses a flexible agent and manager architecture to scale the product over the enterprise. This architecture lets you adapt Symantec ESM to changes in network structure by adding agents for new operating systems and platforms. Figure 11 shows how the Symantec Enterprise Security Manger works.

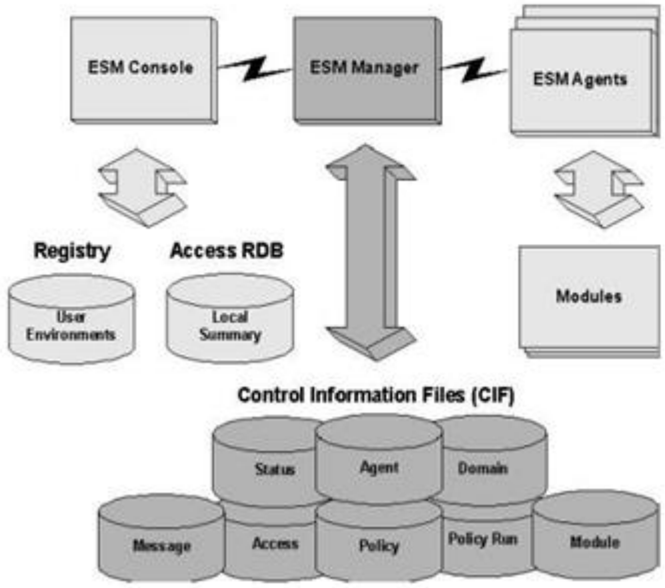


Figure 11: Symantec Enterprise Security Manager Architecture

The Symantec ESM structure consists of the following components: the agent, manager, and ESM console. In addition, Symantec ESM provides the command-line interface (CLI) as an alternate way to run security functions. Symantec ESM also provides utilities to do the following:

- Copy security information from the managers to a database
- Produce standard or custom reports from the information in the database

Another main feature of Symantec Enterprise Security Manager is how will be the viewing the summary and detailed data. Symantec Enterprise Security Manager presents its findings in either a summary or detailed format. The summary data provides an overall picture of the organization's security. The detailed information provides information on specific security violations. Symantec Enterprise Security Manager helps focus your efforts on critical security issues through identification and presentation of compliance issues in multiple formats.

To use Symantec Enterprise Security Manager, you must be able to interpret the information in the ESM console grid and chart. The ESM console displays security data in the following modes:

- Drill-down
- Summary
- Trend

1) Drill-down mode

The drill-down chart displays the current level and score of the objects that are directly beneath the selected object in the summary branch. For example, if you select a policy in the summary branch, the drill-down chart displays the security level and score of the modules that are in that policy. You can expand the tree and access successively lower levels of information. You can access the information by clicking the nodes that are next to the objects in the summary branch. You can access the information also by clicking the colored portions of the chart or chart legend.

2) Summary mode

The summary chart shows a count by security level of the objects that are under the selected object in the summary branch. For example, if you select a policy, the summary chart displays a count by security level of the modules in that policy. The summary chart appears in pie chart format by default. You can select the toolbar icon, click the chart or legend, and change the display to drill-down mode.

3) Trend mode

The trend chart portrays changes in a selected object's security level and score over time. You can view changes in security level and score on a daily or a weekly basis. An explanation of each follows:

- Daily
  Symantec Enterprise Security Manager displays the security level and score of the last run that occurred before 11:59 PM each day.
- Weekly
  Symantec Enterprise Security Manager displays the security level and score of the latest run that occurred before 11:59 PM each Saturday.

