SECURING COMPUTER NETWORKS USING CYBER ANALYTICS

By

Hafsa Hafeez

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Information Security

July 2017

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis written by ~~Mr~~/MS **Hafsa Hafeez** Registration No. **NUST2013-62700-MMCS25213F**, of **Military College of Signals** has been vetted by undersigned, found complete in all respect as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial, fulfillment for award of MS/MPhil degree. It is further certified that necessary amendments as pointed out by GEC members of the student have been also incorporated in the said thesis.

Signature: ___________________________

Name of Supervisor Col Baber Aslam, PhD

Date: _______________________________

Signature (HoD): ______________________

Date: _______________________________

Signature (Dean): ____________________

Date: _______________________________

ABSTRACT

Cyber threat environment has changed drastically over the past few years. Attacks are increasing in sophistication. Organizations use various security tools for keeping them secure. Still, many organizations face data breaches. To keep up with changing landscape of the threats there is a need to have a well-equipped Security Operation Centre (SOC). SOC contains people, processes and technology. Organizations invest a lot in security devices (technology). Inadequacy of the tools makes them suffer through huge losses. There are various independent security tools available for securing networks. These tools are area specific and generate alerts for few specific attack scenarios. For detecting widespread attack scenarios, there is a need of correlation of alerts generated by various tools. SIEM addresses the need of central management and correlation of alerts. This thesis provides the evaluation criteria for selecting the best suitable SIEM solution according to organization's needs. Also, it tests SIEM for various context-aware and behavioral analysis test cases which highlights its incapability of handling advance cyber-attacks. Furthermore, it proposes a solution for handling advance cyber-attacks based on their contextual information and behavior. The proposed solution once integrated with SIEM would help in central management of alerts for known signature based attacks and would generate alerts for advance cyber-attacks.

ACKNOWLEDGMENTS

I am in debited to Almighty Allah who gave me health, strength, courage and wisdom to accomplish another milestone of my academic career. I would first like to express my profound gratitude to my thesis advisor who guided and motivated me at every step during the research phase; His continuous encouragement always helped me to cross the trouble spots during my research phase. His consistent guidance steered me in the right direction to achieve this target. I would also like to thank the faculty members of the Department of Information Security, Military College of Signals whose patronage led to accomplishment of this research.

Finally, I must express my sincere thanks to my parents and to my spouse for providing me with unflinching support, continuous encouragement and prayers throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without their support.

TABLE OF CONTENTS

1. INTRODUCTION

2. CYBER THREAT ENVIRONMENT AND DEFENCE MECHANISIM

3. SECURITY INFORMATION AND EVENT MANAGEMENT

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

C&C	Command and Control Server
DOS	Denial of Service
DPI	Deep Packet Inspection
HIDS	Host-Based Intrusion Detection System
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
MSSP	Managed Security Service Provider
NIDS	Network-Based Intrusion Detection System
OSSEC	Open Source Host-Based Intrusion Detection System
OTX	Open Threat Exchange
Prads	Passive Real-time Asset Detection System
SIEM	Security Information and Event Management System
SMB	Small medium business
SOC	Security Operation Centre
SSH	Secure Socket Shell

Chapter 1

INTRODUCTION

1.1 Introduction

Computer networks are an important part of today's IT world. The number of internet users in Pakistan is increasing rapidly with the passage of time. According to the statistics published in 2013, internet users in Pakistan have exceeded 30 million in number [1]. Most of the organizations are now using computers, laptops and smart devices for storing, processing and transferring their information. It helps them to access the information easily from within or outside the organization's network. The confidentiality, integrity and availability of the information decide the organization's fate. Therefore, the level of protection of the computer network against attacks represents the maturity of organization. Every organization needs defense mechanisms to keep the network safe against attacks.

Cyber-attacks are becoming sophisticated day by day. Even with the increase in implementation of security controls, according to Verizon Breach Report [2], 43% of the companies suffered data breaches. Data breaches occur because of the three main reasons; malicious attacks, system glitches that are exploited and human negligence. Attackers nowadays use advance mechanisms to attack the organizations and individuals. Previously, attackers only had short term goals e.g. invading in the network for getting particular sensitive data and leaving the network afterwards. But now, they have both short term and long terms goals. The main aim of an attacker is to get access to the resources for a long period, stay undetected and capture maximum sensitive information e.g. exfiltration of terabytes of private data from Sony's network [3]. To meet the challenge of keeping the network secure, there are two basic approaches; proactive defence approach and reactive defence approach. No single approach is sufficient to keep the network secure. An appropriate combination of both reactive and proactive mechanisms along with the post attack analysis is required to deal with the attacks effectively. The focus of this thesis is to suggest comprehensive defence mechanism to protect the network against advance cyber-attacks. SIEM is used in many organization for monitoring the network security. In this research SIEM has been tested against advance cyber-attacks. This chapter provides the introduction to the problem domain, research methodology followed in this research and objectives of the research.

1.2 Cyber Threat Environment

Cyber threat environment has changed over the period of time. Attacks are increasing in sophistication. The top ten common threat techniques include phishing, network scanning, denial of service attacks or distributed denial of service attacks, privilege abuse attacks, web application attacks, SQL injection attacks, malwares including downloaders, command and control, backdoor and spyware [4]. Usually attackers use various reconnaissance and probing techniques to identify potential victims, as next step attack vectors are used to exploit potential loopholes. Attackers nowadays use more than one attack vectors to attack an organization’s network. The aim of the attacker is to become part of the network and remain undetected for a longer duration. Once they become part of the network, they try to escalate the privileges. Such threats are called Advanced Persistent Threats (APTs) [5]. APTs are involved in large amount of data exfiltration. They use multiple kill chains for a success. A common kill chain scenario is demonstrated in the figure 1.1.

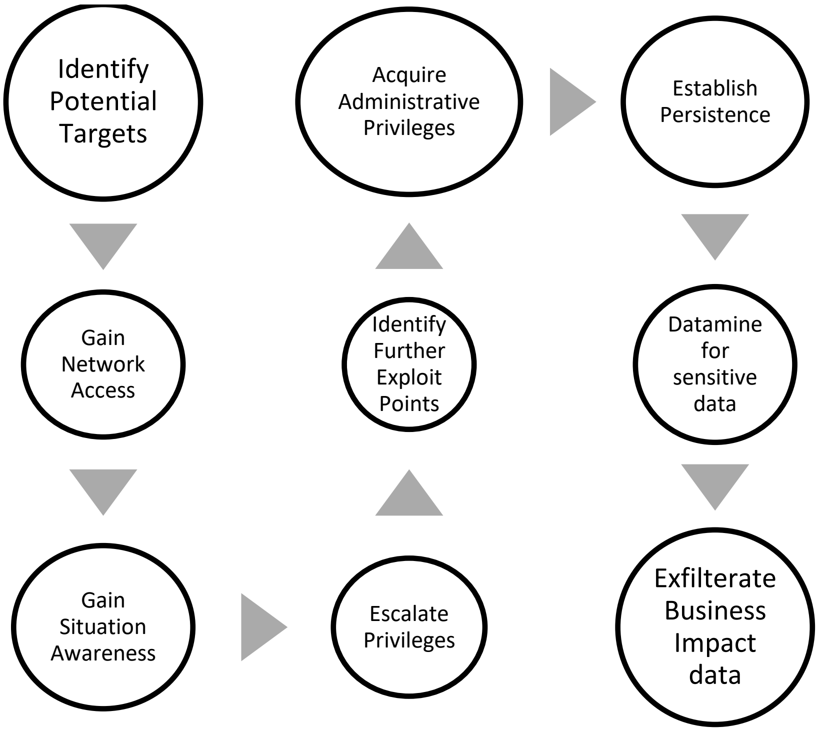

Identify Potential Targets
Acquire Administrative Privileges
Establish Persistence
Gain Network Access
Identify Further Exploit Points
Datamine for sensitive data
Gain Situation Awareness
Escalate Privileges
Exfilterate Business Impact data

Figure 1.1 Kill Chain Process [5]

1.3 Independent Security Controls

Every organization has an IT infrastructure to support their business goals. Security controls are used to ensure confidentiality, integrity and availability of the organization's information. Independent security controls like Firewalls, IDS, IPS, and Antiviruses are used by organizations at network perimeters to ensure network security. Every tool has its own console which shows sets of alerts whenever an anomaly is detected. Usually each tool generates a huge set of alerts along with many false positives and false negatives. Therefore, it is difficult for the network administrator to manage and evaluate huge network alert reports. Also, each control defends against a specific attack. For Example, a firewall is added in the network as a single gateway through which all the incoming and outgoing traffic passes. Firewall examines the traffic and blocks the intrusions based on the ingress rules but attacker these days use the protocols and ports (e.g. http:80) allowed by firewall to enter the network. Similarly, Intrusion Detection Systems are incorporated in organizations to detect intrusions in the system, but some malwares may bypass the security checks. Whenever multiple alerts are triggered by tools it is usually in response to some malicious activity. Therefore, there is a need to aggregate the alerts generated by separate controls over a certain period to detect a widespread attack. Aggregating and correlating alerts manually requires terrific efforts by the network analyst. Moreover, broader risk assessment, prioritization and compliance reporting is nearly impossible. Manually managing the pile of tools is also not a cost-effective approach and is prone to user errors.

1.4 Security Information and Event Management

The term security information and event management was introduced in 2005. Security information and event management (SIEM) is defined by [6], as a unified system designed according to customer's requirement for applying security analytics in real time on event data. It helps in detection of attacks and collects, stores, analyzes the log data and generates report based on the analysis for incident response, forensics analysis and compliance reporting. SIEM is a combination of SIM (security information management) and SEM (security event manager). SIM provides log storage, monitoring and analysis while SEM is responsible for real-time correlation and monitoring of events. SIEM collects and aggregates the Logs and event alerts from the nodes in the network, security devices (e.g., firewall, intrusion detection and prevention systems,) and application services. SIEM's primary data is event data from external devices which is aggregated with contextual information and network packet data for advance alert generation. Data from heterogeneous data sources is normalized, correlated to convert it into meaningful data, and stored in the database. Alerts are generated based on the correlated events. These alerts help in monitoring network traffic and user activity. It also retains the generated data, which is used for compliance reporting and forensic analysis.

1.5 Motivation and Problem statement

There are various organizations using computer networks including cooperate organizations, educational institutes, government and military organizations. These organizations connect to internet for execution of day to day work. Use of internet makes them vulnerable to cyber threats. Moreover, Cyber-attacks are increasing in sophistication. Organizations require advance protection mechanisms to keep the network secure. This research work is beneficial for the organizations in keeping their network and critical data secure.

Individual security controls generate multiple security alerts. Each tool generates specific kind of security alerts. Attacks that use multiple attack vectors and proceed slowly require aggregation of the alerts for detection. Aggregation and correlation of security alerts require terrific human efforts. To get a holistic view of the organization’s security situation, SIEM has been introduced by the professionals. SIEM capabilities include log management, compliance reporting and generation of threat alerts. SIEM depends mainly on external logs and alerts to generate threat alerts. Due to this reason, most of the attacks go undiscovered in SIEM system. These attacks are mostly advance cyber-attacks requiring advance analytical skills for detection. So, there is a need to carry out research in the field of situation awareness for providing a solution to overcome the shortcoming of SIEM in presenting holistic view of the current situation the network.

1.6 Objectives

The main objectives of thesis are:

a. Study of existing independent controls and identifying their limitations.

b. Study of SIEM solutions and identifying their limitations.

c. Study of existing Cyber analytics techniques and identifying their limitations.

d. Study of the essential metrics for Cyber analytics techniques.

e. Presenting a cyber-analytics solution based on the findings of the research.

1.7 Research Methodology

For achieving the objectives, a detailed literature review has been done. The steps followed in the research are presented in Figure 1.2 and are given below:

a. Identifying the problem statement and objectives

b. Understanding various situation awareness models presented in the publications

c. Understanding various independent security controls by collecting data from the official websites and practically evaluating the tools to identify limitations.

d. Understanding open source SIEM by collecting data from official website and practical evaluation of it.

e. Based on the results of the analysis, designing the criteria for evaluating various SIEM solutions. The research has been conducted in two steps. In the first step, the functional and non-functional requirements for SIEM solutions have been identified based on the previous research work and the existing SIEM solutions. For supporting the identified functional requirements, a survey has been conducted as a second step. For conducting the Survey, a Questionnaire has been prepared consisting of multiple choice questions. For each functional requirement, a separate question has been composed highlighting the need of the requirement. Two results were expected as an outcome of the survey.

    i. Validation of the identified functional requirement

    ii. Relative rating of the functional requirements.

    The survey has been conducted using LinkedIn (www.linkedin.com) as questionnaire distribution medium. 50% of the respondents of the survey have information security professionals with minimum 2 years of experience with SIEM technology. All respondents have been found to be well aware of SIEM technology.

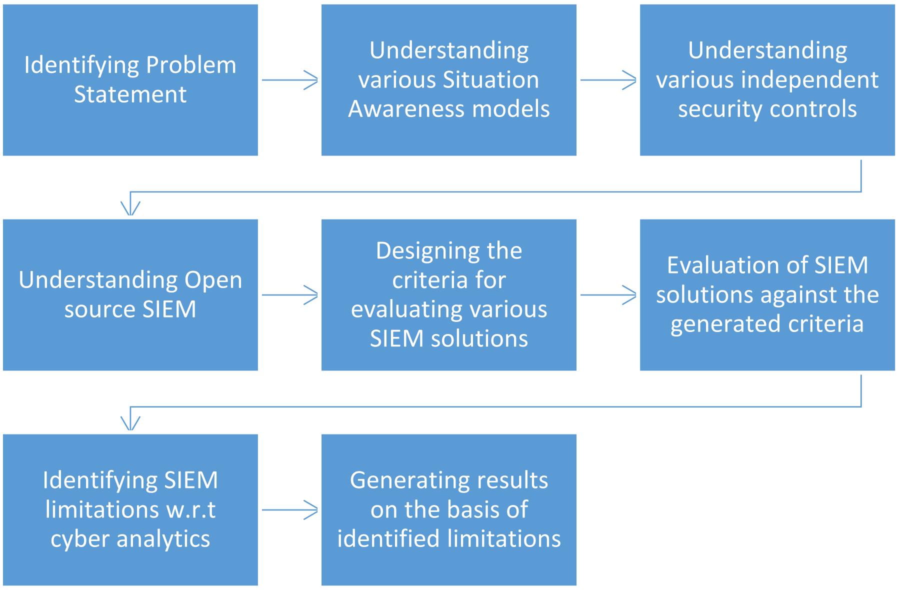

Identifying Problem Statement
Understanding various Situation Awareness models
Understanding various independent security controls
Understanding Open source SIEM
Designing the criteria for evaluating various SIEM solutions
Evaluation of SIEM solutions against the generated criteria
Identifying SIEM limitations w.r.t cyber analytics
Generating results on the basis of identified limitations

Figure 1.2 Research Methodology

f. Evaluation of SIEM solutions against the generated criteria; followed by analysis

g. Identifying the limitations in SIEM

h. Generating results based on the identified limitations.

i. Proposing a solution for the identified limitations.

1.8 Contribution

The output of the research includes evaluation criteria for evaluating SIEM solutions for selecting the best suitable SIEM solution for an Organization and cyber analytic solution for addressing the limitations of SIEM. The proposed criteria help in selection of SIEM according to the requirements of the stakeholders. If organization does not have any specific requirement, the criteria can be used without adding weights. If organization have specific requirements, the criteria is used by adding more value to the client required capabilities. The best suitable solution is selected based on the highest total score value. The proposed cyber analytic solution incorporates deep packet inspection and contextual information which helps in detection of wide spread and context specific attacks. Correlation of events from proposed solution with SIEM can provide a better holistic view of the organization's security.

1.9 Thesis Organization

This chapter discusses the problem statement, objectives and aim of the research and research methodology followed throughout the research. Chapter 2 explains cyber threat environment. Also, it discusses phases of network security monitoring, independent security controls used for network security monitoring and their limitations. The chapter concludes on the statement that independent security controls cannot provide complete picture of the organization's security. They have limited scope and can provide limited capabilities. Using large number of independent controls for network monitoring require manual correlation of the results for a holistic view and for detection of wide spread attacks. It indicates the need of a management tool for providing a complete picture with less efforts. Chapter 3 includes detailed discussion on Security Operation Centre, its composition and technological aspect. In the technological aspect, it covers SIEM in detail and it effectiveness for network security monitoring. Further, it also covers OSSIM architecture and working. OSSIM is an open source solution and it provides limited capabilities as compared to other commercially available solutions. There are no standards available to evaluating SIEM according to user requirements. Chapter 4 defines evaluation criteria for evaluating SIEM solutions. Also, few SIEM solutions are evaluated based on the defined criteria. Evaluation of SIEM solutions and research of SIEM indicates its ineffectiveness in detecting advance cyber-attacks. Chapter 5 designs test cases for advance cyber-attacks and defines cyber security analytics and its features. The test environment for SIEM is discussed in detail. Open Source SIEM solution (OSSIM) is tested against the test cases and the limitations of SIEM are identified. Chapter 6 provides a solution for the limitations of SIEM highlighted in the previous chapter. Chapter 7 concludes the thesis. It highlights the key points of the research and proposes the future work.

1.10 Conclusion

This chapter provides an introduction to the threat environment, problem at hand and research carried out to propose a solution. Cyber threats nowadays using various attack vectors. To detect and protect against cyber-attacks, various independent security controls were introduced. Independent security controls are difficult to manage and protect against specific attack scenarios. For central management and correlation of alerts generated by independent security controls, SIEM was introduced. SIEM only correlates the alerts generated by various independent controls hence doesn’t detect wide spread attacks. A solution is proposed for addressing the limitations of SIEM. The solution incorporates deep packet inspect and contextual information for detecting wide spread attacks.

Chapter 2

CYBER THREAT ENVIRONMENT AND DEFENCE MECHANISMS

2.1 Introduction

Securing organization’s network against attacks is a major concern today. Cyberattacks are becoming more refined. Attacks are carried out using multiple attack vectors. Cyberattack vary in the attack vectors they use, the resources they impact and the defence methods required for containing the attack. The aim of the attacker is to remain undetected for a longer duration and get insight into critical data. Individual security controls are used as defending tools by organizations. Every tool displays set of alerts when an anomaly is detected. Usually each tool generates huge number of alerts making it difficult for the security analyst to evaluate all security alerts.

This chapter explains the present threat landscape and the impact of the threats on organizations. It also provides a brief overview of the security cycle of organization. Organizations follow four phase security cycle for keeping them secure. It provides literature review of the situation awareness tools and independent security controls, identifying the features and limitations of them. This chapter also provides a brief overview of the essential attributes required for a situation awareness tool.

2.2 Information Security Threats

A threat is something having the potential to cause some damage to a host machine or a network as a whole. Cyber threat taxonomy has changed over the period of time. Top six threats are discussed below. [4]

2.2.1 Denial of Service Attacks

Denial of service attack deprives the legitimate users from the system resources or network resources. It can interrupt or suspend services and result in massive damage.

Recent DDoS attack against Dyn DNS service was of more than 1Terabyte/second [7]. It resulted in outage of popular apps like Instagram, twitter and GitHub.

2.2.2 Phishing Attacks

Social Engineering attacks use individuals for compromising computer networks. Usually technical defence methods cannot protect against such attacks. For controlling such attacks, security awareness of the users is required. Most commonly used attack technique is phishing [4]. Phishing is a type of social engineering attack. It is a way of getting confidential information from an individual through an electronic communication by masquerading as a trustworthy entity. These attacks can be performed through emails, instant messengers, telephone calls, social networks, cloud services and through websites [8]. In Phishing attacks, attackers use certain tricks to steal victim's personal and financial data. Spoofed emails are presented in a way to misdirect them to a forged website and reveal personal and financial data [9].

2.2.3 Unauthorized Access

Unauthorized access to the system can be used by the attacker to exfiltrate critical information and data. Unauthorized access can be gained by exploiting vulnerabilities of the system and applications and using password cracking [10].

2.2.4 SQL Injection and Cross-Site Scripting Attacks

Web application attacks are performed by exploiting application level vulnerabilities. Top web application vulnerabilities include cross-site scripting and SQL injection [4]. Cross-site scripting can be used to embed client-side script to the web pages. SQL injection attack is performed by inserting SQL query into the client-side input to the application which is then executed by SQL server [11].

2.2.5 Malware Based Attacks

Malware are designed to gain access to personal information, disrupt operations, use system resources in attacks like DDoS or simply for displaying advertisements.

Malware based attacks include spywares, ransomware, key loggers, command and control, backdoors, downloaders.

2.2.6 Privilege Abuse Attack

Insider's attacks are the most dangerous ones. They can misuse the privileges to steal sensitive data, commit fraud or leak data. Privilege abuse attacks are difficult to detect but can be very dangerous.

For keeping the network secure, organizations need to follow security cycle.

2.3 Security Cycle of an Organization

There are four phases in a security life cycle of an organization: planning phase, resistance phase, detection and response phases. These phases are essential in securing an organization against threats. Figure 2.1 shows operational model of a security cycle. In real life scenarios, all four phases can be taking place simultaneously. New defences are planned by the teams for enhancing security posture while existing defences protect the network against intruders.

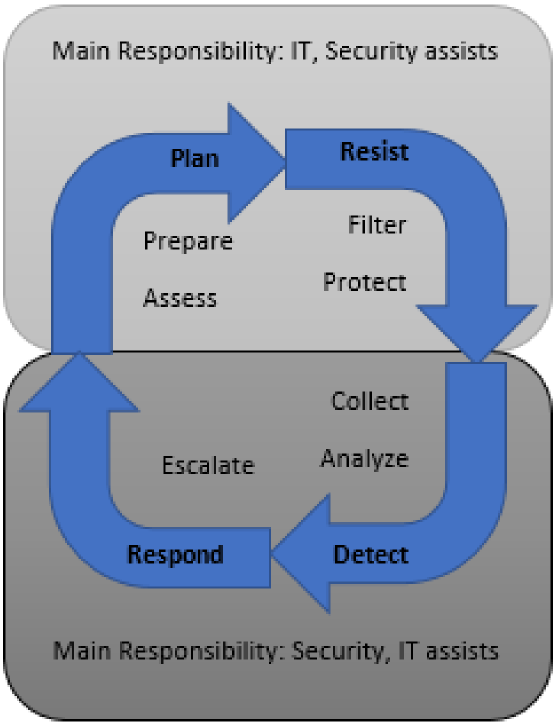

Main Responsibility: IT, Security assists
Plan
Resist
Prepare
Assess
Filter
Protect
Collect
Analyze
Escalate
Respond
Detect
Main Responsibility: Security, IT assists

Figure 2.1 Security Cycle of an organization [15]

2.3.1 Planning phase

In the Planning phase, organization is accessed against the potential threats and its position to resist or counter intrusions. Auditing, compliance checking, training teams, security assessments of the infrastructure, developing secure software and budgeting comes under the phase of planning.

2.3.2 Resistance phase

In the resistance phase, preventive mechanisms are used to keep the network protected. Automated prevention tools like firewalls, antiviruses, whitelisting certain IPs/apps etc. are used to stop or at least hinder the intrusion. Vulnerability management, hardening configurations and security awareness trainings for teams also hinder the intrusion.

2.3.3 Detection and Response phase

Attackers still get access to network one way or the other, which makes these two phases important. Detection and response phase comes under Network security situation awareness. Network security situation awareness is gathering, analyzing and interpretation of network data intelligently for effective decision making for network defence. Endsley in her article presented in 2001, defined Situation Awareness (SA) as key to provide relevant information whenever needed because, according to her, absence of information is not a problem now but to find right information at right time is [12]. It provides the critical information for decision making. The theoretical model of Situation Awareness was presented by Endsley in 1995 [13]. It is a generic model applicable in many domains. Model proposed three levels of Situation Awareness as Perception, Comprehension and Projection. Figure 2.2 shows the pictorial view of the model.

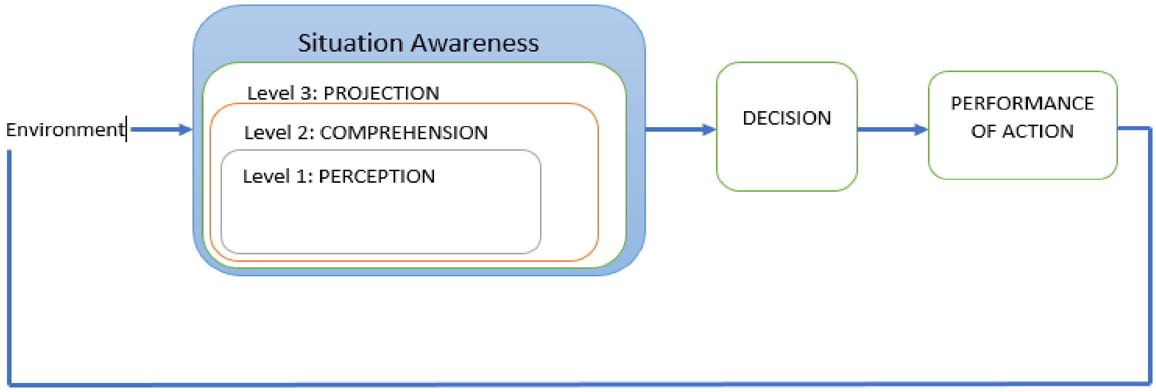


Figure 2.2 Endsley's SA model [13]

Perception is gathering knowledge about the devices and the security controls in the network. Comprehension involves aggregation and correlation of network data into an understandable and threat oriented knowledge. Comprehension depicts the current security picture of the network. Projection is the ability of SA to predict the future events based on the perceived and comprehended network data. It helps the analysts to make decisions. McGuinness and Foy proposed another level in SA as Resolution [14]. Resolutions include countermeasures to address the future security conditions.

