# SIEM

### Security Information Management (SIM)

Security Information Management, also known as SIM is specialized security software that helps with the collection, monitoring, and analysis of data and event logs generated from all security devices in a network (IDS, IPS, Antivirus Software, Firewalls).

- Monitoring of events in real-time.
- Sending and generating alerts and reports.
- Automatic response to incidents.
- Correlation of data from multiple sources to improve the quality of the information presented.
- Translation of event logs from different resources through XML files

**Advantages:**

- Easy to deploy.
- They can store and analyze large volumes of data.
- They allow a fast and efficient analysis of all events in a system.
- They correlate logs and events to provide the most accurate overview of the system.
- They allow for easy threat management (assessment, containment, and analysis)

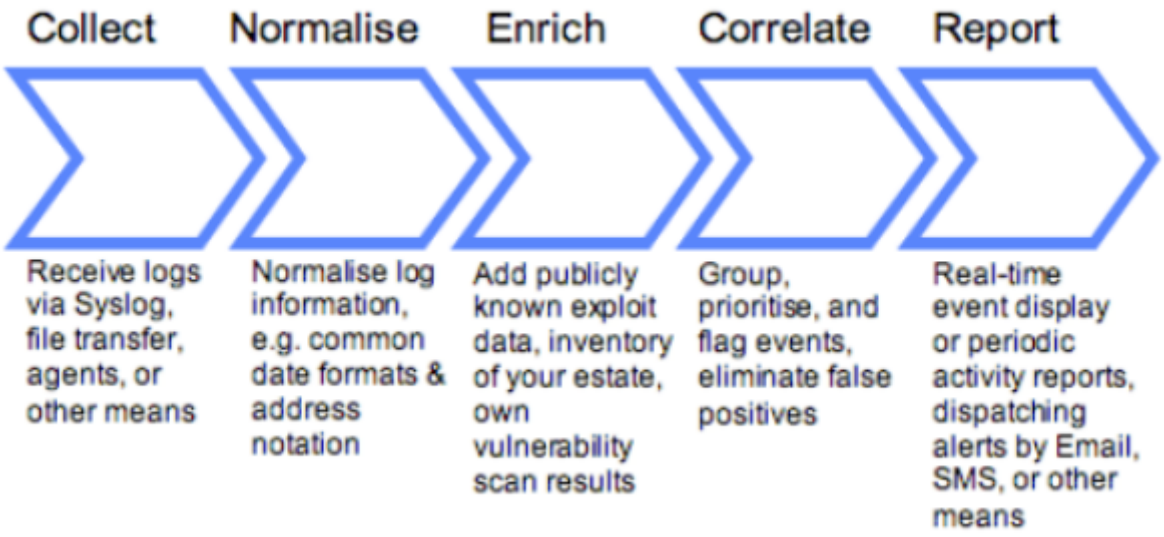
**Disadvantages**:

- They can be very expensive tools.
- It is not completely certain that they can be properly adapted to the working environment.
- Some providers do not provide full technical support for this type of service.

### Security Event Management (SEM)

Security Event Management, also known as SEM is a security software specialized in the identification, collection, monitoring, evaluation, notification and correlation in real-time of events and alerts of a computer system (network devices, security systems (IDS, IPS, Firewall), specialized software (Antivirus), etc.), whose purpose is to identify “suspicious” behavior within the system, to provide an effective and timely response from the security team to any incident that occurs within the network.

- Real-time events monitoring.
- Obtaining security events in devices and applications within the system.
- Correlation of events to provide a clear picture of the information system.
- Analyze logs according to their level of importance.
- Real-time incident response.




**Advantages:**

- Centralization of information from different devices and network elements.
- Reduction of false positives and false negatives.
- Considerable improvement in response time to internal and external threats.

