itb
cyber solutions

LOGPOINT

GETTING STARTED WITH SIEM

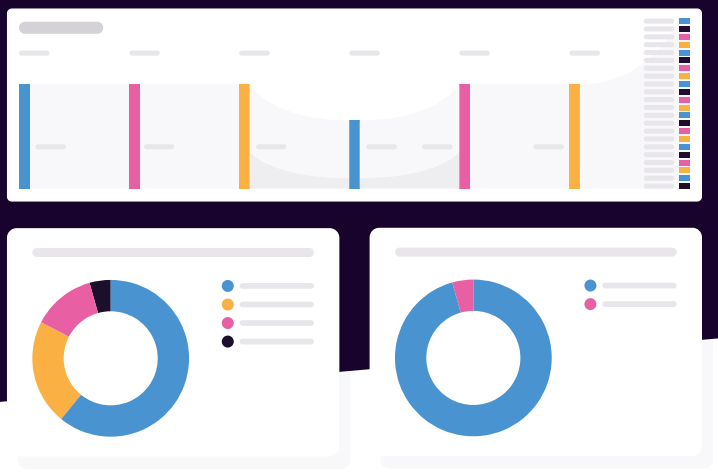
Considering investing in a leading security solution? Here's where to begin implementing it.

As enterprise technology becomes ever more intuitive and consumerized, it's easy to assume new tools can be implemented with minimal human intervention. With security information and event management (SIEM) that's largely true, but even the most modern solutions need to be set up for success.

So where do you begin?

Implementing a SIEM solution can be confusing if you're working without a guide. There's a lot to consider: which logs to ingest, what rules to set, what are the business-critical network assets that need to be prioritized?

The answers will differ from one organization to the next. To get your journey started we've outlined some essential questions and best practices. Follow these steps and ensure your SIEM investment delivers full value.



QUESTIONS YOU NEED TO ASK

1. What are the crown jewels in our system?

STEP 1	STEP 2	STEP 3
Look across the IT estate and ask, 'which network elements would expose the business to serious damage if they were hacked?' *For example:* sensitive network infrastructure, data repositories holding customer information, data assets with financial information or IP.	Look at the supporting systems that enable, interact with, or protect the crown jewels.	Consider the threats to each of these systems. *For example:* How do these threats behave and manifest in my network? Where are the vulnerabilities threats of this nature could potentially exploit?

2. What do I need to monitor, and how do I ensure that I see it?

STEP 1	STEP 2
Consider the network events and activities you might be missing, and that you want your SIEM solution to capture and flag up. *For example:* Make a list of the anomalies, indicators of compromise, and other potentially adverse effects of a breach or attack. • Then consider how they could manifest in devices, in end-user behavior, or network architecture. • The exercise needs to encompass software, hardware, Cloud services, and external service providers.	Given the breadth of this exercise, use industry standards to guide you. For example: Consider following NIST's cyber security framework. It offers a standard list of critical detections and follow-up processes organizations should adhere to. • It's also useful to reference the Mitre ATT&CK framework. It explains how different types of cyber-attack execute and how attack phases can show up in the network.

3. Logs and events: a Mitre framework top 10

Using the MITRE ATT@CK framework we've pinpointed 10 sensitive log and event clusters your SIEM solution should monitor.

For each one we've included **the tactic** (the goal the attacker wants to accomplish), **the technique** (how they would seek to accomplish the goal), and **what to look for** in each cluster.

	TACTIC	TECHNIQUE	ACTION
1 **User Authentication Events**	Initial Access, Defense Evasion, Persistence and Privilege Escalation	Valid Accounts (T1078)	Track successful and failed logins, especially for privileged accounts. Look for unusual login times or attempts from unexpected locations
2 **Email Activity and Phishing Attempts**	Initial Access	Phishing (T1566)	Review email logs to detect suspicious email attachments, URLs, or phishing patterns
3 **Account Creation and Privilege Escalation Logs**	Persistence and Privilege Escalation	Valid Accounts (T1078) and Create Account (T1136)	Monitor for new user account creations and privilege changes which could signal attempts to establish persistence or escalate privileges
4 **Process Creation Logs**	Execution	Command and Scripting Interpreter (T1059)	Monitor process executions and commands run on endpoints. Look for unexpected or suspicious processes, particularly those associated with system utilities like cmd.exe and powershell.exe
5 **File Modification Events and Registry Changes**	Defense Evasion	Impair Defenses (T1562) and Modify Registry (T1112)	Detect changes to critical system files that adversaries use to circumvent defense mechanisms, such as uninstalling applications and disabling antivirus or other important protection features Look for signs of unauthorized modification, which may indicate tampering or malicious code injection
6 **External Network Traffic (DNS, HTTP, HTTPS)**	Command and Control	Application Layer Protocol (T1071)	Look for DNS requests and outbound traffic to suspicious IP addresses or domains to detect Command and Control (C2) activity, such as data exfiltration or communication with malware
7 **Endpoint Security Alerts**	Execution	System Services (T1569)	Collect logs from endpoint security solutions (e.g., antivirus or EDR) Look for alerts indicating malware detection, suspicious activity, or unauthorized access to sensitive files
8 **Network File Shares Access**	Collection	Data Staged (T1074)	Monitor access to network shares, particularly for bulk file access, deletion, or encryption, as this can signal data exfiltration or ransomware
9 **Scheduled Task Execution**	Execution, Persistence, Privilege Escalation	Scheduled Task/Job (T1053)	Look for the creation or modification of scheduled tasks, especially outside of typical IT maintenance periods
10 **Suspicious or Unusual Network Behavior**	Lateral Movement	Lateral Tool Transfer (T1570)	Look for unusual file creation events, shared folder access, and network connections, which can be indicative of lateral movement of attackers transferring tools via shared directories.

WHAT ELSE SHOULD I CONSIDER?

It's important to look at the impact of log ingestion on other aspects of network operations.

For example:

Performance

Ingesting every possible log can be complicated and expensive, while processing large volumes of log data can take a toll on performance.

- Ensure that your hardware and software are scalable and have sufficient capacity to handle the current volume an accommodate future growth.

Storage

Every SIEM customer needs to establish how long they will need to store log messages.

Considerations include:

- **Compliance** - PCI, GDPR and corporate policies can all dictate which data needs to be kept and the data that needs to be discarded
- **Legal and administrative** - Look at use cases where having a log message would be beneficial after the fact; for example, handling a copyright claim against a student who downloaded movies on the university network
- **Cost** - log messages take up disk space, and disk space costs money. Some vendors even charge for the amount of data stored using their solutions

Make SIEM your co-analyst

Cybersecurity attacks can reveal themselves in many ways across multiple systems, but without a central console there's no way to see all the indicators all at once. That's what an effective SIEM should deliver – a way to catch the important signals, analyze them, and decide which need interrogation.

Once it's set up and working, your SIEM solution should augment your SOC analyst team, helping overcome alert fatigue by piecing together and prioritizing all the disparate signals and indicators that network devices throw up.

Want to know more?

At ITB, we've been helping organizations successfully implement SIEM solutions acrosss in-house and managed SOCs. Contact us at solutions@it-b.co.uk or visit WWW.IT-B.CO.UK for more information.