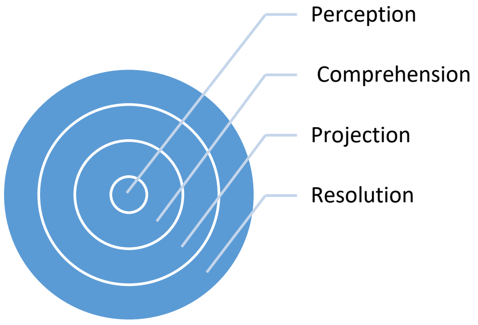


Figure 2.3 Dependency of SA levels

Figure 2.3 describes the dependencies of the SA level. If a situation is not perceived correctly, the error will propagate through all outer levels and ripples will be denser. Perception of the network is an essential and critical level of a situation awareness tool. An ideal situation awareness tool should understand the network situation in depth, aggregate and correlate the findings and predict future accordingly. These four phases are considered essential for detection and response phases and are described as: [15]

a) Collection: Collecting the data from network devices, security devices and Endpoints for deciding an event to be normal or malicious.

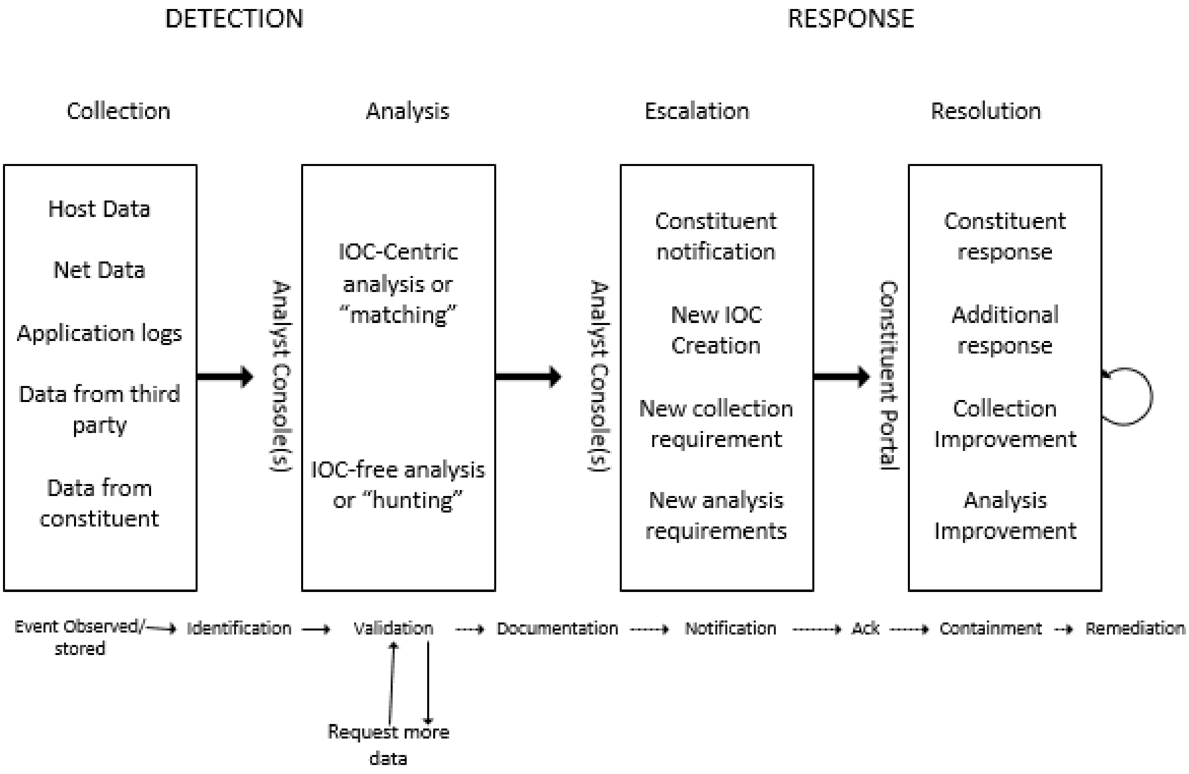


Figure 2.4 Detection-Response Phase [15]

b) Analysis: Analyzing and validating the nature of an event based on facts.

c) Escalation: Notifying the organization about the current situation of a compromised asset.

d) Resolution: Actions taken to reduce the loss risk.

2.4 Situation Awareness Tools

Several tools are proposed and developed by various authors in order to provide situation awareness of the network. The aim behind developing such tools is to help security analysts in monitoring and analyzing the network traffic. Below is a literature review of few SA tools:

2.4.1 NVisionIP

It focuses on visualization of security events. It uses NetFlow data to present the complete network on one screen (class B IP address Network) [16, 17, 18]. It represents the data flow in terms of bytes to and from a host in a network.

2.4.2 VisFlowConnect-IP

It focuses on visualization of traffic within the network and between the network and the outside world. It also has the functionality to monitor traffic on specific ports [16, 19].

NVisionIP and VisFlowConnect-IP are more focused on visualization and do not employ any method for data fusion from heterogonous controls [20]. Moreover, they only visualize the network flow of the traffic and network topology but do not provide any visualization of threats, vulnerabilities and security alerts of the network [21].

2.4.3 SiLK

It is a toolkit by [22] for network traffic analysis and storage. It is further improved to analyze large datasets. The aim is to achieve true situation awareness and making it scalable for larger networks [23]. SiLK data collection and storage tools help in optimizing analysis of network data. It is the only open source tool known till now that analyzes the data without sampling [23].

2.4.4 CNSSA

It is a network security situation awareness architecture proposed in [21]. It has three modules: information collection, situation awareness and situation visualization. It displays collected information on the basis of tools like nmap, OpenVas, Snort, Iptraf. It provides a centralized console to view network situation. It only provides a limited view. It is prone to lots of false positives. Figure 2.5 shows the overall architecture diagram of CNSSA.

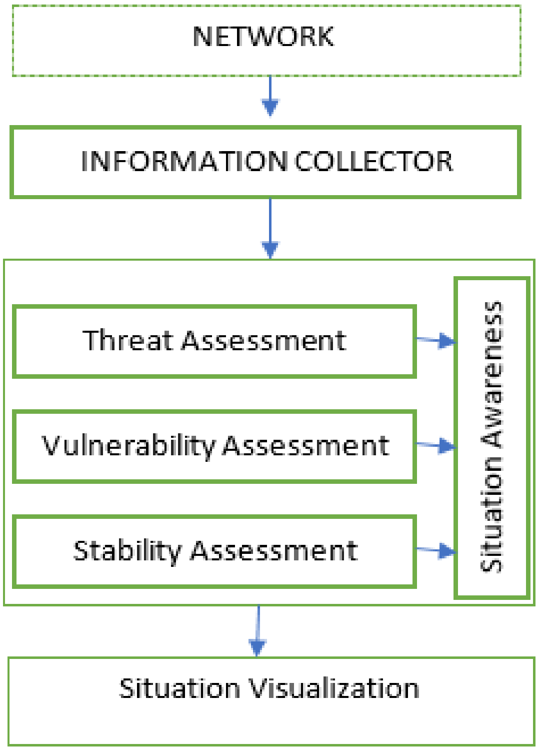


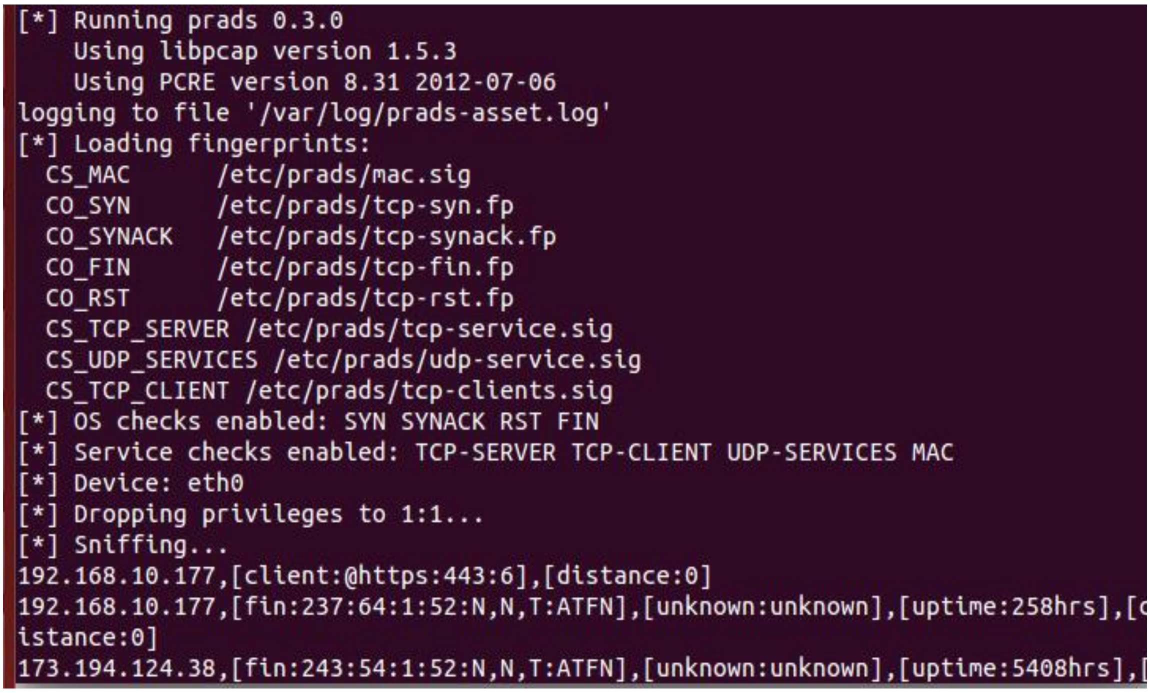
Figure 2.5 the Network Architecture of CNSSA [21]

2.5 Independent Security Controls

Independent security controls are used to perform monitoring of a specific domain. There are various tools designed to support network situation awareness, few of them are discussed below:

2.5.1 Prads

Prads detects the assets passively in real-time. It does not send the packets for gathering information. It silently captures the traffic being in promiscuous mode. It identifies the hosts and services in the network [26]. Figure 2.6 shows prads scan based on the traffic being generated in the network.

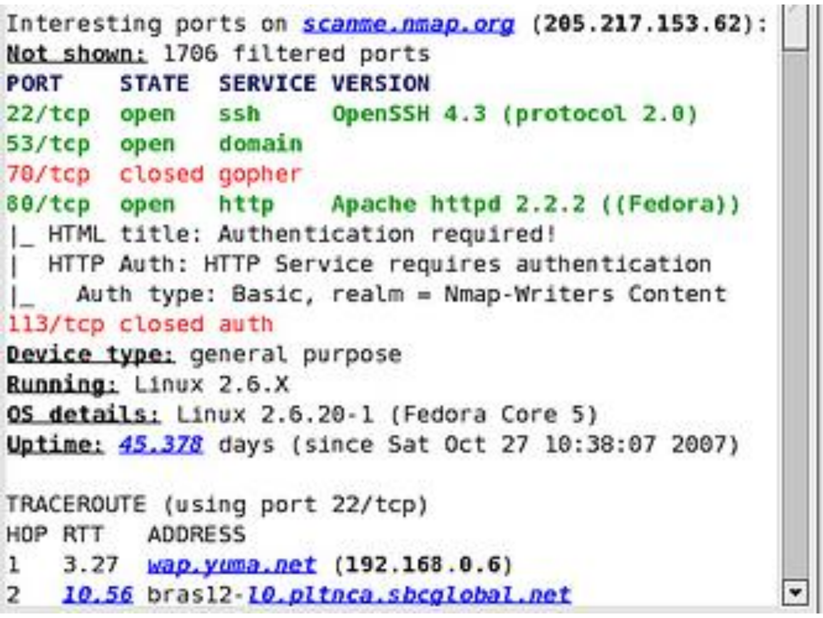


```
[*] Running prads 0.3.0
    Using libpcap version 1.5.3
    Using PCRE version 8.31 2012-07-06
logging to file '/var/log/prads-asset.log'
[*] Loading fingerprints:
  CS_MAC      /etc/prads/mac.sig
  CO_SYN      /etc/prads/tcp-syn.fp
  CO_SYNACK   /etc/prads/tcp-synack.fp
  CO_FIN      /etc/prads/tcp-fin.fp
  CO_RST      /etc/prads/tcp-rst.fp
  CS_TCP_SERVER /etc/prads/tcp-service.sig
  CS_UDP_SERVICES /etc/prads/udp-service.sig
  CS_TCP_CLIENT /etc/prads/tcp-clients.sig
[*] OS checks enabled: SYN SYNACK RST FIN
[*] Service checks enabled: TCP-SERVER TCP-CLIENT UDP-SERVICES MAC
[*] Device: eth0
[*] Dropping privileges to 1:1...
[*] Sniffing...
192.168.10.177,[client:@https:443:6],[distance:0]
192.168.10.177,[fin:237:64:1:52:N,N,T:ATFN],[unknown:unknown],[uptime:258hrs],[d
istance:0]
173.194.124.38,[fin:243:54:1:52:N,N,T:ATFN],[unknown:unknown],[uptime:5408hrs],[
```

Figure 2.6 Prads

2.5.2 Nmap

Nmap is used for discovering the hosts in the network and services running on the network [27]. It performs active scanning. Packets are sent from Nmap to hosts in the network for gathering information about the open ports and services running on the hosts. It also detects the operating system of the hosts. Figure 2.7 shows Nmap results.



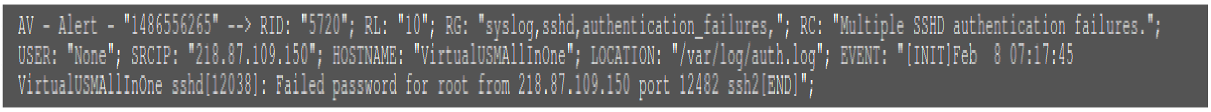
```
Interesting ports on scanme.nmap.org (205.217.153.62):
Not shown: 1706 filtered ports
PORT     STATE  SERVICE VERSION
22/tcp   open   ssh     OpenSSH 4.3 (protocol 2.0)
53/tcp   open   domain
70/tcp   closed gopher
80/tcp   open   http    Apache httpd 2.2.2 ((Fedora))
|_ HTML title: Authentication required!
|  HTTP Auth: HTTP Service requires authentication
|_   Auth type: Basic, realm = Nmap-Writers Content
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20-1 (Fedora Core 5)
Uptime: 45.378 days (since Sat Oct 27 10:38:07 2007)

TRACEROUTE (using port 22/tcp)
HOP RTT   ADDRESS
1   3.27  wap.yuma.net (192.168.0.6)
2   10.56 bras12-10.pltnca.sbcglobal.net
```

Figure 2.7 Nmap

2.5.3 OSSEC

OSSEC is a host intrusion detection system. It monitors activities on the host including file integrity monitoring, rootkit detection, log monitoring and process monitoring. It generates alerts for various malicious situations. Alerts can be in the form of alert logs and email alerts. It uses client server architecture. Individual hosts push the data towards server where it is analyzed and responded. These alerts can be pushed to any SIEM system [28]. Figure 2.8 shows alerts generated by OSSEC.

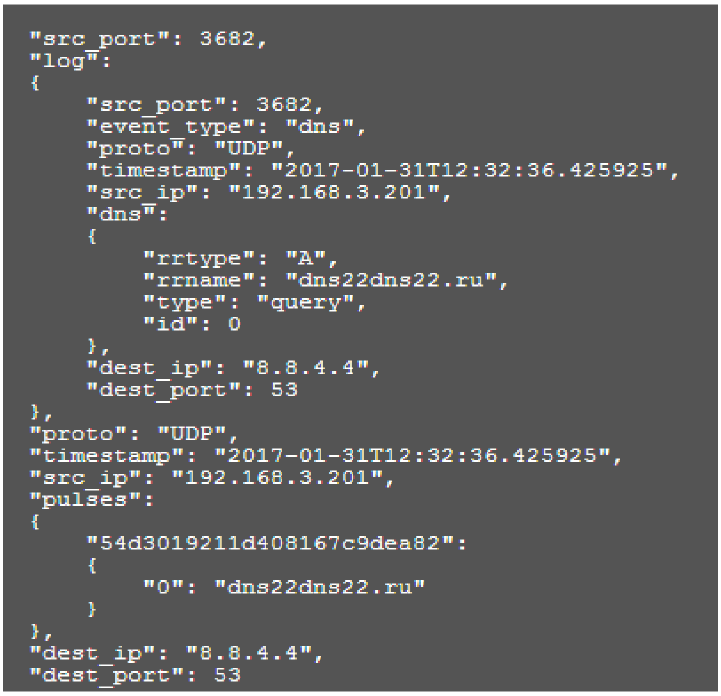


```
AV - Alert - "1486556265" --> RID: "5720"; RL: "10"; RG: "syslog,sshd,authentication_failures,"; RC: "Multiple SSHD authentication failures.";
USER: "None"; SRCIP: "218.87.109.150"; HOSTNAME: "VirtualUSMAllInOne"; LOCATION: "/var/log/auth.log"; EVENT: "[INIT]Feb  8 07:17:45
VirtualUSMAllInOne sshd[12038]: Failed password for root from 218.87.109.150 port 12482 ssh2[END]";
```

Figure 2.8 OSSEC

2.5.4 Snort

Snort is a network intrusion detection system. It is used for detecting and analyzing network traffic [29]. It works on the basis of signatures. It helps in detection of known worms and Trojans, RATs, Dos attacks etc. Figure 2.9 shows the DNS response for Anunak malware detected by snort.



```
"src_port": 3682,
"log":
{
    "src_port": 3682,
    "event_type": "dns",
    "proto": "UDP",
    "timestamp": "2017-01-31T12:32:36.425925",
    "src_ip": "192.168.3.201",
    "dns":
    {
        "rrtype": "A",
        "rrname": "dns22dns22.ru",
        "type": "query",
        "id": 0
    },
    "dest_ip": "8.8.4.4",
    "dest_port": 53
},
"proto": "UDP",
"timestamp": "2017-01-31T12:32:36.425925",
"src_ip": "192.168.3.201",
"pulses":
{
    "54d3019211d408167c9dea82":
    {
        "0": "dns22dns22.ru"
    }
},
"dest_ip": "8.8.4.4",
"dest_port": 53
```

Figure 2.9 Snort Result

2.6 Shortcomings of Independent Security Controls

Each tool has its own dashboard or display presenting alerts when certain conditions are fulfilled. Also, each tool detects a specific attack along with many false positives and false negatives. For example, Snort may detect an attack based on the network traffic. A host may not accept the attack packet or the attack may be designed for a host with different specifications resulting into a false positive. Also, each control defends against a specific attack. For understanding the holistic picture of the network situation, the alerts from various sources need to be aggregated. If an organization is using independent security controls, the security analyst needs to aggregate and correlate the alerts manually. Moreover, broader risk assessment, prioritization and compliance reporting is nearly impossible. Manually managing the stack of tools is also not a cost-effective approach and is prone to user errors.

2.7 Essential attributes for Situation Awareness

The essential attributes of NSSA as proposed in [24] are; i) effective handling of fast changing dynamic and complex networks ii) providing automation of operations iii) processing of data in real time iv) efficient multisource data fusion v) gathering of data from multiple heterogeneous security controls vi) providing complete visualization of the network security conditions vii) accurately predict future risks based on current situation viii) providing countermeasures for the predicted risks.

Situation awareness systems should generate reports on the network situation and vulnerabilities, reports highlighting internal and external incidents, and reports highlighting patch management of software, services and operating system. Output and the feedback provided by the situation awareness tool are valuable and should be clearly presented. As ambiguity in the output can lead to wrong judgement by the analyst and it may lead to compromise of the organization's network [25].

2.8 Conclusion

Computer security networks need to be monitored and safeguarded against threats. Top security threats faced by organizations include denial of service attacks, phishing attacks, web application attacks, unauthorized access and privilege abuse attacks, malware based attacks. Security cycle of an organization includes four phases: planning, resistance, detection and response. These phases are overlapping and continuous. In detection and response phase, the incidents are identified, contained and mitigated. Various Independent tools are used for detection and monitoring of networks. Each independent security control defends against specific kind of attack. Using a myriad of tools is not cost effective and a good choice. A tool providing complete picture of organization is required. Next chapter describes the need of security operation center for monitoring network security.

Chapter 3

SECURITY INFORMATION AND EVENT MANAGEMENT

3.1 Introduction

Security Operation Center (SOC) is an essential part of an organization dedicated for the protection and monitoring of the digital assets in real time. All information security incidents are reported, assessed, contained and mitigated using the services of security operation center. Monitoring of the IT assets and the network traffic flowing between them and outside IT world is critical in a SOC. The technical security controls may indicate abnormalities in the traffic but it requires human intervention to mitigate them. Most of the firewalls and Intrusion Detection System (IDS) may not be able to detect the application based attacks and zero-day attacks; therefore, there is a need of SOC for advance protection and monitoring of an organization’s network. In every SOC, there are three components: people, process and technology. Trained people under standard processes can secure the network using right technology. Effective analytic capabilities, forensic capabilities, awareness of the organization’s network, and reactive techniques are critical aspects of SOC. Initially, there were few independent security tools in a SOC. Later more security tools were introduced with vendor specific interfaces. Managing the interfaces of those individual tools and correlating the output manually was a terrific job. Security Incident and Event Management was designed as an essential technical component of SOC. SIEM collects, normalizes, correlates, analyzes and stores logs and events in real time and generates alerts highlighting the anomalies. Mainly SIEM is composed of SIM and SEM but vendors provide additional functionalities too. SIM stands for Security Information Management. It is a way to collect, monitor and analyze the computer logs related to information security. This software automates the collection, monitoring and analysis of security events and log data. SEM stands for Security Event

Management. It provides threat analysis and visualization, incident response and forensic analysis capabilities. SEM can be used for running Managed Security Service Provider (MSSP).

This chapter explains SOC structure briefly, introduction to the SIEM technology, working of SIEM, Open source SIEM solution and its features.

3.2 Structure of SOC

The goal of a SOC is to detect, investigate and mitigate incidents that can impact business. Security Operation Centre mainly consists of three components: People, Process and Technology [Fig 3.1].

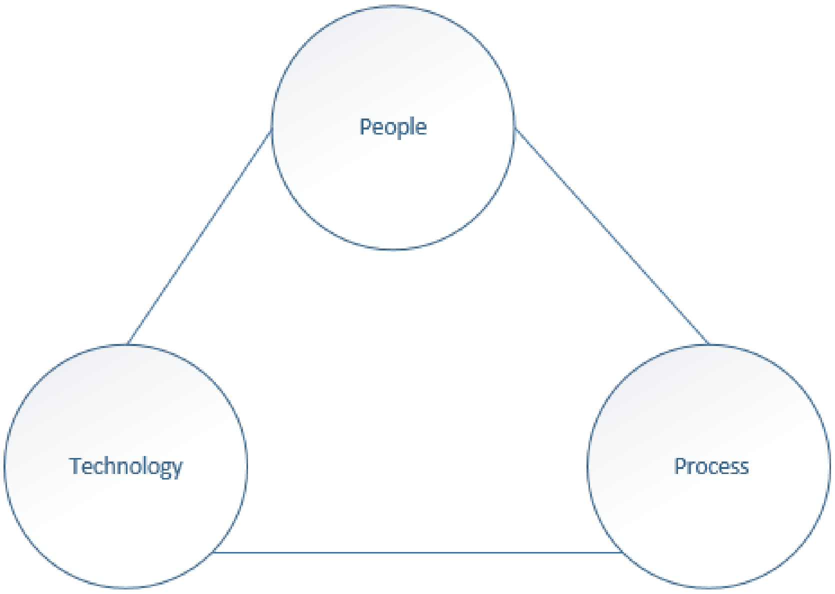


Figure 3.1 Components of SOC

3.2.1 People

SOC staff should be trained to deal with challenging and drastically changing threat environment. Job roles in a SOC are divided in four categories: Security Analyst, Incident investigator, subject matter expert and security manager.

a) Security Analyst

The duty of security analyst is to monitor the alerts, health status of security sensors and endpoints, gather information about alerts through initial analysis.

b) Incident Investigator

The duty of the incident investigator is to perform deep analysis of incident by correlating data from various sources, determines if the critical asset is affected and suggests remedies.

c) Subject matter expert

Subject matter experts have in-depth knowledge of their respective domain. They deeply look into network traffic for detecting zero-day incidents.

d) SOC Manager

Manager manages budgeting, shift scheduling, provides overall direction to the SOC including task allocation and reports to the management. SOC Manager is responsible for organizing resources and prioritizing the SOC tasks.

The organization of the SOC is as shown in the figure 3.2. SOC Manager should set SOPs for incident handling and develop a workflow strategy for the SOC analysts.