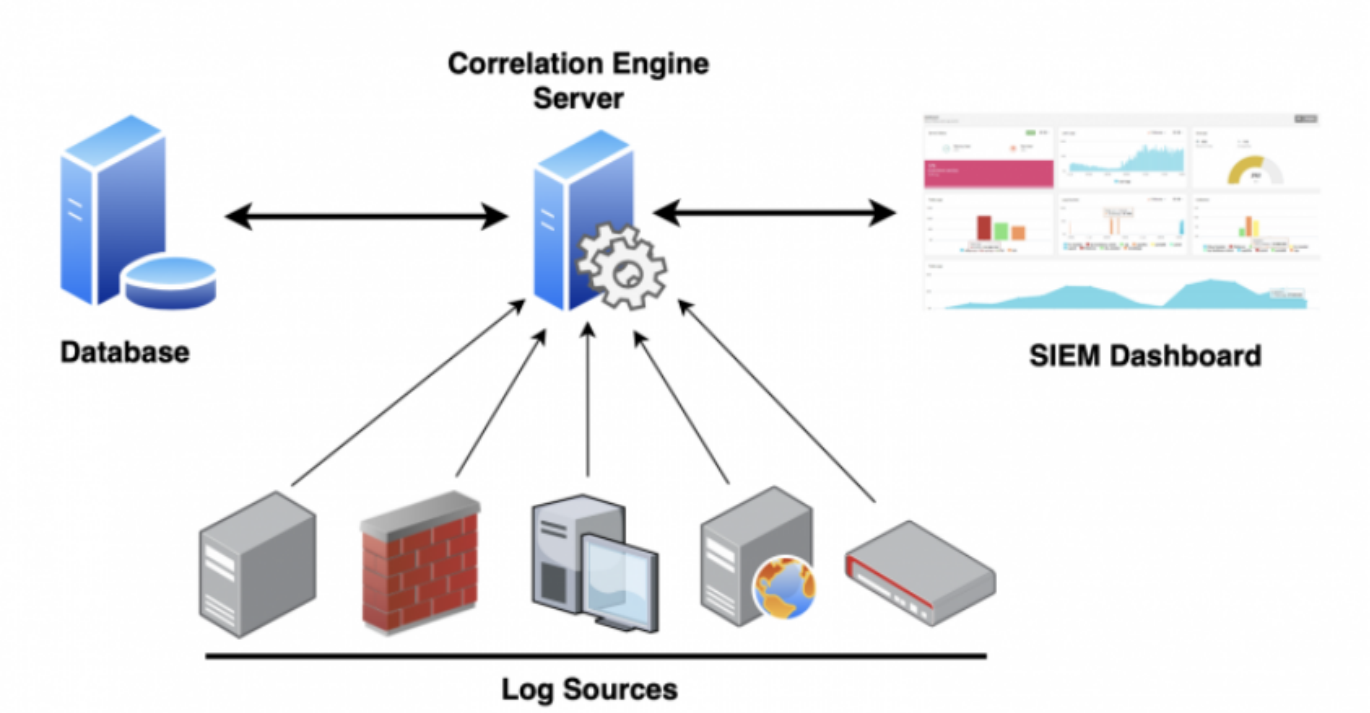
**Disadvantages**:

- They are hard to deploy.
- They have a high market cost
- As they are automated systems, they can present failures that allow for false positives and negatives.

### What is a SIEM?

Security Information and Event Management (SIEM) is a software solution that aggregates and analyzes activity from different resources across an organization's entire IT infrastructure. SIEM is a combination of security information management (SIM) and security event management (SEM) that uses rules and statistical correlations to help organizations detect threats and turn log entries, and

events from security systems, into actionable information.




**Benefits of a SIEM**:

- Advanced Threat Detection
- Forensics and Incident Response
- Compliance Reporting and Auditing:

