SIEM Basics

A. Introduction to SIEM

Security Information and Event Management (SIEM), is a solution that enables companies and organizations to collect, store, analyze, and generate reports from security events and data logs.

The main purpose of SIEM is to centralize and analyze large amounts of log and event information from organizations' IT infrastructures and to detect and manage security threats using this data. Under this broad purpose, SIEM has several specific goals:

1. Central Surveillance
Modern IT infrastructures are often dispersed and contain numerous components: servers, endpoints, network devices, applications, and more. SIEM tools collect logs and events from these components in a central point, which allows security experts to monitor the entire infrastructure from a single location.

2. Threat Detection
SIEM systems quickly detect abnormal or suspicious activities using correlation rules and advanced analysis techniques. This is especially critical for detecting unknown and complex attacks, such as zero-day threats.

3. Compliance Reporting
Many industries require organizations to comply with certain security standards (e.g. PCI DSS, HIPAA). SIEM tools store the logs required for compliance with these standards and creates compliance reports.

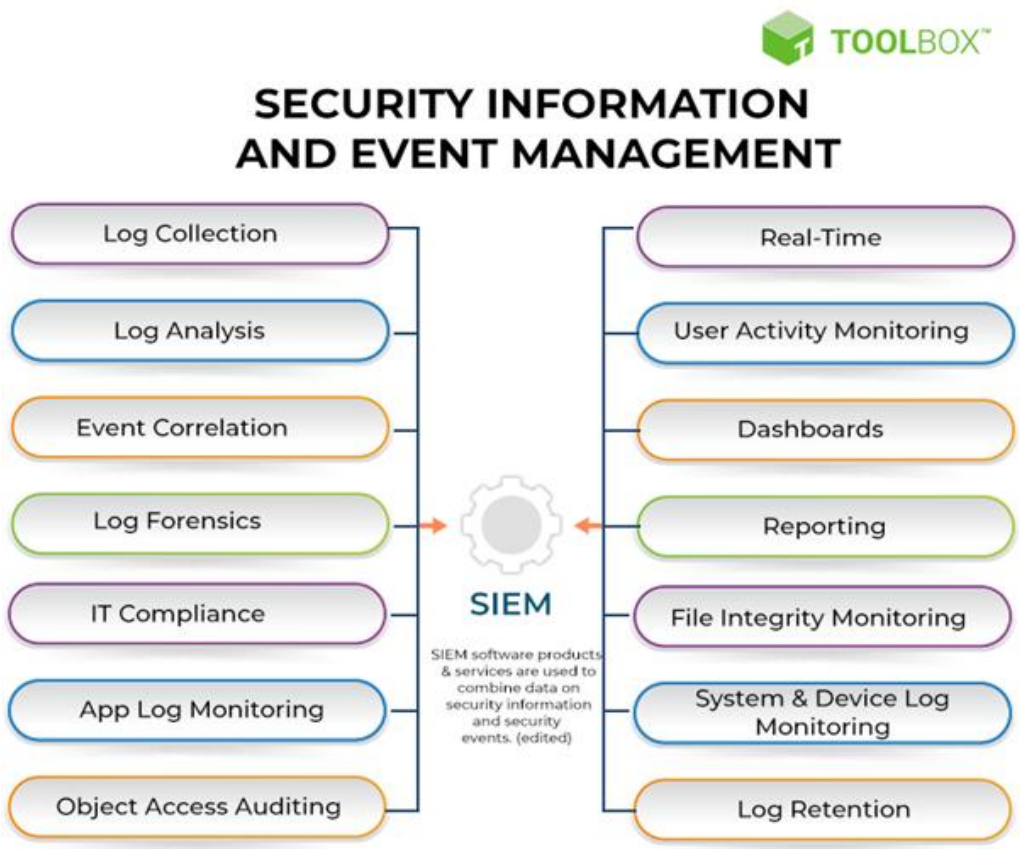
4. Forensic Analysis and Incident Response
After security incidents occur, SIEM tools store detailed log information for forensic analysis. This information is critical to understanding how an attack occurred and what its impact was.