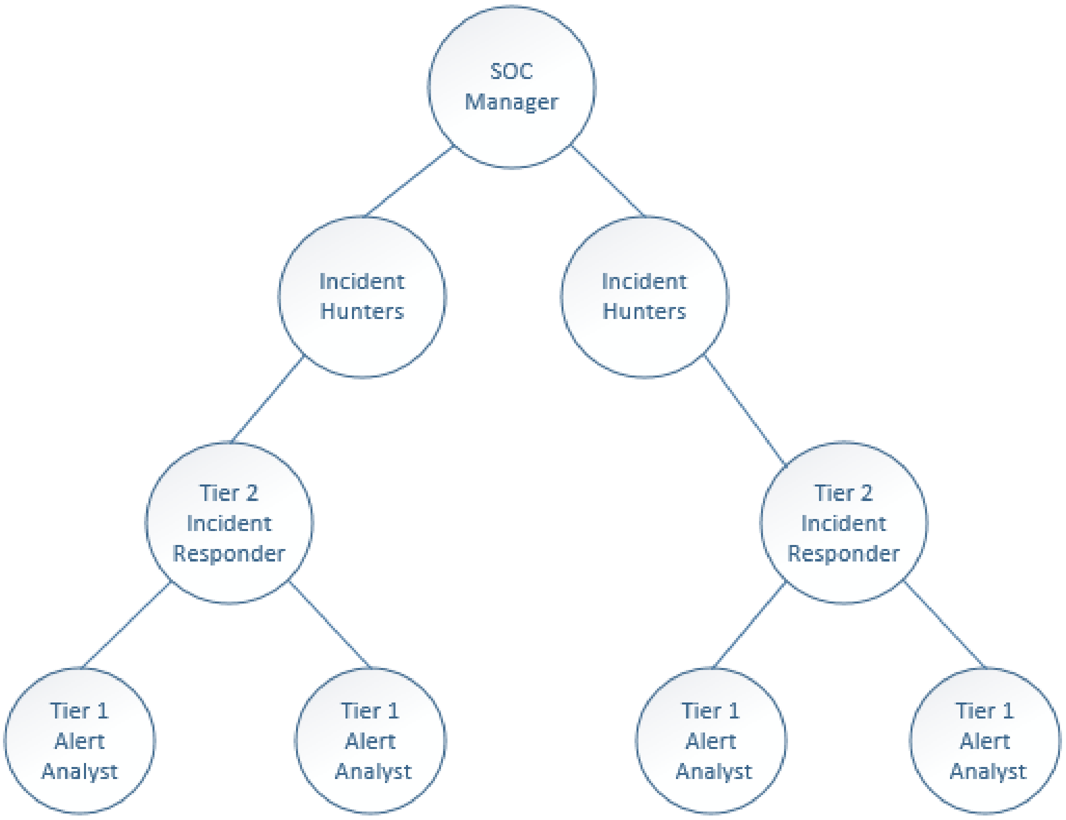


Figure 3.2 Organization of SOC

3.2.2 Processes

Repeatable processes can help the SOC to work in a systematic and well-defined way, making it sure that no important task is missed. By having a repeatable workflow for SOC, activities and actions can be well aligned.

3.2.3 Technology

A solution for collecting, aggregating, detecting, analyzing and managing enterprise data is core technology in SOC. Network security monitoring solution gathers data from endpoints, network devices and security devices. Network security monitoring solution usually takes network traffic, system logs, threat intelligence feeds, events from security devices, asset context and vulnerability reports about the network as input and aggregates them. By aggregating the data centrally, organization gets visibility of the network status and the possible anomalies. It also facilitates analysis of security incidents hence, actions can be taken more conveniently. SIEM is a security monitoring tool considered essential for SOC. SIEM provides a management interface to reduce the efforts required to effectively monitor the network and respond the attacks.

3.3 Basic SIEM Features

SIEM technology is usually used by organizations for defence against internal and external threats, policy compliance, monitoring user activities and for monitoring critical servers and databases [30]. The basic capabilities of SIEM are discussed below.

3.3.1 Log Collection

Each organization can have a unique network. Organizations may have set policies and designs regarding basic network topology, still there can be a variation in network topology in similar organizations or even within different departments of the same organization. SIEMs can gather network logs from many different nodes. The logs provided by the nodes contain records of the activities and can be analyzed using SIEM tool.

3.3.2 Event Normalization

Events are collected and normalized from heterogeneous sources. Before correlation of events and logs, they should be translated and converted into a common format. Normalized events can be analyzed using minimal number of correlation rules. Also, it is easier to develop reports and dashboards using normalized events [30].

3.3.3 Correlation

After normalization of logs they must be correlated with each other. Correlation can be done between events from same source or multiple different sources. Each node generates a huge amount of data. Correlating the events manually can be a difficult job and requires terrific human efforts. It may lead to a situation where it becomes difficult to manually correlate the large amount of data and critical malicious activities go undetected. SIEM solutions use predefined rules to analyze the normalized data. Correlation of related events can provide insight into activities that may need further investigation.

3.3.4 Dashboards

Dashboards increase the visibility of network situation of an organization. Dashboards provide a central console for monitoring network activity. Logs from all the assets serve as data sources for the events. Dashboards allow the analyst to dig down an event in detail.

3.3.5 Alerts and Reports

Alerts are generated based on the event’s risk level to let the analyst know about the security situation. Reports are generated about security events, logs, user activity, compliance and security operations.

3.3.6 Log Storage

Logs are stored for compliance with certain standards and policies. Also for forensic investigation of incidents logs must be stored.

3.4 Working of SIEM

Security information and event management tools are considered to increase the ability of an organization to identify inappropriate activities through network monitoring, network performance data, vulnerability reports of the network and audit logs [31]. SIEM works as an essential component of SOC. During early days, there were few vendor specific tools for performing variety of security operations. Managing the user interfaces of those vendor specific tools and correlating their outputs to reduce false positives became a mandatory operation [32]. SIEM was introduced to reduce the workload of the SOC officers in management of various interfaces and correlation of events to dig out the malicious alerts.

SIEM collects and aggregates the logs and event alerts from the hosts in the network, security devices (e.g., firewall, intrusion detection and prevention systems, VPNS) application servers, database servers, web application servers, network devices and access management servers. These logs contain activity proofs that can be analyzed after collection in a SIEM implementation [33]. Data from heterogeneous data sources is collected, normalized, correlated to convert it into meaningful data, and stored in the database. Alerts are generated based on the data stored. These alerts are used for network traffic monitoring and user activity monitoring. It also retains the generated data, which is used for compliance reporting and forensic analysis. Fig 3.3 shows the basic workflow of the SIEM.

3.5 Open Source Security Information Management (OSSIM)

Open Source Security Information Management is SIEM solution by Alienvault. The primary purpose of OSSIM is to monitor the assets. Assets are the devices that add value to an organization’s business.

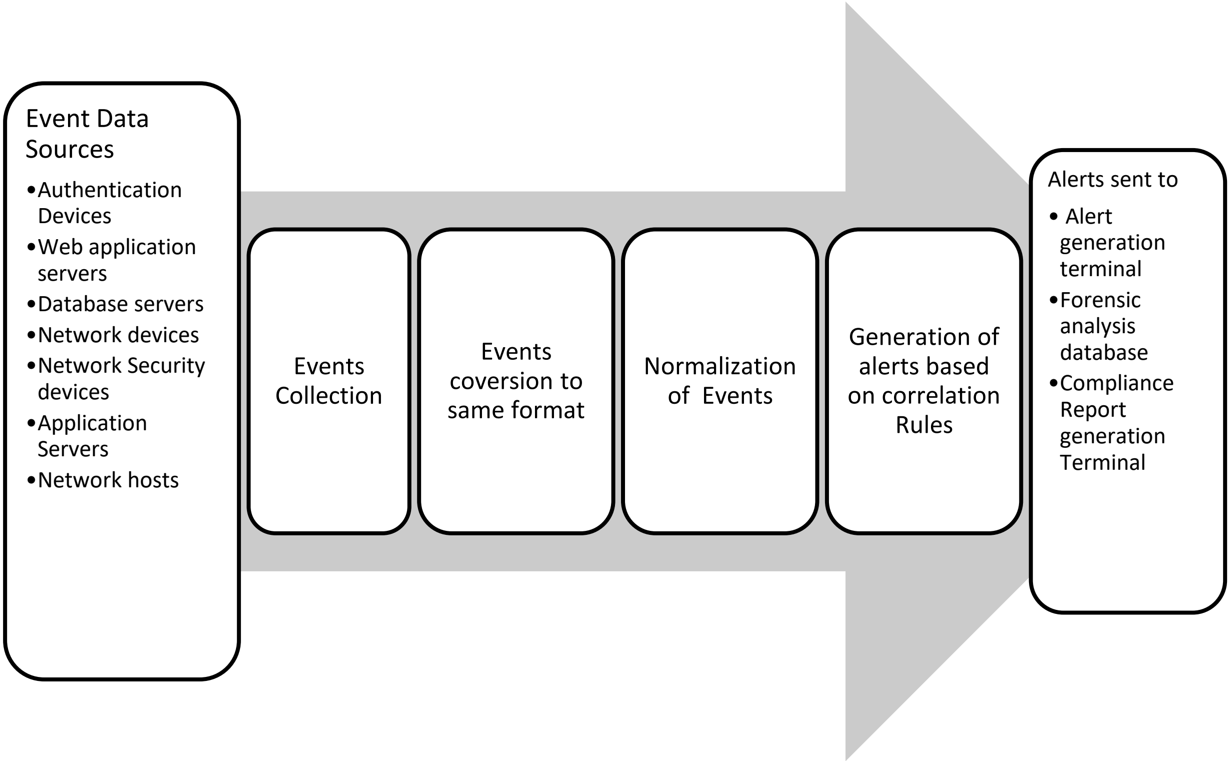

Event Data Sources
•Authentication Devices
•Web application servers
•Database servers
•Network devices
•Network Security devices
•Application Servers
•Network hosts
Events Collection
Events coversion to same format
Normalization of Events
Generation of alerts based on correlation Rules
Alerts sent to
• Alert generation terminal
•Forensic analysis database
•Compliance Report generation Terminal

Figure 3.3 Workflow of SIEM

3.5.1 Underlying OSSIM tools

OSSIM uses various open source tools. Figure 3.4 shows the architecture of OSSIM. The third-party tools are connected to OSSIM via special connectors. The tools used as baseline data source are as follows:

a) Snort

OSSIM uses snort as a NIDS data source. It generates alerts whenever a snort pattern matches with network traffic. Snort works on basis of predefined signatures. Signatures are present for detecting port scans, worms, malwares, policy violations etc.

b) OSSEC

OSSIM uses OSSEC as a HIDS data source. OSSEC agents are required to be installed on each asset to be monitored. OSSEC helps in detection of rootkits, file integrity monitoring and log analysis. Logs include operating system logs, application logs and Security audit logs.

c) Nagios

OSSIM uses Nagios for Asset's availability monitoring. It provides both agentless and with agent monitoring. In Nagios agent monitoring, specific services can also be monitored. Alerts are generated when a service goes down.

d) OpenVas

OSSIM uses OpenVas as a vulnerability scanner. OpenVas identifies the vulnerabilities in the host using signatures. Vulnerabilities are cross correlated with attacks in order to generate alerts when certain vulnerability is exploited.

e) NMap

OSSIM uses NMap (port scanner) for asset discovery, open port discovery, service version discovery and OS version discovery.

f) Arpwatch

Arpwatch is MAC anomaly detection. It detects MAC IP association. OSSIM uses it for Inventory management, IP address change detection and detecting ARP spoofing.

g) Pads

Passive asset detection system (Pads) is used to passively detect assets. It uses signatures to detect running services on assets by pattern matching. OSSIM uses it for passive asset detection, service version changes, detecting policy violations and inventory correlation.

h) OSVDB

Open Source Vulnerability Database is a vulnerability database. OSSIM uses this knowledge database in correlation rule creation, as a vulnerability identifier in cross correlation and for verifying OpenVas scanning information.

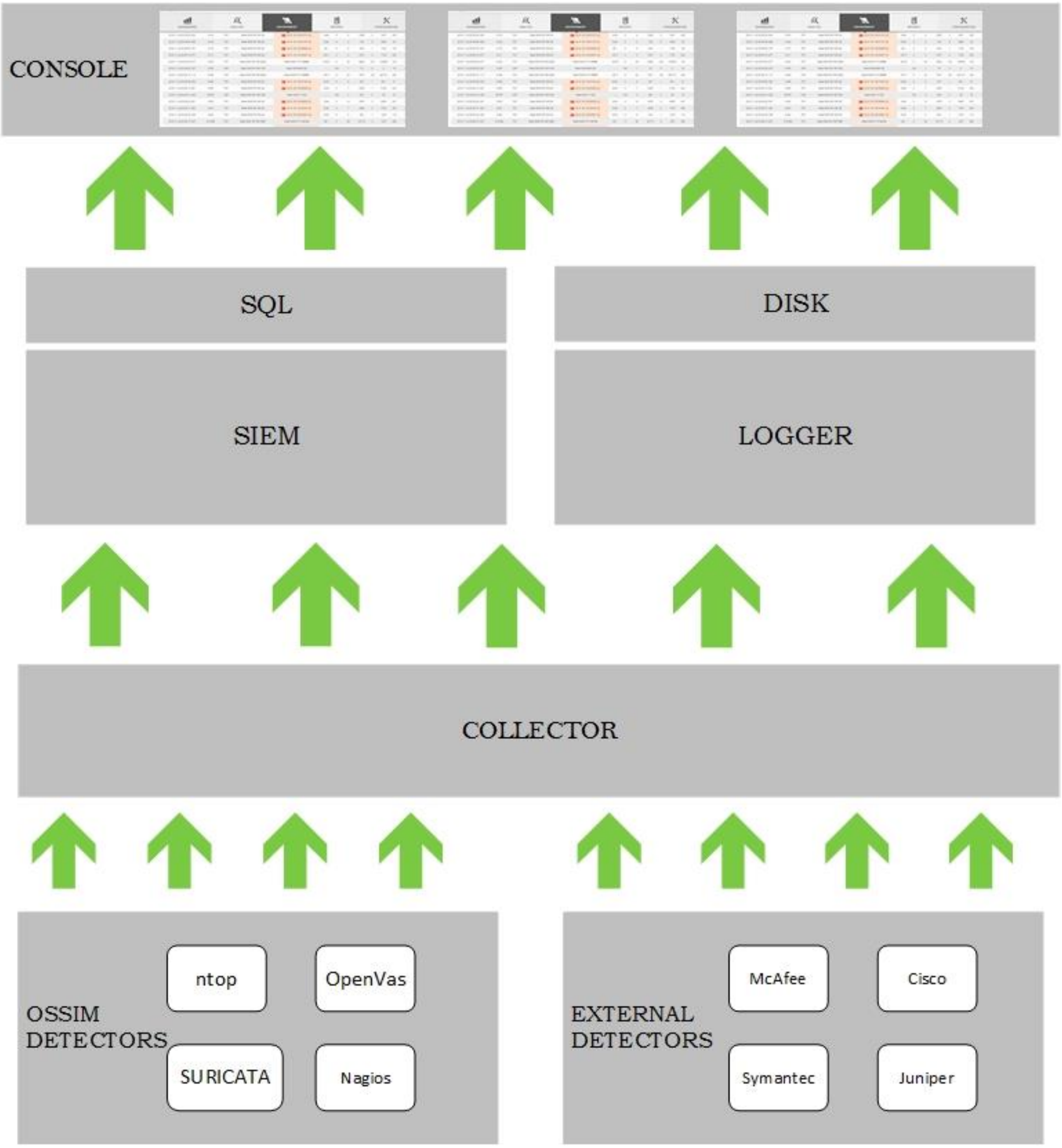


Figure 3.4 Underlying tools

3.5.2 Components of OSSIM

There are two main components of OSSIM:

a) Sensor

Sensor aggregates the data collected from logs, IDS, vulnerability scanning results, asset discovery and net flows.

b) Server

Server evaluates the data forwarded by sensor, correlates the events, performs risk analysis and generates alarms. It also stores data for reporting and assessment.

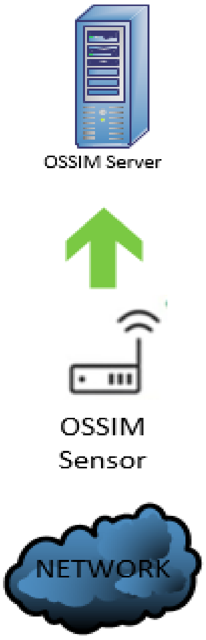


Figure 3.5 Architecture of OSSIM

3.5.3 Detection using OSSIM

Identifying behaviors that leads to event generation is called detection. OSSIM uses various elements for providing detection capability. For detection, OSSIM uses existing tools in use for business processes like database etc. and existing security devices like Firewalls and IDS. There two kinds of detection tools: -

a) Detectors

Detectors constantly listen for data and send the detected events to OSSIM server.

b) Monitors

Monitors are used when needed by correlation engine for gathering additional information.

3.5.4 Workflow in OSSIM

The workflow of OSSIM is described as following phases:

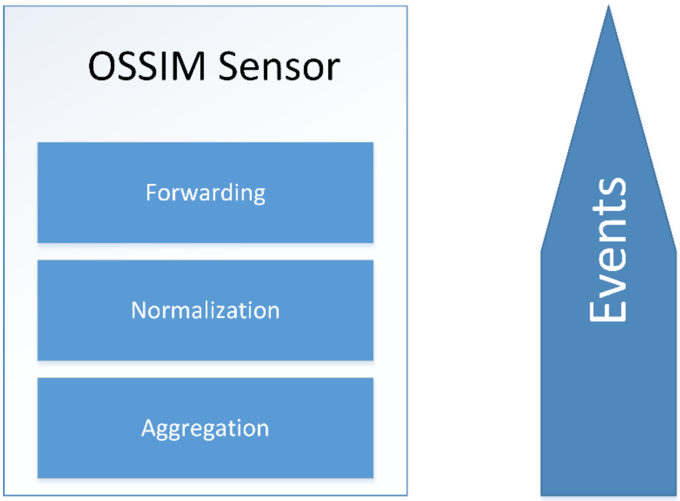


Figure 3.6 Workflow in OSSIM (Sensor)

a) Data Sources

Data source can be any application or device which generates data that can be of any value for analysis. OSSIM has number of integrated data sources for monitoring traffic. OSSIM is capable of collecting data from external data sources. For collection of data, OSSIM needs data source plugins. Plugins are used for understanding and translating the external events. OSSIM has built-in support for popular data sources. Data source plugins has two files:

- .cfg : It is present on the sensor and location is specified from where plugin can read data. It uses regular expressions to parse logs.
- .sql: It is present on the server. It provides the classification of data to be used for risk assessment, correlation and storage.

b) Data Collection

In OSSIM data is collected using multiple methods:

- Using Mirrored ports to send data to OSSIM Sensor
- Configuring data sources to send events to OSSIM server.
- Configuring OSSIM server to pull the events from devices / Endpoints or applications.

c) Data Aggregation

In OSSIM, data is aggregated by Sensor before Server can process events.

d) Normalization

Normalization is performed at Sensor end. The data aggregated must be normalized to a unique format that OSSIM server understands. It uses regular expressions to convert the data into unified format. Normalized data is helpful in identifying behavior patterns occurring in the monitored networks.

e) Events

Log data gathered through a data source plugin and normalized by OSSIM server is known as Event. Each event is assigned an event type ID and Plugin ID for identifying data source.

f) Policy

Policies instruct how events are processed at the server end when they arrive. It acts as filtering agent. It reduces event processing and improves performance. They reduce false positives, generate email notifications and increase priority of a specific event.

Policies consist of policy rules which are triggered in descending order. When a rule is triggered, system stops further processing of that event. Rules are defined from very specific at the top to generic at the bottom.

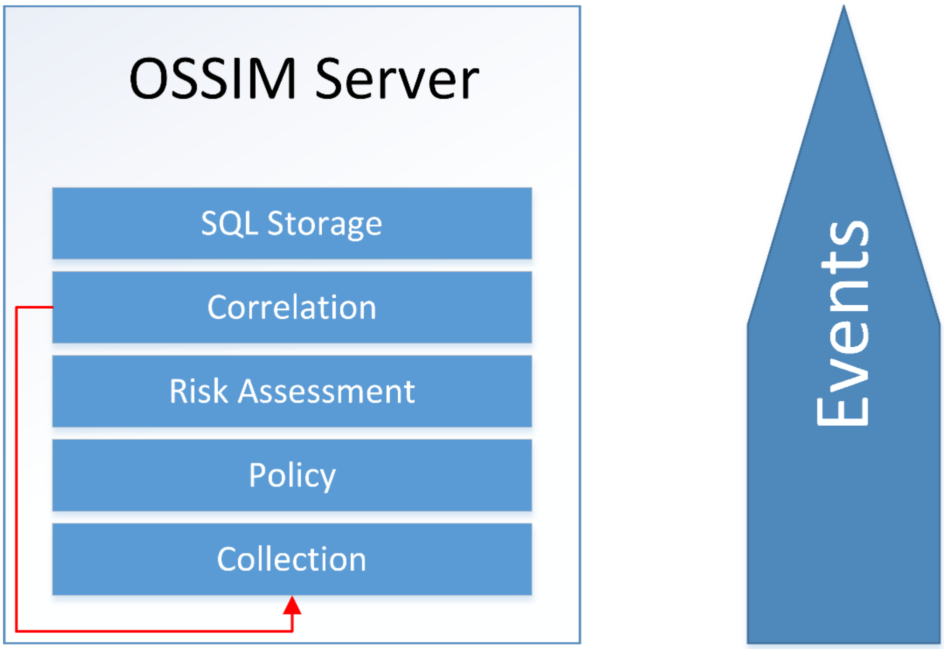


Figure 3.7 Workflow in OSSIM (Server)

g) Risk Assessment

All events go through risk assessment phase. Risk value is between 0 to 10. It is calculated on the basis of asset value, event priority and event reliability.

- Asset value: Value assigned to asset.
- Event priority: It identifies the event importance. Its value can be between 0 to 5.
- Event reliability: The probability of an event to be accurate.

h) Alarms

Alarms are generated on the basis of risk value. If the risk value of event turns out to be >= 1, it is classified as an alarm. Such events require immediate attention, as it can be indication of an attack in progress.

i) Correlation

It detects potential security threats by matching behavior patterns in the monitored networks. In the correlation engine, multiple events are matched against configured rules to generate highly reliable directive events.

- **Directive events:** An event generated as an output of correlation. It has high reliability. The plugin ID for directive event is 1505. Directive ID is the event type ID.

j) Types of Correlation

There are two types of correlation: Logical correlation and Cross correlation.

- Logical correlation: Logical correlation uses logical trees. Individual events are combined in the form of logical trees. In a tree, horizontally OR operation is performed and vertically AND operation is performed between individual events.

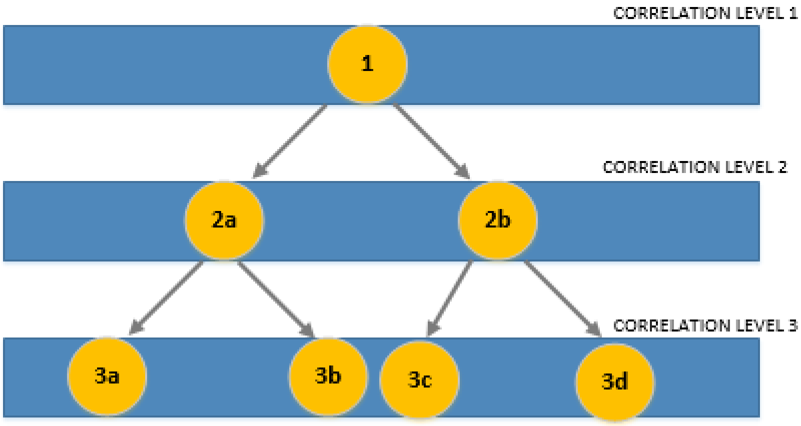


Figure 3.8 Logical Correlation

- Cross correlation: In cross correlation, different events by different data sources are correlated. It generates an event when two events from different data sources are triggered against the same asset.

k) Working of Directives

Correlation engine performs the following steps when an event arrives.

- Matches the event with the directive that is already started in the correlation process.
- If the event does not match directives in correlation process, the correlation engines looks for other enabled directives to match event with.
- Once the event matches a directive its correlation starts inside the directive.

Directives have various attributes. Attributes can be sticky and non-sticky. In default settings, attributes are configured as sticky. When an event arrives and its attributes matches with the directive already in correlation process, it sticks with the already open directive. Figure 3.9 shows an example of sticky attribute. If the attribute is configured as sticky different mode, an event with different attribute set as sticky different will correlate with already started event. It is useful to use sticky different mode when aim is to detect port scanning attacks. In this scenario, destination port is set as sticky different. Figure 3.10 shows an example of sticky-different attribute.

