International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Addressing Security Issues of Small and Medium Enterprises through Enhanced SIEM Technology

Prateek Shivhare[1], Savaridassan .P[2]

SRM University, Chennai, India

Abstract: ***Today's information security threats are increasing in numbers and severity but diversity of network and information technology is increasing exponentially. So it is a challenge for small and medium enterprises, those who cannot give more importance to security because of their capital investment. This Paper actually focuses on an efficient approach to address security issue with small and medium enterprises. All business faces the same challenges like keeping costs down to maintain your competitive edge presses. So these enterprises cannot spend much resource and capital on security. As a solution open source SIEM will provide an enhance and complete security solution.***

Keywords: SIEM, OSSIM, Security, Open Source, Enterprise

1. Introduction

The Security Information and Event Management (SIEM) system is new to information technology (IT). The SIEM system is a complex gathering of advancements intended to give vision and clarity on the corporate IT System as a whole, benefitting security experts and IT administrators as well. Security experts and investigators utilize the SIEM system to monitor, identify, document, and sometimes respond to security affronts. The art and science of implementing Security Information and Event Management on any network requires a number of moving pieces. Perhaps those of responsible for the security of small and medium-size business have already reached the conclusion that SIEM is beyond grasp. But these industries can use open source SIEM so they can save their capital and resources. It is essential to be able to detect attacks in a timely manner and implement the relative countermeasures, following appropriate procedures to respond to incidents, thus minimizing the effects and the damages they can cause. In order to detect intrusions and attacks, system administrators and information security analysts make use of tools, such as IDS/IPS (Intrusion Detection/Prevention System) and analysis of logs (event records) of servers and network devices, looking for any significant events from a security point of view. A network of an organization of average size produces, as a whole, such a quantity of logs that it is very difficult (and still very expensive) to check them all, one by one, to obtain meaningful information. A further difficulty is that there is no single standard used to record the logs and often, depending on the type and size, they are not immediate or easy to understand. It is even more difficult to relate other logs produced by many different systems to each other manually, to highlight anomalies in the network that would not be detectable by analyzing the logs of each machine separately. SIEM (Security Information and Event Management) software, therefore, is not limited to being a centralized solution for log management, but also (and especially) it has the ability to standardize logs in a single format, analyze the recorded events, highlight the most important information and relate the logs to each other (correlation), allowing analysts to detect anomalies and attacks more easily.

2. Information Security Challenge for Small and Medium Enterprises

The growing complexity of information systems combined with their regulatory compliance issues, public-network connections and competitive necessity presents even large enterprises with significant challenges managing information security. For the small and medium enterprise it can seem impossible to truly get control of the security and availability of the systems you need to stay ahead in business.

Emerging at the same time as these challenges are potential solutions to them. Security Information and Event Management (SIEM) systems have matured considerably over the past decade and are beginning to offer solutions fit for the small and medium enterprise. AlienVault SIEM technology is deployed at more than half of all SIEM installations worldwide. SIEM solutions aim to simplify security operations and compliance reporting by integrating all of the functions of individual security products into a single platform. While all SIEM solutions integrate with existing security and network devices.

3. How SIEM can be helpful

Every business faces the same challenges like keeping costs down to maintain your competitive edge presses on one side while managing an effective information system and compliance risk presses on the other. For smaller businesses without the economies of scale of global multinationals, the choice is often between spending more than you can afford for something you cannot be sure will be worth it or muddling along bearing more uncertainties than you would choose.

A SIEM solution that a small business could afford to deploy and that did not require extensive and expensive customization could do a lot to centralize and summarize the security and compliance concerns of small and medium enterprises.

4. A Solution with Open Source SIEM (OSSIM)

OSSIM is a free, Open Source version of AlienVault's Professional SIEM. While OSSIM does not include some of the scalability, performance, Managed Security Service Provider (MSSP) features, forensic logging. It still provides a fully functional SIEM and all the security tools integrated with the AlienVault Professional SIEM.

