LOGICALIS
Architects of Change

Microsoft

Unifying fragmented defences to form Intelligent Security Operations

Why SIEM is the foundation of modern cyber resilience

Digital transformation: How organisations operate

With hybrid and multi-cloud platforms scaling, hybrid working expanding, and AI shaping the pace of innovation, the traditional perimeter has dissolved. Cybersecurity teams are now responsible for protecting a sprawling and constantly shifting digital ecosystem of identities, data, devices, and services.

Despite significant investment in cybersecurity, threats continue to evolve faster than many organisations can respond. Tools are no longer the issue; fragmented visibility is. Scattered security insights across multiple systems and dashboards lead to IT teams missing critical signals. Security must move beyond isolated tools to become unified intelligence, and this is where Security Information and Event Management (SIEM) comes in.

A blind spot is still a blind spot, no matter how many tools you throw at it.

Many organisations already own powerful security technologies, but they need to be actively managed, tuned, and aligned with business objectives — this is the part most organisations forget about. Even the best security team can become overwhelmed by the sheer volume of alerts and data, leading to missed threats and ineffective security programmes.

Defence against the cyber attack arts

Brute force attacks and technical expoits are outdated

Microsoft's research shows a growing pattern: adversaries increasingly compromise legitimate identities and access to blend into everyday operations, making them much more challenging to detect. Threat actors now operate with speed and precision, aided by automation and AI. The first sign of an attack may only appear after they've already gained access to what they're looking for.

A SIEM changes the defender's position. It brings diverse signals together into a coherent picture, highlights suspicious behaviours before they become disruptive, and enables faster, more informed intervention.

Microsoft Sentinel plays a transformative role here. As a cloud-native SIEM, Sentinel ingests telemetry from identities, endpoints, workloads, networks, applications, and other sources, correlating seemingly unrelated signals into a coherent, risk-informed picture. Microsoft Sentinel enhances threat detection by:

- **Applying advanced analytics and behavioural modelling to detect malicious actions hidden within legitimate credentials**
- **Harnessing Microsoft's extensive global threat intelligence to identify evolving attacker tactics in real time**
- **Enabling AI-driven investigation tools that reduce the time between detection and response**

Sentinel recognises the difference between ordinary activity and actions that indicate intent, helping security teams see early warning signs before they escalate into business disruption.

SIEM, camera, **action!**

From chasing alerts, to anticipating adversaries

Through our global Security Operations Centres (SOCs), we provide:

- **Continuous monitoring with dedicated analysts**
- **Rapid response to emerging threats**
- **Ongoing detection development based on real-world activity**
- **Threat intelligence aligned to business risk**

Boards and executives now ask practical, business-critical questions:

- **How effectively can we detect threats that target our operations?**
- **How quickly can we respond to an emerging incident?**
- **Do we truly understand the risks in our environment?**

A SIEM managed by Logicalis provides confident, evidence-based answers aligning cybersecurity with resilience, business continuity, and stakeholder trust.

A secure organisation isnt one that simply owns security technology

The maturity of your cybersecurity is no longer defined by how many tools you have, but by how many threats those tools prevent. A modern SIEM, like Microsoft Sentinel, is more than a repository of alerts; it's the active intelligence layer that transforms signals into clarity and action.

To keep yourself protected from evolving cyber threats, your visibility has to keep up and grow, too. The combination of Microsoft Sentinel and Logicalis' managed security expertise can ensure your organisation comes out ahead of the threats it faces.

Contact Logicalis today, and our team of cyber security experts can keep your business protected against cyber threats!

Keep my business safe!