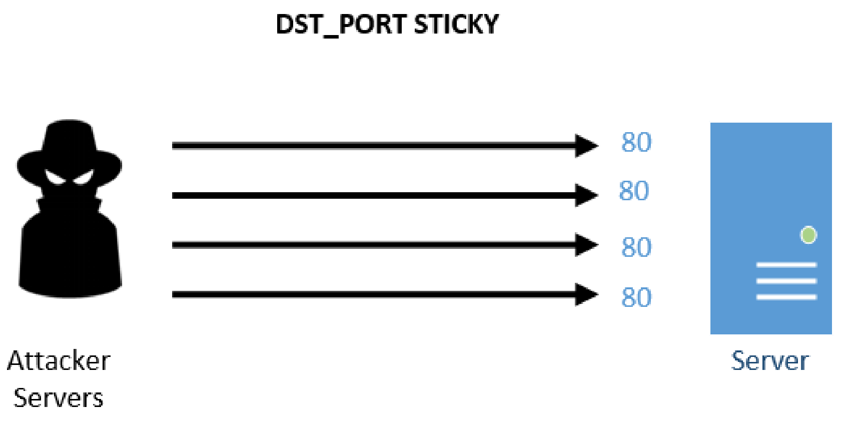


Figure 3.9 Sticky attributes

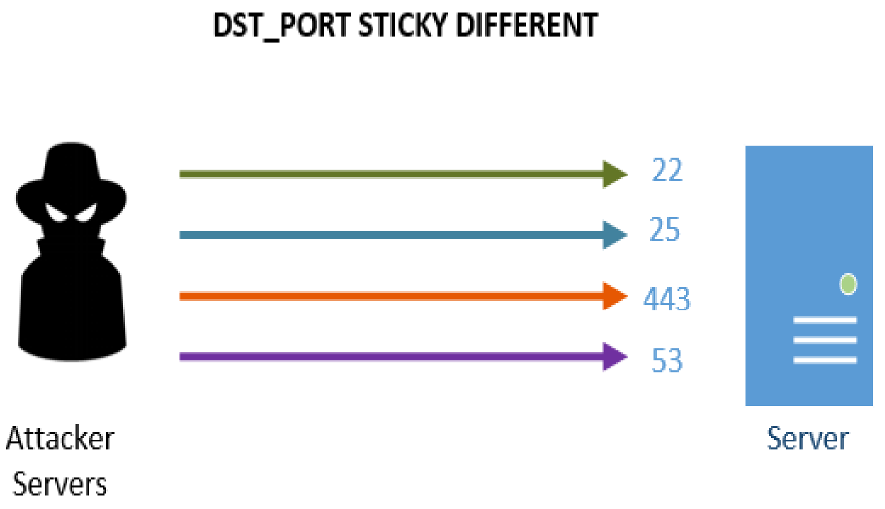


Figure 3.10 Sticky different attributes

3.5.5 Features of OSSIM

There are five important features of OSSIM.

a) Asset Discovery

OSSIM performs active asset discovery scan and passive asset discovery scans for detecting assets in the network. In Active asset scan, OSSIM sends packets for detecting the alive hosts and services running in the network. In passive asset scan, OSSIM passively listen to network traffic and detect assets. Once a new asset is detected, it is added in the asset management database present at server end in OSSIM. Software inventory for each host, the operating system details and services running on the system are also stored in the asset management database.

b) Threat Detection

For threat detection, OSSIM uses NIDS placed in the network and HIDS deployed on all the endpoint devices. NIDS monitors all the traffic within a network or between a device in a network and the internet cloud. It works in promiscuous mode and requires network tap for its working. It has a database of known signatures which is used in performing network traffic analysis. HIDS uses event logs for detection of incidents. It performs log monitoring and collection, detects rootkits installed, uses checksum for file integrity monitoring and performs windows registry integrity monitoring. HIDS agents are installed on the endpoint devices and logs are sent to the OSSIM server for monitoring.

c) Vulnerability Assessment

OSSIM has a built-in vulnerability scanner. It is used for detecting vulnerabilities in assets. Vulnerabilities discovered can be cross correlated with events for increasing the reliability of the event. It can perform both authenticated and unauthenticated scans. In unauthenticated scan services features that do not require credentials are examined. SSH and SMB services are accessed in authenticated scan.

d) Behavioural Monitoring

OSSIM uses logs collected from endpoints and network devices for analyzing network behavior, NetFlow for live traffic analysis and availability monitoring for assets. NetFlow tells details about number of packets (and bytes) exchanged between two end points. It helps in analyzing critical alerts. Availability monitoring is used to monitor critical assets that are involved in business valued services.

e) Security Intelligence

OSSIM uses SIEM Correlation engine and OTX feed for providing security intelligence. OTX is an open threat intelligence community. Threat indicators are collected in the pulse. User of SIEM can subscribe to latest threats related to the environment. OTX updates the defense mechanism to detect the indicated threat in the subscribed pulse. OTX indicated alarms and alerts are mostly true positive as they are based on indicators of compromise collected by threat intelligence community.

3.6 Analysis of OSSIM

OSSIM is an open source tool developed by Alien Vault. It is developed using combination of other open source tools. OSSIM is using SNORT as a NIDS. SNORT performs signature based detection and therefore cannot detect zero-day attacks for which signatures are not developed yet. Similarly, HIDS agent can also detect rootkit patterns based on signatures, thus, they cannot detect a little variant in the payload. The critical feature of a vulnerability scanner is its knowledge base. The knowledge base of OpenVAS is limited thus cannot identify certain vulnerabilities. For behavioral monitoring of network traffic, OSSIM reserves netflow stats. Netflow stats can only give an overview of a situation. For example, it can only share the amount of data transferred between the hosts but cannot give an insight into the actual data transferred. The actual data transferred can be seen in traffic captures only. OSSIM provides wide set of functionalities but it lacks product maturity. There is a need of solution that can perform detection based on signatures as well as behavior and capture traffic for more in-depth analysis.

3.7 Conclusion

This chapter explains SOC structure. SOC consists of people, processes and technology. People having security specialties using monitoring technologies under right processes can analyze the security picture of an organization. Recently SOC’s have started using SIEM technology for easing the analysis work. SIEM provides a unified platform for getting a holistic view of the organization. The basic features of SIEM include event collection and normalization, correlation of events, alerts and reports generation, providing visibility through dashboards and log storage for forensic purposes. Further this chapter analyzes OSSIM. Its components are mainly divided into server and sensors. Data collection, aggregation and normalization is performed on sensor end whereas risk assessment, policy determination, correlation is performed on server end. OSSIM provides asset discovery, threat detection, vulnerability monitoring and security intelligence. OSSIM provides wide set of capabilities but these capabilities lack maturity. OSSIM can be used by various organizations that desire to setup SOC in minimum cost. There is a need of a tool that can overcome the limitations of OSSIM and provide more in-depth network analysis.

Chapter 4

Evaluating SIEM Solutions

4.1 Introduction

In the past few years, organizations have developed the need of using SIEM beyond compliance management. Security intelligence is beneficial for improving the organization’s ability to deal with the emerging threat landscape. An increase in the successful targeted attacks, organizations now require advance security monitoring, early attack detection and incident response capabilities. As discussed in the previous chapter, OSSIM lacks maturity. There is a need to identify a solution that can help in monitoring and analysis of network at an advance level. In order to evaluate available solution a standard set of parameters are required. Unfortunately, so far there is no such standard available. This chapter focuses on selecting set of parameters for evaluating various SIEM solutions. Further, based on the evaluation criteria, this chapter provides an analysis of existing SIEM solutions.

4.2 Parameters for Evaluating SIEM Solutions

SIEM tools are considered to increase the ability of an organization to identify inappropriate activities through network monitoring, network performance data, vulnerability reports of the network and audit logs. There are no standard set of capabilities listed to be included in a SIEM implementation. For an organization, SIEM should be evaluated based on functional requirements, non-functional requirements and cost effectiveness. Based on [34], no two SIEM implementations provide same functionalities but all implementations listed as SIEM provide basic capabilities of SIM and SEM. No software qualifies for being a SIEM unless it provides the two essential capabilities SIM and SEM.

Vendors provide additional functionalities integrated with the SIEM like Availability and Performance Monitoring (APM), File Integrity Management (FIM), Integrated Advance Visualization Dashboards, Access Management, Advance Threat Intelligence feeds, Actionable SIEM component, Integrated Advance Compliance Reporting interface and Deep Network Inspection etc. The functional capabilities provided within SIEM include:

4.2.1 Security Information Management

According to [32, 34, 35], SIM includes log collection, log parsing and formatting, normalization of logs, analysis of logs based on correlation rules and log compliance reporting. Log retention in terms of size limit and time limit is considered crucial for detection of slowly progressing attack [33].

4.2.2 Security Event Manager

SEM provides real time monitoring of security events including log based monitoring, network flow based monitoring, application activity monitoring, user activity monitoring [34]. Real time monitoring of events can be made effective using predefined monitoring rules requiring minimum customization. It provides basic or advance level of incident management depending on the vendor specific implementation. Also, the retained data can be used for querying supporting forensic investigations.

4.2.3 Availability and Performance Management

Few seconds of downtime of a single IT resource can result in a loss of millions of dollars. Also, performance issues of network devices can result in losses too. Availability and Performance Management of the network devices is important for solving performance issues, increasing the operational efficiency to reduce the downtime, monitoring the health of security devices and reducing the fault occurrence rate. APM in integration with SIEM can help in early detection of anomalies [36].

4.2.4 Advance Visualization Dashboards

Network activity can be conveniently monitored using dashboards within SIEM. Customized dashboards provide flexibility in performing the operations [37]. All the network nodes are highlighted in the dashboards. Advance Visualization Dashboard interfaces provide real time insight into the network state. SOC officers can drill down the information to investigate the event closely using advance visualization dashboards. They are considered to highlight anomalies and intrusions, thus resulting in early response to the events [38].

4.2.5 File Integrity Management

File Integrity management is a process used to validate internal operating system files, core software applications, user specific software applications and user files. Current file state is compared with the defined baseline for the verification process. FIM can be used along with the SIEM to detect intrusions by comparing current operating system and software states to the baseline [39].

4.2.6 Actionable SIEM

Actionable SIEM can intelligently suggest remedial actions on occurrence of specific events. It requires constant training of dataset based on the daily changing threat landscape. It is assumed to reduce the involvement of human resources and to speed up the actions.

4.2.7 Identity and Access Management

Identity and Access Management helps in only authorized access to resources and in recording individual activities. Access management along with SIEM can be used for user activity monitoring [40]. User activity reports for auditing can be generated through SIEM. Also, Exception monitoring can be done using SIEM by providing information about user roles.

4.2.8 Threat Intelligence

Threat Intelligence feeds provide alerts about existing and emerging threats that can be used in early decision making. Threat intelligence feeds along with SIEM can detect call home malwares, relating old threat intelligence feeds to new one to detect slow progressive attacks, threat Intelligence feeds can be used in other context based alerts and reports [41].

4.2.9 Deep Packet Inspection

Deep packet inspection is the examining of network packet data in depth. Along with basic correlation, Deep packet inspection and end point data capture can be used for real time monitoring.

4.2.10 Advance Compliance Reporting

Compliance reports are required to fulfill regulatory requirements. Advance reporting formats in SIEM can minimize the job of auditors.

Besides these functional capabilities SIEM solutions are evaluated based on the non-functional capabilities. They are considered to be equally essential. The non-functional capabilities include:

4.2.11 Support for 3rd party components

There are tools that support components from same vendor which limits the usability of the tool, overall cost of the process and reduces performance of the organization. There should be a support for 3rd party components. It allows the organizations to integrate and correlate the outputs and data from various tools.

4.2.12 Ease of Deployment

Difficulty level of deployment and time to value is an essential feature to be considered while evaluating SIEM solutions. The best solution is considered to be the one with minimum deployment difficulty and fastest time to value.

4.2.13 Ease of Customization

Organizations have different security needs; same solution cannot be feasible for many. Customization of correlation rules, visualization dashboards, and compliance reports may be required. Ease of customization can help increase the productivity.

4.2.14 Availability, Reliability and Response time of the Product

In real time applications, availability, reliability and response time are considered to be highly critical attributes. Like all other software products, SIEM should be evaluated based on availability, reliability and response time too. SIEM should be available 24/7 with minimum downtime and high response rate.

4.2.15 Support for multiple Operating systems

An organization can be using multiple operating systems. SIEM should be compatible with all of them. It is not cost effective for an organization to purchase multiple solutions because of operating system compatibility issues.

4.2.16 Usability and Scalability of the Product

The ability to easily use the SIEM solution can increase the productivity of the organization. Minimum learning requirements for a solution can increase customer satisfaction. Also on increase in number of users or the size of network, the ease of scalability is a critical attribute too.

4.3 Analysis of SIEM Parameters

A SIEM solution should be evaluated based on the above mentioned functional and non-functional parameters. These parameters are selected after studying various SIEM solutions. According to our research these parameters should be considered while evaluating SIEM solutions. Nonfunctional attributes are considered to be highly critical and must have parameters of an evaluation. Most of the SIEM solutions do not provide all of the listed functional requirements. There is a need to determine the relative weight of the functional capabilities to increase the effectiveness of the evaluation. The weight of the attributes can vary based on the customer organization. It depends on the importance of certain features for an organization in comparison to others. In this research, the relative weight of the parameters is determined based on the survey. Survey was based on the questionnaire. The prepared questionnaire has multiple choice questions. A separate question was composed indicating the need of the functional requirement. . Questions are designed to find the effectiveness and weight of the capabilities. The purpose of the survey was validation of identified requirements and identify their relative weight. The survey was conducted using LinkedIn (www.linkedin.com) as questionnaire distribution medium. 50% of the respondents of the survey were information security professionals with minimum 2 years of experience with SIEM technology. All respondents were well aware of SIEM technology

4.4 Relative Weight of Parameters

As discussed above, survey was conducted with the aim to verify the functional requirements. Each functional capability and its survey response are discussed below.

a) SIM provides log collection, parsing, formatting and normalization. It also provides log retention and compliance reporting sub functionalities. Figure 4.1 shows the sub functionalities on x- axis and no of responses in their favor on y axis. According to survey results, more than 50% of the survey population supports the presence of SIM sub functionalities in a SIEM solution. Other responses include easy to use, Netflow monitoring, import/export of asset scan results etc.

b) SEM provides real time monitoring, incident management and forensic analysis capabilities. Figure 4.2 shows the graphical results. 94% of the respondents consider real time event monitoring to be a sub functionality of SEM and more than 50% are confident about incident management and forensic analysis as an essential functionality of SEM. Other features as discussed by responders include event correlation, capability of integrating third party forensic suites.

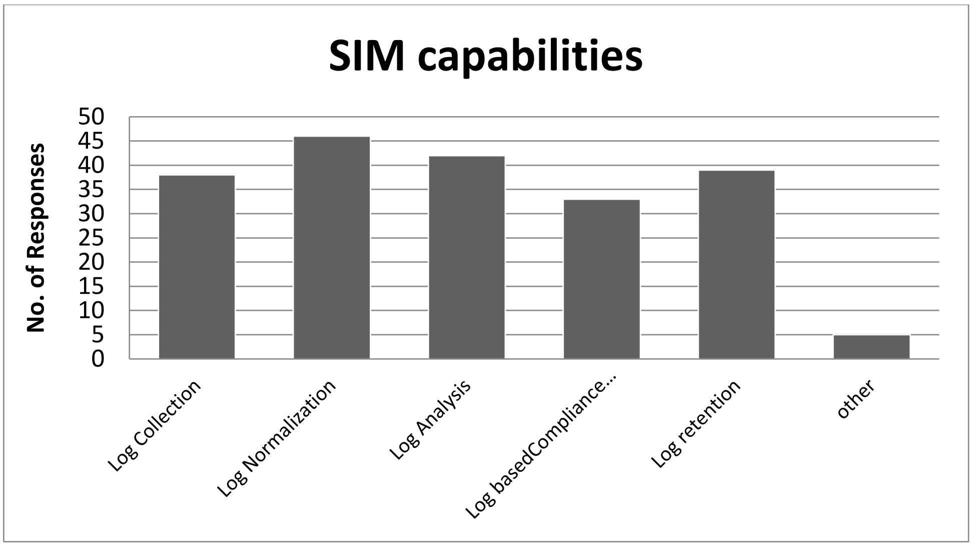


Figure 4.1 SIM capability graph

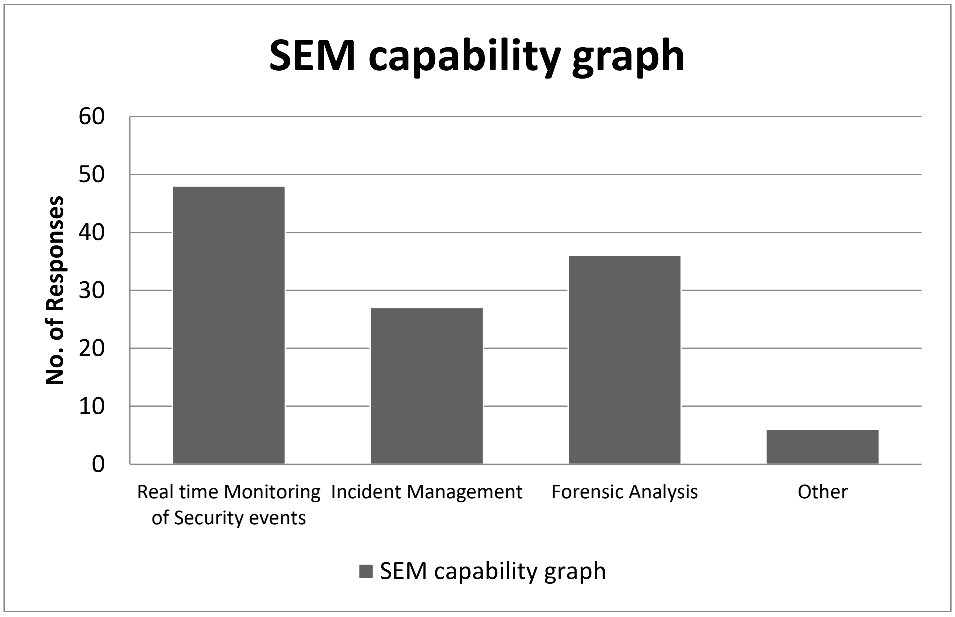


Figure 4.2 SEM capability graph

c) As discussed before, File integrity management is used for validating the files. With SIEM it helps in detection of malwares, rootkits and maintaining the integrity of critical user files and system directories. 53% of respondents consider FIM should not be provided as an integrated functionality. According to the responders, FIM can only be critical for few organizational servers, it should be integrated only on user requirement. Figure 4.3 provides a graphical view of the responses. Y axis shows the number of responses and on X axis questions along with the response categories are represented.

Response categories include ‘yes’, ‘no’ and ‘other’. Responders are of the opinion integrating FIM with SIEM would make it difficult of administer though it can be provided on demand for critical machines.

d) Availability and Performance management along with SIEM can help in detection of anomalies affecting the performance or health of the systems. Performance feeds can be used by SIEM to closely monitor IT assets. 59% of the respondents consider APM to be an entirely separate functionality and should not be provided as an integrated functionality with SIEM. While 41% are in favor of including it, one of the respondents highlighted that though availability and performance monitoring is complementary to SIEM but it should not be included as a compulsory part of SIEM.

e) Advance visualization dashboards are considered to enhance the visibility into the network. It allows the SOC officers to drill down the information to closely examine the anomalies. According to the survey result, 73% of the respondents consider it to be an essential part of SIEM. Other respondents highlighted it to be really helpful in performing incident response as well.

f) Actionable SIEM is an advance SIEM feature. It recommends the remedial actions to be taken on occurrence of an event. 68% of the respondents consider it to be an important feature. According to a Senior Information Security Consultant, fully automated remedial actions cannot be done using any SIEM implementation, it requires human involvement. However, generation of remedy suggestions can ease the work of SOC officer. Other respondents also highlighted that Actionable SIEM should not be fully automated, it should involve analysts. Figure 4.3 shows 35 respondents responded with ‘yes’ for having an actionable SIEM, 11 responded with a ‘no’ and other 5 believes it to be partially automated.

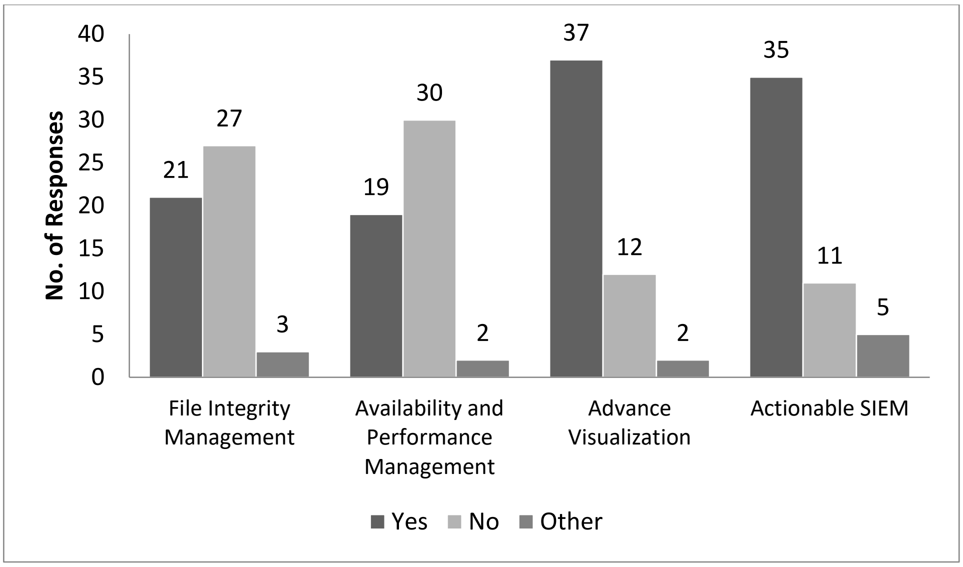


Fig 4.3. Functionalities survey response (a)

g) Identity and Access Management helps in only authorized access to resources and in recording individual activities. Using IAM with SIEM can help in tracking the role based user activities in the network. It helps SIEM in user activity monitoring and tracking deviations from the standard user behavior. 51% of the population consider it be an essential capability while other considers it be a total different layer of security. Figure 4.4 shows the number of responses plotted against response category for each question.

h) Threat intelligence helps in keeping the network secure by proactive intelligent decisions and early actions against attacks. Threat intelligence feeds fine-tune the SIEM alerts. According to 86%of the respondents, threat intelligence feeds should be included in SIEM.

i) Along with basic correlation, Deep packet inspection and end point data capture is considered crucial for real time monitoring. It is a security probe used to deeply analyze and investigate a security event. 67% of the respondents consider that deep packet inspection should be included in SIEM solution. It helps in incident investigation. Other respondents raised the concern of keeping balance, as real-time detection is far more important than late deep investigation.

j) Scheduled compliance reporting with various report formats can help auditors in checking regulatory compliance. 75% population among the respondents is positive about including advance compliance reporting formats with SIEM. They are intended to reduce the workload of the auditors.

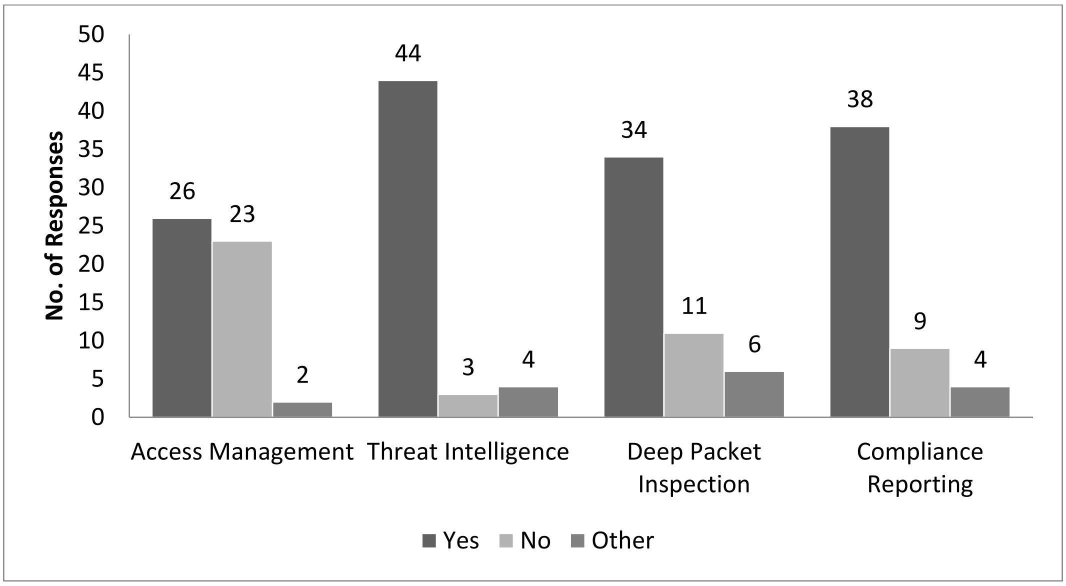


Figure 4.4. Functionalities survey response (b)

Based on the survey results, a capability-weight table is populated shown as Table 4.1. Capability weighting is the term used to define relative value of the capabilities. The weight of the capability determines the impact its presence or absence will make. Assigning weights to capabilities help selecting the suitable SIEM solution for the organization. Currently, it is defined based on the survey responses as it indicates majority requirements. It can be readjusted according to the organization's needs. Different vendors provide SIEM solution having different capabilities and one SIEM solution cannot fit every organizations requirement. Assigning weights to capabilities help choosing the most appropriate SIEM solution according to the user requirements. Organizations should evaluate the SIEM solution before purchasing. The relative weight of the functionalities can also vary with specific requirements of the organization.

TABLE 4.1 CAPABILITY RATING

Functional Capability	Weighing
SIM	Very High
SEM	Very High
Threat Intelligence	High
Advance Compliance reporting	High
Deep packet inspection	High
Actionable SIEM	High
Advance Visualization Dashboards	High
Access Management	Medium
Availability and Performance Management	Low
File Integrity Management	Low

4.5 Available SIEM Solutions

The SIEM solutions that meet the basic criteria of having two main capabilities i.e. SIM and SEM are evaluated. Evaluation is performed based on capability weighting defined as a result of survey. Below is the brief description of each product. Data is collected from the officially available data sheets of each product highlighting the main capabilities.

4.5.1 HPE ArcSight SIEM

HPE ArcSight SIEM a solution available for detecting threats and compliance management. It has a flexible architecture to allow the organizations to include their existing deployment elements.

a) Deployment

It is available in the form of appliance hence it’s easy to deploy. Deployment involves only few steps.

b) Data Collection and Storage Engine

HPE ArcSight collects stores and analyzes security events through one appliance. It has the capability to capture data up to 400,000 events per second and has the storage capability of up to 480TB. The collected data is compressed and encrypted to keep it secure during motion and at rest.

c) Dashboards for Security Analytics

It provides built-in dashboards for security analytics. Dashboards support analytics for detecting malware activity user activity, endpoint logs, firewall logs and IPS logs.

d) Compliance Reporting

Audit reports and compliance dashboards are easily acquired with downloadable report packs.

4.5.2 IBM QRadar

IBM QRadar aggregates logs from devices present in the network, stores the collected data in its raw form, performs correlation to detect threats. It captures layer 4 and layer 7 data using deep packet inspection method for intelligently detecting threats.

a) Deployment

IBM QRadar is available as hardware and virtual appliance both.

b) Security Analytics

Deep packet inspection makes IBM QRadar specialist in threat intelligence. It reduces the number of events generated to limited list of suspected intrusions. It uncovers advance threats that may be overlooked by other solutions using extended time frame for detecting and tracking malicious activity.

c) Visualization of information

It provides dashboard for visualization which makes it easy for analyzing alerts and detect early attack activity. It provides 5 dashboards including security intelligence, network activity monitoring, application activity monitoring, system monitoring and compliance reports.

d) Compliance Reporting

It has built-in compliance with security standards like ISO-27001 etc.