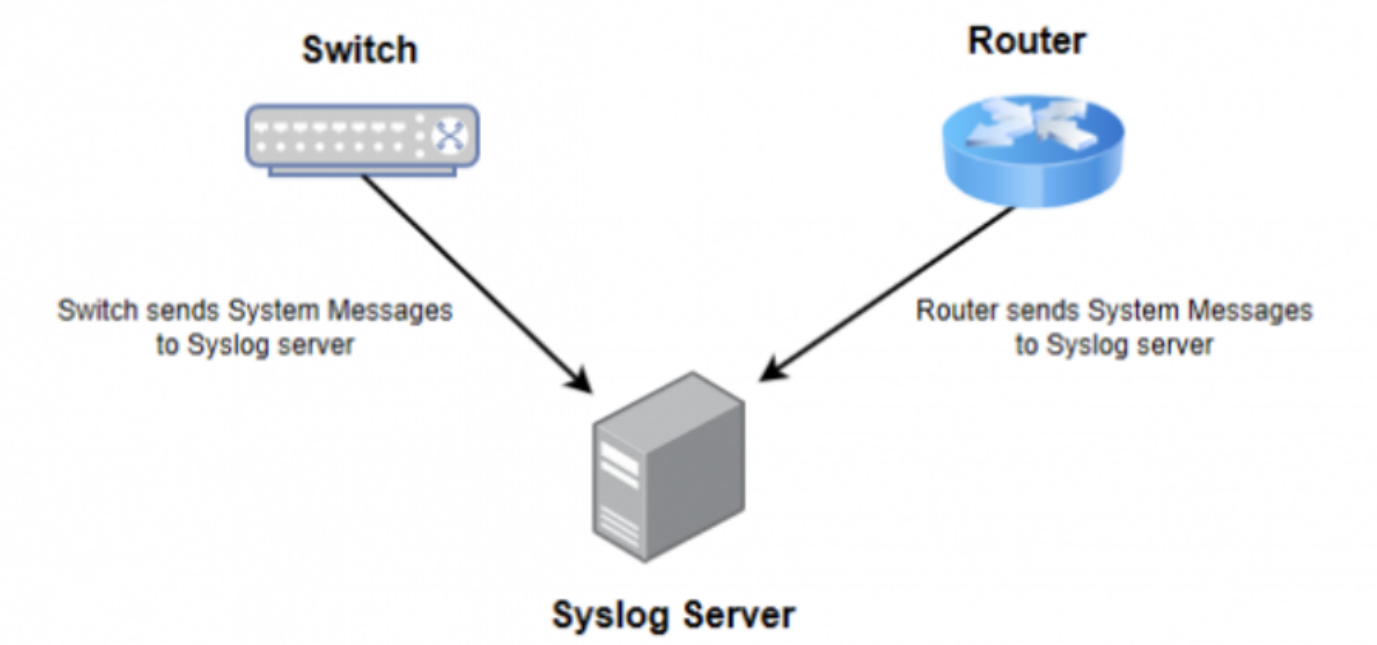
---

## Logging and Aggregation

Logs are detailed lists of application information, system performance statistics, or user activities. Every activity in your environment, from emails to logins to firewall updates, is considered a security event. Events are, (or should be,) logged to keep tabs on everything that's happening in your technology landscape.

### Syslog

- System Logging Protocol (Syslog) is a standard protocol used to convey event or system log notification messages to a designated server, known as a Syslog server.
- The Syslog server centralizes data collection from various devices for analysis, review, and intervention.
- The protocol can be enabled on most network equipment such as switches, routers and firewalls, and even endpoint devices.
- Syslog is available on Unix and Linux-based systems and many web servers.
- Syslog uses UDP 514 by default; TCP 514 can be used for more reliability;
- Syslog does not offer authentication or encryption built-in, so it may be susceptible to attacks.




**A Syslog message is made of three components:**

- Priority Value (PRI)
- Header
- Message

### Windows Event Logs

“Windows Event logs” or “Event Logs” are files in binary format (with .evtx extension) stored locally in the Windows directory of a computer with that operating system:

- Windows 2000 to WinXP/Windows Server 2003: %WinDir%\system32\Config*.evt
- Windows Server 2008 to 2019, and Windows Vista to Win10: %WinDir%\system32\WinEVT\Logs*.evtx

On Windows 10 we can view Windows Events using the Event Viewer.

**Categories of registered events include:**

- Application: Events logged by an application (Execution, Deployment error, etc.)
- System: Events logged by the Operating System (Device loading, startup errors, etc.)
- Security: Events that are relevant to the security of the system (Logins and logouts, file deletion, granting of administration permissions, etc.)
- Directory Service: This is a record available only to Domain Controllers, it stores Active Directory (AD) events.
- DNS Server: It is a record available only to DNS servers; logs of DNS service are stored.
- File Replication Service: Is a record available only for Domain Controllers, it stores Domain Controller Replication events.

## Sysmon

- Sysmon is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log.
- It provides detailed information about process creations, network connections, and changes to file creation time.
- By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them.
- In this way, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network.
- In an organization, we could then feed this into our SIEM to provide additional detailed logs from Windows endpoints, working alongside Windows Event Logs!

## Other Log types

### Microsoft Azure

- Azure Monitor is able to pick up logs from a multitude of different Azure services such as, virtual machines, virtual networks, Azure Active Directory, and Azure Security Center, as well as on-premises services.
- Azure has three primary categories of logs: Control/Management logs, Data Plane logs, and Processed Events.
- These logs are fed to Azure through the Azure REST API, the Microsoft Graph API, JSON, and various other sources.
- Azure logs can also be connected to different kinds of SIEMs such as Splunk or even Microsoft's own Azure Sentinel.
- Kusto Query Language (KQL) to query logs

### Amazon Web Services

### OSQuery

- Osquery is a universal endpoint agent
- According to the official osquery docs, osquery (os=operating system) is an operating system instrumentation framework that exposes an operating system as a high-performance relational database.
- Using SQL, you can write a single query to explore any given data, regardless of the operating system.

