Using Event Management Systems to Block Attacks on Networks

Albarghathi Mohammed Adrees Abdullah,
Oleksandr Fediushyn

Department of Information Technologies Security, Kharkiv National University of Radio Electronics, UKRAINE, Kharkiv, pr.Nauki,14,
E-mail: mohamed.albarghati@gmail.com, oleksandr.fediushyn@nure.ua

Annotation – A comparative analysis of the characteristics of modern event management systems to block attacks on networks was performed. The comparison this system was performed on the following indicators: monitoring and audit level, response type, adaptive capacity, architecture, detection method supported for platform deployment, principle of construction, method of extending functionality.

Keywords – security information and event management, network security, log management, IDS.

I. Introduction

The Internet is a large network that connects people around the world. Companies have networks that connect their employees to each other, and some people have networks in their homes that connect them to family members.

But like all things, there are threats that can affect networks; threats that could potentially cause service interruption, or harm. Because of this, it is important to protect them against those types of eventualities. One solution is to implement network security, and to perform a network security audit on a regular basis.

Network security is the collection of hardware and software tools that protect a company's network infrastructure. They are intended to address a number of possible threats that include:

Unauthorized Access - any user trying to gain access without the proper credentials. For example, a malicious user logging in from the outside.

Malicious Use - any user trying to perform something they shouldn't. For example, a user trying to delete important information.

Faults - any piece of software or device that fails in some way. For example, a printer that runs out of toner.

Tampering - any action that changes a piece of software or a device such that it behaves differently than it should. For example, changing the configuration of a secured door so that it can be opened without a key or credentials.

Destruction - any fault that is created in a willful fashion. For example, breaking a mouse or keyboard.

Disclosure - revealing important information. For example, letting intellectual property fall into a competitor's hands.

Network security is achieved by various tools including firewalls and proxy servers, encryption, logical security and access controls, anti-virus software, and auditing systems such as log management.

II. Problem analysis

As more businesses operate online, it's increasingly important to incorporate cybersecurity tools and threat detection to prevent downtime. Unfortunately, many unscrupulous cyber attackers are active on the web, just waiting to strike vulnerable systems. Security Information and Event Management (SIEM) products have become a core part of identifying and addressing cyber attacks.

SIEM stands for Security Information and Event Management. A SIEM [2-4] system provides real-time analysis of security alerts generated by applications and network hardware.

This term is somewhat of an umbrella for security software packages ranging from Log Management Systems to Security Log / Event Management, Security Information Management, and Security Event correlation. While a SIEM system isn't foolproof, it's one of the key indicators that an organization has a clearly defined cybersecurity policy. Nine times out of ten, cyber attacks don't have any clear tells on a surface level. To detect threats, it's more effective to use the log files. The superior log management capabilities of SIEMs have made them a central hub of network transparency.

Most security programs operate on a micro scale, addressing smaller threats but missing the bigger picture of cyber threats. An Intrusion Detection System (IDS) alone can seldom do more than monitor packets and IP addresses. Likewise, your service logs only show user sessions and configuration changes. SIEM puts these systems and others like it together to provide a complete overview of any security incident through real-time monitoring and the analysis of event logs.

Security information management (SIM) is the collection, monitoring and analysis of security-related data from computer logs. Also referred to as log management.

Security event management (SEM) is the practice of network event management including real-time threat analysis, visualization and incident response.

III. Solve a problem

SIEM's basic capabilities are as follows:

- Log Collection;
- Normalization – collecting logs and normalizing them into a standard format).
- Notifications and Alerts – notifying the user when security threats are identified
- Security Incident Detection.

Threat response workflow – workflow for handling past security events SIEM records data from across a users' internal network of tools and identifies potential issues and attacks. The system operates under a statistical model to analyze log entries. SIEM distributes collection agents and recalls data from the network, devices, servers, and firewalls. All this information is then passed to a management console where it can be analyzed to address emerging threats. It's not uncommon for advanced SIEM systems to use automated responses, entity behavior analytics and security orchestration. This ensures that

vulnerabilities between cybersecurity tools can be monitored and addressed by SIEM technology.

Once the necessary information reaches the management console, it is then viewed by a data analyst who can provide feedback on the overall process. This is important because feedback helps to educate the SIEM system in terms of machine learning and increasing its familiarity with the surrounding environment.

