International Journal for Innovative Engineering and Management Research

PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL

www.ijiemr.org

IJIEMR Transactions, online available on 04th Dec 2021. Link :http://www.ijiemr.org/downloads.php?vol=Volume-10&issue=Issue12

10.48047/IJIEMR/V10/ISSUE 12/39

Title **Anomaly Detection for Data Security in SIEM: Identifying Malicious Activity in Security Logs and User Sessions**

Volume 10, ISSUE 12, Pages: 295-298

Paper Authors **1ShivaDutt Jangampeta, 2Sukender Reddy Mallreddy, 3Jaipal Reddy Padamati**

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Anomaly Detection for Data Security in SIEM: Identifying Malicious Activity in Security Logs and User Sessions

[1]ShivaDutt Jangampeta, [2]Sukender Reddy Mallreddy, [3]Jaipal Reddy Padamati
[1]VicePresident, JPMorgan Chase, Dallas,USA, shivadutt87@gmail.com
[2]Salesforce Consultant, City Of Dallas, Dallas, USA, sukender23@gmail.com
[3]Senior Software Engineer, Comcast, Dallas, USA, padamatijaipalreddy@gmail.com

Abstract
Data security is a major concern in business. Many businesses experience security breaches resulting in manipulation, damage, and theft of sensitive, valuable information. Prevention and mitigation of security incidents require robust anomaly detection solutions to identify both external and internal threats in an organization’s IT infrastructure and eliminate them before they can be executed. The Security Information and Event Management (SIEM) systems are popular for their capacity to provide a comprehensive view of IT environments. SIEM solutions monitor data sources to detect an anomaly and contextualize them to generate security insights. The SIEM systems esnable efficient analysis of huge amounts of data, enabling security teams to thwart threats and cyber-attacks. This study reviews the use of SIEM systems to identify malicious activities in data environments.

Keywords - Security Information and Event Management (SIEM), SIEM detection, SIEM Alert.

I. Introduction

Security Information and Event Management (SIEM) systems are cybersecurity solutions used to detect, analyze, and respond to security events by gathering and correlating real-time data from different sources [1]. The collected data could be logs and incidents captured by firewalls, network elements, or intrusion detection systems (IDSs). Fundamentally, SIEM systems amalgamate the functions of two technologies: Security Information Management (SIM) which collects and stores data about security incidents; and Security Event Management (SEM) which analyzes security incidents to detect anomalies and malicious activities.

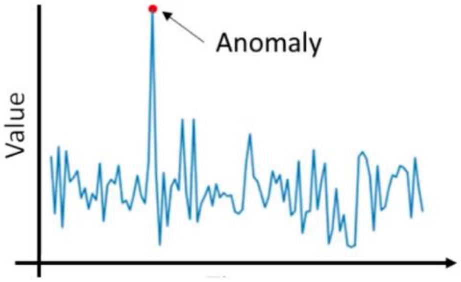

Fig. 1. Anomaly detected during a security scan

Normally, traditional SIEM systems continually monitor and analyze IT environments to identify abnormal behaviors and suspicious activities including unauthorized access, and abnormal network traffic – and notify security teams to mitigate them [2]. Modern SIEM solutions integrate AI to enhance the detection of suspicious user and system behaviors and patterns that may signify potential security threats and mitigate them. Besides, significant improvements in next-gen SIEMs over conventional SIEMs enable the former to spot advanced and ever-evolving threats. Once an anomaly is detected, SIEM equates it to a potential security threat thus it generates alerts to prompt immediate examination and mitigation by security teams.

II. Using SIEM tools to Identify Malicious Activity in Security Logs and User Sessions

The first SIEM systems were log management solutions that combined SIM and SEM tools, security information management and security event management respectively, to allow real-time monitoring and detection of malicious activities, as well as logging of security information for regulatory and auditing purposes. Essentially, SIEM tools are used to monitor at least six types of security logs, including Endpoint logs, Windows event logs, perimeter device logs, application logs, IoT logs, and proxy logs.

- *Endpoint Logs:* endpoints encompass devices like PCs, Laptops, Mobile phones, printers, etc. connected across a computer network. *SIEM tools* monitor endpoint logs to detect anomalies in user activities associated with these devices.
- *Windows Event Logs:* these comprise all activities that take place on a Windows platform, including security logs, system logs, Windows application logs, DNS server logs, File replication service logs, and directory service logs. SIEM tools monitor Windows event logs to guarantee server security, hardware components security, and Windows workstation security.
- *Perimeter Device Logs:* perimeter devices/solutions, including VPNs, IDSs, IPSs, etc. generate logs that contain vast amounts of security data. SIEM tools monitor perimeter devices to identify malicious traffic, detect cyber-attacks, and identify security misconfigurations.
- *Application Logs:* enterprises run on different applications like webserver applications, databases, etc. that generate log information that provide insights on the activities that take place in the applications. SIEM tools monitor application logs to enable troubleshooting o security issues and identify malicious activities.
- *IoT Logs:* like endpoint devices, IoT devices generate log data. Since most IoT devices do not store log data, the information is forwarded to a SIEM's centralized log management to be analyzed, troubleshoot errors and identify malicious activities.
- *Proxy Logs.* Proxy logs reveal sensitive, valuable information about user behaviors because all web requests pass through proxy servers. SIEM tools monitor proxy logs to detect anomalies in user behavior and monitor packet lengths.