5. Overview of an OSSIM: An Open-Source SIEM Solution

OSSIM is a SIEM software platform, free and open-source developed by AlienVault and based on a Debian 64-bit Linux distribution. OSSIM has four major components:

1. Sensor
2. Server
3. Framework
4. Database

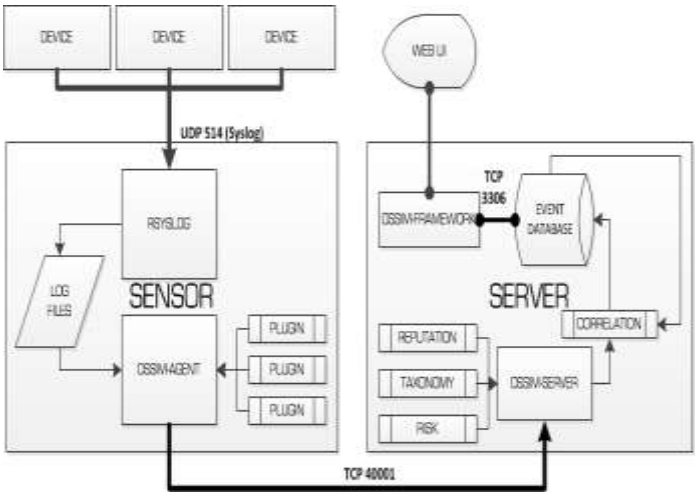

Figure 1: OSSIM Architecture

You can install these components on a single physical machine (the default installation), on a single virtual machine, on different virtual machines and/or physical machines, depending on the size and configuration of the network to monitor. For a relatively small network, installation on a single machine, which is the simplest configuration, may be the right solution. For larger networks, it is advisable to install the Sensor and the Database separately. Figure 1 shows the OSSIM architecture.

Sensor: The Sensor has two main components:

1. The syslog service, which listens on TCP/UDP port 514, receives the logs from network devices and stores them locally, according to the configuration.
2. The OSSIM-agent, using a series of modules called plugins, one for each type of log, performs log analysis and normalization, and sends that to the Server component. Plugins are of two types: detectors, which detect anomalies and possible attacks (such as Snort, P0f, Arpwatch), and monitors to monitor the network status (like Ntop and Nagios).

Server: The Server performs the essential SIEM functions: aggregation, risk assessment and correlation of events that are received from the sensor through TCP port 40001. The server also sends the information concerning the events to the Database for storage.

Framework: The Framework connects and manages the OSSIM components and security tools included, and it provides the system administration Web interface. It is the component that needs the least hardware resources and is usually installed together with the Server component.

Database: The database is a MySQL server instance that stores event and system configuration data.

6. Functionality

OSSIM is more than the sum of all its parts; a synergy is created by the way AlienVault have laced the tools together. The following diagram shows how all the tools work together (from the lowest to the highest level).

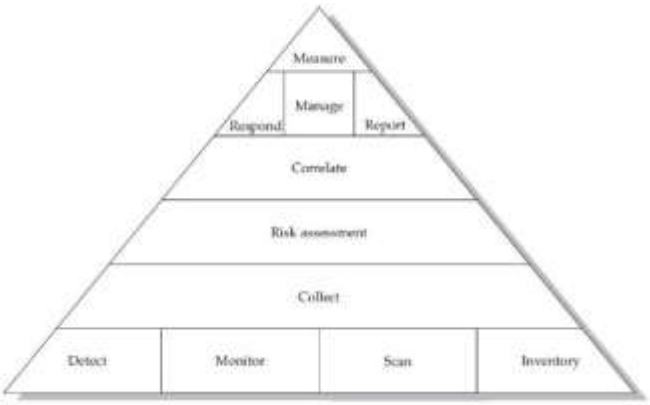

Figure 2: Functionality

Detect
AlienVault defines a detector as any program that listens on the network, monitors files or logs looking for signs of attacks, and issues alerts accordingly. There are basically two types of detectors: pattern based (signature) and anomaly based.

Pattern-based (Signature) Detectors Pattern-based detectors use a signature of known bad behavior and alert when activity matches that signature. Most of the security devices in place today are pattern-based (or signature-based).

