Components of SIEM architecture

Enterprises have to constantly defend themselves from the ever-increasing number of cyberattacks they face everyday. Security information and event management (SIEM) is a security system widely adopted by various enterprises to protect their networks from these cyberattacks.

A SIEM solution consists of various components that aid security teams in detecting data breaches and malicious activities by constantly monitoring and analyzing network devices and events.

The 9 components of a SIEM solution's architecture

- ### 1. Data aggregation

  This component of a SIEM solution is responsible for collecting log data generated by multiple sources within a corporate network, such as servers, databases, applications, firewalls, routers, cloud systems, and more. These logs, which comprise a record of all the events that took place in a particular device or application, are collected and stored in a centralized location or data store.

  The various SIEM log collection techniques include:

  - Agent-based log collection:

    In this technique, an agent is installed on every network device that generates logs. These agents are responsible for collecting the logs from the devices and forwarding them to the central SIEM server. Apart from these responsibilities, they can also filter the log data at the device level based on predefined parameters, parse them, and convert them to a suitable format before forwarding. This customized log collection and forwarding technique helps in optimal usage of bandwidth.

    The agent-based log collection method is predominantly used in closed and secured zones where communication is restricted.

  - Agentless log collection:

    This technique does not involve the deployment of agents in any network device. Instead, configuration changes have to be made in the device so they can send any generated logs to the central SIEM server in a secure manner. In devices such as switches, routers, firewalls, etc., the installation of third-party tools for log collection is often not supported, so collecting log data through an agent becomes difficult. In such cases, an agentless log collection technique can be used. It also reduces the load on the network device as the deployment of an additional agent is not necessary.

- API-based log collection:

  In this technique, logs can be collected directly from the network devices with the help of application programming interfaces (APIs). Virtualization software provides APIs, which enable the SIEM solution to collect logs from virtual machines remotely. Also, when companies shift from on-premises software to cloud-based solutions, it becomes difficult to push the logs to the SIEM directly as the services are not connected to any physical infrastructure. When this happens, cloud-based SIEM solutions utilize APIs as an intermediary to collect and query the network logs.

2. Security data analytics (reports and dashboards)

SIEM solutions come with a security analytics component, which predominantly includes live dashboards that intuitively present security data in the form of graphs and charts. These dashboards are updated automatically, helping the security team identify malicious activities quickly and resolve security issues. With the help of these dashboards, security analysts can detect anomalies, correlations, patterns, and trends that might be present in the data, and gain various insights into events taking place in real time. SIEM solutions also provide users an option to create and customize their own dashboards.

Another facet of this security analytics component is predefined reports. Often, SIEM solutions are bundled with hundreds of predefined reports that help in providing visibility into security events, detecting threats, and easing security and compliance audits. These reports, which are mostly built based on known indicators of compromise (IoCs), can also be customized to suit internal security needs.

Most SIEM solutions also provide users options to filter, search, and drill down into these reports, set schedules for report generation as per the user’s needs, view data in the form of tables and graphs, and export the reports in different formats.

3. Correlation and security event monitoring

A correlation engine is one of the most vital components of a SIEM solution. Using predefined or user-defined correlation rules, the collected log data is analyzed for any relationships existing between different network activities, common attributes, or patterns that might be present. Correlation engines have the ability to put different security incidents together to give a holistic view of security attacks. They are capable of detecting signs of suspicious activity, compromise, or potential breach early in the network, and the SIEM system will generate alerts for those activities as well.

An example of a correlation rule:

“If a user has a successful login attempt after multiple failed login attempts in a short period of time, trigger an alert."

Most SIEM solutions come with predefined correlation rules constructed based on the IoCs. However, as attackers are continuously using more advanced techniques to hack into a system, the rules have to be modified and improved on a regular basis, or they will become obsolete. Building correlation rules requires an in-depth understanding of an attacker’s behavior and tactics.

4. Forensic analysis

This component of a SIEM solution is used for performing a root cause analysis and generating an incident report that provides a detailed analysis of an attack attempt or an ongoing attack that helps enterprises take appropriate remedial action immediately.

In spite of having the best defense mechanisms in place, it's not always possible for an enterprise to thwart all cyberattacks. However, an enterprise can perform forensic analysis to reconstruct the crime scenes and ascertain the root cause of the breach. Since log data comprises a record of all the events that took place in a particular device or application, it can be analyzed for traces left by malicious attackers.

SIEM solutions help the security team browse through the logs, generate forensic reports, and discover the time at which a particular security breach occurred, systems and data that were compromised, hackers behind the malicious activity, as well as the point of entry.