5. Automation and Integration
SIEM can integrate with other security tools to respond to security incidents automatically. For example, it can trigger a firewall rules automatically when suspicious traffic is detected.

6. User and Asset Tracking
SIEM tools detect abnormal behaviors by creating behavioral profiles of users and IT assets. This is especially important for detecting insider threats.

7. Operational Efficiency
SIEM tools can improve overall operational efficiency by providing valuable insights for IT operations. For example, it can detect system errors, performance issues, and configuration errors.

B. SIEM Components



Data collection

It enables SIEM to collect log and event information from devices, servers, and other systems on the network. Collection methods can be agent-based (via device-specific software) or non-agent (directly from the device's log outputs). This collected data helps the SIEM process centrally for analysis. In summary, data collection is the process of obtaining log and event data from various devices, servers, applications, and other sources on the network.

To ensure visibility, SIEM needs this data to monitor activities within and around the network. This is crucial for detecting, analyzing, and responding to potential threats. Furthermore, the SIEM correlation engine analyzes data from various sources and searches markers for potential security events.

- Briefly, the most basic data sources are:
- Network Devices: Network devices such as routers, switches, firewalls, and IDS/IPS systems.
- Servers: Logs of different operating systems.
- Applications: Databases, web servers, email servers, and other enterprise applications.
- Other Resources: Cloud services, IoT devices, authentication systems and more.

- Log collection methods:
- Agent-Based Collection: Agents designed specifically for SIEM are installed on source systems and send logs directly to the SIEM system.
- Agentless Collection: Collecting logs through central log servers or syslog servers without using an agent.
- API and Integrations: Integration via APIs to retrieve data from modern platforms such as cloud services.

In short, data collection process is critical for SIEM to work effectively. This process ensures that the organization can comprehensively monitor its entire network and react quickly to potential threats. Therefore, choosing the right data collection strategies and tools is essential.

Log and Data Storage

Another important component of SIEM systems is log and data storage capacity. This helps the SIEM systems meet compliance requirements besides its capabilities to monitor, analyze, and report events. SIEM systems collect logs and event data from network devices, servers, applications, and other sources. This data is stored for extended periods of time for analysis, research, reporting, and compliance purposes.

Examining past incidents is critical for threat hunting and can help identify trends in security incidents. In many industries, logs must be retained for a certain period of time. For example, regulations such as PCI DSS may require to retain certain logs for a year or longer. When security breaches or other incidents occur, access to old logs is critical to understanding what happened.

As a result, the log and data storage capacity of the SIEM system allows a historical review of events, meeting compliance requirements and better understanding of potential security threats. Therefore, it is essential to properly design and manage the storage strategy and infrastructure.

Log Normalization

Log normalization is the process of converting event and log data from different systems, devices, and applications into a standard format or structure.

Different sources use different log formats and structures. These differences make it difficult to consolidate, analyze, and correlate events. Normalization addresses these challenges by standardizing this data, making it an essential issue in SIEM projects.

As a working structure, SIEM systems collect log and event data and apply predefined transformation rules to this data. These rules know what formats log and event data come in and define what to do to convert them to a certain standard. As a result, events from different sources are represented in SIEM in the same format.

Correlation is extremely important in terms of query, search, report, and performance. In conclusion, event normalization is a fundamental process that ensures SIEM systems operate effectively. By converting data from different sources into a standard format, it facilitates the analysis, correlation, and reporting of this data.

Log Correlation

One of the key features of SIEM systems is log correlation. Log correlation helps detect a specific pattern or event by analyzing log information from different sources. Log correlation is the process of analyzing log entries from different systems, applications, and devices and combining them to detect a specific event, security breach, or other potential threat. Correlation is usually performed automatically, based on predefined rules or algorithms.

- Features and Functions of Log Correlation:
- Multi-Source Log Processing: Correlation is often used to analyze logs from multiple sources. This is critical for detecting correlated events between different systems.