Anomaly-based Detectors Anomaly-based detectors have a baseline of known good behavior and alert on anomalies or deviations from that baseline. Anomaly-based detectors are the only types of detector that can identify zero-day (or previously unknown) attacks. Anomaly-based detectors offer a strong complement to pattern based detectors.

Monitor
OSSIM uses monitors to provide perspective on network traffic and quickly find changes in the network. Along with detectors, OSSIM uses monitors for correlation.

Scan
Network vulnerability scans are critical to the correlation process. These scans attempt to simulate attacks and determine if a network device is vulnerable to a particular attack.

Inventory
OSSIM employs multiple agent-based and agent-less tools to provide automated asset inventory collection. Then it can manually insert or adjust the information on the server.

Collect
The purpose of the collection infrastructure is to capture and normalize all disparate security device information and provide it to the server for further processing. This function is very important because of the varying data formats used by security device vendors. After the data has been collected and normalized, it can be used in conjunction with other data from other sources, now in the same format, to discover potentially malicious traffic emanating on your network.

Risk Assessment
Risk assessment is the process of measuring risk and attempting to determine what is important and what is not. This risk assessment is meant to be an aide to the decision making process. OSSIM calculates a risk parameter for each event.

Correlate
The most important aspect of any SIEM tool is the correlation engine. The job of the correlation engine is to reduce false positives (false alarms) and prevent false negatives (where intrusions go unnoticed).

Respond
OSSIM is capable of responding automatically to a given event or set of events. Responses include sending an email or sending a network change directive, such as adjusting a firewall or switch configuration. It should be stated that this type of activity should be well thought-out and poses a risk to network operations. That said, OSSIM offers tools to help you do this if you need to.

Manage
Once an attack is detected, collected, assessed for risk, correlated, and validated by the analyst as real, a ticket may be generated to track the incident through resolution. Tickets may be generated from several places: Alarm Panel, Forensic Console, and the Risk Dashboards. Each ticket contains information about the owner of the incident, the events contained in the incident, the current status of the incident, and history of the incident. The ticket is stored in a database that can be searched for trending analysis and reports can be drawn from that data.

Report
From time to time, an analyst will need to produce reports for analysis or management. OSSIM contains a robust report engine with many canned reports and the ability to customize and create reports for specific purposes.

Measure
Dashboards are provided to visually present data in a manner that is easy to digest. Again, OSSIM comes with standard dashboards, and you have the ability to create your own. Existing dashboards include Executive views, Compliance views, Map views, and Network Diagram views, to mention a few. Each analyst can select and work with the dashboards that allow him or her to complete required tasks more efficiently.

7. Conclusions

The complexities of securing small and medium sized businesses added with the maze of regulatory compliance places a heavy burden on those who are charged with building and operating these networks.

SIEM solutions promise to bring integration among the complexity but often introduce too much cost for too little value for SME organizations today. So this Organization can go for open source SIEM.

8. Future Work

OSSIM is a viable open-source SIEM solution and a free alternative to other commercial SIEM products. But since it is an open source few feature may not be present. So when an enterprise wants to upgrade their SIEM they can go for AlienVault USM (Unified Security Management) and other commercial SIEM. Commercial SIEM have some features like scalability, performance, Managed Security Service Provider (MSSP) features, forensic logging. Which are not present in open source. So for enhance result enterprise can use commercial SIEM.

References

[1] Igor Kotenko, Andrey Chechulin, Common Framework for Attack Modeling and Security Evaluation in SIEM Systems, Green Computing and Communications (GreenCom), 2012 IEEE International Conference, November 2012, pp. 94-101
[2] OSSIM: a Careful, Free and Always Available Guardian for Your Network, page no68-83 / JUNE 2014 / LINUXJOURNAL
[3] Network Pro Library: David Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask Security Information and Event Management (SIEM) Implementation (Network Pro Library) 2010
[4] AlienVault_Industry_Whitepaper_SME from AlienVault website.

Author Profile

[1]**Prateek Shivhare** is an M.Tech Student in SRM University. His Specialization is Information Security and Cyber Forensics.

[2]**Savaridassan .P** is an Asst. Professor in department of Information Technology at SRM University. His area of interest is Secure Coding.