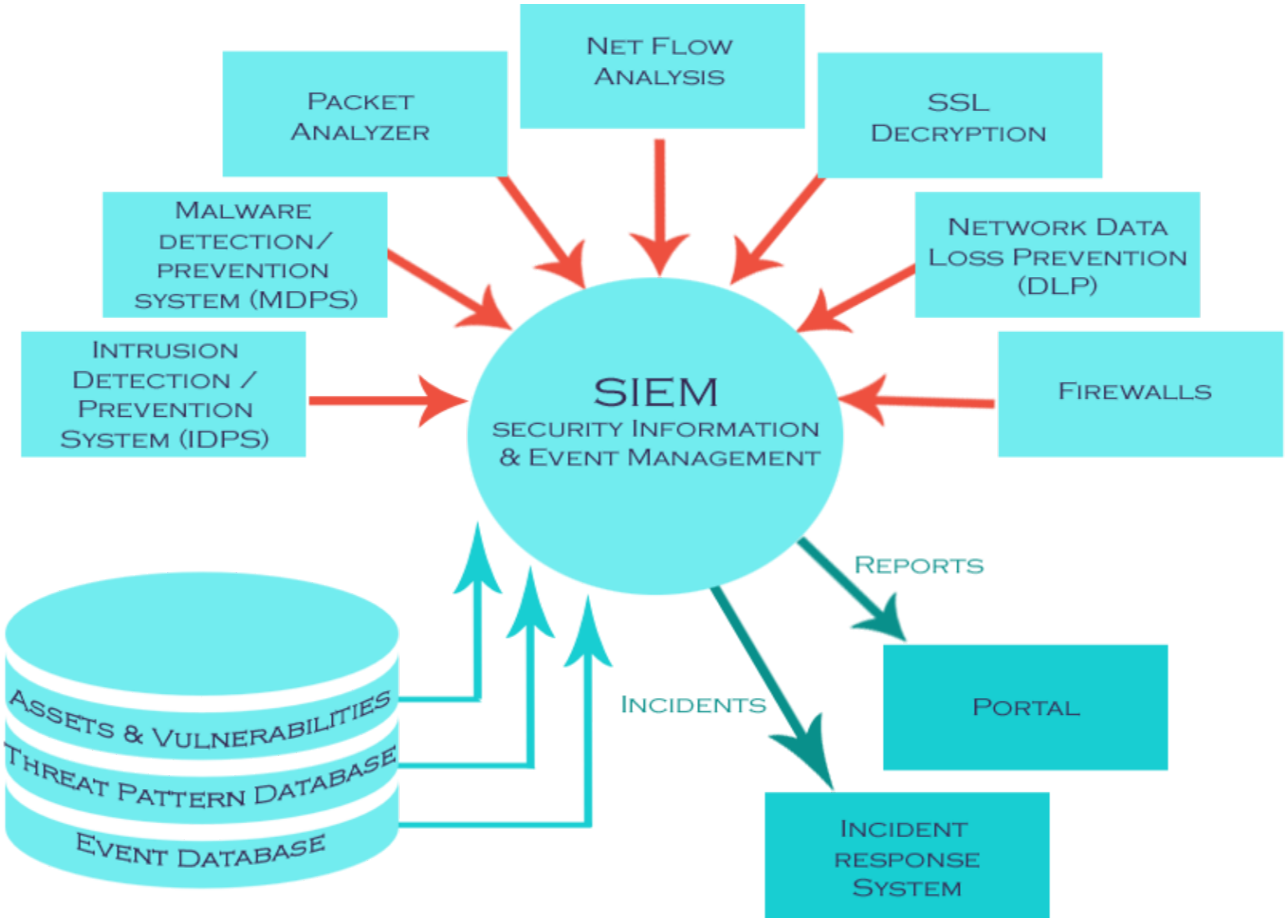
Security Information & Event Management (SIEM)



Security Information and Event Management (SIEM) is an approach to security management that seeks to provide a holistic view of an organization's information technology (IT) security. SIEM combines SIM (security information management) and SEM (security event management) functions into one security management system provides real-time analysis of security alerts generated by network hardware and applications.
SIEM system collects logs and other security-related documentation for analysis.
And it's work by deploying multiple collection agents in a hierarchical manner to gather security-related events from end-user devices, servers, network equipment and even specialized security equipment like firewalls, antivirus or intrusion prevention systems. The collectors forward events to a centralized management console, which performs inspections and flags anomalies.