- Predefined Rules: SIEM systems can use predefined correlation rules to detect specific threat scenarios or security events.
- Automatic Alerts and Notifications: Correlation can automatically generate alerts or notifications when a specific pattern or event is detected.
- Advanced Diagnostics: Through correlation, security professionals can better understand the cause and effect of events.
- Historical and Real-Time Analysis: Correlation can operate on both real-time and historical log data, allowing it to analyze past events and detect what is happening right now.

➢ Importance of Log Correlation:

- Comprehensive Visibility: Provides an overview of events in an organization's IT infrastructure by combining logs from different systems and sources.
- Rapid Threat Detection: Correlation quickly identifies specific threat patterns, allowing security teams to respond faster to potential security incidents.
- Effectiveness and Efficiency: Automatic correlation allows security teams to save time by automatically detecting threats instead of manually reviewing logs.
- Fewer False Alarms (F/P): Proper correlation rules can reduce the number of false positives so teams can focus only on real threats.
- Forensic Analysis: Identifying the chronological order of events and associated events is critical to understand the root cause and impact of a security incident.

In short, log correlation is a critical component of modern SIEM systems. This feature is essential to quickly detect, understand, and respond to security incidents and threats. Correlation gives security teams broader and deeper visibility so they can make more informed and effective decisions.

Real-Time Monitoring and Analysis

Real-time monitoring is the process of keeping an organization's network, applications, users, and other components under constant and immediate surveillance. Real-time analysis refers to the automatic evaluation of the data collected during this monitoring against certain security rules, algorithms, and other parameters.

The SIEM system collects logs and events from sources (servers, network devices, security solutions, etc.). This data is processed, normalized, and stored by the SIEM tools in real-time. SIEM tools detect threats by applying predefined rules, correlations, and algorithms to this data.

Real-Time Monitoring and Analysis is critically important because time is critical for detecting and responding to security breaches and other critical incidents. We are able to detects threats almost instantly thanks to real-time monitoring and analysis reducing response time. It monitors every single asset in the organization, ensuring threats are detected when they occur anywhere.

Warning and Alarm

Alerts and alarms are automatic notifications that indicate a specific security event or a certain threshold has been exceeded. SIEM systems create these notifications according to specified criteria. This component instantly detects potential security breaches, allowing the organization to respond quickly to the incident. Manually reviewing all logs and events is a challenging task. Automatic alarms automate this

process allowing you to focus on only important events and keep track of important events on a regular basis.

- Warning and Alarm Types:

- Predefined Alerts: Alerts created in response to known threats or specific activities. (i.e. too many failed login attempts)
- Customized Alerts: Alerts created based on the organization's specific needs and related to a specific workload, application, or process.
- Alert Creation Process:
- Data Collection: Transferring relevant data to the SIEM system.
- Data Analysis: Analyzing the collected data and checking whether it meets certain criteria.
- Correlation: Combining and analyzing data from different sources.
- Alert Creation: Automatic creation of an alert if a certain criterion is met.

- Alert Management :

- Prioritization: Not all alarms are of equal importance. Prioritization of alarms according to importance and urgency.
- Verification: Checking whether the alarm represents a real threat and filtering false alarms.
- Response: Responding quickly and effectively to the event/incident.

In short, the alert and alarm mechanism of SIEM systems allows organizations to quickly detect potential threats and breaches and respond to them accordingly. Therefore, it is essential that this mechanism works effectively and is constantly updated.

Reporting

SIEM reporting involves analyzing and compiling collected log and event data and presenting it in specific formats. These reports present complex data in an understandable format, often through graphs, tables, and text.

- Reporting Types:
- Security Reports: Contains information on security incidents, threat detections, and other security-related issues.
- Compliance Reports: Reports on whether organizations comply with certain regulatory standards and regulations.
- Operational Reports: Contains information about system performance, user activities, and other IT operations.

- Importance of Reporting:
- Briefing: Obtaining information about the organization's overall security posture and becoming aware of potential vulnerabilities.
- Compliance: Ensuring and monitoring compliance with various regulatory standards and regulations.
- Decision Making: Making effective decisions about shaping security strategies and IT investments.
- Incident Response: Responding more effectively to similar incidents quicker by obtaining information about past events.

