DEFENSE.COM™

WHITE PAPER

The essential guide to Security Information and Event Management (SIEM)

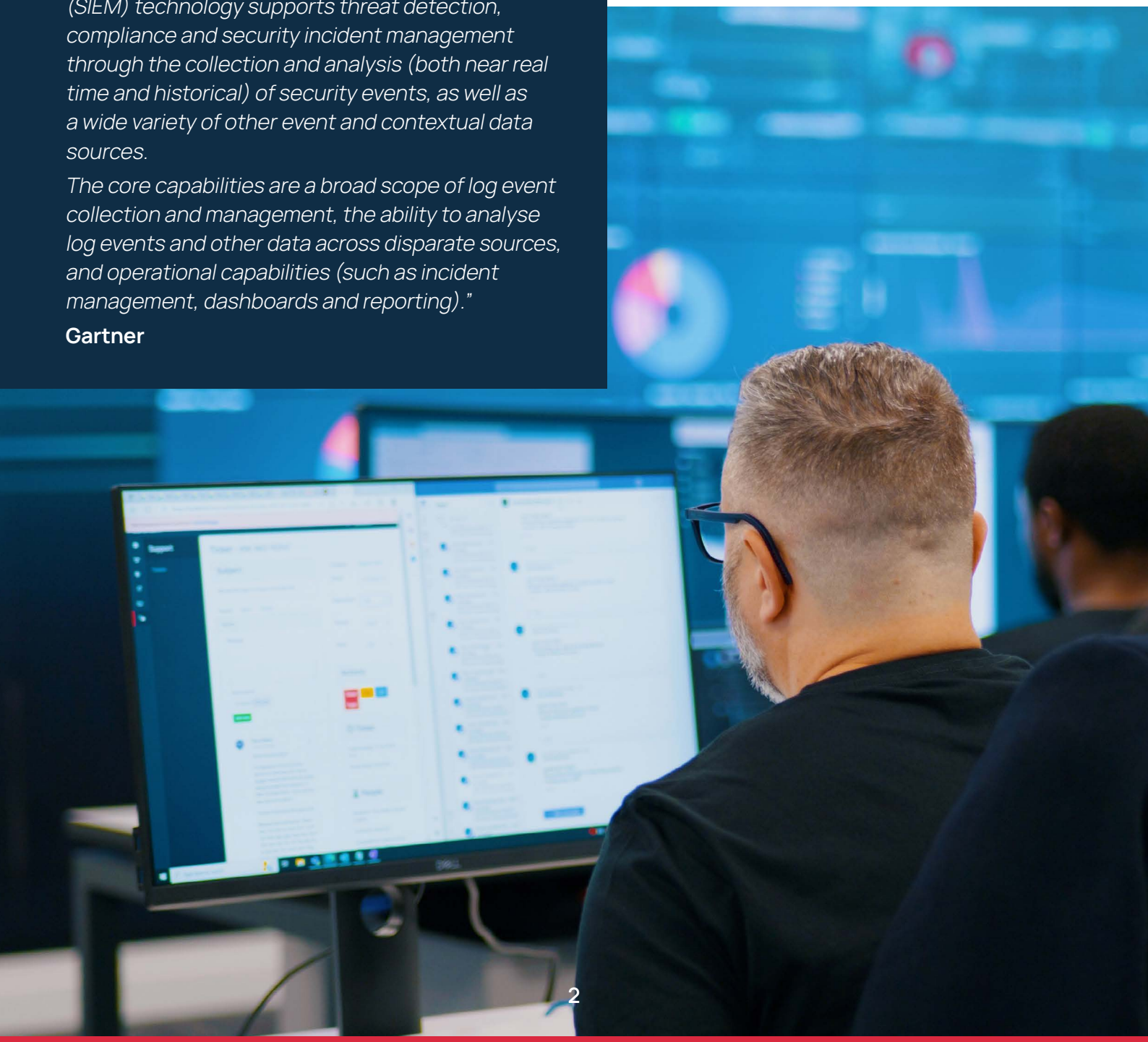
What is SIEM?