Why SIEM Necessary ?

- ➔ Rise in data breaches due to internal & external threats.
- ➔ Attackers are smart and traditional security tools just don't suffice.
- ➔ Mitigate sophisticated cyber-attacks.
- ➔ Manage increasing volumes of logs frommultiple sources.
- ➔ Meet straigent compliance requirements.

SIEM Capabilities :

- ➔ **Data aggregation :** Log management aggregates data from many sources, including network, security, servers, databases, applications, providing the ability to consolidate monitored data to help avoid missing crucial events.

- ➔ **Correlation :** looks for common attributes, and links events together into meaningful bundles. This technology provides the ability to perform a variety of correlation techniques to integrate different sources, in order to turn data into useful information. Correlation is typically a function of the Security Event Management portion of a full SIEM solution.

- ➔ **Alerting :** the automated analysis of correlated events and production of alerts, to notify recipients of immediate issues. Alerting can be to a dashboard, or sent via third party channels such as email.

- ➔ **Dashboards :** Tools can take event data and turn it into informational charts to assist in seeing patterns, or identifying activity that is not forming a standard pattern.

- ➔ **Compliance :** Applications can be employed to automate the gathering of compliance data, producing reports that adapt to existing security, governance and auditing processes.

- ➔ **Retention :** Employing long-term storage of historical data to facilitate correlation of data over time, and to provide the retention necessary for compliance requirements. Long term log data retention is critical in forensic investigations as it is unlikely that discovery of a network breach will be at the time of the breach occurring.

➔ **Forensic analysis :** The ability to search across logs on different nodes and time periods based on specific criteria. This mitigates having to aggregate log information in your head or having to search through thousands and thousands of logs.

➔ **Netflow Analysis :** Flow-based monitoring solution delivers complete, real-time visibility into all hosts and traffic on the network, providing actionable insight for addressing a wide variety of network and security issues. NetFlow essentially answers the following questions about network traffic: Who, what, when, where, and how. Each flow is a collection of packets characterized by flow-specific information, such as the source and destination IP addresses, as well as port information. The packets in a particular flow are counted and reported via a collector. The collector classifies all the traffic collected on a network, based on its source, destination and application. NetFlow creates a behavior-based system that profiles the typical connections made between devices. NetFlow data is aggregated with data from other sources. such as IPSes, firewalls, VPNs, the application layer and, in some systems, identity data. This data is then correlated using several techniques including:

- Rules-based.
- Statistical.
- Historical.
- Vulnerability.

➔ **Logging :** Logging is a very critical component because it gives visibility into the environment. This type of visibility can be key to determining the root cause of a failure or narrowing in on a system attack, as it will allow to review events that took place prior to the failure or attack.
Key things to keep in mind when implementing a logging strategy in an environment:

- Timestamps : Make sure to use Network Time Protocol and time zones correctly on all devices collect logs from.

- Data retention : Ensure that enough storage allocated to retain the amount of data required for retention policy (30 days, 90 days, etc.).

- Event correlation : The ability to correlate between devices by using timestamps and specific data to narrow in on which event actually took place prior to an incident (vSphere hosts, storage, network, etc.).

- Auditing : To use syslog data from devices to track logins, password changes and events like privileged execution of tasks. Each of these are important during an audit.

➔ **Intrusion Detection System (IDS) :** An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity, policy violations or detecting vulnerability exploits against a target application or computer.

- How does IDS works : Any detected activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms.

