Guide

Essential Buyers Guide to SIEM

For enterprises

Huntsman®
Defence-Grade Cyber Security

Contents

Overview of SIEM and Core Capabilities

What is a SIEM?

Security Information and Event Management software (SIEM) grew out of a need to collect and retain log information from systems and security controls. Originally, this was compliance-driven, with many early solutions simply gathering log data to allow security teams and other stakeholders to examine logs for non-complaint or suspicious activity. This remains a requirement for many SIEM buyers.

SIEMs evolved to be able to detect predefined or learned patterns of log events, network sessions and user activity that could be flagged as policy breaches or signs of attack. This enabled operators to detect and run queries against event data to identify and investigate security incidents and compliance breaches.

SIEM sits at the nexus of endpoint and network information technologies. It informs security teams, and other stakeholders, of relevant security events across databases and business applications as well as inbound and other endpoint activity.

For a checklist of important considerations when buying a SIEM, refer to our SIEM BUYER'S GUIDE CHECKLIST in the Appendix

> "The growing scale and sophistication of threats has driven the need for greater security"

How SIEM works

SIEM solutions collect, store, analyse and identify security incidents and events, before categorising them for resolution. SIEMs deliver on four main objectives:

- To collect relevant data for the investigation of, reporting on and response to security threats in a timely manner.
- To identify and send alerts of potential security incidents that have breached predetermined policies, filters or rules.
- To provide reports on security-related and activity-related events and incidents, across "all things" be they applications access, network connections or suspicious activities.
- To provide compliance reporting in line with regulatory requirements.

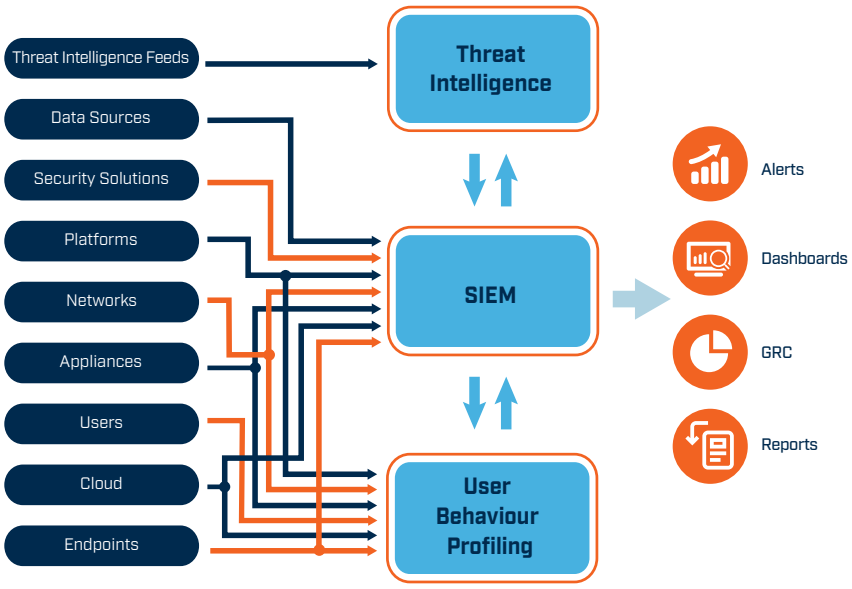

Fig 1. How a SIEM works

The growing scale and sophistication of threats has driven the need for greater security. As a result, new capabilities have emerged. To this end, Next Generation SIEMs now:

- Provide Security Analytics capabilities that incorporate Behaviour Anomaly Detection or User and Endpoint Behaviour Analytics to identify and help qualify unusual or suspicious patterns of activity.
- Add externally sourced Threat Intelligence to supplement event data for incident correlation and analysis.
- Manage large volumes of data using machine-based learning and correlation for faster and more accurate threat detection and better informed decision making.
- Automation of analyst workflows to streamline the threat validation, management and response activities.

Buying SIEM for enterprises

The ability to detect threats is important but efficient workflow management of security events and alerts is equally important when choosing a SIEM. If your team is over-loaded with alerts and investigations then adding further detection capabilities will only slow down the overall security operations process.

Technical environments change over time, so SIEM flexibility to cope with changes in scale, or new information sources to be monitored, will only impact established workflows and practices.

One example has been the global shift to home working during the COVID-19 pandemic. This resulted in a need to include endpoint and cloud-based system monitoring as part of an effective enterprise-wide solution.

