Guide

Essential Buyers Guide to SIEM

For Managed Security Service Providers

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. As a result, SIEM continues to be one of the most common technology purchases made by security operations teams, although there is a noticeable trend towards organisations supplementing some of their own security operational capabilities with external expertise. Managed Security Service Providers (MSSPs) are increasingly offering supplementary and specialist SIEM based security services to assist organisations address the complexity of successful cyber security management.

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.

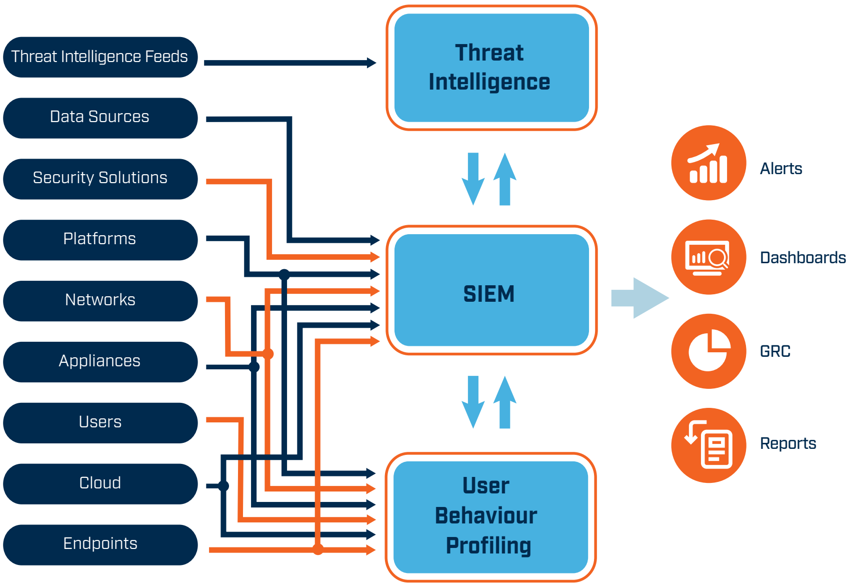

Fig 1. How a SIEM works

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 MSSPs

MSSPs look to a SIEM as the platform to support and deliver security monitoring and alert handling services to their customers. In targeting organisations of varying sizes, planning services of various levels of customisation or simply seeking to offer a standardised offering across their portfolio - the choice of the right SIEM is fundamental. The ability to cost-effectively provide both initial service offerings as well as future ones to the full range of your customers is a key to your success as an MSSP.

Challenges for buyers

For MSSPs, the economic, commercial and operational requirements are as important as technical security capabilities. The technical features determine the services that can be offered, and how cost effectively those services can be provided:

- **Wanting to grow a profitable business** - The reliability and flexibility of the system are important to minimise the time to onboard new customers so as not to impact the time to revenue. Also, the more streamlined the setup and configuration processes the better the scalability.
- **Needing to provide customer visibility or reports** - Having the ability to create customer reports across multiple tenants, while also informing operational performance and service levels at a glance through a web and mobile interface, ensures visibility of security activities for all stakeholders.
- **Wanting to offer services to large numbers of customers** - MSSPs need a multi tenancy capability as their operations expand to multiple customers. Low start-up costs, reduced cost of onboarding and operation are vital to fit with their revenue model.

Core functionality for MSSPs

For MSSPs the issue is very much the cost-effective delivery of core SIEM functionality. Those core technical functions for an MSSP are common with those important for Enterprise solutions. The capabilities of the technology however must support the cost-effective delivery of services offered:

Ease of adding new collectors (new types and new instances)

For MSSPs anything that delays or complicates the addition of a new customer can delay the commencement of services and therefore revenue. The ability to add new collection sources and configure the solution to accept new technologies must be straightforward.

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

Operational simplicity and workflow support

Where multiple customers are being served by one technology platform and one team, common operational tasks can be quick, easy and efficient to carry out. This translates to smooth operational processes and economies of scale.

Data management

Similarly, the management of data in an MSSP is sometimes complicated by the fact that different customers will have different data volumes and different data retention periods. The ‘industrialisation’ of MSSP service operations needs to ensure the task of collecting, storing and archiving data is configurable and automatic.

Flexible and comprehensive monitoring

For the best security reconnaissance across modern, distributed IT environments, MSSPs 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. MSSPs need the facility to detect, monitor, analyse and visualise threats at speed from across their customer environments.

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

MSSPs 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 other organisations can forewarn security operations centre (SOC) teams of an imminent threat; as can knowledge of particular vulnerabilities currently existing in customer organisations 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

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 SOC 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.

Market differentiators

In a mature market like SIEM, most vendors have comparable functionality, but not all are built with MSSP customers in mind. Careful attention to those aspects of the technology that facilitate quick setup of multiple customers, ease of adding additional services and efficiency of operations will directly impact the profitability of an MSSP service.

True multi-tenancy

The hosting of multiple customers with a range of requirements on a single platform means scalability and huge operational efficiencies; both at the time of purchase as well as ongoing operation. Some solutions approach this segregation of customer data on an access control basis while others offer full data sovereignty for each tenant. A SIEM that offers data sovereignty across all tenants can make a significant difference in cost savings for both MSSPs and customers that are seeking confidence in the protection of their data.

Standardised configurations

For MSSPs the ideal situation is to build a set of standardised services that can be easily replicated and sold for rapid on-boarding. Standard templates for data collection, analysis and alerting rules can therefore be packaged for easy adoption.

> “For MSSPs the ideal situation is to build a set of standardised services that can be easily replicated and sold for rapid on-boarding.”

Web and mobile dashboards and reporting

Increasingly customers are seeking greater visibility of the service, granular alert and incident details and performance reporting against service levels. The MSSP SIEM technology needs to provide customer portals that clearly publish customers’ security and service performance levels.

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

Multi-tenancy

□ Does the SIEM have multi-tenancy capacity to enable you to manage ALL your customers on a single platform with a single screen for lower up front and operating costs? Or do you need to deploy a standalone platform for each customer?

□ What scope is there to vary the settings, policies, alert and risk profiles of different customers based on their needs or budgets? Can you deliver this from a single platform?

□ Does the vendor also offer managed security services that will potentially compete with your own?

Licencing arrangements

□ Is the SIEM cost model in line with your MSSP services revenue model? The traditional Capex, and even some subscription, models can mean upfront set-up costs, "per customer" charges that can significantly delay payback periods; an MSSP can end up with high levels of commercial risk. Ask about Opex and pay-as-you-go cost models.

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 out of the box? 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

Customer portal

□ Reporting requirements of MSSP end-customers have changed significantly in recent times. With customers now increasingly focused on security, standardised weekly or monthly "beige" reports are no longer adequate. Customers are looking for clear visibility of their security status with access to real-time information via a web portal or a mobile device.

Operational management

□ How easy is it to add a new customer or new group of systems to the SIEM platform?

□ How easy is it to (a) configure and copy across standard settings and policies to a new set of customer systems; and (b) define customer specific requirements in support of their unique service needs?

□ Does the platform include the features that support the core services you are looking to offer?

□ Does the platform allow the extension of add-on service capabilities in ways that customers might reasonably require?

□ 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