Security Information and Event Management (SIEM) tools collect and aggregate logs and event data from servers, endpoints, network devices, cloud systems and other devices. SIEM helps businesses to detect suspicious activity, address security threats and maintain compliance.

The term 'SIEM' was first introduced by Gartner in 2005. Here's how they define it:

> *"Security information and event management (SIEM) technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources.*
>
> *The core capabilities are a broad scope of log event collection and management, the ability to analyse log events and other data across disparate sources, and operational capabilities (such as incident management, dashboards and reporting)."*
>
> **Gartner**

While a SIEM solution does a lot of the hard work to highlight security issues, it is just the technology. A SIEM needs security analysts (usually as part of a SOC team) to configure, investigate and review the alerts in order to promptly respond to threats.



How does it work?

SIEM solutions combine two different technologies, SIM and SEM:

SIM

Security Information Management (SIM) refers to the collection, aggregation and analysis of log files, and is also known as log monitoring. Every application, networking device, workstation and server creates log files, which are required to monitor system and network activity. Security teams need to be able to search these logs to diagnose issues or investigate potential threats.

SEM

Security Event Management (SEM) is the process of detecting, correlating and evaluating security alerts and events in order to identify threats. SEM helps to parse security events from different systems and raise alerts based on pre-defined detection rules.

When combined together, SIEM solutions collect, store and analyse security telemetry from multiple sources for the purposes of threat detection and compliance. By aggregating and parsing data from all areas of an environment, SIEM tools make it easier for companies to identify suspicious activity and investigate security events.

Why use SIEM?

Centralised log data: The core benefit of log monitoring is that the tool stores all log files centrally, making it easier to search, manage, monitor and store log data from one place.

Faster response: Log monitoring tools automate processes, such as raising security alerts in real-time, to enable faster and proactive incident response.

Optimise performance: The insights gathered about an application enable you to understand its usage, so you can identify inefficient configurations and fine-tune its performance.

Event correlation: Aggregating security telemetry from multiple sources helps security analysts make informed decisions on how to investigate and respond to incidents.

Improved security: Proactively identifying security threats and suspicious behaviour helps your organisation to defend against attacks and prevent breaches.

Compliance: To remain compliant with standards such as ISO 27001 and PCI DSS, the retention of log data is necessary to show that your organisation demonstrates a high level of information security and protects customer data.

Types of log data

A SIEM solution can only inform you of potential security threats to the areas of your business it is monitoring. That means it's important to understand exactly what types of log data you are collecting.

The following log types are a good starting point for any environment:

- System-level logs
- Network logs
- Logs from security investments such as endpoint protection products and application firewall

Additionally, logs such as audit logs, cloud logs, and application logs contain valuable information that can be correlated with other log types to provide a more complete understanding of your security landscape. Maximising coverage and enabling relevant correlation rules based on specific log data sources, such as security events from AWS or Microsoft 365, is highly recommended.

Logs contain very granular details such as timestamps, user actions, error codes, and other relevant metadata, which provides a clear picture of what occurred in your systems for effective troubleshooting, debugging, and analysis. Additional contextual information may also be available via log data, such as session IDs, request headers, and detailed stack traces, which are useful for diagnosing complex issues.

Ultimately, the more data you have to bring into your SIEM solution that provides security value, the easier it is to form correlations and conduct investigations. Here's some examples of log sources that can be collected and analysed for security incidents:

- WAF, Load Balancers, etc.
- Office 365
- Firewalls, switches and routers
- AV/endpoint
- Windows/Linux servers
- All AWS services (EC2, Lambda, CloudWatch, etc.)
- All Azure services (Event Hubs, AD, ATP, etc.)
- Custom application logs
- Cloud services (GCP, Mimecast, Salesforce, etc.)

High fidelity vs. low fidelity alerts

High fidelity and low fidelity refers to the level of detail and context that a security alert provides. Combining these two types of alerts from your log data gives your business a much better understanding of what is happening in your environment when a security event occurs.

High Fidelity

A high fidelity alert could be a clear indication that a security incident or data breach has already occurred. This type of alert usually provides enough context on its own for a SOC analyst to instantly understand that it is a genuine issue that needs attention. These type of alerts usually contain detailed information about particular security events, actions and system activities.