V. Case Study of Various Cyber attack

Organizations that invest in a SIEM are often frustrated and disappointed by the amount of investment in technology and people it takes to generate useful information. Whether it is maintaining the separate data sources that supply the SIEM tool with security events to analyze, or writing the correlation rules to make sense of the mountain of event data, SIEM platforms are not easy to maintain as seen above. Unified Security Management (USM), which has built in data sources and over 2000 correlation rules provides any IT team with limited resources and all in one threat detection and compliance management Platform. Below are some SIEM use cases examples that show how a SIEM using USM can detect a range of threats and deliver the insight of threats that include:

A. SQL Injection and Other Web Application Attacks:

Identify the vulnerable public-facing systems that are easily targeted, detecting attacks directed at vulnerable systems, and using alerts on compromised systems communicating with attackers.

SQL Injection attacks are one the most common attacks of public-facing websites due to the high number of SQL vulnerabilities. The attacks succeed when an attacker sends specially crafted commands to the SQL server that exploit vulnerability in the software. An essential first step in detecting this SIEM use case example is to identify all systems running SQL (particularly public-facing systems). This is available through the USM. An asset group of all systems running SQL can be created and monitored to ensure you are aware of any changes to the status of those systems. Alerts are sent of any compromised systems communicating with known malicious hosts. Malware, once it compromises a system on a network might attempt to communicate with the Command and Control server. The SIEM software, plus global visibility of known malicious hosts, will send alert notifications of those compromised systems communicating with the Command and Control servers.

B. *Watering Hole Attacks:*

Detect malware that attempting to install on systems and alerts when multiple malware threats are from the same compromised website.

Watering Hole attacks target specific groups of users (such as government agencies, industries, or political organizations) who are likely to frequent specific websites. The attacker installs malware on the site that then attempts to compromise visitors' systems. In this SIEM use case example, the USM can detect the different stages of a Watering Hole attack and send alerts of its presence in the network before any infiltration of user credentials or confidential data occur. The built-in IDS within the USM platform will detect the delivery of the malware payload from the compromised website. The continuously updated correlation rules can correlate multiple malware infections from the same comp IDS will also detect malware attempting to traverse the network and compromise other systems. The SIEM capability's built-in correlation rules will also detect the outbound communication as the malware attempts to establish a communication channel with the Command and Control server before infiltrating the harvested data.

C. *Malware Infection:*

Identify the communication from known malicious hosts, detecting malware infecting systems, and alerts on changes to services and/or privilege escalation as a result of a successful attack.

Malware is still the preferred method for gaining an initial foothold within a network, because of the ease with which attackers can install it on at least one system. Traditional preventive security technologies cannot keep all malware out, and the best defense is to be able to spot the malware and remove it before it can facilitate a data breach. In this SIEM use case example, the SIEM software correlates events within the USM platform to send alerts of the presence of malware in several ways. One way is that the integrated community-powered threat data from the Open Threat Exchange (OTX) detects inbound communication from known malicious hosts, alerting you to those hosts in your network that may have inadvertently installed malware contained in an email or drive-by download. It detects outbound communication with malicious hosts as well, which could indicate a compromised system communicating with the Command and Control server.

Additionally, the USM's built-in IDS detects malicious code on the network and correlates that data with the built-in Asset Discovery and Vulnerability Assessment capabilities to alert you to traffic that is specifically targeting vulnerable systems. The USM will also generate alerts when malware attempts to stop essential security services and change files on the targeted systems, a technique used to hide signs of the compromise from you. It can also detect privilege escalation on targeted systems as attackers seek "Admin" or "root" access.

D. *Ransomware Threat/Attack*

Ransomware threats such as Cryptowall, which encrypts the data and demands payment to unlock the data, are increasing. These threats are delivered via malicious email attachments or links to websites, and once they execute and connect to an external command and control server, they start to encrypt files throughout the network.

The USM uses several built-in security controls that work in unison to detect ransomware, usually as soon as it attempts to connect to the hackers' command and control server.

E. *Continuous Compliance Management:*

Consolidate and automate critical security controls, understand critical events and compliance status with network-wide visibility, and utilize hundreds of built-in, customizable reports.

It is a challenge for organizations to achieve compliance while managing competing priorities, limited budgets, and small IT security teams with limited expertise. Regardless of which standard that is trying to be met, it is essential to be able to consolidate and automate the critical security controls to simplify the compliance efforts.