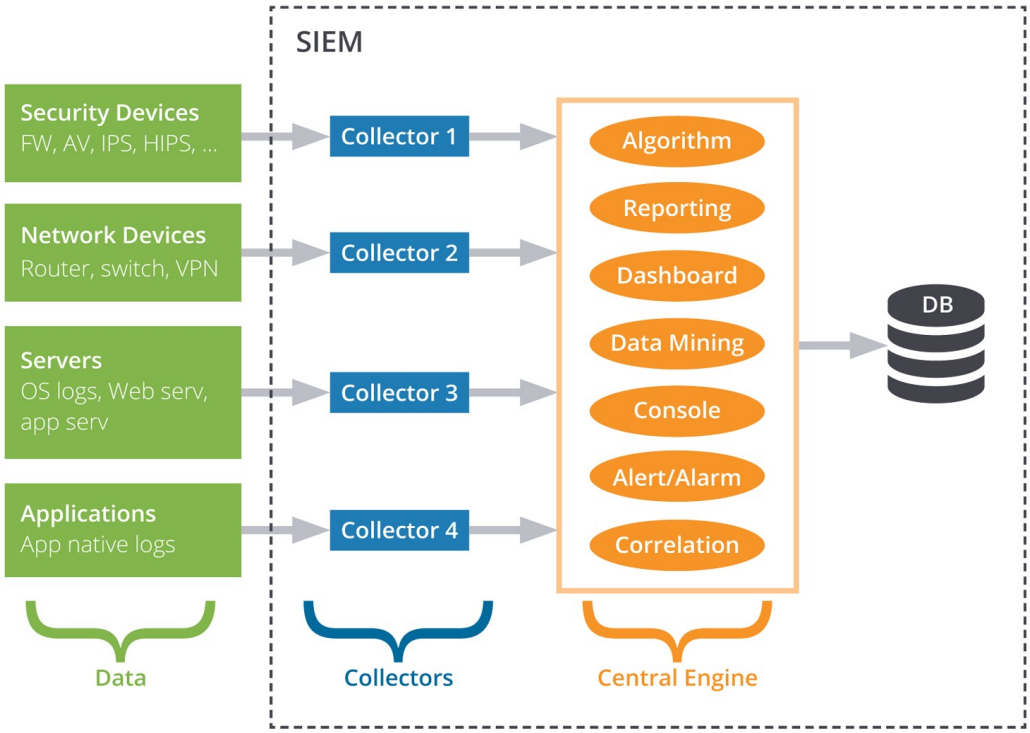
  Three IDS detection methodologies are typically used to detect incidents :

- Signature-Based Detection : Compares signatures against observed events to identify possible incidents. This is the simplest detection method because it compares only the current unit of activity (such as a packet or a log entry, to a list of signatures) using string comparison operations.

- Anomaly-Based Detection : Compares definitions of what is considered normal activity with observed events in order to identify significant deviations. This detection method can be very effective at spotting previously unknown threats.

- Stateful Protocol Analysis : compares predetermined profiles of generally accepted definitions for protocol activity for each protocol state against observed events in order to identify deviations.

➔ **SIEM Database :**



Devices send their logs directly to the SIEM where collectors, central engine, and database are located in a single appliance. In a distributed environment, the collectors and database can be physically located at a different place.

➔ **Data Loss Prevention (DLP) :** DLP solutions are often used to help protect sensitive data as it moves around the network and makes its way to endpoint devices. To prevent a user's sensitive data from making its way outside the corporate network, DLP solutions execute responses based on pre-defined policies and rules, ranging from simple notification to active blocking.

DLP typically covers three high level use cases: endpoint protection, network monitoring of data in motion, and classification of data at rest.

- Endpoint protection use cases include hard drive encryption, optical drive and USB port locking to prevent exfiltration, and malware protection.

- Data in motion technologies inspect email and web traffic to attempt to identify sensitive data potentially being exfiltrated so that data

remains in the organization, and may also help ensure that content is only accessed over encrypted channels.

- Data at rest classification inspects the content of file to identify where sensitive data may exist on server and cloud platforms so that additional action can be taken to ensure proper access controls.