SIEM Definition & Fundamentals

What Is SIEM?

Crucial within the realm of computer protection, Security Information and Event Management (SIEM) encompasses the utilization of software offerings and solutions that merge the management of security data with the supervision of security events. These instruments facilitate real-time evaluations of alerts related to security, which are produced by network hardware and applications.

SIEM tools possess an extensive range of core functionalities, such as the collection and administration of log events, the capacity to examine log events and supplementary data from various sources, as well as operational features like incident handling, visual summaries, and documentation.

Employing SIEM innovations, IT personnel can detect cyberattacks at the time of or even prior to their occurrence, thereby enhancing the speed of their response during incident resolution. Consequently, SIEM plays an indispensable role in the effectiveness and ongoing supervision of a company's information security framework. It serves as the bedrock of an organization's security tactics, offering a holistic method for identifying and managing potential threats.

The Evolution Of SIEM Technology

The acronym "SIEM" emerged from the collaboration of two Gartner analysts who suggested a novel security information framework that integrated two preceding technologies: Security Information Management (SIM) and Security Event Management (SEM). This proposition appeared in a 2005 Gartner paper titled "Enhance IT Security through Vulnerability Management."

First-generation SIM technology was developed upon conventional log collection management systems, allowing for extended storage, examination, and reporting of log data while incorporating logs with threat intelligence. Conversely, the second-generation SEM technology tackled security events by delivering consolidation, correlation, and notification of events from a range of security apparatuses, such as antivirus software, firewalls, Intrusion Detection Systems (IDS), in addition to events disclosed directly by authentication, SNMP traps, servers, and databases.

In the years that followed, vendors amalgamated the capabilities of SIM and SEM to devise the SIEM, leading to a fresh definition as per Gartner's investigation. This nascent technology gained widespread acceptance as it offered a comprehensive methodology for detecting and managing threats, including the ability to amass, preserve, and scrutinize logs and security events from various origins.

How Does A SIEM Solution Work?

SIEM systems function by gathering data from a variety of sources, including PCs, network devices, servers, and more. This data is then standardized and consolidated to facilitate ease of analysis.

SIEM platforms employ security experts who scrutinize the data in order to identify and detect potential threats. This procedure allows businesses to locate security breaches and examine alerts, offering crucial insights into the organization's security standing.

Alerts notify Security Operations/Monitoring personnel that they must look into a (possible) security event or incident. These notifications are usually concise and inform staff of a specific attack targeting the organization's information systems. Alerts can be conveyed through multiple channels, such as emails, console pop-up messages, text messages, or phone calls to smartphones.

SIEM systems generate a vast number of alerts owing to the substantial volume of events produced for each monitored platform. It is not unusual for an hourly log of events to range from hundreds to thousands. As a result, fine-tuning the SIEM for detecting and alerting on high-risk events is crucial.

The capacity to accurately pinpoint high-risk events is what distinguishes SIEM from other network monitoring and detection tools, such as Intrusion Prevention Systems (IPS) or Intrusion Detection Systems (IDS). SIEM does not supplant the logging capabilities of these devices; rather, it operates in conjunction with them by processing and amalgamating their log data to recognize events that could potentially lead to system exploitation. By integrating data from numerous sources, SIEM solutions deliver a holistic strategy for threat detection and

management.

SIEM Business Requirements & Use Cases

Log Aggregation & Normalization

The importance of threat visibility through log consolidation offered by SIEM systems cannot be overstated. In its absence, an organization's cybersecurity holds as much value as a mere paperweight. Log consolidation entails gathering terabytes of security information from vital firewalls, confidential databases, and essential applications. This process empowers the SOC team to examine the data and discern connections, significantly improving threat visibility.

Utilizing SIEM log consolidation, the SOC team can identify and scrutinize security incidents and events throughout the organization's IT infrastructure. By centralizing and correlating information from various sources, SIEM delivers a holistic strategy for threat detection and handling. This approach allows organizations to recognize patterns, tendencies, and irregularities that could suggest potential security hazards. Consequently, SOC teams can react promptly and efficiently to security incidents, reducing the repercussions on the organization.

Threat Alerting

Having a SIEM solution that can identify and notify IT security teams about possible threats within the vast volume of collected security event data is essential. This feature is critical as it allows the IT security team to carry out swifter, more targeted investigations and respond to potential security incidents in a timely and efficient manner.