SIEM reporting capability helps organizations understand their security posture, operational status, and compliance status. These reports play a critical role in both daily operations and strategic planning processes. An effective SIEM reporting process enables organizations to better manage security-related risks, ensure compliance, and generally make more informed and proactive IT and security decisions.

Forensic Analysis

SIEM systems are valuable not only for real-time event monitoring and threat detection but also for forensic analysis which refers to a detailed examination of the aftermath of a security incident. This investigation aims to determine how and why the incident occurred, who carried it out, and what impact it had.

In terms of the importance of SIEM in forensic analysis, it is critical to quickly determine what happened in the immediate aftermath of a security breach. SIEM provides quick access to this information and collects data from multiple sources, which helps forensic analysts get a complete picture of the incident. Chronological event tracking and correlation features help analysts determine how and why events occur. Forensic analysis also includes the collection and preservation of evidence. SIEM ensures that this evidence is verified and preserved.

To summarize, SIEM systems are a critical tool for forensic analysis. Following a security incident, the data collection, storage, and analysis capabilities provided by SIEM help organizations quickly determine what happened, plan how to respond to the incident, and understand how to prevent similar incidents in the future.

User and Asset Tracking (UEBA)

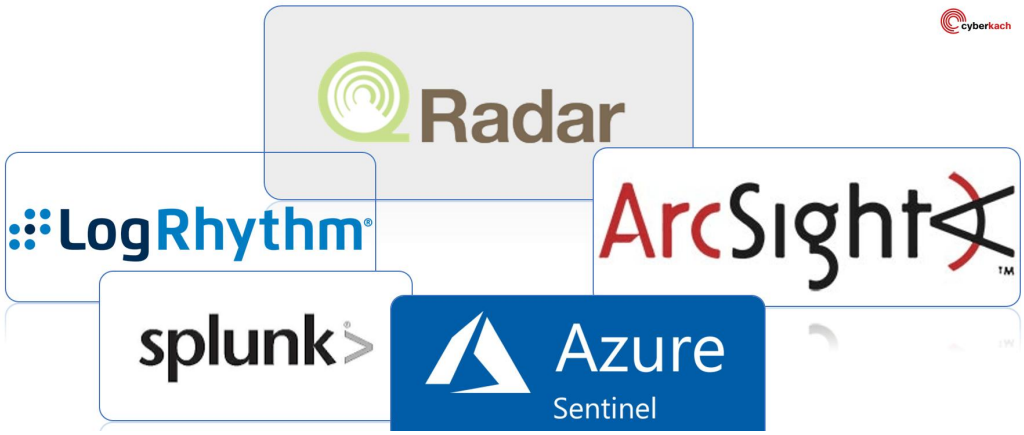
UEBA learns the normal behavior of users and assets (servers, devices, applications, etc.) on the network and is used to detect deviations from this behavior. UEBA creates a profile of "normal" behavior by analyzing the historical activities of a particular user or entity. If a user or entity displays activity that does not fit the normal behavior profile, this is considered an anomaly, and such activity can be processed as an alarm or warning.

- Importance of UEBA:
- More In-Depth Threat Intelligence: UEBA adds an additional layer to traditional signature-based threat detection, meaning more in-depth and accurate threat intelligence.
- Fast Response Times: UEBA's continuous monitoring and automatic detection capability allows security teams to respond faster to potential threats.
- Proactive Security Approach: Behavioral analysis can help take a proactive security approach by detecting potential security incidents at an earlier stage.
- Comprehensive Internal Threat Protection: Internal threats are often more difficult to detect than external threats. UEBA is an effective tool for identifying such threats.

In short, the UEBA capabilities of SIEM systems play a critical role in protecting against modern security threats. This helps organizations take a more effective and proactive security approach against both internal and external threats.

