White Paper

# The Essential Guide to SIEM

## Next Generation Security Monitoring

Huntsman®
Defence-Grade Cyber Security

# What is SIEM software?

Security information and event management (SIEM) software gives information security professionals insight into and a track record of the activities within their IT environment.

SIEM technology has been in existence for more than a decade, evolving from simple log management solutions that acted as data repositories.

It combines:

### Security Information Management (SIM)

SIM collects and analyses log and event data into correlated and simplified formats, which is ideal for long term storage.

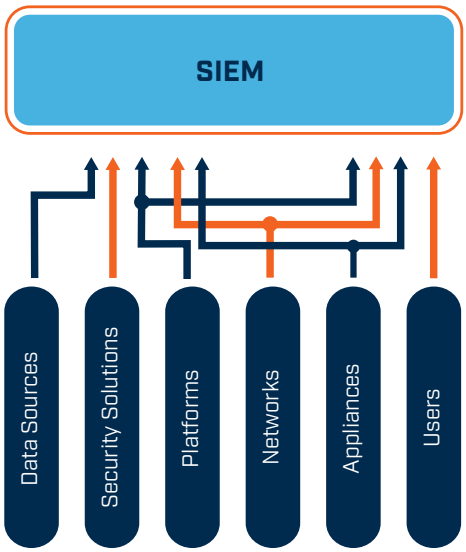
### Security Event Management (SEM)

SEM provides more complex security event management than SIM. Capabilities include real-time threat analysis, ticketing, incident response and security operations.

As the drivers for SIEM have evolved from pure operational data gathering, through compliance to providing effective cyber security defence; some of the next generation solutions now expand into deeper security analytics, incident management and automation/orchestration.

## How SIEM works

SIEM software collects and aggregates log data from across the organisation's technology infrastructure, from host systems and applications to network and security devices such as firewalls and antivirus gateways.




### Traditional SIEM

The software collects, stores, analyses and identifies incidents and events, before categorising them for resolution. SIEMs deliver on three main objectives:

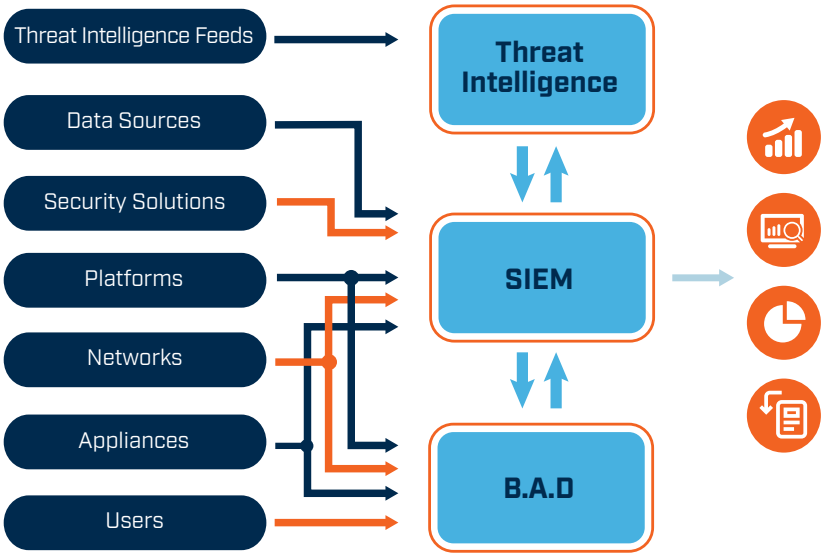
- To provide reports on security-related and activity-related events and incidents, such as successful and failed logins, application accesses, network connections, malware activity and other possibly malicious activities;
- To identify and send alerts of potential security issues if analysis shows that an activity appears suspicious or, in fact, breaches predetermined policies, filters or rules;
- To enable access to collected data for investigative analysis during the threat/incident resolution process; dashboards, charting, reports and queries.

Business requirements for better compliance management drove much of the early adoption of SIEM. This emerged for two reasons:

1. It was necessary to have controls in place;
2. To provide evidence of their operational effectiveness.

Auditors needed these records to see whether compliance standards such as the Payment Card Industry Data Security Standard (PCI-DSS) or other internationally recognised security frameworks were supported by fully operational controls.