Once the SIEM software system identifies a threat, it then communicates with other security systems on the device to stop the unwanted activity. The collaborative nature of SIEM systems makes them a popular enterprise-scale solution. However, the rise of pervasive cyber threats has made many small- and mid-sized businesses consider the merits of a SIEM system as well.

SIEM has become a core security component of modern organizations. The main reason is that every user or tracker leaves behind a virtual trail in a network's log data. SIEM systems are designed to use this log data in order to generate insight into past attacks and events. A SIEM system not only identifies that an attack has happened, but allows you to see how and why it happened as well.

As organizations update and upscale to increasingly complex IT infrastructures, SIEM has become even more important in recent years. Contrary to popular belief, firewalls and antivirus packages are not enough to protect a network in its entirety. Zero-day attacks can still penetrate a system's defenses even with these security measures in place.

SIEM addresses this problem by detecting attack activity and assessing it against past behavior on the network. A SIEM system has the ability to distinguish between legitimate use and a malicious attack. This helps to increase a system's incident protection and avoid damage to systems and virtual property.

The use of SIEM also helps companies to comply with a variety of industry cyber management regulations. Log management is the industry standard method of auditing activity on an IT network. SIEM systems provide the best way to meet this regulatory requirement and provide transparency over logs in order to generate clear insights and improvements.

1. SolarWinds Security Event Manager

One of the most competitive SIEM tools on the market with a wide range of log management features. The real-time incident response makes it easy to actively manage your infrastructure and the detailed and intuitive dashboard makes this one of the easiest to use on the market. With 24/7 support, this is a clear choice for SIEM.

2. ManageEngine EventLog Analyzer (FREE TRIAL) – A SIEM tool that manages, protects, and mines log files. This system installs on Windows, Windows Server, and Linux.

3. Micro Focus ArcSight ESM – Comprehensive SIEM tool that runs on Windows environments and is very well suited to large organizations.

4. Splunk Enterprise Security – This tool for Windows and Linux is a world leader because it combines network analysis with log management together with an excellent analysis tool.

5. LogRhythm Security Intelligence Platform – Cutting-edge AI-based technology underpins this traffic and log analysis tool for Windows and Linux.

6. AlienVault Unified Security Management – Great value SIEM that runs on Mac OS as well as Windows.

7. RSA NetWitness – Extremely comprehensive and tailored towards large organizations but a bit too much for small and medium-sized enterprises. Runs on Windows.

8. IBM Qradar – Market-leading SIEM tool that runs on Windows environments.

9. McAfee Enterprise Security Manager – Popular SIEM tool that runs through your Active Directory records to confirm system security. Runs on Mac OS as well as Windows.

Conclusions

Not all SIEM systems are built the same. As a result, there is no one-size-fits-all solution. A SIEM solution that's right for one company may be incomplete to another. As mentioned above, log data management is a core component of any enterprise-scale SIEM system. A SIEM system needs to pool log data from a variety of different sources, each with their own way of categorizing and recording data. When looking for a SIEM system, you want one that has the ability to normalize data effectively.

In terms of convenience and regulatory requirements, having a SIEM with extensive compliance reporting features is very important. In general, most SIEM systems have some kind of onboard report generating system that will help you to conform to your compliance requirements. If a breach or attack occurs, you can generate a report that details how it happened extensively. You can then use this data to refine internal processes and make adjustments to your network infrastructure to make sure it doesn't happen again. This uses SIEM technology keeps your network infrastructure evolving to address new threats.

Having the ability to set the criteria for future security alerts is essential for maintaining an effective SIEM system through threat intelligence. Refining alerts is the main way you keep your SIEM system updated against new threats. Innovative cyber attacks are emerging every day, so using a system that's designed to add new security alerts stops you from getting left behind.

References

[1] Nicolett.M., Williams.A.T., Proctor.P.E. 'Magic Quadrant for Security Information and Event Management, 2006 1H06' RA3 1192006.

[2] Sandeep K. B. The Operational Role of Security Information and Event Management Systems / K. B. Sandeep/ IEEE Security and Privacy Magazine, 2014. Vol. 12(5)— 35 pp.

[3] Effective Use Case Modeling for Security Information & Event Management [Електронний ресурс]. – URL: https://www.sans.org/reading - room/ whitepapers/ bestprac/paper/33319.