4.5.3 SPLUNK App for Enterprise Security

SPLUNK provides built-in correlation rules, displays alerts and reports, incident review functionality and the dashboard for visualization. It integrates third party intelligence feeds with its SIEM to provide threat intelligence. It has a non-modular structure.

a) Deployment

SPLUNK is available as software. It can be installed on wide range of operating systems. It has an easy deployment method.

b) Data Collection

Data collection can be done through SPLUNK collectors. It supports 3rd party collectors as well. It uses Flat file system for data storage with no schema or normalization. All the data collected is stored in original state and can be searched.

c) Security Analytics

It detects known threats and can also use non–security data to detect zero-day threats. It detects application based attacks and insiders' frauds.

d) Reporting

It provides ease of creation and modification in reporting. It displays the data in the form of tables, charts and scatterplots

4.5.4 LogRhythm

LogRythm is a security intelligence platform specially designed keeping in view the MSSPs.

a) Deployment and Scalability

It has an easy to deploy infrastructure. It can be scaled according to the customer needs.

b) Dashboard

Operation and management of LogRythm can be done through a wizard driven console.

c) Security Analytics

It provides a comprehensive security intelligence platform.

d) Multi tenancy

As this solution is designed for MSSPs, it supports multi tenancy of multiple user data. It logically separates the customer data while ensuring each customer can view its data only.

4.5.5 McAfee SIEM

McAfee provides few capabilities as core SIEM functionalities. They include Event Receiver, Log Manager and Security Manager. Others are provided as additional modules.

a) Deployment

It follows a modular approach for deployment which allows the deployment in centralized or distributed structure. It is easily scalable in terms of adding capabilities.

b) Compliance Reporting

McAfee has partial support for compliance. It has wide range of templates available. It only stores user specified data for long duration which is against compliance standards.

c) Security Analytics

It only highlights the data as event data as risky, bad or normal but remedial actions require SOC officer involvement. It supports real time threat monitoring.

4.6 Drawbacks of SIEM solutions

This section provides the drawbacks of each solution.

4.6.1 HPE ArcSight SIEM

It is not available in the form of virtual appliance. It has limited actionable SIEM features. It does not support deep packet inspection for detecting intrusions and anomalies. The Workflow within SIEM is not completely automated and requires manual actions to be taken. It does not support endpoint level analytics like file integrity monitoring, service availability and performance management. Also, it does not support role based access control monitoring.

4.6.2 IBM QRadar

IBM QRadar does not support data compression and encryption. It also has limited reporting templates available for report generation.

4.6.3 SPLUNK App for Enterprise Security

It partially supports forensic use cases. It does not provide host based monitoring. Also, it does not support DPI. Remedial actions in case of an incident require SOC officer involvement. It does not use contextual information for detecting advance cyberattacks.

4.6.4 LogRythm

It has partial support for forensic use cases and does not monitor availability and performance of individual endpoints.

4.6.5 McAfee SIEM

It only retains user specified data for long duration therefore it has limited support for forensic and compliance reporting use cases. It does not support DPI.

4.7 Comparison of SIEM solutions based on core functionalities

The comparison of SIEM solutions on the basis of core functional requirements is given in table 4.2. Here F represents full capability, P represents partial capability, and N represents absence of capability.

TABLE 4.2 Comparison on the basis of essential functionalities

Capability Indexing/ SIEM Vendors	HPE ArcSight	SPLUNK	Intel Security (McAfee)	Log Rhythm	Solar Winds	NetIQ	IBM Qradar
Country of Origin	USA	USA	USA	USA	USA	USA	USA
Comparing SIEM Solutions Based on Essential functional capabilities							
Log Collection Automation	F	F	F	F	F	P	F
Log Management Automation	F	F	P	F	P	F	F
SIEM Analysis Automation	F	F	F	F	F	F	F
SIEM Workflow Automation	P	F	F	F	F	F	F
Event Analysis(Real time monitoring events)	F	F	F	F	P	F	F

Capability Indexing/ SIEM Vendors	HPE ArcSight	SPLUNK	Intel Security (McAfee)	Log Rhythm	Solar Winds	NetIQ	IBM Qradar
SIEM Compliance Automation	F	F	F	F	F	F	P
optimized for SIM	F	F	F	F	F	F	F
Optimized for SEM	F	F	F	F	P	P	F
Data Retention	F	F	F	F	F	F	F
Support for Forensic Use cases	F	P	P	F	F	P	F
Total Full capabilities	9	9	8	10	7	7	9
total Partial Capabilities	1	1	2	0	3	3	1
Total No capabilities	0	0	0	0	0	0	0

4.7.1 Analysis

On the basis of core functionalities, tools can be rated as shown in the figure 4.6. According to the analysis, LogRhythm provides all core functionalities, HP ArcSight, IBM Qradar and SPLUNK provide 9 out of 10 core functionalities.

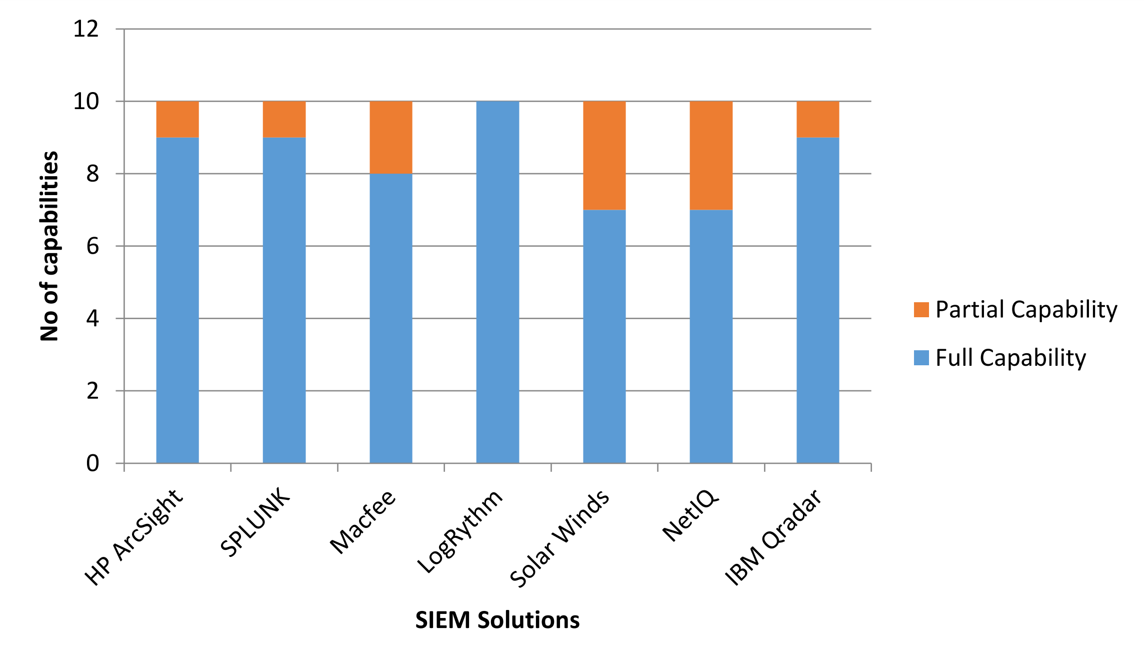


Figure 4.5 Analysis on the basis of core functionalities

4.8 Comparison on the basis of advance capabilities

The comparison of SIEM solutions on the basis of advance Functional requirements is given in the table 4.3. Here F represents full capability, P represents partial capability, and N represents absence of capability. According to the analysis, LogRythm provides maximum full and partial capabilities. If the functionalities are equated, LogRhythm stands out to be the best one. Weights can be applied specific to organizational needs for selecting the best suitable option for the company.

TABLE 4.3 Comparison on the basis of advanced functionalities

Capability Indexing/SIEM Vendors	HPE ArcSight	SPLUNK	Intel Security (McAfee)	Log Rhythm	Solar Winds	NetIQ	IBM Qradar
Context Based Analysis	F	F	F	F	P	P	F
Threat Intelligence Feeds	F	F	F	P	P	P	F
Deep Packet Inspection	N	N	N	P	N	N	P
Out of Box Reporting	F	F	F	F	P	F	F
Availability and Performance Monitoring	N	N	N	N	N	N	N
advance visualization dashboards	F	F	F	F	F	P	F
File Integrity Management	N	N	N	F	F	N	N
Identity and access management (role based monitoring) (user activity monitoring)	P	P	P	P	N	F	P
Advance Compliance reporting	F	F	P	F	P	P	P
Actionable SIEM	P	P	P	P	N	N	P
Cyber analytics	P	N	N	P	N	N	P
Total Full capabilities	5	5	4	5	2	2	4
total Partial Capabilities	3	2	3	5	4	4	5
Total No capabilities	3	4	4	1	5	5	2

4.9 Conclusion

Security Information and Event Management is an essential part of Security Operation Center. This chapter highlights that the effectiveness of SIEM for an organization depends on the functional capabilities it provides and nonfunctional capabilities it fulfills. Since the SIEM solutions differ in functional and non-functional capabilities, no single solution can be suitable for all organizations. Before selecting the SIEM solution for the organization, each organization should carry out the evaluation of SIEM capabilities and organization’s requirements. The criteria proposed by this research can be used by adding weights according to organizational needs, giving more weight to organization’s core requirements. In the end selecting the SIEM solution having more total score. Organizations should consider all the aspects of SIEM that are of more importance to the organization since every SIEM solution addresses a specific set of problem statements. A carefully selected SIEM Software can play an important role in protecting the network against security breaches.

Chapter 5

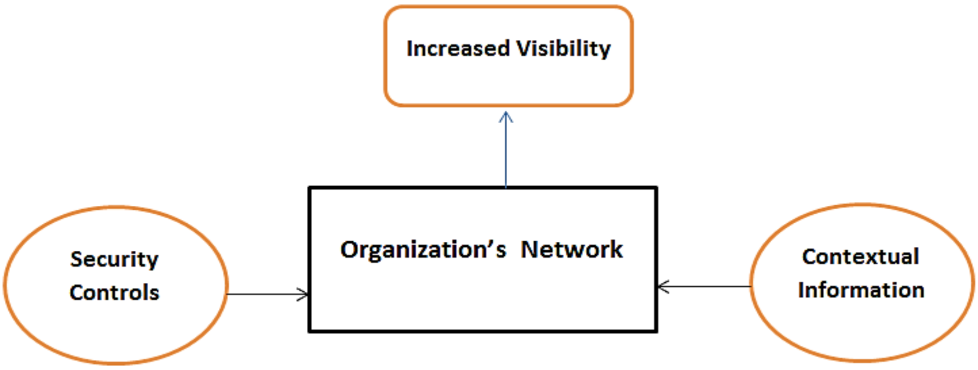
Cyber Security Analytics

5.1 Introduction

In this chapter SIEM is tested for cyber analytic features. Cyber Security analytics is a computational analysis of the cyber data for making effective security decisions. It helps in detection of possible attacks at early stage to contain and respond to the attack at early stage. In cyber analytics context, rich data is used in analysis of network traffic for separating the actual data from noise. Cyber analytics is used for tracking and monitoring of suspicious events, using bit patterns to build behavioral patterns, detecting probes before a full attack, containing the attack before massive destruction. Therefore, they appear to be necessary in detecting advance cyber-attacks. The chapter defines use cases for testing open source SIEM (OSSIM) against cyber analytic features. The results of the test cases highlight the effectiveness of SIEM in detecting advance cyber-attacks.

5.2 Contextual Metrics for Cyber Security

Contextual metrics describes the attributes and circumstances that result in a certain event. Contextual Information can be organization dependent. It includes contextual information related to business, threats and risks. The security controls and contextual information when applied on the right data of the organization gives better visibility of the network situation.



5.1 Increased Visibility

Few advance cyber analytic techniques involving contextual information for detection of intrusions are discussed below. These techniques require deep packet analysis of individual packets and statistical analysis of packets at a certain period.

5.2.1 Beacon Detection

Malware communicates with external hosts through short messages sent after definite interval. These messages are usually sent to inform master that client is alive. They originate from the infected host and sent to C&C server. This strategy is used by malware administrators to track and manage huge range of infected hosts and use them for their desired purposes. Detecting beacons is useful as it is the indication of first network level indication of presence of malware in the network. If the presence of malware is detected and the infected host is contained before malware download tools or upload sensitive data, the damage can be minimized.

5.2.2 Remote Administrator Sessions Detection

Remotely unauthorized network activity can cause irreparable damage to the organizations. Suspicious remote network sessions include applications that are administrative in nature and the end points are geographically far apart.

5.2.3 Data Exfiltration through HTTP

Attackers commonly use open ports for data exfiltration like HTTP, HTTPS, DNS port etc. Exfiltration of Data through HTTP traffic usually goes unnoticed. Data uploads above 100MB are usually rare and should not go unnoticed. Normal web traffic usually indicates more traffic towards the network than outward. If the client to server traffic ratio indicates data upload to a remote server, it should be investigated. Although if a data upload is detected at this point, it means damage has been done, but it is still useful to detect exfiltration at early stage to stop it at that point.

5.2.4 Detection of Port Scanners

According to the kill chain mechanism [42], reconnaissance is the first phase of attack activity. In this phase, attacker searches for the potential target. Usually attackers perform network scanning for identifying potential targets in the network. Attackers look for open ports with vulnerable services that can be exploited. Port scans are usually detected by monitoring TCP or UDP packets having no data are sent to certain number of distinct ports on the network. If an analyst can identify port scanning attempts early, he can identify the potential attackers and the exploitable vulnerabilities.

5.2.5 Detection of Protocol Abuse

Protocol abuse is the mismatch between the port used for communication and the service being used. Attackers after successful intrusion, make hidden access paths and backdoors to remain undetected. The most common technique used so far is to encrypt the traffic using custom encryption protocol and using port 80 for communication. As common ports are usually allowed by the firewall, attackers tunnel their communication through them. Such traffic is considered to be abusing the established standards. Detecting deviations from established standards is essential for network security.

5.2.6 Relay Finder

The hosts used by attackers while attacking a network are called relays. Finding relays are essential for gaining insight of an incident. It works on an assumption that chain of relays is used side by side. Relays can be detected by taking as an input known compromised hosts and then detects the machines it talks to and mark them as potential victims and then take those potential victims as an input and detects the machines it talks to. It helps in recreating the path an attacker took. By drawing the path between the compromised hosts and the potential hosts' incident responders can find the exact path attacker took and chance of going undiscovered becomes negligible.

5.2.7 RDP Keyboard Layout

A network analyst looks for anomalies in the network traffic. RDP is a protocol used by remote desktop application for connecting remotely to a network. By performing DPI, use of RDP service can be detected and metadata can be extracted. Detecting the anomalies in the RDP traffic like different keyboard layout. Typically, administrators of organization use keyboard layout depending on the location. Difference in keyboard layout could indicate the presence of foreign attacker.

5.2.8 Suspicious Admin Tools

Remote Administration toolkits are used for remote administration. Mostly such tools are used by attackers to access victim's network. They are used to direct and control the malicious actions. Detecting RATs can be difficult, as they are programmed in a way to avoid detection therefore signature based search can rarely help in the detection. Using behavioral analysis can help in detection of suspicious admin tools. Defining a baseline line and determining the deviations from it.

5.2.9 Analyzing two distinct IPs

Drawing a map of common activity between two hosts can help in detecting the relationship between the hosts. It helps in detection of compromised hosts or the host involved in launching attack. It helps to narrow down the area of interest and helps on focusing the affected area only.

5.2.10 Use of Unknown Service

Attackers use well known ports usually allowed in the firewall to communicate. Attackers frequently try to hide their communication by using open ports on network. Another way to further remain hidden in the traffic is to use unknown service on known ports. Unknown service means the services that are not well known and does not match any known application service. Detecting unknown service on ports can be used to separate out normal traffic and malicious traffic.

5.3 OSSIM and Cyber Security

OSSIM claims to support basic cyber security use cases like known malware detection based on the signatures, scans, policy violations and brute force attacks. Advance cyber-attack scenarios require behavior monitoring and monitoring the deviations from the standard baseline. There was a need to test OSSIM against advance cyber security use cases based on the defined contextual metrics. Following test cases were developed for testing OSSIM's behavior on occurrence of advance level attacks.

a) Beacon detection based on its behavior can help in detection of command and control communication with the server having no signatures developed yet. Table 5.1 shows the test case details.

TABLE 5.1 Beacon Detection

Test case id	001
Test case name	Beacon Detection
Test case Description	This test case is designed to check if OSSIM detects malware beaconing from internal network to a remote host. In this test case events and alarms will be observed under ANALYSIS tab. It should detect beacons based on the behavior and not signature.
Precondition	1. Alienvault Server is installed in the network 2. Network Tab is provided to the server 3. HIDS agent are installed
Input state	Beacons are generated after every 10 minutes for an external host
Validation	After 5 beacons, OSSIM server should detect malware presence
Expected Output	An alarm should be generated under ANALYSIS TAB for presence of malware in the network

b) Remote Administrator Sessions from geographically far locations does not make sense except if the administrator is travelling. OSSIM should detect based the remote session based on IP geolocation. Table 5.2 provides details of test case.

TABLE 5.2 Remote Administrator Sessions Detection

Test case id	002
Test case name	Remote Administrator Sessions Detection
Test case Description	This test case is designed to check if OSSIM detects remote administrator sessions from geographically far apart location
Precondition	1. Alienvault Server is installed in the network 2. Network Tab is provided to the server 3. HIDS agent are installed
Input state	1. Remote desktop application (Team Viewer) is running on an internal host 2. A connection is established between a host in Pakistan and Australia 3. A file transfer was performed from within a network to the remote location.
Validation	OSSIM should detect remote desktop usage after successful connection establishment.
Expected Output	An alarm is generated under ANALYSIS TAB for remote desktop usage.

c) After a successful compromise, an attacker can exfiltrate the data through common well-known ports. This test case is designed to detect data exfiltration based on the data upload rate.

TABLE 5.3 Data Exfiltration through HTTP

Test case id	003
Test case name	Data Exfiltration through HTTP
Test case Description	This test case is designed to check if OSSIM detects data exfiltration through HTTP(S) port.
Precondition	1. Alienvault Server is installed in the network 2. Network Tab is provided to the server 3. HIDS agent are installed

Input state	Data Upload of more than 100MB were performed through HTTP port of a remote server
Validation	OSSIM should detect Data Upload over 100MB
Expected Output	An alarm is generated under ANALYSIS TAB for data exfiltration

d) Reconnaissance is the first step performed by an attacker. Detecting attack at this stage can minimize the attack ratio. Table 5.4 explains a test case for detecting port scans.

TABLE 5.4 Detection of Port Scanners

Test case id	004
Test case name	Detection of Port Scanners
Test case Description	This Test case is designed to check if OSSIM detects port scans performed internally or externally.
Precondition	1. Alienvault Server is installed in the network 2. Network Tab is provided to the server 3. HIDS agent are installed
Input state	Port scan using Nmap is performed internally and externally both.
Validation	OSSIM should detect port scans
Expected Output	An alarm is generated under ANALYSIS TAB for Port scans

e) Using standard ports to send malicious non-standard traffic comes under protocol abuse. Table 5.5 explains the test case.

TABLE 5.5 Detection of Protocol Abuse

Test case id	005
Test case name	Detection of Protocol Abuse
Test case Description	This test case is designed to check if OSSIM detects protocol abuse.

Precondition	1. Alienvault Server is installed in the network 2. Network Tab is provided to the server 3. HIDS agent are installed
Input state	HTTP packet created using scapy sent over DNS port.
Validation	OSSIM should detect protocol abuse
Expected Output	An alarm should be generated under ANALYSIS TAB for Protocol abuse

f) Detecting relays can help in finding the path attacker took till the destination. Path will provide an insight into all the machines that may be compromised and participating in attack. Table 5.6 provides the details of the test case.

TABLE 5.6 Detecting Relay

Test case id	006
Test case name	Detecting Relay
Test case Description	This test case is designed to check if OSSIM detects relay or path attackers takes in a network.
Precondition	1. Alienvault Server is installed in the network 2. Network Tab is provided to the server 3. HIDS agent are installed
Input state	Making a master-salve malware zombie and make them communicate with Command and Control server.
Validation	OSSIM should detect Relays
Expected Output	An alarm should be generated under ANALYSIS TAB for demonstrating the path malware took.

g) Detecting difference in RDP keyboard layout indicates the presence of foreign attacker. Defining a test case to detect such anomalies can help in early detection of an incident and can avoid the network breach.

TABLE 5.7 RDP Keyboard Layout

Test case id	007
Test case name	RDP Keyboard Layout
Test case Description	This test case is designed to check if OSSIM detects the change of remote desktop keyboard layout than the one used by organization.
Precondition	1. Alienvault Server is installed in the network 2. Network Tab is provided to the server 3. HIDS agent are installed
Input state	Using Chinese keyboard to connect to the network
Validation	OSSIM should detect difference in Keyboard layout
Expected Output	An alarm should be generated under ANALYSIS TAB for different keyboard usage.

h) Remote Administration toolkits are usually used by attackers to access victim's network. Analyzing the malicious behavior in the network can help in detection of RATs. Table 5.8 explains the test case for detecting RATs.

TABLE 5.8 Detecting RATs

Test case id	008
Test case name	Detecting RATs
Test case Description	This test case is designed to check if OSSIM detects usage of RATs.
Precondition	1. Alienvault Server is installed in the network 2. Network Tab is provided to the server 3. HIDS agent are installed
Input state	Luminosity Link is used for remote administration.
Validation	OSSIM should detect the presence of RATs
Expected Output	An alarm should be generated under ANALYSIS TAB for detection of RATs.

i) Extracting the common activity between two IPs and drawing a map between them can help in detection of attack pattern. Table 5.9 defines the test case for it.

TABLE 5.9 Detecting Communication of an IP with other IPs

Test case id	009
Test case name	Detecting Communication of an IP with other IPs
Test case Description	This test case is designed to check if OSSIM analyze the communication of specific IPs and drawing a map between them.
Precondition	1. Alienvault Server is installed in the network 2. Network Tab is provided to the server 3. HIDS agent are installed
Input state	Exploring the features of OSSIM to check if it supports the feature of building communication map of specific IPs.
Validation	OSSIM should draw maps of specific IPs
Expected Output	Given two input IPs OSSIM should draw map of their communication highlighting the common areas of communication.

j) DPI can be used to detect unknown service on well-known ports. It can help in detection of attacker’s communication which is otherwise hidden in the normal traffic. Table 5.10 provides the test case for it.

TABLE 5.10 Detecting Unknown Service

Test case id	010
Test case name	Detecting Unknown Service
Test case Description	This test case is designed to check if OSSIM detects the use of unknown service on open ports.

Precondition	1. Alienvault Server is installed in the network 2. Network Tab is provided to the server 3. HIDS agent are installed
Input state	Sending raw packets over port 80 used for HTTP communication
Validation	OSSIM should detect usage of unknown service
Expected Output	An alarm should be generated under ANALYSIS TAB for detection of raw packets.

5.4 Test Environment

The environment for testing OSSIM against the designed test cases includes three local PCs, a layer three switch having port mirroring enabled on it. OSSIM server is installed on another machine in the network. The network tab taken from the switch is dropped into one of the NICs of OSSIM. In the current environment, any communication between these three machines or between a machine from this network and the outside world is mirrored and sent to OSSIM. HIDS agents are installed on all three PCs. HIDS pushes system logs to OSSIM through management NIC. HIDS uses port 1514 UDP to push the logs to OSSIM. An attacking computer is placed outside the network and is used for creating defined attack scenarios. Figure 5.2 shows the test environment created to perform various test cases.

a) For executing test case 001, a malware from Zeus family is installed on PC1 and is allowed to communicate with its command and control server.

b) For executing test case 002, team viewer is installed on PC2 and is allowed to communicate with a machine located in Australia. File transfer was also performed outward and inward both.

c) Environment Setup for test case 003 involves, a specially crafted packet using scapy [43] sent over port 80 from within the network to outside.

d) Setting up the environment for test case 004 includes installing Nmap on one of the internal machines and on the external machine.

e) Environment Setup for test case 005 involves, a specially crafted HTTP packet using scapy sent over port 53.

f) For test case 006, a malware zombie in master slave mode is installed on two systems and are made to communicate with C&C server.

g) Modification for executing test case 007 incudes using Chinese language keyboard on the outside network computer and trying to connect to any PC from the network using Windows remote desktop application.

h) For execution of test case 008, Luminosity Link Rat was used for remote administration.

i) While executing test case 009, two machines from the network are made to do few similar communications and few different.

j) Environment Setup for test case 010 involves sending a raw packet crafted using scapy sent over port 80.

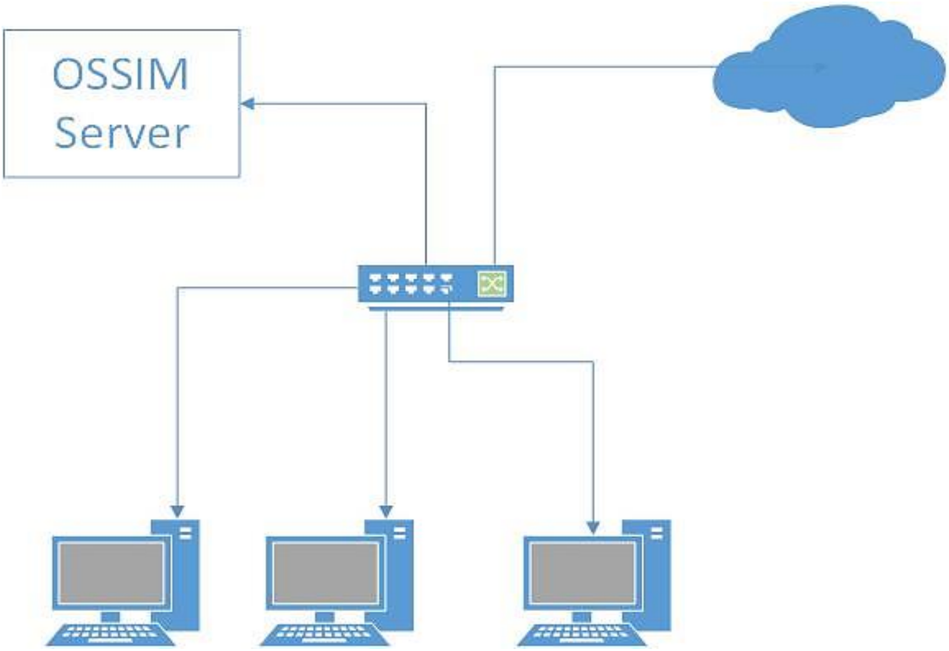


Figure 5.2 Testing Environment for OSSIM

5.5 Test case Execution Results

All test cases were executed in the above-mentioned environment. Only 1 out of 10 test cases ended up with the pass criteria. This indicates that OSSIM does not support context-based use cases. Also, it does not detect threats based on the behavioral analysis. It only detects the threats based on the signatures and IP reputation. Zero-day attacks having no signatures developed will remain undetected. The test case execution results are given in the Table 5.11.