### Moloch

## Log Aggregation

Log aggregation is the process of collecting logs from multiple computing systems, parsing them, extracting structured data, and putting them together in a format that is easily searchable and explorable by modern data tools.

There are four common ways to aggregate logs, and many log aggregation systems combine multiple methods:

**Syslog**
A standard logging protocol. Network administrators can set up a Syslog server that receives logs from multiple systems, storing them in an efficient, condensed format that is easily queryable. Log aggregators can directly read and process Syslog data.

**Event Streaming**
Protocols like SNMP, Netflow, and IPFIX allow network devices to provide standard information about their operations, which can be intercepted by the log aggregator, parsed, and added to central log storage.

**Log Collectors**
Software agents that run on network devices, capture log information, parse it and send it to a centralized aggregator component for storage and analysis.

**Direct Access**
Log aggregators can directly access network devices or computing systems, using an API or network protocol to directly receive logs. This approach requires custom integration for each data source.

**Data Types:**

- Structured data: These are usually logs for Apache, IIS, Windows events, Cisco logs, and some other manufacturers. They have clearly-defined fields (such as “src_ip“) and are similar to other structured logs, making them relatively easy to parse and normalize.
- Unstructured data: This type of logging typically comes from a custom-built application where each message can be printed differently in different operations and the event itself can span multiple lines with no defined event start point, event endpoint, or both. This is likely to be the majority of the data being sent to the SIEM.

---

## Correlation

- Normalization merges events containing different data into a reduced format that contains common event attributes.
- Most logs capture the same basic information – time, network address, operation performed, etc.
- Categorization involves adding meaning to events – identifying log data related to system events, authentication, local/remote operations, etc.

**Log Enrichment**

- Log enrichment involves adding important information that can make the overall data more beneficial for security analysts when investigating alerts or unusual activity.

- One example could be logs that contain public IP addresses, but not their geographical location. Performing a simple lookup to see what geographical range the IP belongs to, can now immediately provide analysts with the country this IP is based in, which can aid investigations and help to build metrics.

**Log Indexing**

- SIEMs can hold an absolute ton of data, and to search through all of that, especially when looking over a long period of time such as a couple of weeks, can be extremely slow.
- By indexing attributes that are shared by a large number of logs, it can make searching for specific attributes across large data faster compared to having to scan every single piece of data in the SIEM storage to get the answers you need.

**Log Storage**

- For large organizations, the amount of storage needed to support a SIEM can be a large effort on the part of infrastructure and security teams.
- While alternatives to on-premises servers exist, such as Amazon Web Services S3 buckets or Hadoop, it is important for teams to consider all of their options, weighing in factors such as cost, ease-of-use, and scalability.

**Normalization**

- Different software, hardware, and devices produce their own format of logs, as there is no universal format
- SIEM log normalization is the process of changing log formats into a format that is as similar as possible across all devices and log sources, giving the SIEM a break and allowing for more consistent searching and information breakdown.

## SIEM Rules

- They are search queries that are looking for specific activity, looking at any imported or real-time data that is being fed into the SIEM solution.
- If the rule query matches a piece of data, different actions can be triggered, such as generating an alert, sending an email to a team, or recording the activity to a separate location.
- These search queries can be running continuously (real-time detection), or set to run at specific scheduled times, such as every day, or every week.
- False positives are alerts that have been generated but do not actually represent a malicious event.

## Sigma

- Sharing SIEM rules can be an extremely beneficial process for a security team, whether they’re sharing them or retrieving them, but SIEM rules are written in specific structures depending on the SIEM platform.
- Sigma is a generic and open signature format that allows you to describe relevant log events in a straightforward manner.

- The main purpose of this project is to provide a structured form in which researchers or analysts can describe their detection methods and make them shareable with others.
- Rules can be written in the Sigma language and then using a converter (Sigmac) they can be exported as rules in the correct format for a number of different SIEM platforms.
- This process can also be reversed allowing security professionals to export rules from their vendor format to Sigma format so they can be used by teams with a different SIEM.


**Benefits of Using Sigma:**

- Describe your detection method in Sigma to make it sharable
- Write your SIEM searches in Sigma to avoid vendor lock-in (meaning you can flexibly change the SIEM solution without having to lose all of your custom rules)
- Share the signature in the appendix of your analysis or research report along with IOCs and YARA rules to allow others to replicate your work and build detection rules
- Share the signature in threat intel communities (ISACs) – e.g. via MISP (which we covered in the Threat Intel domain!)