Realtime Information Monitoring System

Swati Chavan
Bachelor of Engineering in Computer
JSPM NTC
Pune, India

Saili Pharate
Bachelor of Engineering in Computer
JSPM NTC
Pune, India

Gayatri deochake
Bachelor of Engineering in Computer
JSPM NTC
Pune, India

Pallavi Joshi
Bachelor of Engineering in Computer
JSPM NTC
Pune, India

Prof. Nilesh Khochare
Professor in JSPM
JSPM NTC
Pune, India

Prof. R. H Kulkarni
Professor in JSPM
JSPM NTC
Pune, India

***Abstract*—Security is one of the major issues of Information Systems. Our system relies on integration of software and hardware. It provides real times analysis of security alerts generated by network hardware and application for restricted area.**

Keywords— Information Security, Asset, Sensor, SIEM, OSSIM

I. INTRODUCTION

The growing connectivity of computers through the internet, the increasing extensibility of system and complexity of system has made software security a bigger problem now than the past. SIEM (Security Information and Event Management) system provides capability and should be obtained in order to maximize efforts in detecting today's advanced threats. This allows to indicate timely reaction for administrator in order to monitor communication and working of network to make the system information secure.

The SIEM system focuses on corporate IT world, and is advantageous to security experts and IT administrators. It is essential to be able to detect attacks and unwanted interruptions in timely manner and implement a way to notify in order to convey about the incidents, thus, the effects of attacks and threats to the network system may be reduced.

Computer security is mostly used for controlling how data are shared for reading and modifying. Three terms on which security is based: confidentiality, integrity, Availability. Unauthorized users cannot access to data or information is called confidentiality. Integrity assures that information is not modified without authorized person. The information is accessible to authorized person when required; this is nothing but Authorization and availability.

II. LITERATURE REVIEW

There are many tools and Operating systems that are mainly introduced for security of information available on the network.

Sr. No	Tools	Description
1	QRadar	Ease of extracting information from raw logs and events. There are some Improvements for Qradar like: To allow restriction on who can close alerts. Restrictions on easily updating alerts with reading text templates. There are some Stability Issues also.
2	**Splunk**	It comes in both paid and free form of a tool. Free version of Splunk have maximum indexing volume Per day is 500 MB. Cost of Paid version of splunk is $1000 per month
3	**Solar Winds**	It allows 30 nodes in a network. Its Cost $4495 for 30 nodes with Validity of 30 days.
4	**Alien Vault**	Open Source SIEM Tool. All in one platform designed and priced to ensure that mid-market organizations can effectively defend themselves against threats. It uses one of the best features of splunk of data collection capabilities with its expertise on threat detection. As from above all the tools and OS Alien Vault is most secured, so it's mainly used for the security purpose because Alien Vault covers all the drawbacks of previous system.

First, confirm that you have the correct template for your paper size. This template has been tailored for output on the A4 paper size. If you are using US letter-sized paper, please close this file and download the file "MSW_USltr_format".

III. PROBLEM STATEMENT

In existing system, the aim to collect security events, analyze them, assess the risk they bring and inform the administration. This system is based on open source toolset. The OSSIM system seems to satisfy basic needs and requirements of SIEM class system for rather small organization.

Security is one of the major issues of Information. SIEM system provides capability and should be obtained in order to maximize efforts in detecting today's advanced threats.

IV. System Architecture

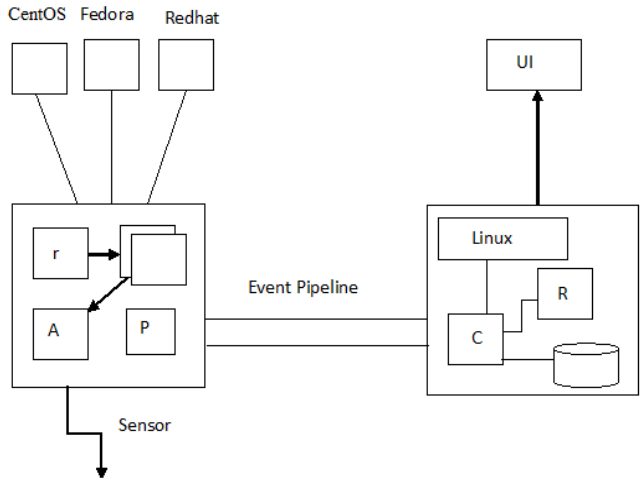

Fig. 1. System architecture.

- Assets: In our system Redhat, fedora, centos are assets. Assets mean nothing but the client.
- r: rsyslog present in OSSIM. Logs pooled from assets in one file.
- A: Agent is created in OSSIM server as per asset present.
- P: Plugins gathered from assets.
- Event Pipeline: Event is passed to server through pipeline.
- C: correlation engine is doing the job of classification and management of logs.
- R: Necessary risk factor is decided as per risk assigned to it.
- UI: Web server is getting parsed and processed event details in UI forms like chart, graph and tables.

V. Future Scope and Conclusion

This system tends to provide security using an SIEM tool that is named as Alien vault. The main objective of the system is to provide security even in the absence of administrator, which means, availability of administrator all the time is not mandatory. This project mainly focuses on both internal as well as external security by means of a fire alarm and IP Camera. Detecting threats with the help of elements like IP Camera and fire alarm is one of the major tasks. This will reduce the requirement of having the administrator to monitor the system all the time and will also alarm the administrator in case of some external threat.

References

[1] Juan Manuel Madrid; Luis Eduardo Múnera; Carlos Andrey Montoya ;Juan David Osorio ,"Functionality, reliability and adaptability improvements to the OSSIM Information Security Console", ICT Department Universidad Icesi Cali, Colombia.

[2] Damian Hermanowski, "Open Source Security Information Management System Supporting IT Security Audit", C4I Systems Department, Military Communication Institute. 05-130 Zegrze, Poland.

[3] Filip Holik; Josef Horalek; Sona Neradova; Stanislav Zitta;Ondrej Marik" The deployment of security information and event management in cloud infrastructure", Faculty of electrical engineering and informatics ,University of Pardubice, Czech Republic.

[4] M.M.Anwar;M.F. Zafar; Z. Ahmed,"A Proposed Preventive Information Security System", Informatics Complex(ICCC),H-8/1, Islamabad.

[5] "Threat Intelligence Sharing &the Government's Role in It", www.AlienVault.com or follow us on Twitter (@AlienVault).

[6] Jim Beechey,beechey@northwood.edu "SIEM Based Intrusion Detection with Q1Labs Qradar " 2010 The SANS Institute.

[7] "Enhancing Security and Trustworthiness with Next-Generation Security Information and Event Management" white-paper from web.