In this SIEM use case example, the USM platform works as a single solution that automatically identifies audit events, generates alarms on those events that require immediate attention, and creates reports that satisfy the auditor. Regardless of which set of requirements or guidelines that are trying to be met, the USM has a complete solution that builds in asset discovery, vulnerability assessment, host and network intrusion detection, file integrity monitoring (FIM) and SIEM –all in a single platform and console view.

With the USM, the insight needed to understand the location and compliance status of critical assets, network segmentation, vulnerabilities on those assets, access privileges to those assets, and so on, can quickly be obtained. [4]

VI. OBSERVATION

One aspect that the authors have noted is that what might be considered a non-issue for a cyber-attack such as an invalid password, could possibly be a potential cyber-attack over time. For example, if a hacker repeatedly tries a password knowing that the alert is raised on the fourth attempt then they may stop at just three and go to another login source or wait for some time period. The event by itself is not an alert, but grouped together would be an alert. The problem exists in storing this data that on its own is not an issue and for how long to store the data. Another issue is what data is then mined for analysis it is not deemed a threat. How does the ESM determine if a user just left the caps lock on versus a hacker? Acceptable Use Monitoring covers a basic questions, i.e. what resource is being accessed by whom and when. Organizations generally publish policies for users to understand how they can use the organization's resources in the best way. Organizations should develop a baseline document to set up threshold limits, critical resources information, user roles, and policies, and use that baseline document to monitor user activity, even after business hours, with the help of the SIEM solution.

VII. SIEM Data Experimental results

The authors have experimented with data from AlienVault in the following three categories.

1) Security systems: includes systems and devices that perform some security function on the network. For example, authentication systems, firewalls, network intrusion detection and prevention systems (IDS/IPS), virtual private network devices (VPNs), host-based intrusion detection systems (HIDS), wireless security devices, and anti-malware systems.

2) Business critical systems: includes those systems that are important for running the network. For example, mail servers, DNS servers, web servers, authentication servers. When establishing which infrastructure systems are most critical, try to determine what the business impact would be if the system was unavailable. This category of system also includes more traditional network devices such as routers, switches and wireless network devices.

3) Critical infrastructure systems: includes those systems that are important for running the network. For example, mail servers, DNS servers, Web servers, authentication servers. When establishing which infrastructure systems are most critical, try to determine what the business impact would be if the system was unavailable. This category of system also includes more traditional network devices such as routers, switches, and wireless network devices.

In the experiment, a centralized logging architecture was used to collect the data logs. Commercial SEM systems all have their own solutions for collection, processing and storage of security events. However, generally the approach is to centralize these functions so that security events are forwarded to centrally managed, dedicated SEM servers. There are many advantages to this approach such as centralized backups, searching, and analysis capabilities of huge data. For scalability, the SEM servers can be organized in a hierarchical manner, with local SEM servers situated near to the monitored systems. The function of local SEM servers is to collect, process, and queue events for transmission to the next tier. Figure 12 depicts a hierarchical system with local SEM servers and a master SEM server.