TABLE 5.11 Test case execution results

Test case ID	Test case name	Result
001	Beacon Detection	Fail
002	Remote Administrator Sessions Detection	Fail
003	Data Exfiltration through HTTP	Fail
004	Detection of Port Scanners	Pass
005	Detection of Protocol Abuse	Fail
006	Detecting Relay	Fail
007	RDP Keyboard Layout	Fail
008	Detecting RATs	Fail
009	Detecting Communication of an IP with other IPs	Fail
010	Detecting Unknown Service	Fail

5.6 Limitations of SIEM

SIEM is useful in managing alerts and logs from multiple separate security and network devices. It helps in detection of attacks that require aggregation and correlation of logs and various alerts. It helps analysts in management of all the security alerts by providing a single console to view the network situation. But SIEM does not help in detection of advance security attacks. Limitations are discussed below:

5.6.1 No deep packet Investigation

Alarms are only generated for certain packets while forensic investigation of the incident requires full packet captures to build the scenario. Alarms are generated based on correlation of NIDS rules and HIDS rules, no deep packet investigation is involved. It supports limited cyber analytics scenarios, providing a room for attackers to get-in undetected. Detecting advance attacks require advance analytics techniques, unfortunately, SIEM use cases cover basic detection only.

5.6.2 Context-based analytics

SIEM does not add the element of context to an incident itself. Context along with controls and expertise helps in increasing the visibility of the situation. It requires tuning of existing NIDS and HIDS rules, adding host details and permissions to build the basic context according to the organization. Adjustment of number of alerts or tuning of rule triggering is also context specific. If too tightly bond, there is a chance to miss important alarms. If too loosely bond, number of alerts generated can overwhelm the analyst. Defining the right threshold can be tricky, there is always a chance to miss an important alert.

5.6.3 Customization for pulling logs and alerts

Every machine generates logs in its own specific format. Normalizing the logs into common searchable format requires customization. OSSIM requires writing of custom plugins to pull data in a normalized format. Time spent on customization should be spent of malicious activity detection. Missing any important logs from a machine can certainly lead to blindness from threats.

5.6.4 Logs- Incomplete picture of situation

Logs provide incomplete picture of the situation. Logs cannot be relied upon for making conclusions as sometimes the information is incomplete and vague. Moreover, logs can be tempered by attackers to remove the evidence of breach or intrusion. They can be used as a supporting evidence with DPI of PCAPs to support a scenario.

5.7 Conclusion

This chapter explains the role of contextual information in detecting advance cyber-attacks. Contextual information increases the visibility of the network situation. SIEM did not pass most of the test cases discussed in this chapter, which proves the lack of contextual information. SIEM is capable of providing a holistic view of the organization. It is basically a management tool that provides a single console to get a complete network picture. It monitors and detects wide spread attacks. However, SIEM does not integrate contextual information to the scenarios. It highlights the limitations of SIEM and a need of solution to integrate contextual information for covering advance cyber-attacks. Next chapter provides a solution for SIEM limitations.

Chapter 6

Analysis and Proposed Solution

6.1 Introduction

SIEM acts as a central management platform for providing holistic view of the network situation. SIEM is of great use when trying to aggregate alerts from various disparate systems. There are various attack patterns that can be detected through aggregation of alerts and logs. It reduces the analysts' work of aggregation and correlation. However, SIEM does not support advance analytic scenarios as discussed in the previous chapter. This chapter summarizes the problem statement and provides a detailed solution of the problem.

6.2 Problem Overview

With an increase in cyber-attacks, the need of advance protection mechanisms has raised. Managing various area specific security controls independently that generates tons of alerts require terrific human resources. SIEM was introduced by security professionals to provide a central management of security alerts and to give analysts a holistic view of organization's security situation. SIEM mainly depends on logs generated by external devices and signature based NIDS. During this research SIEM has been tested against various contextual advance attack scenarios. The results of test case execution show SIEM's incapability of handling advance cyber-attacks that require contextual information, deep packet inspection or behavioral analysis. Hence highlighting the need of a solution that can detect advance cyber-attacks and help in keeping organizations secure.

6.3 Overview of the Solution

The proposed solution will help in detection of advance cyber-attacks. Proposed solution is context-aware, integrating network traffic data with security intelligence data. The features that are included in the solution as proof of concept includes Beaconing

Detection, Remote Administrator Sessions Detection, Data Exfiltration through HTTP, Detection of Protocol Abuse, Relay Finder, RDP Keyboard Layout, Suspicious Admin Tools, analyzing two distinct IPs and Use of Unknown Service. Detecting malicious beacons at early stage and cleaning the infected system can help contain the damage and protect the network against major widespread damage. Similarly having remote administration access can give attacker complete hold over the machine. Detecting remote administration sessions at the earliest stage can help protect organization from data breach or data loss. Therefore, these features are essential in detecting advance cyber-attacks. The proposed features require performing analytics on PCAPs. Integrating the proposed solution with SIEM can help in correlating them with other relevant signature based alerts, hence detecting widespread attacks. Also, integrating the proposed solution will help in getting a better and more accurate holistic view of the organization's security situation.

6.4 Overall Architecture of Proposed Solution

The proposed system works on PCAPs while integrating the contextual information for generating meaningful alerts.

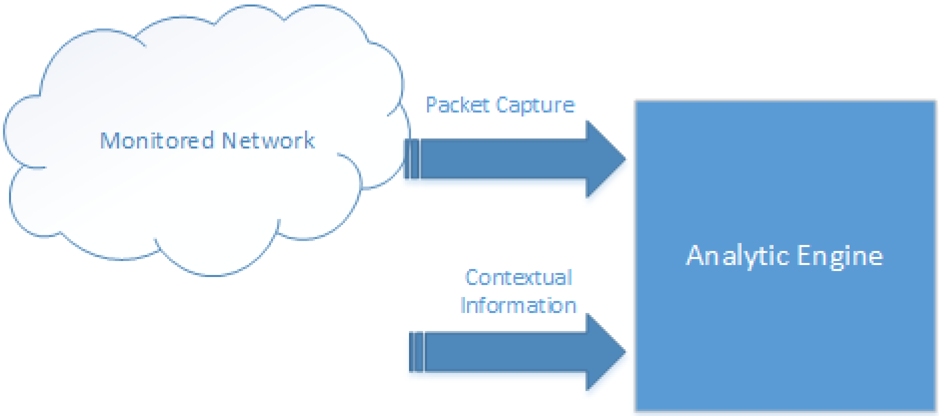


Figure 6.1 Analytical Engine

The three main components of the proposed system consist of PCAP collector, contextual information provider and the analytic engine.

6.4.1 PCAP collector

PCAP collector collects full network traffic packets and extracts the metadata from packets. It stores the raw packets till the requirement is raised. Also, it captures data from other network devices and data sources.

6.4.2 Contextual Information

Contextual information is specific to organization and it adds extra meaning to the data. Other solutions including SIEM do not incorporate contextual information. Thus, many advance threats go undetected. The proposed system adds IP geo locations, organization specific whitelisted IPs, blacklisted IPs, DNS details etc. It also includes known IPs and Domain with bad IP reputation.

6.4.3 Analytic Engine

Analytic engine combines and correlates the collected packets and contextual information. It provides analysts with a platform for searching and inquiring the critical data. Unlike other tools, it not only stores complete packet captures but also provides an automated way for searching the required data. Packets captures perform a major role in investigation.

The data is taken from various points in the network for example from network firewall, from security devices, and PCAPs at network traffic level. Collected PCAPs are sent to PCAP collectors/ sensors which then forwards the collected PCAPs to Cyber analytic module. Metadata of PCAPs is segregated based on protocol type, IPs and various other attributes which speeds up the searching process and alert generation. Analytics works on metadata of the packets which speeds up the process. However full packets can also be viewed by analysts on query. The web Interface can make the tool user friendly allowing analysts to retrieve the valued data easily. For the proof of concept, no web interface is designed.

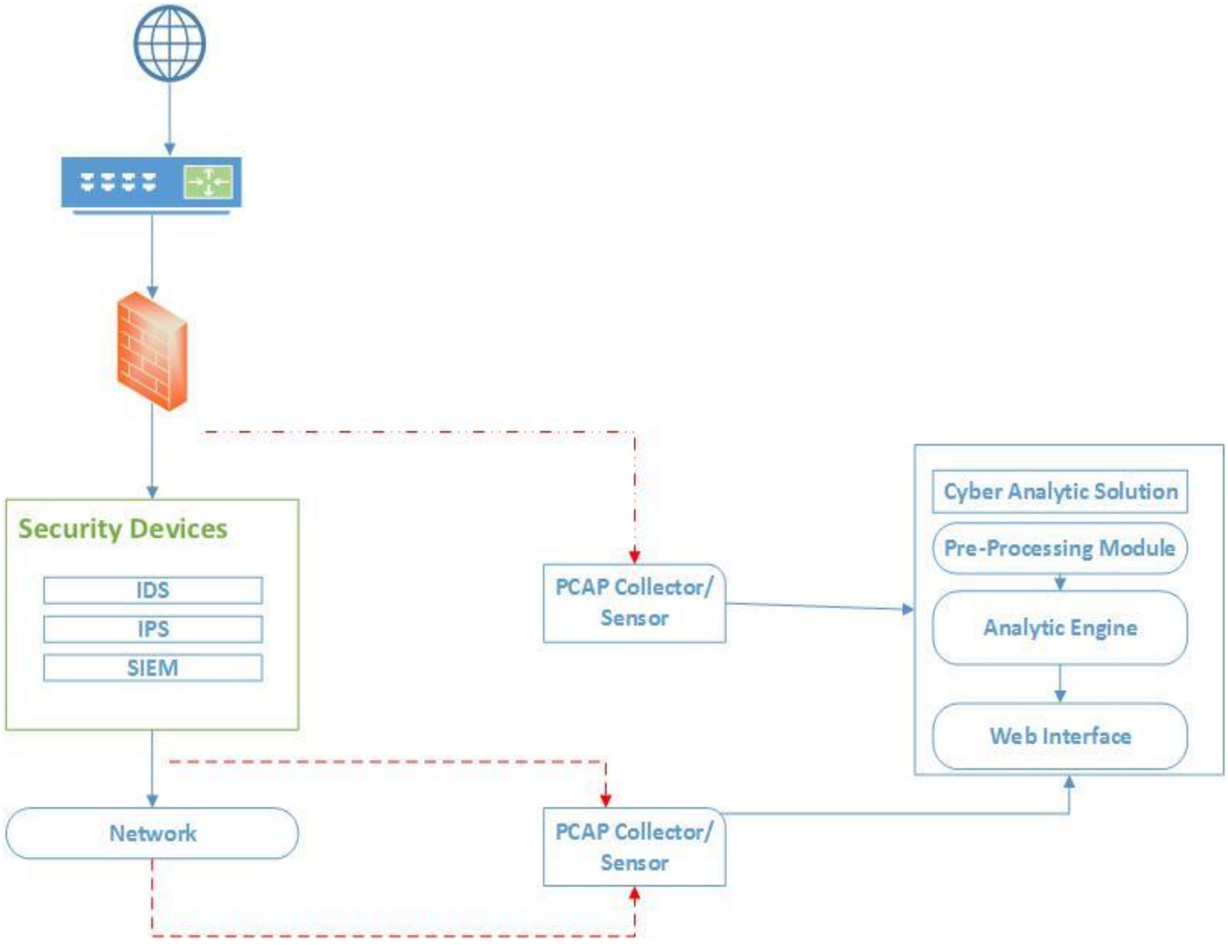


Figure 6.2 Proposed Cyber Analytic Solution

6.5 Composition of Analytic Engine

Analytical engine generates alerts based on the cyber analytical features included in it. It combines the information extracted from network packets with the contextual information for generating alerts. Contextual information may vary depending upon the type of industry, region and other details. Alerts are correlated for generating alarms. Alarm generation process of analytical engine is presented in Fig 6.3. For example, alerts for malware beacons and data exfiltration during a given timeframe for the same internal host is an indication of confirmed compromise and data breach. Similarly, use of a remote administrative tool from a geographically far apart location and keyboard layout difference can be an indication of foreign attacker's successful intrusion into the network. Such alerts require immediate action from the concerned teams. Correlating the alerts help us reduce false positives and figure out situations requiring urgent response.

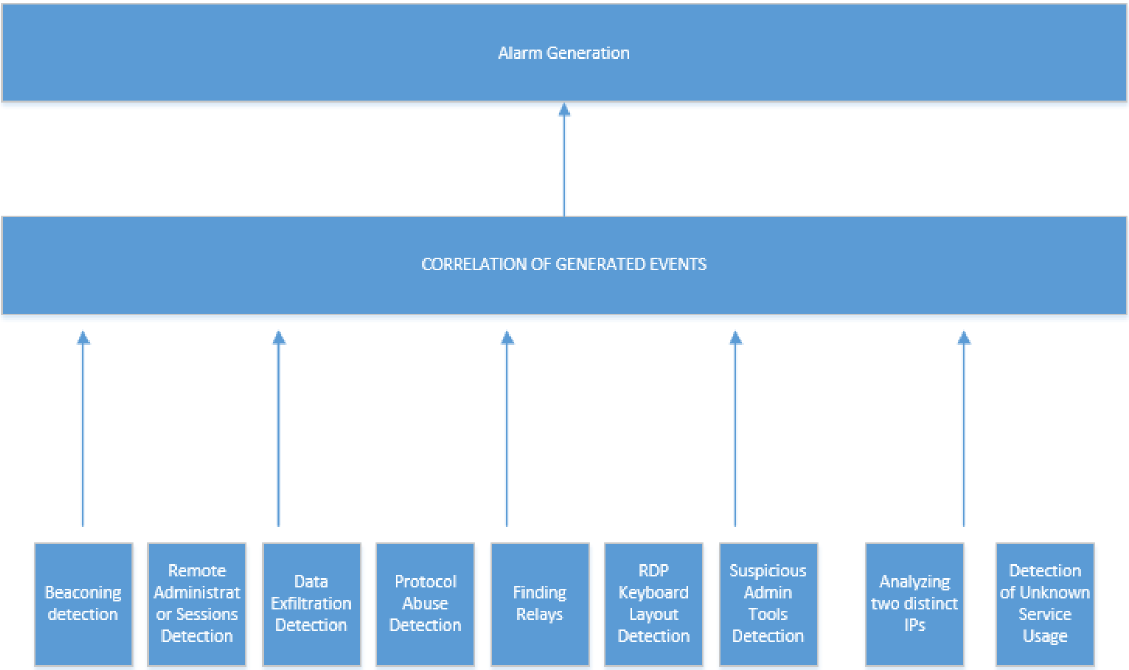

Alarm Generation
CORRELATION OF GENERATED EVENTS
Beaconing detection
Remote Administrator Sessions Detection
Data Exfiltration Detection
Protocol Abuse Detection
Finding Relays
RDP Keyboard Layout Detection
Suspicious Admin Tools Detection
Analyzing two distinct IPs
Detection of Unknown Service Usage

Figure 6.3 Cyber Analytic Engine – Alarm Generation

Indicator of compromise(s) for a confirmed compromise is extracted from the generated alarm. They are fed back into the analytical engine to refine the generation of alarms. The knowledge base helps in constant learning of the system according to environment. Figure 6.4 shows anatomy of cyber analytic engine.

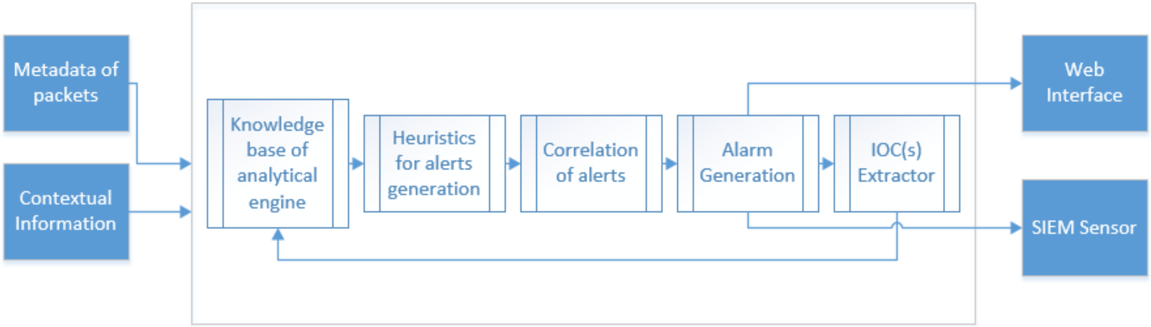


Figure 6.4 Anatomy of Cyber Analytic Engine

6.5.1 Detecting malware beacons

Malware beacons are sent by the infected host to the command and control server on regular basis as an indication that the infected host is up and can take instructions from the server. It helps C&C servers in managing large number of infected hosts. Malware beacons are among the first network related signs for presence of malware. In most of the cases, beacons are sent as soon as the malware gets installed in a host. Depending on the malware, the C&C server gives further instructions that may include downloading some other files or exfiltrating business impact data. Usually beacons are sent through the ports allowed in the firewall that includes http port 80, https port 443and DNS port 53. Companies allow these ports in the firewall for allowing internet browsing etc. from within the network. Applying heuristics on the allowed outgoing traffic can help in detection. Mostly such network packets have no or short data part and are less than 1 MB in size. Determining the mean time between the packets sent can help in calculating interval and frequency of the packets transferred. Moreover, addition of contextual information like IP reputation of the external host reduces the chance of alert to be a false positive. Once the infected host has been identified, it should be immediately isolated from the rest of the network and the cleanup should be performed. Figure 6.5 shows the filters that can be used for detection. In case of alert generation for legitimate beacons, whitelisting can be done.

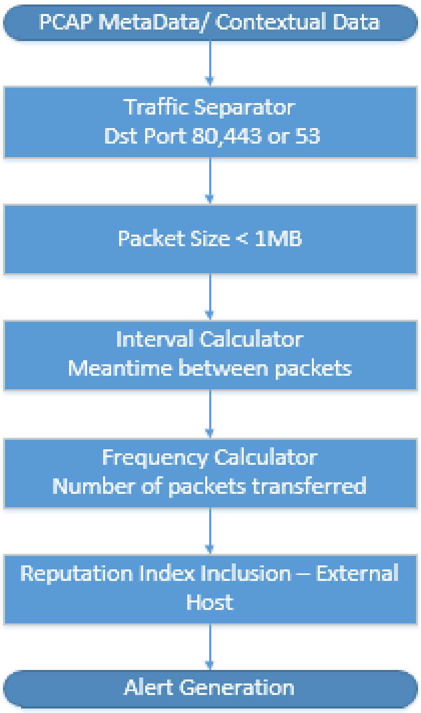


Figure 6.5 Detecting beacons

6.5.2 Remote Administrative Sessions

Remote administration tools are used by network administrators to remotely access the servers and endpoints. But if the administrator traffic is coming from geographically far apart location, it can be an indication of an admin travelling and connecting the server for maintenance. Usually admins that access the servers are usually physically at the same location and even otherwise they use VPNs to connect to the network first. Therefore, this administrator like traffic activity can be an indication of presence of an attacker trying to remotely control a server. Suspicious activities having the service types administrative in nature and the hosts geographically far apart can be detected by applying search filters. Figure 6.6 shows the filters that can be used for detecting remote administrative sessions. In case of legit activity, it can be whitelisted in the application.

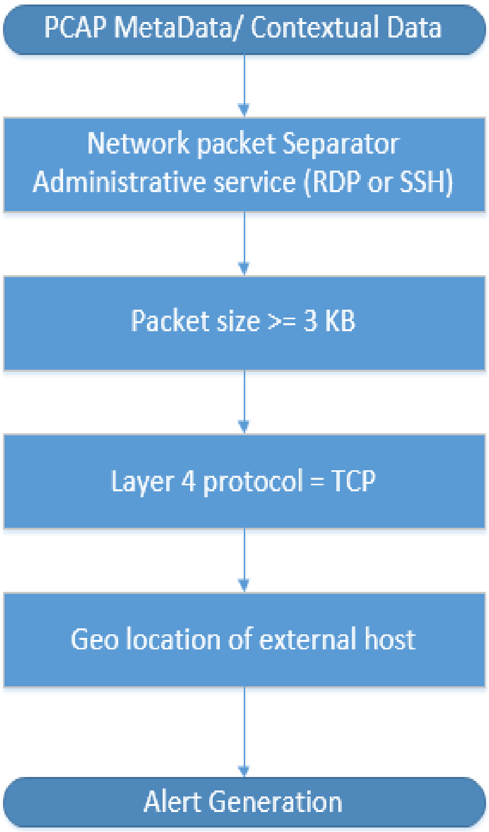

PCAP MetaData/ Contextual Data
Network packet Separator Administrative service (RDP or SSH)
Packet size >= 3 KB
Layer 4 protocol = TCP
Geo location of external host
Alert Generation

Figure 6.6 Detecting Remote Administrative sessions

6.5.3 Detecting data exfiltration through HTTP

Data exfiltration from the compromised network clearly means that the damage has been done. Still detecting data exfiltration at early stage can help contain the damage. Mostly attackers use channels that are allowed in the firewall for exfiltrating data. It helps them hide the transferred data in the noise of network traffic. Exfiltrated data is usually compressed and encrypted by the attacker before uploading it to the remote server. Attackers later get the data from the remote server. Usually HTTP and HTTP(s) channel are used by the attacker for this purpose. Data exfiltration can be detected by applying various heuristics, mainly by identifying HTTP(s) sessions having outbound data transfer more than the inbound. Figure 6.7 shows the filters that can be applied for the detection.

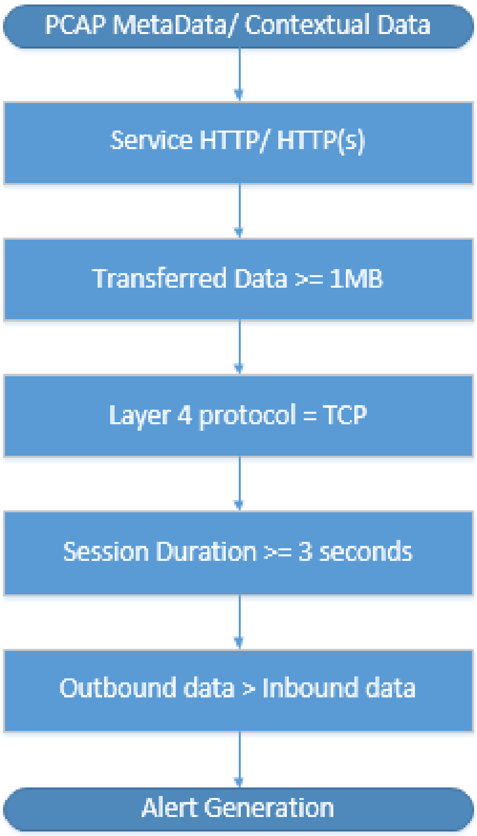

PCAP MetaData/ Contextual Data
Service HTTP/ HTTP(s)
Transferred Data >= 1MB
Layer 4 protocol = TCP
Session Duration >= 3 seconds
Outbound data > Inbound data
Alert Generation

Figure 6.7 Detecting Data Exfiltration

6.5.4 Detecting Protocol Abuse

Internet standards have been defined for communication through well-known ports, for example for communication on port HTTP protocol is used. Attackers mostly use common ports that are allowed in the firewall for communication. They create backdoors that transfer data in raw or encoded form thus leading to protocol abuse. Similarly use of custom encryption techniques for transferring data over port 443 is also an indication of protocol abuse. Mostly such traffic goes undetected because of noise of network traffic. For identifying malicious traffic, a baseline table should be populated having common ports and defined internet protocols for them. Deviations from the baseline can be reported as alerts. Figure 6.8 shows the phases for detecting protocol abuse.

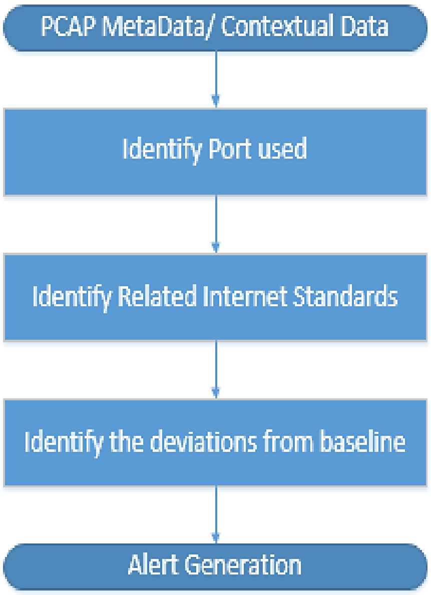

PCAP MetaData/ Contextual Data
Identify Port used
Identify Related Internet Standards
Identify the deviations from baseline
Alert Generation

Figure 6.8 Detecting Protocol Abuse

6.5.5 Detection based on RDP Keyboard Layout

Remote administrative tools are used by admins to operate and maintain the servers remotely. Organizations may allow RDP traffic through the firewall to facilitate the admins for managing the servers from outside the network if required. RDP sessions give user a complete access to the system. It has its advantages but if it is used by the attacker it can cause destructive activities, mostly when attacker uses stolen credentials and the victim is unaware of the credentials being stolen. One way of detecting anomalies is to look for deviations from the baseline user activity. It is a lengthy process and can exhaust resources. Other way is to apply heuristics on the metadata of the network packets to detect anomalies. Figure 6.9 shows the filters that can be applied for the detection of different keyboard layout.