C. Common SIEM Products

The SIEM (Security Information and Event Management) market has a wide range of products offered by many different manufacturers. These products typically offer basic SIEM functions such as log collection, analysis, correlation, and threat detection. However, each stands out with its own unique features. Here are some commonly used SIEM products and features:



Splunk

Splunk is one of the industry's leading SIEM solutions. Splunk has extensive capabilities in big data analytics and real-time business intelligence and is used by many organizations for log management, monitoring, and security analysis.

- General features:
  - Data Collection : Ability to collect log and machine data from different sources (servers, network devices, applications, etc.).
  - Real-Time Analysis : Analyzing and visualizing logs and other data in real-time.
  - Scalability : Splunk is scalable across a wide spectrum, from small businesses to large organizations.
  - Visualization and Dashboards : Visualize data with customizable dashboards, charts, and reports.
  - Research and Query : Ability to make detailed queries on data with powerful search functions.
  - Applications and Integrations : Leveraging various data sources and technological solutions through pre-configured applications and integrations.

- Highlighted Features:

  - Splunk Cloud : As a cloud-based SIEM solution, this version of Splunk offers the advantage of rapid deployment and scaling.
  - Splunk IT Service Intelligence (ITSI) : It is a product developed to monitor and analyze the performance of IT and business services.
  - Advanced Threat Analysis : Advanced threat detection and response with AI and machine learning-based analysis.
  - Threat Hunting : Provides tools for proactive security analysis and threat hunting.
  - Advanced Correlation : Improved event correlation between different data sources.
  - Splunkbase : A marketplace with thousands of pre-made applications and plugins for Splunk. This makes Splunk easier to integrate into a variety of technologies and use cases.
  - Broad API Support : Splunk's APIs make it possible to create customized solutions by integrating with third-party applications.

Splunk goes beyond being just a security solution with its general data analysis and business intelligence features. However, fully evaluating these features requires proper configuration and optimization. Organizations must receive the necessary training and/or work with experienced experts to use Splunk effectively.

IBM QRadar

IBM QRadar is one of the industry's leading SIEM (Security Information and Event Management) products. Below you can find the general and prominent features of QRadar.

- General features:
- Log Management : Collects, normalizes, stores, and analyzes logs from different sources.
- Event Correlation : Identifies complex security threats by correlating data from various log and event sources.
- Network Flow Analysis : Detects potential threats and performs asset discovery by analyzing network traffic.
- Offense Management : Used to identify, prioritize, and track security breaches and other critical events.
- Visualization : Customizable dashboards, charts, and reporting features.
- Scalability : Provides a scalable structure for large-scale corporate networks.

- Highlighted Features:

- QRadar QFlow : Deeply analyzes network traffic, collects content data, and displays application activity.
- QRadar VFlow : Captures and analyzes virtual network traffic.
- Advanced Threat Intelligence: Provides up-to-date threat intelligence and information about well-known malicious IP addresses through integration with IBM X-Force.
- High Customizability : Allows organizations to create customized correlation rules based on their use cases.
- Automatic Incident Responses : The ability to automatically respond to specific security incidents.
- Advanced Search and Query : A user-friendly search interface to quickly research events and streams.
- Detection of Anomalies : Detects abnormal behavior in the network with AI and machine learning-based analysis.

QRadar offers a comprehensive SIEM solution for many different industries and sizes of businesses. However, proper configuration, constant updates, and training are required to use this system effectively.

LogRhythm

LogRhythm is also a well-known industry leader in the field of SIEM market. LogRhythm is designed to provide advanced protection against modern threats.

- General features:

- Integrated Log Management : Ability to collect, normalize, classify, and analyze logs from various systems and platforms.
- Advanced Event Correlation : The ability to create complex correlations between different data sources.
- AI-Based Threat Detection : Using artificial intelligence and machine learning to automatically identify anomalies and suspicious behavior.
- Alert and Incident Management : Ability to respond quickly and manage security incidents effectively.
- Visualization and Dashboards : Customizable dashboards and charts to quickly gain insight into security status.
- Automation and Orchestration : The ability to automate security operations and coordinate between different security products.