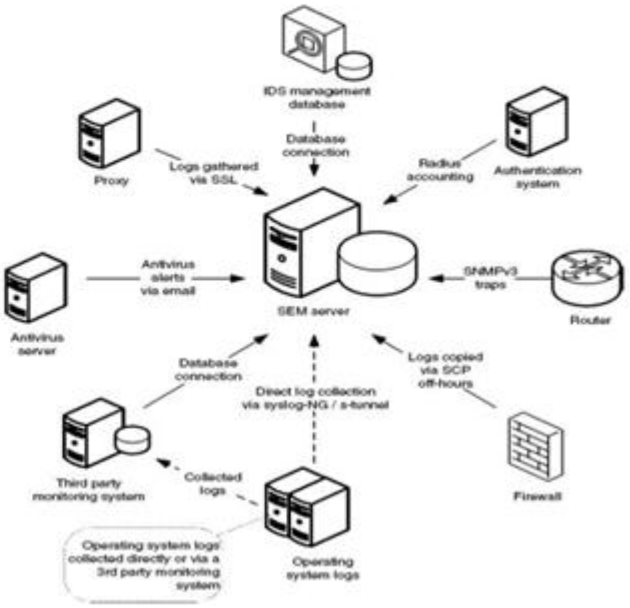


Figure 12: Hierarchical system with local SEM servers and a master SEM server

The primary requirement of the master SEM server is plenty of local storage (hard disk, optical disk, tape). If searches, analysis, or other processing is performed on this server, it also needs fast CPUs, RAM, and disk. Local SEM servers will have leaner specifications because they do not need to store or process as much information. In more complex environments, a relational database (RDBMS) is typically used to store security events. Relational databases organize and index security logs, alerts, and other information for rapid searches and report generation. Commercial SEM systems use databases to organize and store security events for analysis, reporting, and display.

After security events reach the central SEM server, they will be stored on disk for some period of time. How long the logs are on disk depends on the size of the logs, budget, security requirements, and business requirements. Typically, logs will be stored on disk ("online") for a few weeks or months, and this is mostly dependent on how much disk space is available. It is advantageous to keep logs on disk because this allows for convenient access to the data, and all operations such as searching will be quicker. There might be a security requirement to store logs in a read-only form in which case a write-once, read-many (WORM) form of media such as optical disk will be necessary. In our experimental environment, the data was collected from the central logging servers for monthly and daily basis to analysis threats landscapes of malware infection. Figure 13 shows the malware infection results data for a month that were collected during our experiment for various targets

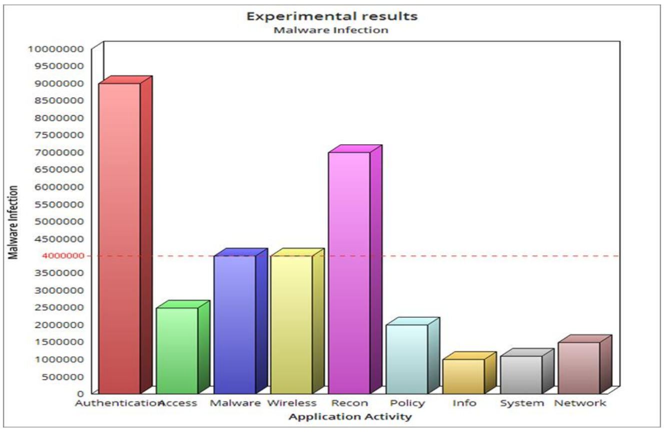
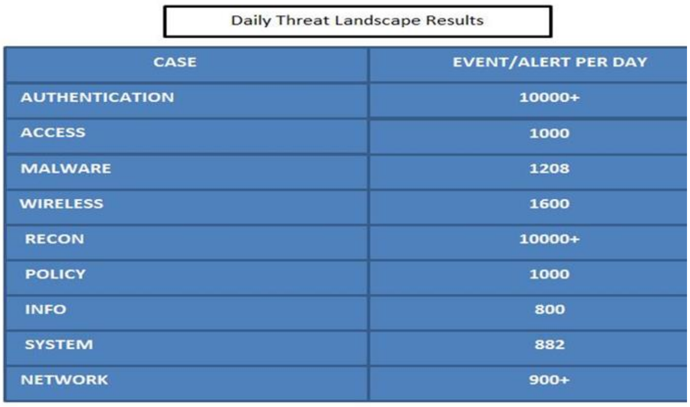


Figure 13: Malware infection data collection results for a month

An organization's data retention policies should dictate how long information such as logs must be stored, and what requirements there are for storage and disposal of the information. If there is no data retention policy, then this needs to be defined so that information is kept for as long as it is needed, but for no longer than is necessary. In the experiment data retention was for a month, as daily and then monthly data was analysis and validated by the team members to make sure that the experimental production environment was collecting the data according to the experiment setup. Figure 14 shows the daily threat landscape data results.



