Security information and event management

In the field of [computer security](https://en.wikipedia.org/wiki/Computer_security), **security information and event management** (**SIEM**) software products and services combine [security information management](https://en.wikipedia.org/wiki/Security_information_management) (SIM) and [security event management](https://en.wikipedia.org/wiki/Security_event_manager) (SEM). They provide real-time analysis of security alerts generated by applications and network hardware.

Vendors sell SIEM as software, as appliances or as managed services; these products are also used to log security data and generate reports for [compliance](https://en.wikipedia.org/wiki/Regulatory_compliance) purposes.

Overview

The acronyms *SEM*, *SIM* and *SIEM* have been sometimes used interchangeably.[[2]](https://en.wikipedia.org/wiki/Security_information_and_event_management#cite_note-Generic-2) The segment of security management that deals with real-time monitoring, correlation of events, notifications and console views is known as *security event management* (SEM). The second area provides long-term storage as well as analysis, manipulation and reporting of log data and security records of the type collated by SEM software, and is known as *security information management* (SIM). As with many meanings and definitions of capabilities, evolving requirements continually shape derivatives of SIEM product-categories. Organizations are turning to [big data](https://en.wikipedia.org/wiki/Big_data) platforms, such as [Apache Hadoop](https://en.wikipedia.org/wiki/Apache_Hadoop), to complement SIEM capabilities by extending [data storage](https://en.wikipedia.org/wiki/Computer_data_storage) capacity and [analytic](https://en.wikipedia.org/wiki/Analytics) flexibility. The need for voice-centric visibility or vSIEM (voice security information and event management) provides a recent example of this evolution.

The term *security information event management* (SIEM), coined by Mark Nicolett and Amrit Williams of Gartner in 2005,

* the product capabilities of gathering, analyzing and presenting information from network and security devices
* [vulnerability](https://en.wikipedia.org/wiki/Vulnerability_(computing)) management and policy-compliance tools
* operating-system, database and application logs
* external [threat](https://en.wikipedia.org/wiki/Threat_(computer)) data

A key focus is to monitor and help manage user and service privileges, [directory services](https://en.wikipedia.org/wiki/Directory_services) and othersystem-configuration changes; as well as providing log auditing and review and incident response.

Capabilities/components[[edit](https://en.wikipedia.org/w/index.php?title=Security_information_and_event_management&action=edit&section=2)]

* **Data aggregation:** [Log management](https://en.wikipedia.org/wiki/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](https://en.wikipedia.org/wiki/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

Usage cases

Computer security researcher [Chris Kubecka](https://en.wikipedia.org/w/index.php?title=Chris_Kubecka&action=edit&redlink=1) identified the following SIEM use cases, presented at the hacking conference 28C3 ([Chaos Communication Congress](https://en.wikipedia.org/wiki/Chaos_Communication_Congress)).[[11]](https://en.wikipedia.org/wiki/Security_information_and_event_management#cite_note-11)

* **SIEM visibility** and **anomaly detection** could help detect [zero-days](https://en.wikipedia.org/wiki/Zero-day_(computing)) or [polymorphic code](https://en.wikipedia.org/wiki/Computer_virus#Polymorphic_code). Primarily due to low rates of [anti-virus](https://en.wikipedia.org/wiki/Anti-virus) detection against this type of rapidly changing malware.
* (In [data mining](https://en.wikipedia.org/wiki/Data_mining),**anomaly detection** (also outlier detection[[1]](https://en.wikipedia.org/wiki/Anomaly_detection#cite_note-:0-1)) is the identification of rare items, events or observations which raise suspicions by differing significantly from the majority of the data.[[1]](https://en.wikipedia.org/wiki/Anomaly_detection#cite_note-:0-1) Typically the anomalous items will translate to some kind of problem such as [bank fraud](https://en.wikipedia.org/wiki/Bank_fraud), a structural defect, medical problems or errors in a text. Anomalies are also referred to as [outliers](https://en.wikipedia.org/wiki/Outlier), novelties, noise, deviations and exceptions)
* **Parsing, log normalization and categorization** can occur automatically, regardless of the type of computer or network device, as long as it can send a log.
* Visualization with a SIEM using security events and log failures can aid in **pattern detection**.
* **Protocol anomalies** which can indicate a mis-configuration or a security issue can be identified with a SIEM using pattern detection, alerting, baseline and dashboards.
* SIEMS can detect covert, malicious communications and encrypted channels.
* [**Cyberwarfare**](https://en.wikipedia.org/wiki/Cyberwarfare) can be detected by SIEMs with accuracy, discovering both attackers and victims.

|  |
| --- |
| Splunk License, daily data usage |
| Identify critical information about environment and users |
| Indexer and infrastructure planning |
| Check feasibility in terms of forwarders installation and configuration |
| Plan Splunk app deployment |
| Identify the impact of clustering  for index replication and for search heads |
| Identify backup and archiving methods |
| Different types of servers and logs |
| data source type |
|  |
| Identify authentication, authorization and access control methodes |
| Role specific user access |
| Permission on specific splunk folders and files |
| Index designing |
| Event breaking |
| Recognizing timestamp |
| Identifying source and sourcetype |
|  |
| Configuration changes while parsing and indexing |
|  |
|  |
| Field extraction |
| Configuration changes on deployment server – Gihub /Linux?? |
| Writing search queries |
| Data enrichment, usiing lookup files, corelation entities |
|  |
| Dashboard & Panel designing |
| report generation |
| alert generation |