# The Emergence of Analytics and Intelligence




## Next Generation SIEM

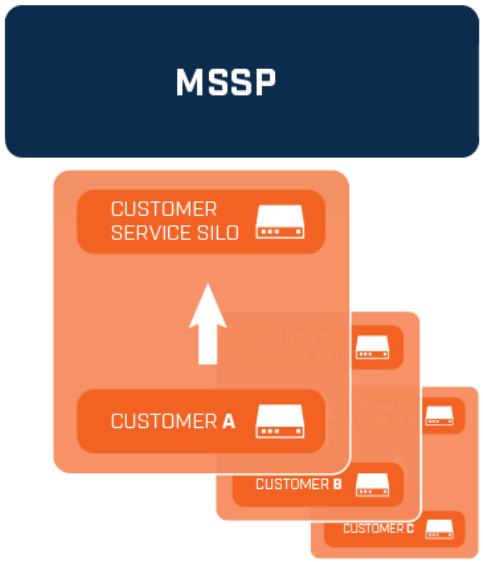
The scale and growing sophistication of threats to which businesses can fall prey has driven the need for greater security; new capabilities have emerged. To this end, next generation SIEMs:

- Provide Security Analytics capabilities that incorporate Behaviour Anomaly Detection to identify unusual or suspicious patterns of activity and gain more insight into whether an activity indicates attack or misuse;
- Import enriched Threat Intelligence from various sources for correlation and analysis with traditional log, event and network data;
- Manage large volumes of data using machine-based learning and correlation for faster and more accurate detection of threats and informed decision making;
- Utilise automation of analyst workflows and playbooks to validate, report on and respond to threats.

## Are SIEM solutions for all organisations?

SIEM software is mostly used by medium to large organisations, where compliance to regulations or the need for auditable security controls is compulsory - and where monitoring is operationalised in an on-premise Security Operations Centre (SOC).

Generally speaking, small companies don't have the governance requirements or the levels of dedicated skills or resources needed to maintain a continuous SOC function. However, all sizes of businesses can have access to security monitoring functionality via Managed Security Service Providers (MSSPs) or other third-party providers.




Information Security service providers use highly capable multi-tenant SIEM technology to meet the varying requirements of customers within their portfolio.

## SIEM within the Cloud

Many large enterprises and government departments run SIEM and security monitoring software on-premises; due to the sensitive nature of the data they manage and the volumes of data generated from their large IT estates.

However, MSS and SaaS offerings are becoming more main-stream in both hybrid and cloud platforms. As Machine Learning and Security Analytics capabilities improve on these platforms the migration or expansion of security governance to sit within the cloud is an inevitable outcome of digital transformation for organisations.

## The six key capabilities of Next Generation SIEM

There are six essential capabilities of a modern analytics-driven SIEM:

| Feature | Benefit |
|---|---|
| **REAL-TIME MONITORING** | Early detection reduces time at risk. Security Analysts need real-time collection and correlation of data for faster analysis and high confidence decision making. |
| **ADVANCED THREAT DETECTION** | Security professionals need an accessible tool to detect, monitor, analyse and visualise threats at high speeds from across the environment. |
| **USER MONITORING** | Behaviour Anomaly Detection is vital; collection of logs that correlate user activity with threshold, behavioural and contextual information to highlight policy breaches or other anomalous incidents of concern. |
| **THREAT INTELLIGENCE** | Both externally and internally sourced Threat intelligence can add context to an event to improve confidence in determining its riskiness and priority. |
| **ADVANCED ANALYTICS** | Analytics quickly refine masses of threat information to manageable proportions. High levels of machine learning and workflow automation deliver situational awareness for enhanced analyst insights and dramatically reduced response times. |
| **INCIDENT RESPONSE** | A Security Operations team needs an Incident Management System to systematically manage, triage, allocate and record the status of security alerts. This ensures the processes of detection, understanding, containment, response and resolution are comprehensive, documented and visualised to improve the existing threat knowledge bases. |

## The six reasons to upgrade to Next Generation SIEM

Where older approaches to log and activity collection, reporting, analysis and management have become inadequate or unwieldy, the advancing nature of technology solutions means that current state-of-the-art technology is likely to be a considerable leap in functionality and capability from a legacy solution.