Endpoint protection tools can be a great source of high fidelity alerts. For example, the detection of Mimikatz on a host would almost certainly indicate malicious activity that requires immediate attention. SOC teams can be presented with an overwhelming number of security alerts every day, as a result, these types of alerts should be prioritised by analysts and investigated as soon as possible.

Low Fidelity

Low fidelity alerts can include day-to-day events like user logins, which may not directly be an indication of compromise but can provide context when investigating high fidelity alerts. Low fidelity alerts are therefore typically not actionable on their own and need further context before a decision can be made.

A low fidelity alert could be multiple failed login attempts from a single IP address. This can be considered as low fidelity because it may be triggered in legitimate scenarios where a user forgets their password or accidently mistypes it multiple times. Such situations may not always indicate malicious activity; however, patterns like this from low fidelity alerts should be monitored as they may indicate a potential brute-force attack.

Getting the most out of your SIEM

SIEM solutions can be invaluable for businesses when deployed and monitored properly. Configuring and tuning the SIEM deployment based on the needs of your environment is the key to unlocking its full value. With focused effort on priority assets and systems, behavioural profiling, detection coverage and response integration, your SIEM can reach its ROI potential.

Here's some tips on how you can get the most out of your SIEM:

1 **Understand your environment:**
Take the time to thoroughly understand what requires protection and prioritisation. Knowing where sensitive data is held or processed, as well as your overall attack surface, allows you to tailor the monitoring to focus specifically on those high-priority areas.

2 **Establish a baseline:**
Get a sense of the day-to-day interactions and operations of your systems. This allows you to define normal behaviour patterns, which will make it easier to identify anomalies and potential threats. For example, by monitoring normal user activities and system events, you can spot and investigate suspicious behaviour.

3 **Correlate your data:**
Combine high fidelity alerts that indicate significant security events such as blocked malware attacks, with low fidelity alerts that capture routine activities, such as user logins. Combining these two types of alerts helps you to enrich your data, correlate events and identify potential threats.

4 **Use the right resources:**
Effective security operations management requires the right expertise. If your organisation does not have a dedicated security team or resource, consider a managed SIEM solution with an outsourced Security Operations Centre (SOC). An outsourced SOC will detect and investigate threats on your behalf, freeing up your team to focus on other tasks.

5 **Incorporate SIEM into your incident response strategy:**
Include log data analysis in your incident response training. During an incident, log data can provide vital indicators that guide the appropriate next steps. Ensure that your internal team is well-versed in the use of the SIEM solution and the incident response process, allowing for a quick and effective response.

Managed SIEM

As SIEM tools rely on security experts to monitor the alerts generated, businesses often prefer to choose a managed SIEM service. This is where a vendor will deploy SIEM technology to your environment and monitor it via their own SOC team to detect cyber threats 24/7 on your behalf. As many businesses don't have the experience or budget to build and manage a SOC in-house, outsourcing is a more affordable and valuable option, delivering comprehensive security coverage and greater ROI.

However, it's important to note that a managed SIEM solution will detect threats, raise alerts and provide remediation advice, but this service doesn't typically respond to threats or remediate issues on your behalf.

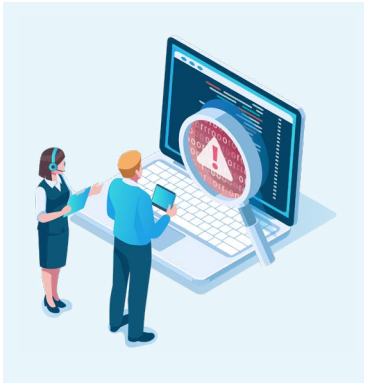
> *"Many businesses don't have the experience or budget to build and manage a SOC in-house, outsourcing is a more affordable and valuable option.*

What is a SOC?

A Security Operations Centre (SOC) combines people and processes with technology. SOC analysts conduct round-the-clock monitoring of an organisation's IT infrastructure, often by using SIEM technology, to quickly identify and investigate potential cyber threats.