This component also helps enterprises meet certain compliance mandates such as the storage and archival of log data for long periods of time, and the capability to perform forensic investigations on them.

- ## 5. Incident detection and response

  Incident detection

  This module of a SIEM solution is involved in detecting security incidents. A security incident refers to an attempted or successful data breach in the network by an unauthorized party, or infringement of an organization's security policies. Denial-of-service attacks, misusing data and resources, unauthorized escalation of privileges, and phishing attacks are some common examples of security incidents. These incidents have to be detected and analyzed, and the appropriate actions have to be taken to resolve the security issue while ensuring the continuity of business operations. During incident detection, organizations strive to keep the mean time to detect (MTTD) as low as possible to reduce the damage caused by the attackers.

  Incident detection can be carried out using the following techniques:

  - Event correlation
  - Threat intelligence
  - User and entity behavior analytics (UEBA)

  Incident response

  This module of a SIEM solution is responsible for the remedial actions that are undertaken to resolve security incidents upon detection. With enterprises facing tons of security issues on a daily basis and with attackers employing more sophisticated techniques, incident response has become a challenging venture. Reducing the mean time to resolve (MTTR) is a major priority for every enterprise.

  Some incident response techniques include:

  - Automate incident response with workflows
  - Conducting forensic investigation

- ## 6. Real-time event response or alerting console

SIEM solutions perform log collection and correlation activities in real time; if any suspicious activity is detected, an alert is raised instantly, and the incident response team will act immediately to mitigate the attack or prevent it from happening.

Alert notifications can also be sent via email or SMS in real time, and can be categorized based on priorities assigned to them: high, medium, or low. Workflows can be assigned to security incidents so when an alert is raised, the corresponding workflow will be executed automatically.

- ## 7. Threat intelligence

Threat intelligence provides contextual information required to identify different types of cybersecurity threats and take appropriate actions to prevent, resolve, or mitigate them. By understanding the source of the attack, the motive behind it, the strategies and methods used to carry it out, as well as the signs of compromise, organizations can better understand the threat, assess the risks, and make well-informed decisions.

In order to add contextual information, companies can either obtain threat feeds from third-party vendors, or compile and use open source threat feeds available in STIX/TAXII format. The type of threat can be identified immediately, and remediation can be initiated, reducing the MTTR.

This component also helps security admins perform threat hunting, a process of actively searching through the entire network for any threats or IOCs that might be eluding the security system.

- ## 8. User and entity behavior analytics (UEBA)

This component helps in detecting security incidents. With attackers constantly developing new techniques to hack into networks, conventional security systems are rapidly becoming obsolete. However,organizations can defend themselves from any type of cyber threat with the help of machine learning techniques.

UEBA components employ machine learning techniques to develop a behavior model based on the normal behavior of users and machines in an enterprise. This behavior model is developed for each user and entity by processing large amounts of data obtained from various network devices. Any event that deviates from this behavior model will be considered as an anomaly, and will be further assessed for potential threats. A risk score will be assigned to the user or entity; the higher the risk score, the greater the suspicion. Based on the risk score, risk assessment is performed, and remedial activities are undertaken.

Some might ask what the difference is between a correlation engine and UEBA. While the former is a rule-based system used to detect incidents and threats, the latter, as the name indicates, spots suspicious events based on behavioral analytics. For an enterprise to thwart attacks effectively, it should rely on both the conventional rule-based mechanism and the modern behavioral analytics.

- ## 9. IT compliance management

  When it comes to data protection and security, generally a company is expected to meet the required standards, regulations, and guidelines imposed by various regulatory bodies. These regulatory mandates vary for different companies depending upon the type of industry and the region where they operate. If the company fails to comply, it will be penalized.

  To ensure an organization meets all the compliance requirements set by the government for protecting sensitive data, SIEM solutions include a compliance management component. Proactive measures such as employing various techniques to identify anomalies, patterns, and cyber threats should also be undertaken to protect sensitive data from being compromised.

  SIEM solutions have the capability to store and archive log data for an extended period of time so auditors can check the audit trails. They can also generate compliance reports such as HIPAA, SOX, PCI DSS, GDPR, ISO 27001 through log collection and analysis, as well as out-of-the-box reports as per the specific requirements stated by the mandate.

All these SIEM components collectively work together to help the security team by providing insights into different kinds of threats, their attack patterns, and malicious activities that may be taking place in the network, as well as the necessary course of action that has to be taken to address any security problems.