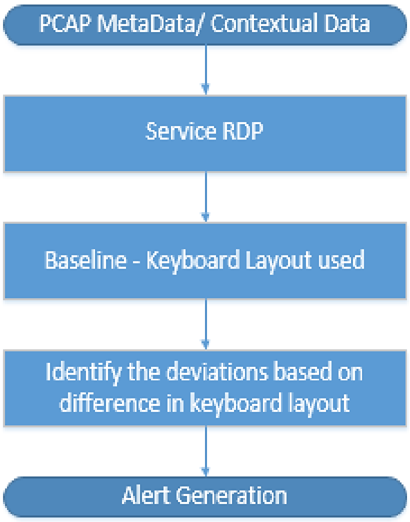

PCAP MetaData/ Contextual Data
Service RDP
Baseline - Keyboard Layout used
Identify the deviations based on difference in keyboard layout
Alert Generation

Figure 6.9 Detecting difference in Keyboard Layout

6.5.6 Finding Relays

Attackers usually after establishing foothold in the compromised host, use it as a relay for infecting other machines. Machines directly communicating with the compromised host has a higher probability of being infected. Further, machines communicating with most of those potentially compromised hosts can be next relays. It helps in detection of the path attacker took. Also, it can be used for containing the attack from spreading all over the network by figuring out all possible paths attacker took. It refines the search for finding all possible relays, reducing the effort required. Figure 6.10 shows relays finder phases.

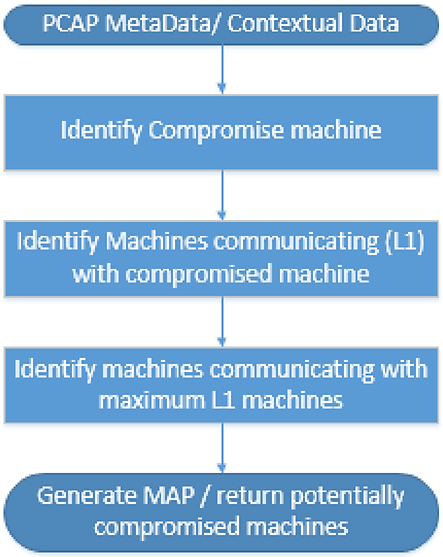

PCAP MetaData/ Contextual Data
Identify Compromise machine
Identify Machines communicating (L1) with compromised machine
Identify machines communicating with maximum L1 machines
Generate MAP / return potentially compromised machines

Figure 6.10 Finding Relays

6.5.7 Suspicious Admin Tools

Admin tools are used by attackers for remotely controlling the compromised hosts. They used these tools to gather sensitive information from the compromised host or to use it to launch a DDoS attack. Due to the network traffic is it not possible to detect admin tools. One of the admin tool is Luminosity Link RAT. There are variety of RATs freely available. Writing IDS signatures for each variant of RAT is not possible. Applying heuristics on session establishment is the one of the behavior based ways to detect RAT tools. For example, PoisonIvy uses 256 bytes challenge/response mechanism for session negotiation. Such heuristics can be used for detecting RATs.

6.5.8 Analyzing two Distinct IPs

During an investigation of a network for identifying compromised hosts trying to find them without any heuristics can be difficult. Use of two IPs as start point for the detection may include attacker machine(s) and compromised host (s). Identifying their communication with other hosts can help in detection of all potentially infected machines. The common portion between the search results should be the focus of the investigation.

Such heuristics can help in detection of all internal infected machines, level of damage caused by the attacker.

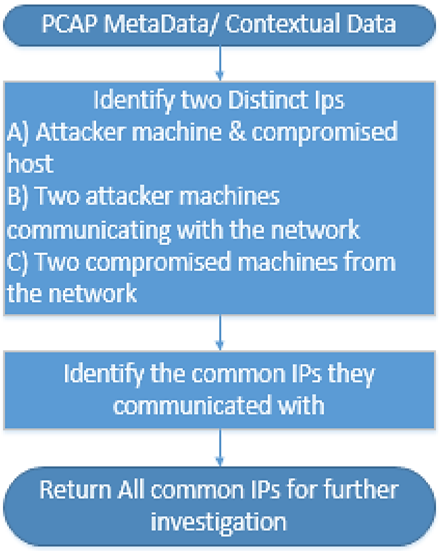

PCAP MetaData/ Contextual Data
Identify two Distinct Ips
A) Attacker machine & compromised host
B) Two attacker machines communicating with the network
C) Two compromised machines from the network
Identify the common IPs they communicated with
Return All common IPs for further investigation

Figure 6.11 Identifying Relation between two IPs

6.6 Integration with the Existing SIEM Solution

SIEM solutions are known for aggregating, correlating and analyzing the events. SIEM does not perform raw packet network analysis. Integrating cyber analytic solution with SIEM will make powerful analytical solution. Cyber analytic solution in combination with SIEM will be able to detect advance attacks and known attacks. While SIEM is capable of generating alerts on known attacks, cyber analytical system will help going more depth and investigate zero-day attacks or insider activities. Cyber analytics solution in combination with SIEM will provide following advantages:

6.6.1 Comprehensive Network Picture

SIEM does not perform DPI so the alerts are generated based the network and host based signatures of known threats. To mark an alert as False Positive or True Positive further analysis of the alert is required. Our proposed system will support DPI and will provide various automated filters for threat detection. Combination of these two tools will provide a comprehensive view of the network. The alerts generated by our solution will also be added to SIEM as a data source and custom correlation rules will be written in SIEM to support and generate alarms on advance threat detection.

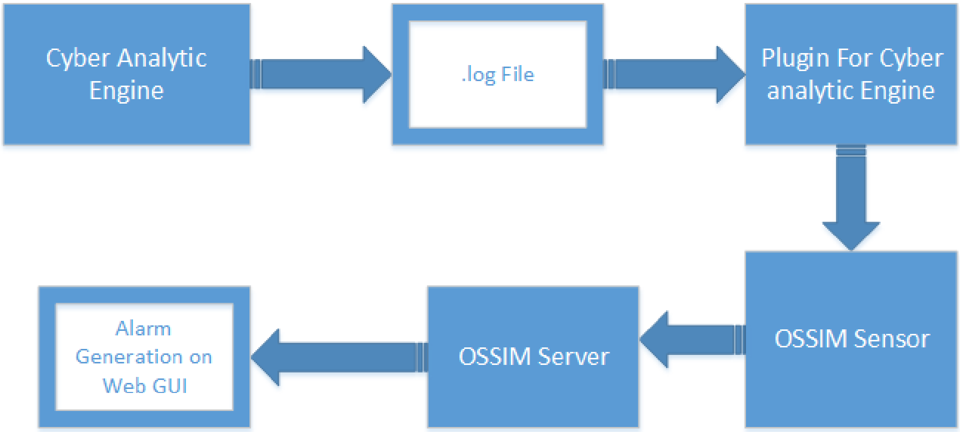


Figure 6.12 Integration of Cyber Analytic Solution with SIEM

6.6.2 Improved alert investigation

Cyber analytic solution will generate alerts on the basis of DPI having more chance of being a true positive. The metadata of the packet will be displayed with an alert as user data attributes of an alert. Further investigation requiring full packet display can be done through cyber analytic GUI. SIEM does not detect the beacons generated from inside. Analytic engine will perform analysis by searching for communication between two IPs after a specific interval and packets are of short length. Similarly, SIEM does not generate alert for data exfiltration. Cyber analytic engine will check for data transfers between two provided hosts and will highlight hosts with large data transfers. Any such case will indicate that the compromise has been done and the breach is in progress. Still detecting and stopping a breach at early stage is better than not detecting it at all. Also, Keyboard layout is usually constant throughout the network of an organization. RDP Layout should also be the same. Different keyboard layout can be identified by examining the metadata of the packet. Difference in keyboard layout may indicate the presence of foreign attacker. Hence, overall it will improve the alert investigation for analysts.

6.6.3 Improved Forensic investigation

Combination of these two tools with a forensic investigation platform will speed up the overall process of investigation. Analyst will be able to see all the alerts on SIEM, he can further investigate it using our cyber analytic system. On finding threat specific PCAPS, he will be able to export them to forensic investigation tool to further dig down. Thus, facilitating the forensic investigation process.

6.7 Conclusion

This chapter provides a solution for addressing the limitations of SIEM. Cyber analytic solution contains three main components: pcap collector, contextual information provider and analytic engine. Combination of Cyber analytic solution and SIEM will provide analysts with a powerful network monitoring solution. The proposed system covers the shortcomings of SIEM and complements the SIEM capabilities by providing DPI. It will increase the effectiveness and efficiency of the SOC team. Also, it will improve the security posture of the SOC team.

Chapter 7

Conclusion and Future Work

7.1 Overview

This thesis reviews various components of SOC and is focused on technological aspect of SOC. Security monitoring platforms play an important role in monitoring and securing an organization. Organizations invest in security devices for securing their critical assets.

In Today's world, cyber-attacks are well planned and are difficult to detect and respond to. Organizations require trained people, mature processes and improved technology for protecting their assets. This indicates the need of improving technologies and processes and training of the people accordingly for a better security posture. This chapter provides research over, research contribution to the topic, limitations and future work required.

7.2 Research Overview

The research is about using the technology in a way to reduce manual efforts required by analyst in keeping a network secure. For this purpose, various security tools are reviewed. SIEM appeared to be the latest tool being used by organizations for security monitoring. In depth research of features, workflow and limitations of SIEM was performed. During the research process, it was figured out that there is no standard or set of guidelines for selecting or qualifying any tool as SIEM. Evaluation criteria was designed for qualifying a tool as SIEM. The base line of this evaluation criteria was developed based on the existing SIEM tools, survey conducted among the analysts from information security domain and essential requirements for securing networks. Available SIEM solutions were evaluated based on the designed criteria. Various shortcomings were identified in the available SIEM solutions. Further, OSSIM was tested against various cyber-attack detection use cases. The results of the test cases executed shows absence of cyber security analytics features. The most critical component was absence of DPI. A solution has been proposed based on the identified limitations of SIEM. The proposed solution would cover the limitations of SIEM and increase the efficiency of analysts in performing analysis of organization’s security condition.

7.3 Contribution

The research provides evaluation criteria for selecting the best suitable SIEM solution for an organization. If organization does not have any specific requirement, the criteria can be used without adding weights. If organization have specific requirements, the criteria is used by adding more value to the client required capabilities. The best suitable solution is selected based on the highest total score value. Also, this research provides a solution to SIEM’s limitations. The proposed cyber analytic system works on deep packet inspection and contextual information. Features are proposed to be included in the solution. Integration of proposed solution with SIEM can provide a better holistic view of the organization’s security.

7.4 Limitations and Future Work

SIEM has been tested against few critical cyber security analytics features. The proposed solution consists of these features only. It is recommended to test SIEM against other cyber-attack scenarios as well. Addition of more context-aware features will help in keeping the organizations’ secure. This research was focused on technological aspect of SOC. There is a need to carry out research on the other aspects of SOC as well namely people and processes.

7.5 Conclusion

Security analysts should be aware of latest attack trends. Organizations need to take advance proactive measures to keep the network secure. Security devices have now become an essential component of an organization’s IT assets. Choosing most relevant device according to the organization’s requirement has become a challenge.

Improvements in technology cannot make improvements in the security posture of organization alone. There is a need to train the human resource of the organization as well to get a complete security posture.

Appendix "A" – Functional attributes Questionnaire

Different Vendors provide additional features along with the essential features of SIEM. The purpose of this survey is to get the SIEM users input about the critical and additional features included in SIEM. This survey is part of a research about cyber analytics.

Name and Designation: ________________________________

1. **Security Information and Event Management (SIEM) must have components include Security Information Management (SIM) and Security Event Manager (SEM). SIM must have functional requirements include:**
   - Automated Log Collection
   - Automated Log management (automated log formatting and normalization)
   - Automated Log Analysis (Based on correlation methods)
   - Log retention
   - Log compliance reporting
   - other
2. **SEM must have functional requirements include:**
   - Real time monitoring of security events
   - Incident Management
   - Forensic Analysis Based on stored events
   - Other
3. **File integrity management (FIM) is a mechanism for validating the integrity of the operating system files, application software files and user data files. As an additional functionality in SIEM, rate FIM from 1 to 4 (1 being most critical to 4 being not required)**
   - 1
   - 2

- 3
- 4

4. **Availability and Performance management is the monitoring of availability, health and performance of network devices. Availability and performance management of the security devices and network equipment as an additional functionality with SIEM can be rated from 1 to 4 on: (1 being most critical to 4 being not required)**
    - 1
    - 2
    - 3
    - 4
5. **Visualization of events in real time helps in decision making. As an additional feature visualization should be rated from 1 to 4 as: (1 being most important to 4 being not required)**
    - 1
    - 2
    - 3
    - 4
6. **Counter measures associated with correlation rules are assumed to reduce the involvement of human resources and to speed up the actions. Remedial capabilities should be included along with other functionalities.**
    - Yes
    - No

7. **Access Management helps in only authorized access to resources and in recording individual activities. Rate Access Management as an additional functionality from 1 to 4: (1 being critical to 4 being not required)**
   - 1
   - 2
   - 3
   - 4
8. **Threat intelligence helps in keeping the network secure by proactive intelligent decisions and early actions against attacks. Do you consider it to be included as an additional capability with SIEM?**
   - Yes
   - No
9. **Along with basic correlation, Deep packet inspection and end point data capture is considered essential for real time monitoring. Do you think it should be included in SIEM?**
   - Yes
   - No
10. **Scheduled compliance reporting with various report formats can increase user satisfaction. Should it be included with basic compliance reporting in SIEM?**
    - Yes
    - No

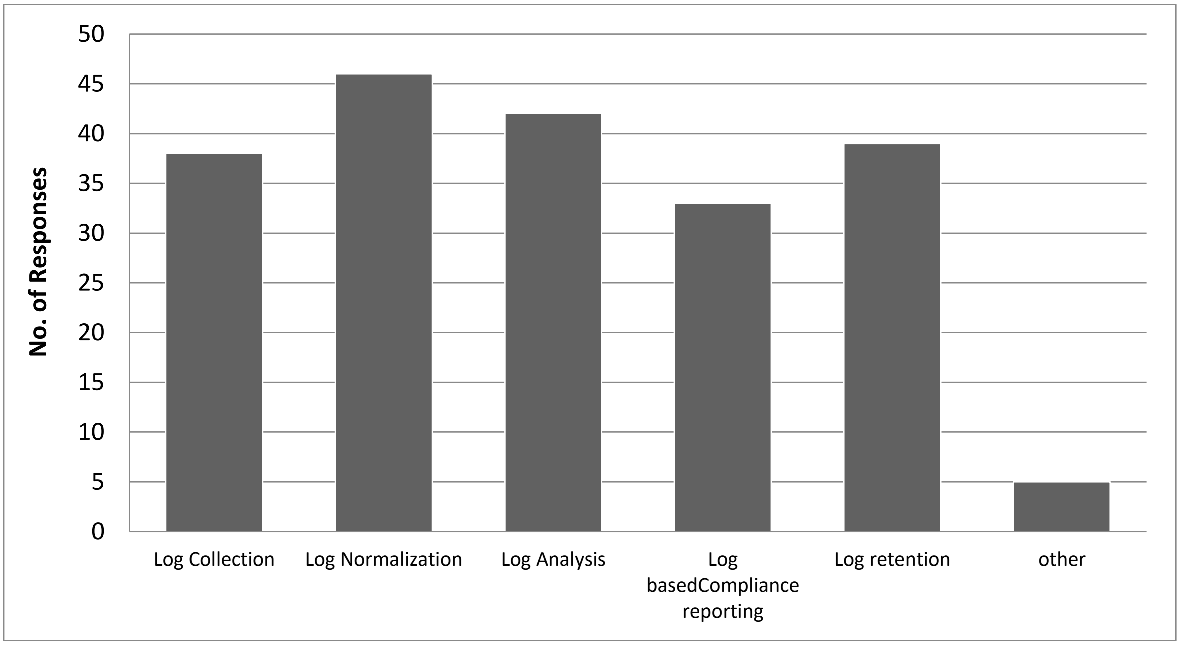
Appendix "B" – Survey Report Defining Functional Requirements of SIEM Solution

Total 50 people responded to the survey questionnaire, including IBM Senior Consultant, Prelude SIEM Product Manager and many other information security professionals using various SIEM products.

Question 1:

Security Information and Event Management (SIEM) must have components include Security Information Management (SIM) and Security Event Manager (SEM). SIM must have functional requirements include:

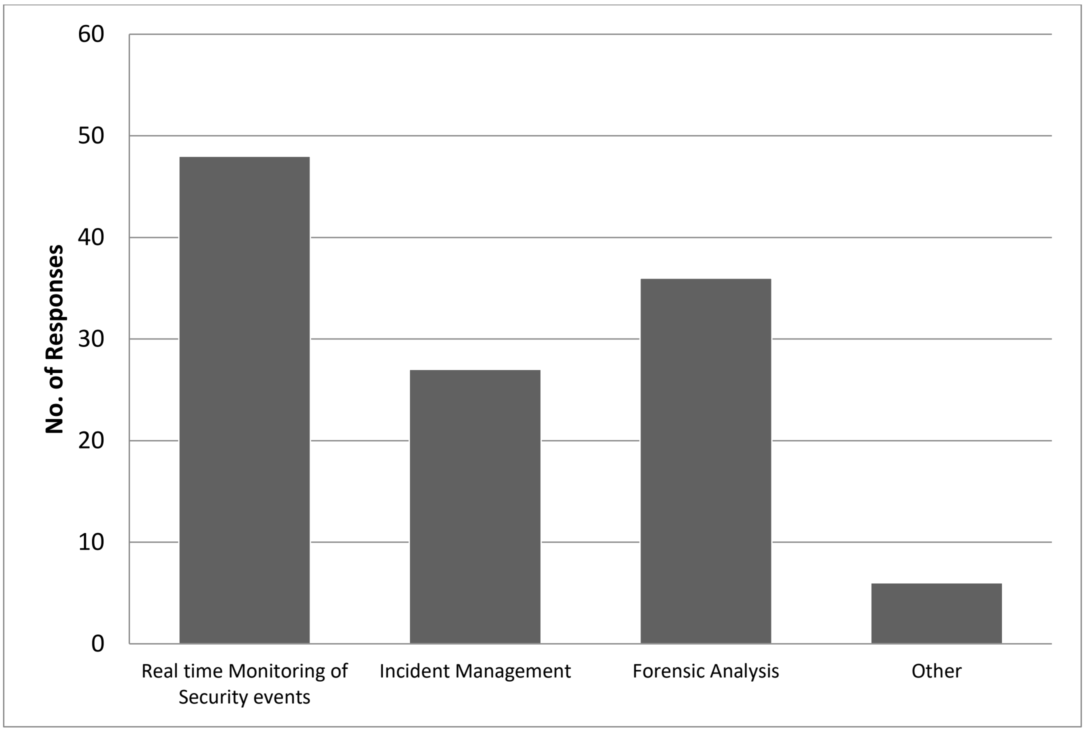
1) Automated Log Collection
2) Automated Log management (automated log formatting and normalization)
3) Automated Log Analysis (Based on correlation methods)
4) Log retention
5) Compliance reporting based on Logs



Question 2:

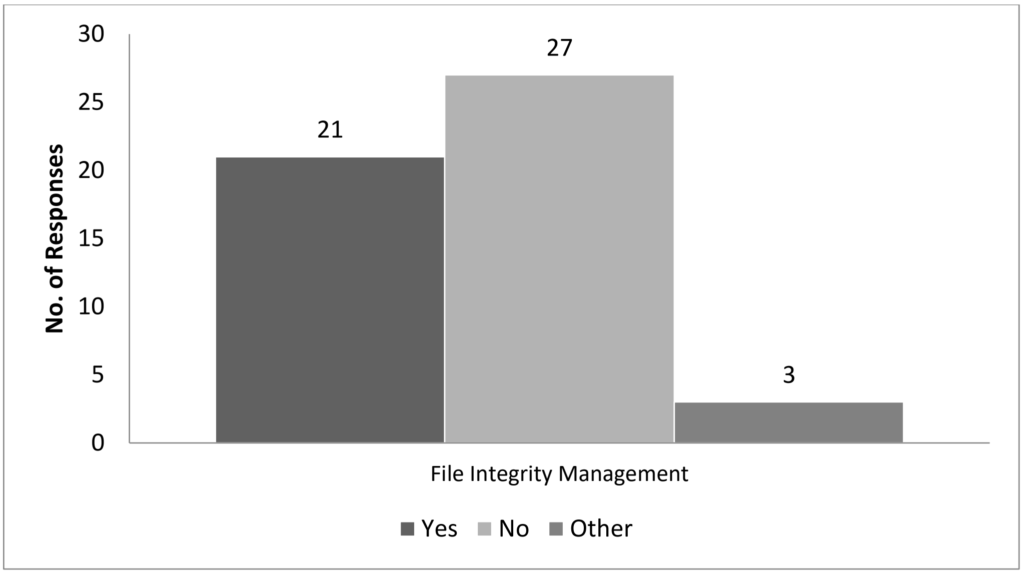
SEM must have functional requirements include:

1) Real time monitoring of events
2) Incident Management
3) Forensic Analysis



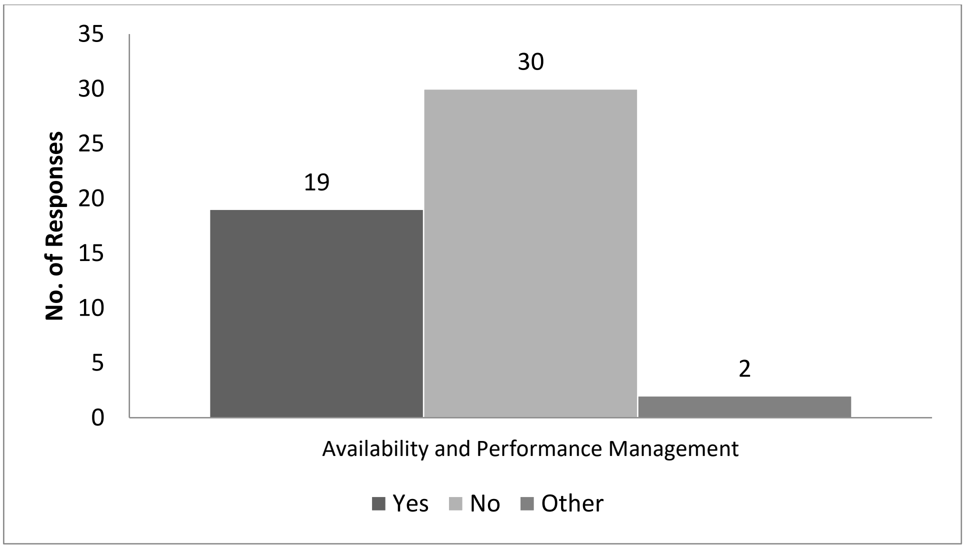
Question 3:

File integrity management (FIM) is a mechanism for validating the integrity of the operating system files, application software files and user data files. As an additional functionality in SIEM, rate FIM from 1 to 4 (1 being most critical to 4 being not required)



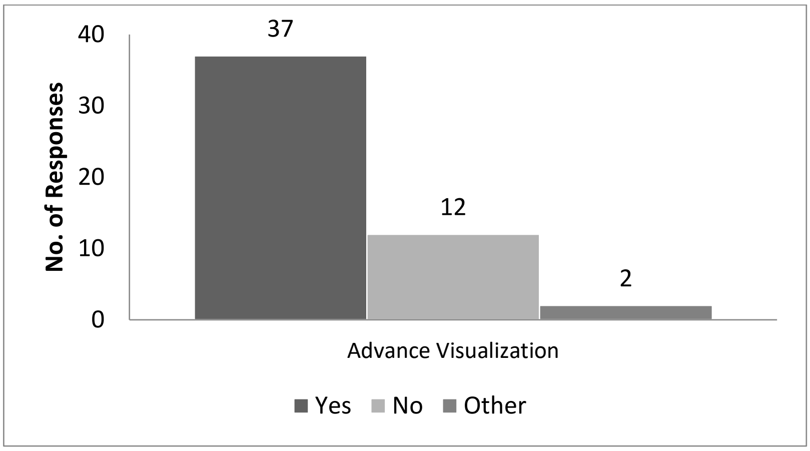
Question 4:

Availability and Performance management is the monitoring of availability, health and performance of network devices. Availability and performance management of the security devices and network equipment as an additional functionality with SIEM can be rated from 1 to 4 on: (1 being most critical to 4 being not required)



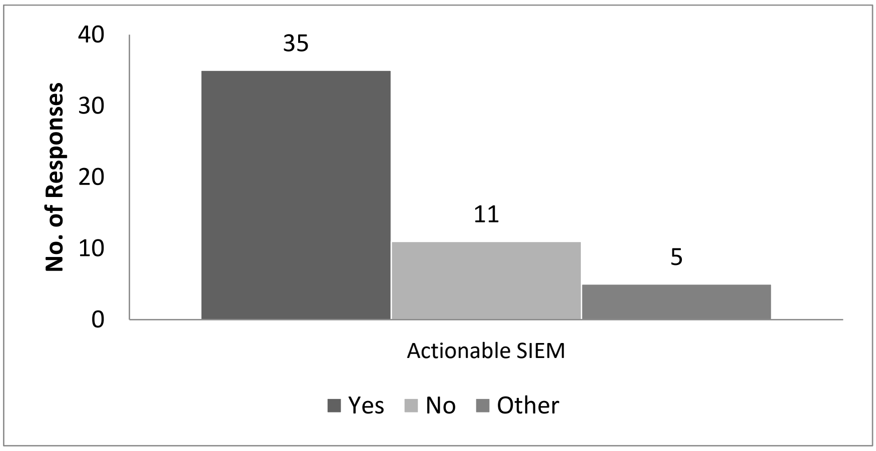
<u>Question 5:</u>

Visualization of events in real time helps in decision making. As an additional feature visualization should be rated from 1 to 4 as: (1 being most important to 4 being not required)



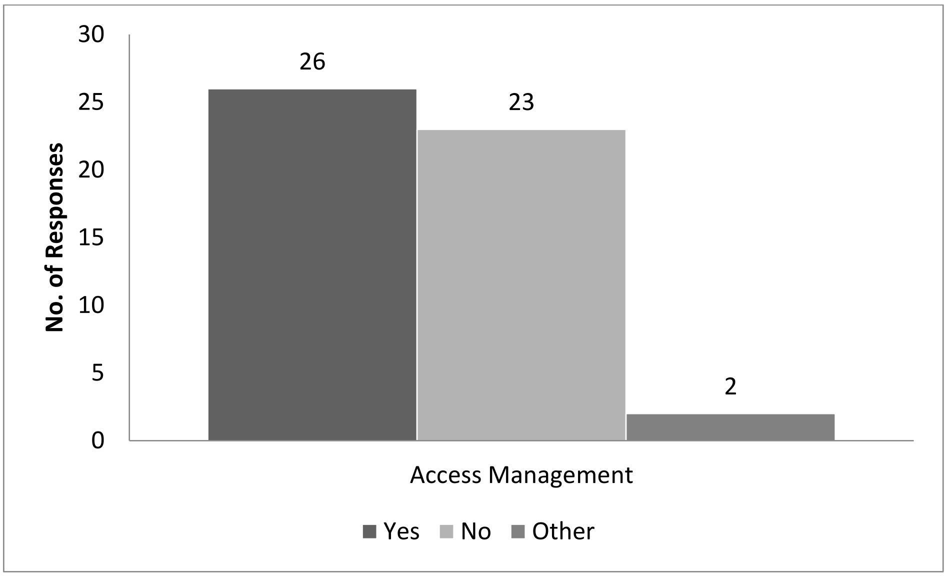
<u>Question 6:</u>

Counter measures associated with correlation rules are assumed to reduce the involvement of human resources and to speed up the actions. Should Remedial capabilities be included in SIEM along with other functionalities?