III. SIEM Detection and Alert Mechanism

A SIEM alert is a notification generated by the system to inform security teams about a potential threat in real time. SIEM systems generate alerts from the identification, correlation, and compilation of metadata and system/user behaviors.

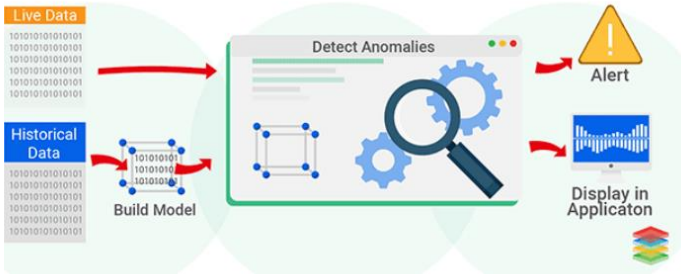

Fig. 2. A Detection and Alert model of a SIEM system

SIEM alerts rely on pre-defined instructions to identify system anomalies like unauthorized access, malware/virus infections, ransomware attacks, social engineering attacks, DDoS, etc. It plays a critical role in identifying and notifying security teams about the detected threats who respond swiftly and effectively. SIEM alert mechanism is a step-by-step process that comprises:

a) ***Step 1: Event Generation* –** Virtually all files within an organization's on-premises or cloud tenancy are creating a continuous flow of logs. The integration of SIEM solutions with these log elements starts to create a notification mechanism of real-time activities occurring in your firewalls, IDSs, antimalware software, servers, and different security solutions.
b) ***Step 2: Event Gathering* –** Since logs are created disparately, the SIEM system needs to establish which logs should be prioritized, thus it gathers a broad swathes of incidents from various sources and consolidates them within a centralized analysis environment.
c) ***Step 3: Normalization*** – Incidents gathered from various sources may have disparate formats and/or standards. Whereas error incidents exhibit a major issue like data loss or operation loss, warning incidents may just signify a potential future problem. Also, the wide range of file types and formats – sourced from OSs, Active Directory, etc. – requires SIEM normalization to standardize the incidents into a uniform format.
d) ***Step 4: Event Storage*** – Normalized incidents are kept in a secure, centralized database. They are used in historical analyses, forensic analysis, and compliance reporting.
e) ***Step 5: Anomaly Detection* –** Detection is fundamentally the analysis of incidents to spot potential security threats. SIEM solutions rely on predefined policies, signatures, and behavioral assessments to identify anomalies and patterns that indicate potential security events. Policies might include circumstances like several unsuccessful login attempts, familiar malware signature, access from uncommon locations, etc.
f) ***Step 6: Correlation*** – Correlation involves the analysis of several related incidents to ascertain if they conjointly represent a security event. It helps detect complex threat patterns that might conceal themselves or pass unnoticed when searching for a specific incident in isolation.
g) ***Step 7: Aggregation*** – Aggregation involves grouping related incidents to create a united view of security events. Essentially, aggregation is meant to reduce alert fatigue to ensure that the system generates a concise and reasonable set of notifications.

The abovementioned process culminates in the system generating an alert. SIEM identifies anomalies through detection, correlation, and then aggregation, and generates an alert. Fundamentally, an alert includes information about the event, like threat type, system(s) infected, description of the event, severity level of the event, action to be taken, etc.

SIEM alerts are modifiable, enabling businesses to customize them to meet their specific security demands. Also, security teams can formulate their set of policies and thresholds for generating SIEM alerts, to ensure that they only receive alerts of security incidents relevant to their environment.

IV. Best Practices for Anomaly Detection

The first step to a proactively monitoring SIEM solution is an effectively working alert system. Therefore, it is important to ensure that all the anomalies are reported and mitigated immediately. An SIEM alert system requires:

1. **Frequent review and revision of alert policies:** SIEM alerts require regular review and updating to guarantee the relevance and accuracy of their notification. This is because threats are constantly evolving and new ones are being created, thus the alert policies and signatures must reflect these modifications to remain efficacious.
2. **Prioritization and grouping of alerts:** SIEM notifications produce nauseating noise that may overwhelming to security teams. Therefore, SIEM alerts can be prioritized and grouped based on their degree of severity to enable security personnel to focus on the most critical incidents.
3. **Implementation of automatic response actions:** with automated response actions, security teams can respond to potential security events swiftly and more effectively. The actions could span from simple malware scan notifications to complex high-impact alerts.

V. Conclusion

Safeguarding your enterprises from security incidents regularly requires robust threat detection solutions to search anomalies and hunt threats [2]. Once detected, security teams are alerted and the mitigation process is initiated promptly.

References

[1] Ambre and N. Shekokar, , “Insider threat detection using log analysis and event correlation,” ProcediaComputer Science,, vol. 45, pp. 436–445, 2015.

[2] E. Akbas, Detecting Unusual Activities Using a Next Generation SIEM: Use Cases, 2020.

[3] A. D. Kent, L. M. Liebrock, and J. C. Neil,, “Authentication graphs: Analyzing user behavior within an enterprise network,” Computers & Security,, vol. 48, pp. 150–166, , 2015.