Daily Threat Landscape Results

CASE	EVENT/ALERT PER DAY
AUTHENTICATION	10000+
ACCESS	1000
MALWARE	1208
WIRELESS	1600
RECON	10000+
POLICY	1000
INFO	800
SYSTEM	882
NETWORK	900+

Figure 14: Daily Threat Landscape Results

The goal of the SEM rule system is to reduce the data volume from an unmanageable number of events down to a small number of actionable alerts that can be reviewed by security analysts. Security events are collected by the system, and pass through categorization, prioritization, filtering, and other stages in which alerts are generated. The end result is that a smaller number of actionable alerts are generated for security analysts to review. Commercial systems generally operate in a similar way with several processing stages. Figure 15 depicts how processing stages affect event volume.

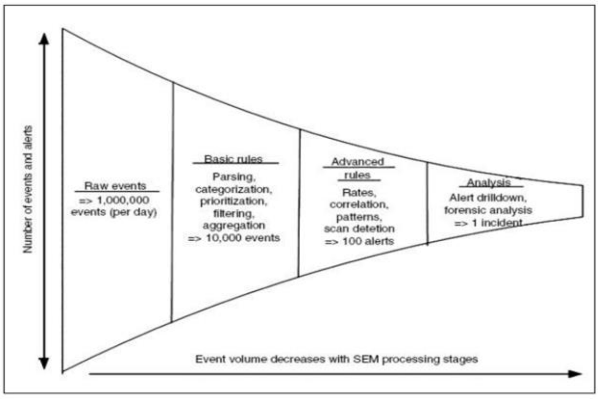
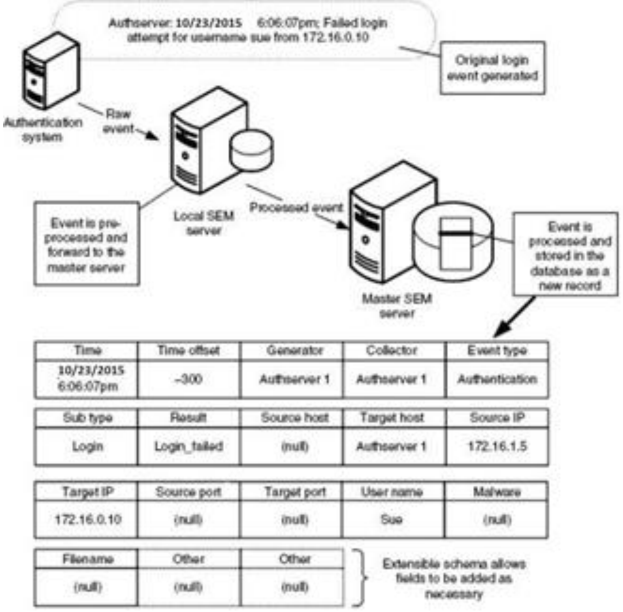

Number of events and alerts
Raw events
=> 1,000,000 events (per day)
Basic rules
Parsing, categorization, prioritization, filtering, aggregation
=> 10,000 events
Advanced rules
Rates, correlation, patterns, scan detetion
=> 100 alerts
Analysis
Alert drilldown, forensic analysis
=> 1 incident
Event volume decreases with SEM processing stages

Figure 15: How processing stages affect event volume

Event parsing is usually the first stage in a SEM system. The goal of this stage is to extract useful information from the security events so that they can be further processed by later stages. Security events are extracted into "fields" of information such as timestamp, event source, event type, username, hostname, source IP address, target IP address, source port, target port, message, etc. Because each device generates events in a different format, specific parsers need to be created for each type of device. Figure 16 shows the authentication failure for the specific user at specific time.