Challenges for buyers

A key consideration is to evaluate SIEM products based on your organisation's specific requirements. One size certainly doesn't fit all; there are solutions for every size and shape of organisation. Here are a few considerations:

- **Compliance reporting & auditing** - If you want a SIEM primarily for compliance reporting and audit support, consider what is available OOTB (out of the box) for particular Standards based reports, dashboards and data management capabilities.
- **Improving cyber security posture** - If it's your cyber resilience that you want to improve, look for a SIEM with more advanced security analytics, behavioural anomaly detection and threat intelligence and hunting capabilities.
- **Large environments** - If your enterprise has petabytes of data to protect, look for high speed collection and analysis; distributed, scalable storage and incident resolution capabilities.
- **Organisations with a low level of cyber risk** - Organisations that have lower levels of assessed cyber risk may choose a log management or lesser SIEM solution that is better suited to the requirements of their operation.

In any of these, it is important to remember that a choice of more sophisticated SIEM capabilities is likely to result in higher acquisition, support and operational costs.

> “Early detection reduces time at risk and gives maximum visibility across data types and threats”

Core functionality for enterprises

The success of your security efforts depend on being able to anticipate and quickly respond to attackers and incidents when they occur. Whether you are trying to detect threats, manage the volume of alerts or provide incident or compliance reports, there are a number of core SIEM/Security Analytics features you should look for:

Flexible and comprehensive monitoring

For the best security reconnaissance across modern, distributed IT environments, security teams need collection, analysis and correlation of data from a wide variety of sensors, systems and applications.

Advanced threat detection

Early detection reduces time at risk and gives maximum visibility across data types and threats. Security professionals need the facility to detect, monitor, analyse and visualise threats at speed from across the environment.

User and activity monitoring

Analysis of the behaviour of users (anomaly detection) – whether at the endpoint or more broadly through a centralised SIEM is vital. This must include collection of logs that correlate user activity with thresholds, behavioural and contextual information; for example, by identifying suspicious activities or behaviour inconsistent with peer users.

Incident response and workflow support

Security operators need an Incident Management System (IMS) to manage, triage, allocate and record the status of security alerts. Like a communication system between stakeholders, the IMS ensures the relevant information about the investigation, containment, response and resolution of a particular incident is effectively recorded and communicated.

Threat intelligence

Both externally and internally sourced threat intelligence adds context to an event to increase the level of confidence in security decision making. The knowledge of the emergence of a particular type of attack being experienced by peer organisations can forewarn security operations centre (SOC) teams of an imminent threat; so too can knowledge of particular vulnerabilities currently existing in the organisation and requiring mitigation.

Stability and scalability

To avoid delays in threat detection and response, solutions must be capable of ingesting large data volumes for efficient and high speed analysis, querying and reporting.

> “Threat investigations are aided enormously by SIEM solutions that provide workflow automation and alert verification”

Advanced features and market differentiators

Future-proof your SIEM purchasing decision, by also looking for these emerging innovations that support SOC team operating efficiencies and speed to resolution:

Threat visualisation and MITRE ATT&CK® heatmaps

The MITRE ATT&CK® framework is one of the most useful technical knowledge bases to emerge to assist security teams in recent years. It classifies techniques used and observed by real attackers and presents them in an ordered and tabular form to reflect the ongoing progress of an attack towards its objective. Incident MITRE ATT&CK® screens reveal the nature and context of the attack, its progress and the identification of the preceding activity so as to identify root causes and mitigation efforts. It also enables SOC teams to anticipate emerging threats.

Advanced analytics and enrichment

Advanced analytics can quickly slice through masses of threat information to reduce the scale of the investigation problems. Machine learning and automated analytics can hasten information gathering and enrichment of data so SIEM solutions can quickly deliver situational awareness and actionable outcomes to greatly assist the efficiency of the SOC analyst.

Automation and workflow support

Threat investigations are aided enormously by SIEM solutions that provide workflow automation and alert verification to enrich data, assist workflows and support decision making. Replacing multiple standalone yet repetitive processes with automated workflows removes the need for time consuming manual processes; for example, correlating data from two separate threat detection sources. This facility also improves accuracy and unburdens analysts from the tedious and time consuming task of data manipulation.

Future-proofing technologies and processes

As businesses undergo “digital transformation” and shift focus to online customer interactions, security operations and solutions (like SIEM) must pivot to operate at a similar level of speed and efficiency across an array of cloud, on-premise and hybrid platforms.

Appendix: SIEM Buyer's Guide Checklist

Security Information and Event Management software (SIEM) is a mature market with most vendors offering similar features. However, there are differences in how each is designed and architected that contribute to varied user experiences.