Advanced analytics and threat intelligence are employed by SIEM solutions to recognize potential threats and generate real-time alerts. When a threat is detected, the system forwards alerts to the IT security team, equipping them with the necessary details to effectively investigate and mitigate the risk. By alerting IT security teams promptly, SIEM solutions aid in minimizing the potential impact of security incidents and safeguarding the organization's vital assets.

Contextualization & Response

It is important to understand that merely generating alerts is not enough. If a SIEM solution sends alerts for every possible security event, the IT security team will soon be overwhelmed by the sheer volume of alerts, and false positives may become a frequent issue, particularly in older solutions. As a result, threat contextualization is crucial for sorting through alerts, determining the actors involved in the security event, the affected parts of the network, and the timing.

Contextualization enables IT security teams to identify genuine potential threats and act swiftly. Automated configuration processes can filter some contextualized threats, reducing the number of alerts received by the team.

An ideal SIEM solution should allow an enterprise to directly manage threats, often by stopping operations while investigations take place. This approach helps to minimize the potential impact of security incidents and protect the organization's critical assets. SIEM solutions provide context and automate threat filtering, allowing IT security teams to concentrate on genuine threats, reducing alert fatigue, and enhancing the efficiency and effectiveness of incident response.

Compliance

SIEM solutions play a significant role in compliance by assisting organizations in meeting regulatory requirements through a comprehensive approach to threat detection and management.

Regulations like PCI DSS, HIPAA, and GDPR mandate organizations to implement robust security measures, including real-time monitoring and analysis of network traffic. SIEM solutions can help organizations fulfill these requirements, enabling SOC teams to detect and respond to security incidents promptly.

Automated reporting and auditing capabilities are also provided by SIEM solutions, which are essential for compliance. These features allow organizations to produce compliance reports swiftly and accurately, ensuring that they satisfy regulatory requirements and can demonstrate compliance to auditors and regulators.

Data Flows Within A SIEM

Let us now briefly see how data travel within a SIEM, until they are ready for analysis.

1. SIEM solutions ingest logs from various data sources. Each SIEM tool possesses unique capabilities for collecting logs from different sources. This process is known as data ingestion or data collection.
2. The gathered data is processed and normalized to be understood by the SIEM correlation engine. The raw data must be written or read in a format that can be comprehended by the SIEM and converted into a

data must be written or read in a format that can be comprehended by the SIEM and converted into a common format from various types of datasets. This process is called data normalization and data aggregation.

3. Finally, the most crucial part of SIEM, where SOC teams utilize the normalized data collected by the SIEM to create various detection rules, dashboards, visualizations, alerts, and incidents. This enables the SOC team to identify potential security risks and respond swiftly to security incidents.

What Are The Benefits Of Using A SIEM Solution

It is evident that the advantages of deploying a Security Information and Event Management (SIEM) system significantly outweigh the potential risks associated with not having one, assuming that the security control is safeguarding something of higher importance.

In the absence of a SIEM, IT personnel would not have a centralized perspective on all logs and events, which could result in overlooking crucial events and accumulating a large number of events awaiting investigation. Conversely, a properly calibrated SIEM bolsters the incident response process, improving efficiency and offering a centralized dashboard for notifications based on predetermined categories and event thresholds.

For instance, if a firewall records five successive incorrect login attempts, resulting in the admin account being locked, a centralized logging system that correlates all logs is necessary for monitoring the situation. Similarly, a web filtering software that logs a computer connecting to a malicious website 100 times in an hour can be viewed and acted upon within a single interface using a SIEM.

Contemporary SIEMs often include built-in intelligence capable of detecting configurable threshold limits and events within specific timeframes, as well as providing summaries and customizable reports. More sophisticated SIEMs are now integrating AI to notify based on behavioral and pattern analysis.

The reporting and notification capabilities of a SIEM empower IT staff to swiftly react and respond to potential incidents, emphasizing its ability to identify malicious attacks before they occur. This intelligence can lower the expenses associated with a full-scale security breach, sparing organizations significant financial and reputational harm.

Numerous regulated organizations, such as those in Banking, Finance, Insurance, and Healthcare, are mandated to have a managed SIEM either on-premise or in the cloud. SIEM systems offer evidence that systems are being monitored and logged, reviewed, and adhere to log retention policies, fulfilling compliance standards like ISO and HIPAA.