Authserver: 10/23/2015 6:06:07pm: Failed login attempt for username sue from 172.16.0.10
Original login event generated
Authentication system
Raw event
Local SEM server
Event is pre-processed and forward to the master server
Processed event
Master SEM server
Event is processed and stored in the database as a new record
Extensible schema allows fields to be added as necessary

Time	Time offset	Generator	Collector	Event type
10/23/2015 6:06:07pm	-300	Authserver 1	Authserver 1	Authentication

Sub type	Result	Source host	Target host	Source IP
Login	Login_failed	(null)	Authserver 1	172.16.1.5

Target IP	Source port	Target port	User name	Malware
172.16.0.10	(null)	(null)	Sue	(null)

Filename	Other	Other
(null)	(null)	(null)

Figure 16: Authentication Failure Results

In a sample data size of 50 days, there were over 800,000 password authentication failures, and of those events about half of them were in excess of the number set in the security policy. Analyzing this subset of data we can find when an IP address has attempted to authenticate with some number of failures less than specified in the security policy, thus not raising an alert to be investigated. Looking at this data over a period of time a pattern may arise that shows repeated attempts. Figure 17 shows a simple chart of this of a subset of the data.

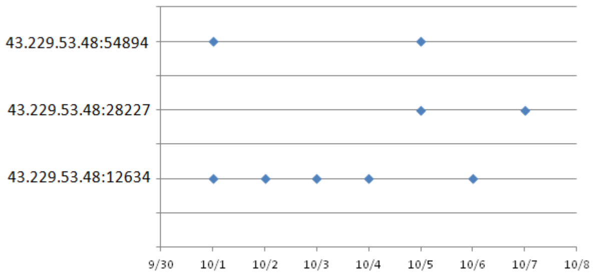


Figure 17: Authentication password tracking by IP over time

In many organizations, security policies or business regulations require that security events are monitored and that security logs are reviewed to identify security issues. Information captured in security logs is often critical for reconstructing the sequence of events during investigation of a security incident, and monitoring security logs may identify issues that would be missed otherwise. The problem is that the amount of information generated by security devices and systems can be vast and manual review is typically not practical. Security event management (SEM, or SIM-security information management) aims to solve this problem by automatically analyzing all that information to provide actionable alerts. In a nutshell, security event management deals with the collection, transmission, storage, monitoring and analysis of huge security events. [17, 18, 19, 20, 21]

VIII. Conclusion

An ESM is compromised of a number of components that work together to provide meaningful data that can be easily and quickly evaluated to detect a cyber attack upon an organization's infrastructure. The ESM uses a variety of graphical displays in order to group, manage and monitor the large amount of data that is constantly streaming. The aspect that this group has noticed is that while the immediate attack is easily recognized, there is a potential for cyber attacks that are not easily patterned within the many given constraints. Additionally, it is feasible to use these same algorithms to analyze specific threats and attacks that occur over time to find a common source. Determining what attributes of the data over what amount of time is a critical and crucial aspect that must be implemented into an organization's policy in order to find these threats.

References

[1] 'Global IT Security Risks 2014 - Online Fraud Protection', 2015. [Online]. Available: http://media.kaspersky.com/en/IT_Security_Risks_Survey_2014_Financial_Security_report.pdf.

[2] Sans.org, 'Security Intelligence in Action: SANS Review of McAfee Enterprise Security Manager (ESM) 9.2', 2015. [Online]. Available: https://www.sans.org/reading-room/whitepapers/analyst/security-intelligence-action-review-mcafee-enterprise-security-manager-esm-92-35095

[3] 'SANS Eighth Annual 2012 Log and Event Management Survey Results: Sorting Through the Noise', 2015. [Online]. Available: https://www.sans.org/reading-room/analysts_program/SortingThruNoise.pdf.

[4] Alienvault.com, 'SIEM Use Cases and Benefits | AlienVault', 2015. [Online]. Available: https://www.alienvault.com/solutions/siem-use-cases.