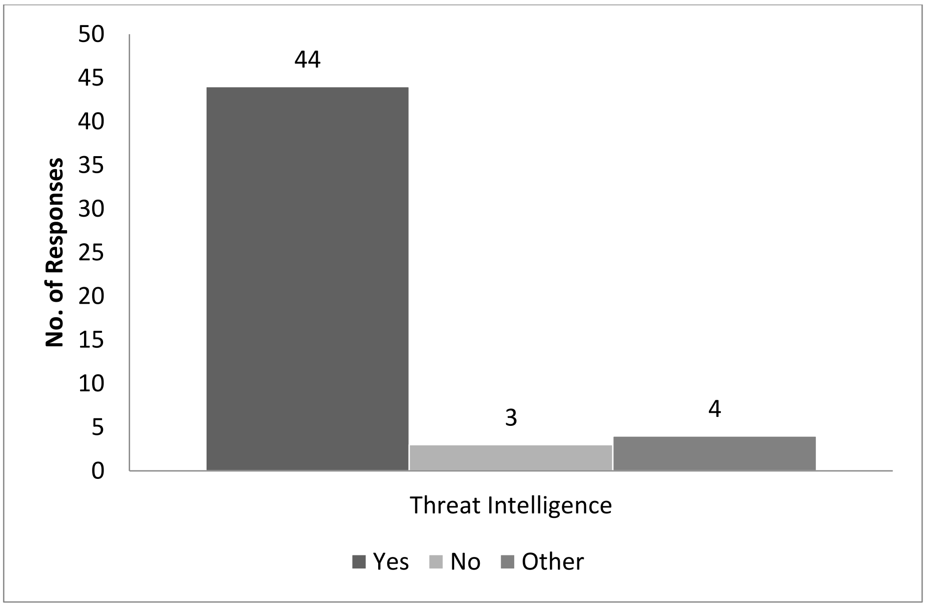
Question 7:

Access Management helps in only authorized access to resources and in recording individual activities. Rate Access Management as an additional functionality from 1 to 4: (1 being critical to 4 being not required)



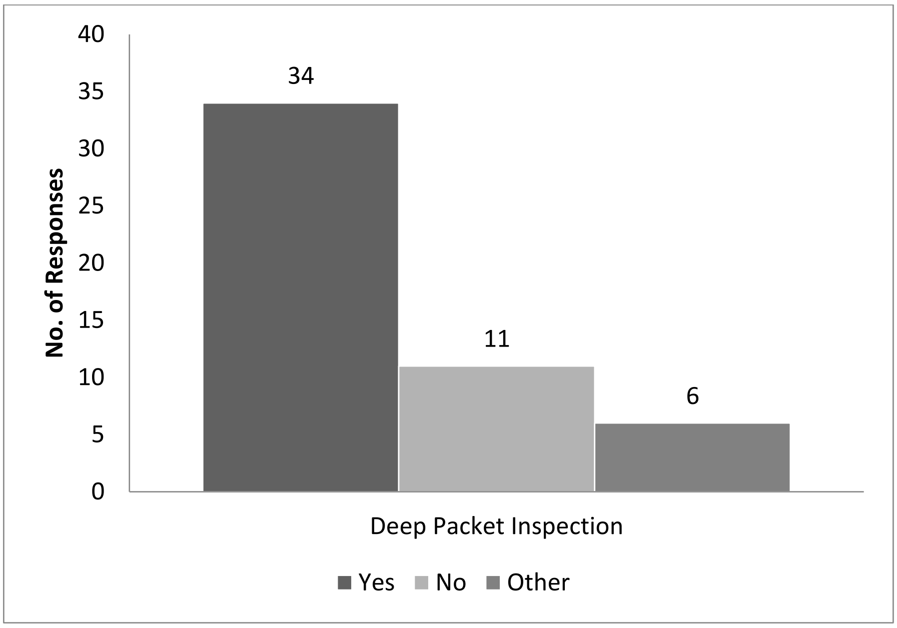
Question 8:

Threat intelligence helps in keeping the network secure by proactive intelligent decisions and early actions against attacks. Do you consider it to be included as an additional capability with SIEM?



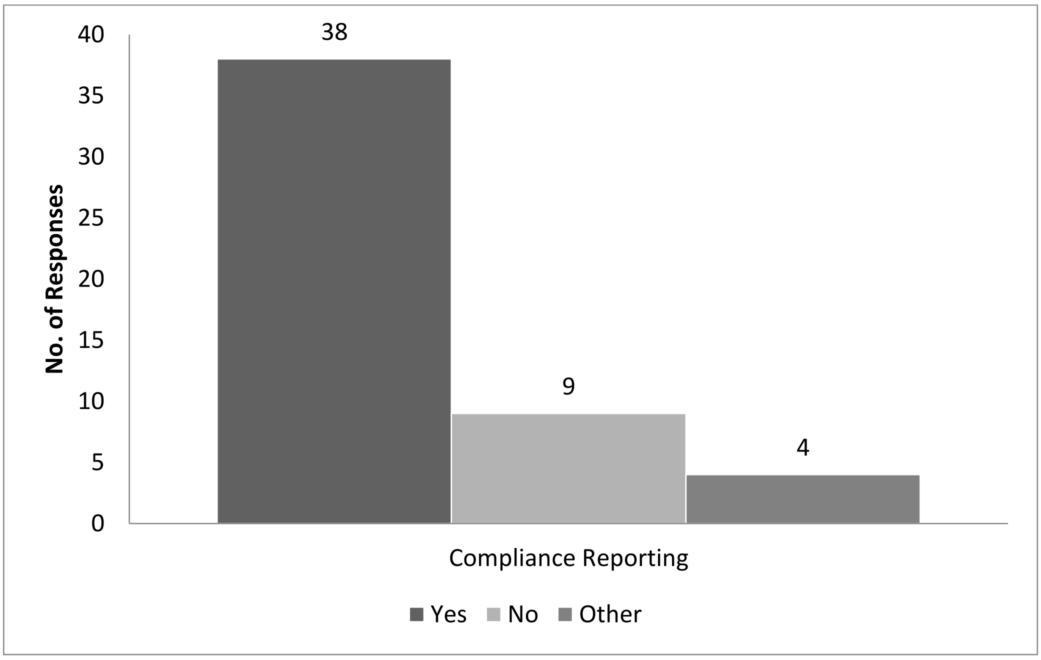
Question 9:

Along with basic correlation, Deep packet inspection and end point data capture is considered essential for real time monitoring. Do you think it should be included in SIEM?



Question 10:

Scheduled compliance reporting with various report formats can increase user satisfaction. Should it be included with basic compliance reporting in SIEM?



Conclusion

As more than 50 % of the respondents chose all the essential SIEM features so we conclude that they are must have attributes of SIEM. They include:

1) Automated Log Collection
2) Automated Log management (automated log formatting and normalization)
3) Automated Log Analysis (Based on correlation methods)
4) Log retention
5) Compliance reporting based on Logs
6) Real time monitoring of events
7) Incident Management
8) Forensic Analysis

Additional Functionalities along with essential attributes are required to keep the network secure and to increase the overall business value. According to the respondents rating:

1) 92.9% respondents consider Threat intelligence as the most important additional feature along with SIEM.
2) 74.1% respondents consider automated remedial actions as an important feature to reduce the human involvement, hence increasing the efficiency and reducing the error rate.
3) 67.9% of the IT security professionals consider Deep packet inspect and end point capture to be included as an advance probe for real time monitoring and proactive defense against attacks.
4) Also , same percentage (67.9%) of the respondents suggest advance compliance reporting formats to be included in SIEM to support auditing process and increasing user satisfaction.

5) 50% of the IT professionals consider advance visualization of the events to be a critical essential feature; other 25% consider being an important feature. Concluding from the responses, advance visualization dashboards should be included in SIEM.

Appendix "C" – Test case Execution Report

Introduction:

These test cases are designed to test OSSIM against cyber analytic use cases.

Environment:

The environment for testing OSSIM against the designed test cases includes three local PCs, a layer three switch having port mirroring enabled on it. OSSIM server is installed on another machine in the network. The network tab taken from the switch is dropped into one of the NICs of OSSIM. In the current environment, any communication between these three machines or between a machine from this network and the outside world is mirrored and sent to OSSIM. HIDS agents are installed on all three PCs. HIDS pushes system logs to OSSIM through management NIC. HIDS uses port 1514 UDP to push the logs to OSSIM. An attacking computer is placed outside the network and is used for creating defined attack scenarios.

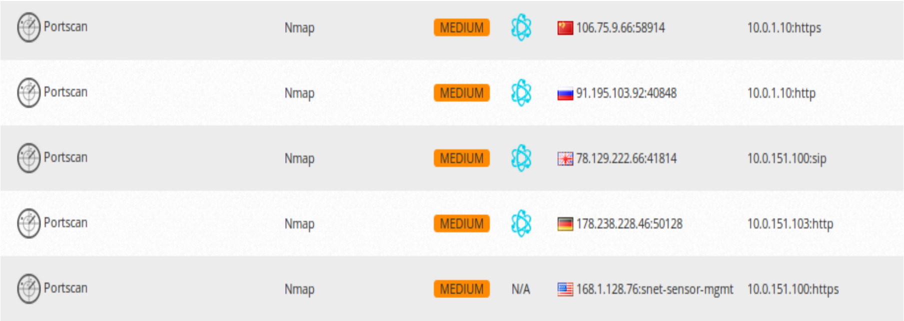
Test Case Execution:

Test case id	001
Test case name	Beacon Detection
Testcase Description	This test case is designed to check if OSSIM detects malware beaconing from internal network to a remote host. In this test case events and alarms will be observed under ANALYSIS tab.
Precondition	1. Alienvault Server is installed in the network 2. Network Tab is provided to the server 3. HIDS agent are installed 4. Zeus malware is installed on the system
Input state	Beacons are generated after every 10 mins for an external host
Validation	After 5 beacons, OSSIM server should detect malware presence on the basis of its behavior not on the basis of its signature.
Expected Output	An alarm should be generated under ANALYSIS TAB for presence of malware in the network
Output	OSSIM did not detect beacons based on its behavior.

Test case id	002
Test case name	Remote Administrator Sessions Detection
Test case Description	This test case is designed to check if OSSIM detects remote administrator sessions from geographically far apart location
Precondition	11. Alienvault Server is installed in the network 12. Network Tab is provided to the server 13. HIDS agent are installed
Input state	4. Remote desktop application (Team Viewer) is running on an internal host 5. A connection is established between a host in Pakistan and Australia 6. A file transfer was performed from within a network to the remote location.
Validation	OSSIM should detect remote desktop usage after successful connection establishment.
Expected Output	An alarm is generated under ANALYSIS TAB for remote desktop usage.
Output	No alarm was generated for remote desktop usage.

Test case id	003
Test case name	Data Exfiltration through HTTP
Test case Description	This test case is designed to check if OSSIM detects data exfiltration through HTTP(S) port.
Precondition	1. Alienvault Server is installed in the network 2. Network Tab is provided to the server 3. HIDS agent are installed
Input state	Data Upload of more than 100MB were performed through HTTP port of a remote server
Validation	OSSIM should detect Data Upload over 100MB
Expected Output	An alarm is generated under ANALYSIS TAB for data exfiltration

Output	No alarm was generated for data exfiltration

Test case id	004
Test case name	Detection of Port Scanners
Test case Description	This test case is designed to check if OSSIM detects port scans performs internally or externally.
Precondition	1. Alienvault Server is installed in the network 2. Network Tab is provided to the server 3. HIDS agent are installed
Input state	Port scan using Nmap is performed internally and externally both.
Validation	OSSIM should detect port scans
Expected Output	An alarm is generated under ANALYSIS TAB for Port scans
Output	OSSIM generates alarm under the tab ANALYSIS for internal port scans as well as external port scan.  Portscan Nmap MEDIUM 106.75.9.66:58914 10.0.1.10:https Portscan Nmap MEDIUM 91.195.103.92:40848 10.0.1.10:http Portscan Nmap MEDIUM 78.129.222.66:41814 10.0.151.100:sip Portscan Nmap MEDIUM 178.238.228.46:50128 10.0.151.103:http Portscan Nmap MEDIUM N/A 168.1.128.76:snet-sensor-mgmt 10.0.151.100:https

Test case id	005
Test case name	Detection of Protocol Abuse
Test case Description	This test case is designed to check if OSSIM detects protocol abuse.
Precondition	1. Alienvault Server is installed in the network 2. Network Tab is provided to the server 3. HIDS agent are installed
Input state	HTTP packet created using scapy sent over DNS port.

Validation	OSSIM should detect protocol abuse
Expected Output	An alarm should be generated under ANALYSIS TAB for Protocol abuse
Output	No alarm is generated for protocol abuse.

Test case id	006
Test case name	Detecting Relay
Test case Description	This test case is designed to check if OSSIM detects relay or path attackers takes in a network.
Precondition	4. Alienvault Server is installed in the network 5. Network Tab is provided to the server 6. HIDS agent are installed
Input state	Making a master-salve malware zombie and make them communicate with Command and Control server.
Validation	OSSIM should detect Relays
Expected Output	An alarm should be generated under ANALYSIS TAB for demonstrating the path malware took.
Output	No alarm is generated for relay existence.

Test case id	007
Test case name	RDP Keyboard Layout
Test case Description	This test case is designed to check if OSSIM detects the change of remote desktop keyboard layout than the one used by organization.
Precondition	4. Alienvault Server is installed in the network 5. Network Tab is provided to the server 6. HIDS agent are installed
Input state	Using Chinese keyboard to connect to the network
Validation	OSSIM should detect difference in Keyboard layout
Expected Output	An alarm should be generated under ANALYSIS TAB for different keyboard usage.

Output	No alarm is generated for different key board layout

Test case id	008
Test case name	Detecting RATs
Test case Description	This test case is designed to check if OSSIM detects usage of RATs
Precondition	4. Alienvault Server is installed in the network 5. Network Tab is provided to the server 6. HIDS agent are installed
Input state	Luminosity Link is used for remote administration.
Validation	OSSIM should detect the presence of RATs
Expected Output	An alarm should be generated under ANALYSIS TAB for detection of RATs.
Output	No alarm is generated for RATs.

Test case id	009
Test case name	Detecting Communication of an IP with other IPs
Test case Description	This test case is designed to check if OSSIM analyze the communication of specific IPs and drawing a map between them.
Precondition	4. Alienvault Server is installed in the network 5. Network Tab is provided to the server 6. HIDS agent are installed
Input state	Exploring the features of OSSIM to check if it supports the feature of building communication map of specific IPs.
Validation	OSSIM should draw maps of specific IPs

Expected Output	Given two input IPs OSSIM should draw map of their communication highlighting the common areas of communication.
Output	OSSIM does not support this feature.

Test case id	010
Test case name	Detecting Unknown Service
Test case Description	This test case is designed to check if OSSIM detects the use of unknown service on open ports.
Precondition	4. Alienvault Server is installed in the network 5. Network Tab is provided to the server 6. HIDS agent are installed
Input state	Sending raw packets over port 80 used for HTTP communication
Validation	OSSIM should detect usage of unknown service
Expected Output	An alarm should be generated under ANALYSIS TAB for detection of RATs.
Output	No alarm is generated for unknown service usage.

Result:

1 out of 10 test cases ended up with the pass criteria. OSSIM works on signature databases for network and host intrusion detection. It does not use behavioral analysis for detecting host intrusions as well as network intrusions. The reason most of the test cases ended up with the fail criteria. Thus highlighting the limitation of SIEM in detection of advance cyber-attacks for which signatures are not build yet.

BIBLIOGRAPHY

[1] “30m internet users in Pakistan, half on mobile: Report - The Express Tribune”, *The Express Tribune*, 2017. [Online]. Available: http://tribune.com.pk/story/567649/30m-internet-users-in-pakistan-half-on-mobilereport/. [Accessed: 15- Jan- 2016].

[2] Verizon, “2014 Data Breach investigations Report”, 2014.

[3] XIPHOS RESEARCH, 'A Sony Story: An Examination of the SPE Breach 18th December 2014', 2014.

[4] Frost & Sullivan, “The 2013 (ISC) 2 Global Information Security Workforce Study,” 2013.

[5] Bhatt, Parth, Edgar Toshiro Yano, and Per Gustavsson. “Towards a framework to detect multi-stage advanced persistent threats attacks.” *Service Oriented System Engineering (SOSE), 2014 IEEE 8th International Symposium on*. IEEE, 2014.

[6] K. Kavanagh and O. Rochford, “Magic Quadrant for Security Information and Event Management”, *Gartner.com*, 2015.

[7] S. Khandelwal, "Massive DDoS Attack against Dyn DNS Service Knocks Popular Sites Offline", *The Hacker News*, 2017. [Online]. Available: http://thehackernews.com/2016/10/dyn-dns-ddos.html. [Accessed: 15- Sept- 2016].

[8] I. Katharina Krombholz, Heidelinde Hobel, Markus Huber and Edgar Weippl, “Advanced Social Engineering Attacks”. SBA Research, Favoritenstraße 16, AT-1040 Vienna, Austria

[9] Khan, Ahmad Alamgir. "Preventing phishing attacks using one time password and user machine identification." *arXiv preprint arXiv: 1305.2704* (2013).

[10] D. Gritzalis N. Virvilis, "The Big Four-What we did wrong in Advanced Persistent Threat detection in Availability, Reliability and Security (ARES)," , 2013.

[11] “SQL Injection”, *Msdn.microsoft.com*, 2017. [Online]. Available:https://msdn.microsoft.com/en-us/library/ms161953(SQL.105).aspx. [Accessed: 15- Dec- 2016].

[12] M.R. Endsley, “Designing for situation awareness in complex systems”. 2001.

[13] M. R. Endsley, “Toward a Theory of Situation Awareness in Dynamic Systems”, Human *Factors Journal,* ***Vol. 37, No. 1, pp. 32****-64, 1995.*

[14] B. McGuinness and L. Foy, “A Subjective Measure of SA: The Crew Awareness Rating Scale (CARS)”, *Proc. of the First Human Performance, Situation Awareness, and Automation Conference,* Savannah, Georgia, 2000.

[15] R. Bejtlich, “*The Practice of Network Security Monitoring: Understanding Incident Detection and Response”*, 1st ed. No Starch Press, 2013.

[16] W. Yurcik, “Visualizing netflows for security at line speed: the SIFT tool suit,” in *Proc. of 19th Usenix Large Installation System Administration Conference (LISA),* San Diego, 2005, pp.169-176.

[17] Kiran Lakkaraju, William Yurcik, Adam J. Lee, “NVisionIP: netflow visualizations of system state for security situational assessment”, *In Proceedings of the ACM workshop on Visualization and data mining for computer security,* 2004.

[18] A. Jakalan, “Network Security Situation Awareness”, *The International Journal of Computer Science and Communication Security (IJCSCS) 01/2013; 3:61-67.,* 2013.

[19] Xiaoxin Yin, William Yurcik, Adam Slagell, “The Design of VisFlowConnect-IP: A Link Analysis System for IP Security Situational Assessment”, *In Proceedings of the Third IEEE International Workshop on Information Assurance,* 2005.

[20] X. Liu, H. Wang, J. Lai and Y. Liang, “Network Security Situational Awareness Model Based on Heterogeneous Multisensor Data Fusion”, *IEEE, 1-4244-1364, 2007.*

[21] R. Xi, S. Jin, X. Yun and Y. Zhang, “CNSSA: A Comprehensive Network Security Situation Awareness System”, in *2011 International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11,* 2011.

[22] CERT/NetSA at Carnegie Mellon University, “SiLK (System for Internet-Level Knowledge),” [Online]. Available: http://tools.netsa.cert.org/silk

[23] M. Thomas, L. Metcalf, J. Spring, P. Krystosek and K. Prevost, “SiLK: A Tool Suite for Unsampled Network Flow Analysis at Scale”, in *2014 IEEE International Congress on Big Data,* 2014.

[24] C. Onwubiko, “Functional Requirements of Situational Awareness in Computer Network Security”, in *IEEE Intelligence and Security Informatics 2009,* USA, 2009.

[25] Rahma, Azizah Abdul, and Rose Alinda Alias. “Situational Awareness needs for system interaction design.” *Industrial Engineering and Engineering Management (IEEM), 2011 IEEE International Conference on*. IEEE, 2011.

[26] “Prads”, *Gamelinux.github.io,* 2017. [Online].
Available: https://gamelinux.github.io/prads/. [Accessed: 15- Jan- 2016].

[27] “Nmap: the Network Mapper - Free Security Scanner”, Nmap.org, 2017. [Online]. Available: https://nmap.org/. [Accessed: 15- Jan- 2016].

[28] “Home — OSSEC”, *Ossec.github.io*. [Online]. Available: http://ossec.github.io/. [Accessed: 15- Jan- 2016].

[29] “Snort - Network Intrusion Detection & Prevention System”, *Snort.org,* 2017. [Online]. Available: https://www.snort.org/. [Accessed: 15- Jan- 2017].

[30] Nicolett, M., and K. M. Kavanagh. “Critical capabilities for security information and event management.” *Gartner RAS Core Research Note G* (2012): 212420.

[31] Dempsey, K., Chawla, N., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., Scholl, M., & Stine, K. “Information security continuous monitoring (ISCM) for federal information systems and organizations.” *(NIST SP800–137). Gaithersburg, MD: National Institute of Standards and Technology*.

[32] S. Bhatt, P. Manadhata and L. Zomlot, "The operational role of Security Information and Event Management Systems", in *IEEE Symposium on Security and Privacy*, 2014.

[33] Schultz, E. (2009). “Security information and event management (SIEM) technology.” in H.F. Tipton & M. Krause (Eds.), *Information Security Management Handbook*, Sixth Edition, Volume 3. New York: Isc2 Press.

[34] K. Kavanagh and O. Rochford, “Magic Quadrant for Security Information and Event Management”, *Gartner.com*, 2015.

[35] “The SIEM Evaluator's Guide”, *alienvault*. [Online]. Available: www.alienvault.com/docs/guides/The-SIEM-Evaluators-Guide.pdf. [Accessed: 19- Apr- 2016].

[36] “SIEM Security Information and Event Management – AccelOps”, *Accelops*. [Online]. Available: www.accelops.com/products/security-monitoring-siem/.

[37] “SPLUNK Software as a SIEM”, *Splunk*. [Online]. Available: www.splunk.com/content/dam/splunk2/pdfs/technical-briefs/splunk-as-a-siem-tech-brief.pdf. [Accessed: 19- Apr- 2016].

[38] “SIEM, Security Information Event Management, ArcSight | Hewlett Packard Enterprise”, *Hp*, 2016. [Online]. Available: www8.hp.com/us/en/software-solutions/siem-security-information-event-management/. [Accessed: 19- Apr- 2016].

[39] “File Integrity Monitoring”, *Logrhythm*, 2016. [Online]. Available: logrhythm.com/solutions/security/file-integrity-monitoring/. [Accessed: 19- Apr- 2016].

[40] “SIEM and IAM Technology Integration”, *NetIQ*, 2009.

[41] “How to Use Threat Intelligence with Your SIEM?”, *Gartner*, 2014.

[42] SANS Institute, “Killing Advanced Threats in Their Tracks: An Intelligent Approach to Attack Prevention.” [Online]. [Available].www.sans.org/reading-room/whitepapers/analyst/killing-advanced-threats-tracks-intelligent-approach-attack-prevention-35302

[43] “Scapy” [Online]. [Available]. www.secdev.org/projects/scapy/doc/usage.html#interactive-tutorial

[44] “DET” [Online]. [Available]. github.com/sensepost/DET