Managed SIEM for Microsoft Sentinel

Get confidence, control, and continuous protection — without building a SOC.

Why Managed SIEM for Microsoft Sentinel?

24/7 Detection. Triage. Response.

Microsoft Sentinel delivers powerful visibility — but without continuous tuning, investigation, and response, alerts quickly become noise. CyberStash's Managed SIEM for Microsoft Sentinel transforms raw signals into validated incidents, guided response, and measurable risk reduction.

Our Approach

- **Operated, Not Observed** – We run Microsoft Sentinel as a living security capability, not a dashboard.
- **Threat-Led Detection** – Tuned analytics and custom use cases aligned to real attack paths.
- **Proactive Defence** – Ongoing tuning and threat hunting to reduce blind spots over time.

Key Benefits

- **Immediate Threat Clarity** – Understand real security incidents, not alert volume.
- **Reduced Cyber Risk** – Detect, investigate, and contain threats before impact.
- **Operational Assurance** – 24/7 monitoring aligned to enterprise and regulatory expectations.
- **Informed Decisions** – Executive-ready reporting that drives action, not confusion.

From Alert Noise to Action

- Continuous monitoring and analyst-led triage across identity, endpoint, cloud, and email.
- Structured investigations with clear scope, impact, and remediation guidance.
- Automated and guided containment actions through Microsoft security controls.
- Clear reporting built for security teams and leadership — no jargon.

Stay protected. Stay informed. Stay in control.

Value & Outcomes

- **Instant SOC Capability** – Gain immediate access to experienced analysts, responders, and detection engineers without hiring or onboarding delays. A scalable SOC capability without staffing or operational burden.
- **Reduced Operational Burden** – Eliminate the complexity of running Microsoft Sentinel internally while maintaining full visibility and control.
- **Skills Continuity** – Avoid dependency on scarce security talent and mitigate key-person risk within internal teams.
- **Stronger Governance** – Consistent processes, escalation paths, and reporting aligned to enterprise and regulatory expectations.

Essentials
Foundational 24/7 monitoring, incident triage, response guidance, and reporting.

Advanced
Proactive threat hunting, custom detections, enhanced tuning, and deeper collaboration.

Active Defence
Real-time threat response, weekly threat hunting, automated containment, and a dedicated security advisor.

Protect your business with confidence.
Run Microsoft Sentinel like a high-performing SOC.

www.cyberstash.com