[5] P. Stephenson, 'McAfee Enterprise Security Manager v9.3.2', SC Magazine: For IT Security Professionals (15476693); April 2014, Vol 25 Issue. 4, p. 46

[6] P. Stephenson, 'McAfee Enterprise Security Manager (ESM), SC Magazine: For IT Security Professionals (15476693); May 2015, Vol 26 Issue. 5, p. 46

[7] Alien vault demo – https://alienvault.com / https://demo.alienvault.com/ossim/session/login.php

[8] SecureNation, 'McAfee Global Threat Intelligence for Enterprise Security Manager SIEM - SecureNation', 2015. [Online]. Available: http://securenation.net/partners/mcafee/mcafee-global-threat-intelligence-for-enterprise-security-manager-siem.

[9] I. Kotenko and A. Chechulin, 'Common Framework for Attack Modeling and Security Evaluation in SIEM Systems', 2012 IEEE International Conference on Green Computing and Communications, 2012.

[10] F. Cheng, A. Azodi, D. Jaeger and C. Meinel, 'Security Event Correlation Supported by Multi-Core Architecture', 2013 International Conference on IT Convergence and Security (ICITCS), 2013.

[11] Www8.hp.com, 'Enterprise Security Management System, ArcSight ESM Software | Hewlett Packard Enterprise', 2015. [Online]. Available: http://www8.hp.com/us/en/software-solutions/arcsight-esm-enterprise-security-management/#!&swanchor=details

[12] Ndm.net, 'ArcSight ESM | arcsight', 2015. [Online]. Available: http://www.ndm.net/siem/arcsight/arcsight-esm.

[13] Mcafee.com, 'McAfee Enterprise Security Manager - SIEM | Intel Security Products', 2015. [Online]. Available: http://www.mcafee.com/us/products/enterprise-security-manager.aspx

[14] Securitywizardry.com, 'Home - securitywizardry.com', 2015. https://www.securitywizardry.com/

[15] Gsialliance.com, 'Cybersecurity Case Studies', 2015. http://www.gsialliance.com/tnewslist.html?lsid=50

[16] Kaspersky.com, 'Kaspersky Lab Patents New Technology to Enhance Virtual Desktop Infrastructure Security | Kaspersky Lab', 2015. http://www.kaspersky.com/about/news/product/2015/Kaspersky-Lab-Patents-New-Technology-to-Enhance-Virtual-Desktop-Infrastructure-Security

[17] K. Laudon and J. Laudon,*Management information systems*. Boston: Prentice Hall, 2012.

[18] D. Miller, *Security information and event management (SIEM) implementation*. New York: McGraw-Hill, 2011.

[19] Hill, Douglas W., and James T. Lynn. "Adaptive system and method for responding to computer network security attacks." U.S. Patent 6,088,804, issued July 11, 2000.

[20] G. Marakas, J. O'Brien and J. O'Brien, *Introduction to information systems*. New York, NY: McGraw-Hill/Irwin, 2013.

[21] Karlzén, Henrik. "An Analysis of Security Information and Event Management Systems-The Use or SIEMs for Log Collection, Management and Analysis." (2009).

[22] Amrit Williams Blog, 'The Future of SIEM – The market will begin to diverge', 2007. https://techbuddha.wordpress.com/2007/01/01/the-future-of-siem-%E2%80%93-the-market-will-begin-to-diverge/

[23] Gabriel, Roland, et al. "Analyzing malware log data to support security information and event management: Some research results." *Advances in Databases, Knowledge, and Data Applications, 2009. DBKDA'09. First International Conference on*. IEEE, 2009.

[24] Aguirre, Idoia, and Sergio Alonso. "Improving the automation of security information management: A collaborative approach." *Security & Privacy, IEEE*10.1 (2012): 55-59.

[25] Cardenas, Alvaro A., Pratyusa K. Manadhata, and Sreeranga P. Rajan. "Big data analytics for security." *IEEE Security & Privacy* 6 (2013): 74-76.