Below is a list of considerations and questions to ask vendors.

Deployment

Data sources

- [ ] What data sources/devices are supported out of the box (OOTB)?
- [ ] How are bespoke or non-supported devices added? Can you perform this function yourself, if so, what skills are needed? Or is this something only the vendor can do, and if so, at what cost?

Platform

- [ ] What type of operating systems and database platforms are required?
- [ ] Does the SIEM deploy onto virtual machines, physical servers and Cloud?

Speed of analysis

- [ ] What is the upper processing threshold? This relates to analysis of incoming events not just inserting data into the database for later correlation. Be aware of the common problem of database contention; if data is being queried for analysis/correlation concurrently with other SIEM processes the performance throughput of the SIEM can be negatively impacted.

Useability

Configuration

- [ ] How easy is it for users to add new rules, alerts, dashboards and reports?
- [ ] Are open-source Threat Intelligence feeds supported OOTB and can commercial feeds be added? If so how?
- [ ] What support for compliance standards is available OOTB? Can additional new or different compliance requirements be added to the reporting function?
- [ ] Can the SIEM be configured to send reports to stakeholders that are not users of the system?

Operation

- [ ] How easy is it for operators to drill down and investigate threats?
- [ ] Does the interface support flexible creation of queries and reports – ideally without having to learn a new or specific query language?
- [ ] How easy is the solution to learn and operate – are advanced features too complex to work with?
- [ ] Does the SIEM have in-built Role Based Access to control who can see what information?

Processing efficiency

- [ ] How well does the system support analysts' workflows and how much time is lost by analysts moving between systems to run queries?
- [ ] Can known issues and false positives be filtered out so as to remove unnecessary noise?
- [ ] Can some analyst functions can be automated or streamlined?
- [ ] Does the SIEM support:
  - Cloud platforms as an input source?
  - Threat frameworks like MITRE ATT&CK®?
- [ ] How do these features help understand or deal with threats?

General

Operational management

- [ ] Does the SIEM have an inbuilt Incident Management capability? Can it integrate with your corporate system like ServiceNow, or Remedy?

Support services

- [ ] Where is the software support team located and can they be reached via email and telephone? Are SLAs important for system up-time?
- [ ] What is the structure of support? Is there a triage Helpdesk that assigns a ticket number etc. A common complaint is that it can be very difficult to find someone with the skill and experience to answer more than basic questions.
- [ ] What training is available and how is it delivered eg. on-line, instructor led?
- [ ] What is the pricing structure of the SIEM? Do you have to pay for agents? Some SIEM vendors have highly modular pricing models so it's best to not assume capabilities are included as they may cost extra.

The importance of a test driver

- [ ] When it comes to SIEM useability, the best way to verify vendor claims is with a test drive. Some solutions are pretty easy to setup and go while others can require the skills of a "data scientist" to make them work properly. That means operating and support costs can be chalk and cheese.

Be aware of costs, they can quickly add up - acquisition, support and operations

- [ ] The best choice of a SIEM relies on getting the right balance between acquisition, support and operational costs. Some SIEMs are comparatively cheap with an extensive range of sophisticated optional security capabilities while others offer a fully integrated set of SIEM functions.
- [ ] This is where you need to confirm, absolutely, your functional requirements; because invariably sophisticated, nice to have or even 3rd party add-on features can result in high integration complexity and cost. Often a reliable solution with organically integrated features designed from the ground up for streamlined operation delivers similar operational efficiencies at a much lower cost.

Want to find out more?

Register for a 15-minute demonstration of our SIEM

Register

Or contact your local Huntsman Security office (listed below) to talk to one of our team today.

About Huntsman Security

Huntsman Security's technology heritage lies in delivering cornerstone cyber security risk management, monitoring and response technology to some of the most sensitive and secure intelligence, defence and criminal justice environments in the world.

Huntsman®

HUNTSMAN | TIER-3 PTY LTD

ASIA PACIFIC

t: **+61 2 9419 3200**

e: **info@huntsmansecurity.com**

Level 2,
11 Help Street
Chatswood NSW 2067

EMEA

t: **+44 845 222 2010**

e: **ukinfo@huntsmansecurity.com**

7-10 Adam Street,
Strand
London WC2N 6AA

NORTH ASIA

t: **+81 3 5953 8430**

e: **info@huntsmansecurity.com**

GINZA EAST SQUARE 4F
3-12-7 Kyobashi Chuoku, Tokyo
Japan 104-003

huntsmansecurity.com linkedin.com/company/tier-3-pty-ltd twitter.com/Tier3huntsman