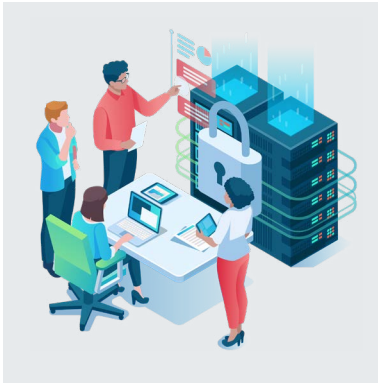
SIEM
Security Information Event Management
The technology

+



SOC
Security Operations Centre
The people

=



Managed SIEM Service

Why choose a managed SIEM service?

Managed SIEM providers have a team of security experts who handle everything from deployment and configuration to maintenance of the SIEM solution. A managed SIEM service usually includes 24/7 monitoring, alerting, and a basic level of incident response, ensuring that any security issues are promptly addressed.

A managed SIEM service offers several benefits such as:

Cost savings – Managed SIEM services reduce internal resource requirements and costs by eliminating the need for an in-house SOC team and SIEM infrastructure.

Rapid response – SIEM tools contextualise security data for rapid incident response and remediation guidance from the external SOC team.

Expertise – SIEM providers leverage experienced analysts trained to analyse security data, reduce false positives, and highlight genuine incidents.

24/7 monitoring – SIEM providers offer 24/7 monitoring to identify threats at any time, not just during business hours.

Choosing the right solution for your business will depend on your requirements and your internal resources.

Operating a SIEM solution in-house may suit businesses that:

- Already have their own SOC team that know how to setup, tune and operate the SIEM
- Need to retain complete control over business monitoring
- Have enough resources and knowledge to interpret logs and action intelligence independently
- Already have technology that can quickly mitigate cyber threats or block attacks
- Can deploy 24/7 threat monitoring and incident response via staffing or automated alerting.
- Understand cyber risks to their business and how a SIEM solution can detect suspicious activity.

Outsourcing to a managed SIEM provider may suit businesses that:

- Don't have any internal resources dedicated to security, such as a SOC team
- Want to conduct security monitoring but don't have an existing SIEM or the time to maintain one
- Don't have the time, resource or expertise to proactively threat hunt or identify attacks
- Don't have an internal team to cover 24/7 threat monitoring requirements
- Require extra support to triage incidents and get step-by-step remediation advice
- Have limited budget to build or maintain a SIEM or SOC in-house

Summary

SIEM is an effective solution for identifying security events and incidents. It offers organisations a centralised place to collect, aggregate and analyse security telemetry, resulting in faster and more accurate threat detection. As part of a wider cyber security strategy, SIEM can help you proactively defend against cyber threats and protect your business critical assets.

Here are some takeaways to remember if your business is thinking about implementing a SIEM solution:

- SIEM tools require constant monitoring and tuning to be effective
- The more log data you can ingest into your SIEM that provides security value, the better
- Combining high and low fidelity alerts helps to contextualise and investigate threats
- Your SIEM deployment should be tailored to your unique environment and business needs
- Consider outsourcing as a cost-effective alternative to building in-house

Defense.com gives me peace of mind that a full team of qualified security professionals are working to meet our SIEM, SOC, and MDR needs. This is the only solution we've found where we trust the vendor has a robust product and security team in place, but is not charging what the enterprise companies can afford to pay."

Tracey Cawdrey, Development, Security and Compliance Manager, LOCTA

About Defense.com

Defense.com offers a Managed SIEM service delivered by a team of UK-based expert SOC analysts.

- **Deploy anywhere**
  Collect security logs from any source, including endpoints, applications and cloud systems.
- **Uncover threats**
  Never miss a security risk with experienced SOC analysts monitoring your network 24/7.
- **Prevent breaches**
  Quickly respond to threats with clear, step-by-step remediation advice.
- **Stay compliant**
  Meet the requirements of PCI DSS, ISO 27001 and more with proactive SIEM log monitoring.

Learn more

+44 (0)1438 500 209 contact@defense.com www.defense.com