The success of your organisation's security defence is dependent on you being able to anticipate and quickly respond to attackers and incidents when they occur. Here are some of the key reasons information security managers have cited for upgrading their traditional approaches. If you recognise these challenges then it is undoubtedly time to consider modernising:

| Challenge/ Drawback | Impact on Operations |
|---|---|
| **LIMITED SUPPPORT FOR SECURITY DATA** | The ability to monitor only a limited range of data types introduces the risk of not seeing the full security picture or missing vital corroborating information for the data that is collected. |
| **DATA COLLECTION ONLY** | Solutions that are optimised for data ingestion and storage alone can compromise important SIEM threat detection capabilities that have been added on as an after-thought. |
| **SLOW INVESTIGATION SPEED** | Threat investigations can be much slower in solutions that don't provide any automation or correlation/ verification of alerts. Consequently, analysts have to undertake each stage of the investigation process manually; all of which takes time. |
| **INADEQUATE STABILITY AND SCALABILITY** | Some solutions are unable to ingest large data volumes and analyse/query/report on them at the same time. This leads to slower generation of results and delays in threat detection that can mean by the time you are able to respond the problem has worsened. |
| **LIMITED INTEGRATION** | Technologies need to interoperate and collaborate across the IT eco-system to maximise the efficiencies from centralised data collection, analysis and investigation. Without this it is difficult to deliver a comprehensive defence against the changing cyber landscape. |
| **INSUFFICIENTLY FUTURE-PROOF** | As businesses undergo the inevitable "digital transformation" and shift focus to on-line/connected customer interactions, the security operations and solutions (like SIEM) that underpin them must also be able to operate across an array of cloud, on premise and hybrid platforms. |

## Choose the right SIEM for your business

You should always evaluate products based on your organisation's requirements to determine which best meet your needs. Here are a few examples:

### SIEM for Compliance Reporting & Auditing

If you want a SIEM primarily for compliance reporting and audit support you will value capabilities such as the integrity of the data collection, evidential capabilities, report outputs, dashboards and longer term data management.

### SIEM for improving Cyber Security Posture

If your organisation is looking to improve its cyber resilience, you'll need a more comprehensive approach than a compliance-focused operation. The key capabilities you should think about adopting are advanced security analytics, behavioural anomaly detection and threat intelligence. These enhancements will arm you with enriched data and the improved insights required for threat hunting.

### SIEM for large environments

If you operate in an enterprise organisation, with petabytes of data to protect, you will need high speed analysis; high levels of automated operation; machine learning; distributed, scalable storage and incident resolution capabilities.

### SIEM for organisations with a low level of cyber risk

Organisations that have lower levels of assessed cyber risk may choose a more commodity based product with modest features and simplified management features. There is also the option of a third party-service.

## Other considerations when selecting a solution

As an Information Security Manager you need to take into account numerous other factors. For example, the initial cost of SIEM software and ongoing support can be quickly exceeded by the operational cost of maintaining a SOC and the people who staff it, not to mention the increasing cost of monitoring larger volumes of data and its ongoing storage. Security resources of all types can become costly to maintain.

The Total Cost of Ownership can be complex to establish once you go beyond easy factors such as the solution price; you will need to include operational workloads required to configure and operate the technology stack as part of the wider process; whether it is on premise or MSSP sourced.

Regardless of your selection criteria for SIEM, you should always take into consideration the level of flexibility engineered into the solution to meet your on-going needs. Having expert local support will allow you to achieve the maximum benefit from your solution; there is no substitute for an experienced engineer who can work with you to meet your objectives in your environment.

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**

Awajicho Ekimae Building 5F
1-2-7 Kanda Sudacho
Chiyodaku, Tokyo 101-0041

**AMERICAS**

toll free: **1-415-655-6807**

e: **usinfo@huntsmansecurity.com**

Suite 400, 71 Stevenson Street
San Francisco California 94105

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