- Highlighted Features:
- Network Monitor : Provides rich content for threat hunting and internal threat detection by examining network traffic in depth.
- CloudAI : Uses artificial intelligence to identify abnormal behavior by analyzing user and asset behavior.
- SmartResponse : The ability to create automation actions to react to specific threat scenarios automatically.
- Case Management : The ability to organize and document processes for responding to security incidents.
- File Integrity Monitoring : Monitoring and alerting on important file and configuration changes.
- Multi-tenancy Support : Particularly useful for environments that support multiple customers or business units.
- Forensic Analytics : Detailed analysis to detect malicious activities by looking deeper into events.

LogRhythm offers a comprehensive and customizable SIEM solution for mid to large-sized organizations. However, using this system with maximum efficiency requires proper configuration, constant updates, and training.

ArcSight (Micro Focus)

ArcSight is another leading SIEM solution provided by Micro Focus and is considered the industry standard. ArcSight is used to detect, analyze, and respond to security incidents and data breaches.

- General features:
- Log Management : Collects, normalizes, indexes, and analyzes logs from various devices and applications.
- Advanced Event Correlation : Detects advanced threats and security incidents by correlating events across different data sources.
- Real-Time Monitoring : Monitors real-time data sources such as network traffic, application activity, and user behavior.
- Warning and Alarm Mechanism : Creates automatic alerts for events that meet certain conditions.
- Visualization and Reporting : Customizable dashboards and reports to assess and analyze security status.
- Data Storage and Querying : Stores large amounts of data for a long time and investigates events with fast query capabilities.

- Highlighted Features:
- Effective Correlation Engine : The ability to detect complex threats and events with a powerful and customizable correlation engine.
- Distributed Event Collection : The ability to collect events from distributed systems in various geographic locations.
- ArcSight Data Platform (ADP) : Provides data collection, enrichment, and normalization functions.
- ArcSight Investigate : High-speed incident investigation and threat-hunting capabilities.
- Integration : Easy integration with various security tools and solutions.
- Flexible Architecture : Thanks to its scalable structure, it can be used in both small businesses and large corporate networks.
- Machine Learning and Artificial Intelligence : AI and ML-based analysis to detect anomalies and suspicious behavior.

ArcSight is particularly popular for large-scale organizations and has a large community and support infrastructure. However, to use this system at its best, proper configuration, constant updates, and training are required.

Microsoft Sentinel

Microsoft Sentinel is Microsoft's cloud-based SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response) solution. It runs on the Azure platform and is used to detect, analyze, and respond to security incidents and data breaches of organizations.

- General features:
- Cloud-Based Structure : Sentinel runs on the Azure cloud, providing scalability and maintenance benefits.
- Log Management : The ability to collect and store logs from various devices, applications, and services.
- Advanced Event Correlation : Detects complex threats and security incidents by correlating events across different data sources.
- Real-Time Monitoring : The ability to monitor security events in real time.
- Integration : Deep integration with other Azure services and Microsoft's security product line.
- SOAR Features : Provides security automation, response, and orchestration capabilities.

- Highlighted Features:
- Comprehensive Visualization Interface : Ability to visualize events and threats with powerful and customizable dashboards.
- AI-Powered Analysis : Smarter threat hunting and incident detection by leveraging Azure's AI capabilities.
- Code-Free Query : With its easy-to-use query interface, users can perform in-depth analysis without code knowledge.
- Playbook Automation : The ability to create automated playbooks to create automatic responses to specific events.
- Integration : Easy integration with other security products from Microsoft (i.e. Microsoft Defender) and third-party solutions.
- Low Cost : With its cloud-based structure, organizations can pay according to their scale.
- Worldwide Data Centers : Leveraging Microsoft's extensive data center network to meet data storage needs in different geographic regions.

Microsoft Sentinel is a very appealing choice, especially for organizations that have existing integrations with Azure and use other products of the Microsoft ecosystem. Its cloud-based structure offers great flexibility in scaling and expansion, unlike traditional SIEM solutions.