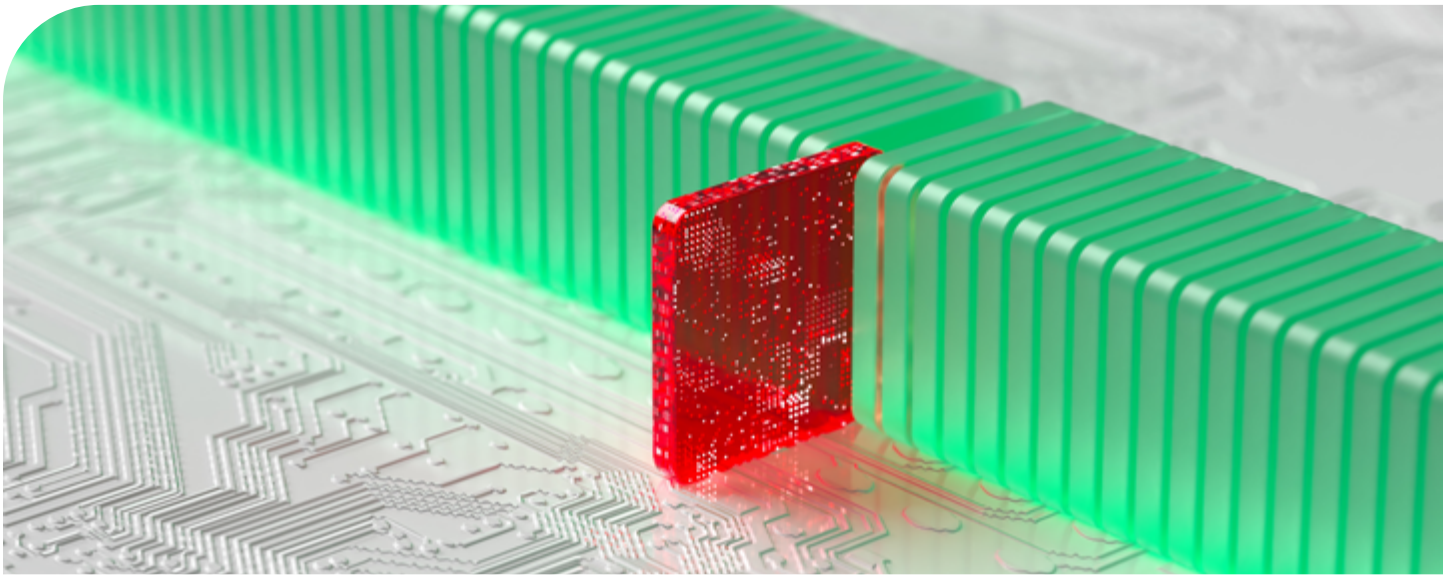

Info sheet

Identify and mitigate security threats

Protect your organization with Unisys Managed Detection and Response

Bolster your organization's cybersecurity

While struggling to handle high-volume alerts, security teams contend with fragmented tooling that obscures the full threat picture and an expanding attack surface. Organizations need protection across endpoints, identities, cloud workloads, and networks.

Built on Microsoft security technologies, the Unisys Managed Detection and Response solution provides continuous threat monitoring, advanced detection, and rapid, coordinated response across hybrid enterprise environments.

Structured adoption, governance, and integration of Security Copilot embeds directly into Security Operations Center(SOC). Copilot agents, native to Defender and Sentinel, accelerate a coordinated incident response:

- Phishing triage agent scales the classification of user-submitted phishing reports, reducing analyst effort and accelerating containment decisions.
- Threat intelligence briefing agent automatically curates threat intelligence tailored to your organization's specific threat profile and sector context.
- Incident investigation and response agent enables analysts to summarize incidents, identify impacted assets, and determine the root cause using natural language in Defender and Sentinel.
- Unisys benign positive agent autonomously evaluates and suppresses low-risk incidents when confidence thresholds are met (and retains a full audit trail).

What you'll gain

With a service delivered from global SOCs and integrated natively into your Microsoft environment, we operationalize your Microsoft 365 E5 investment.

- Reduce tool spread and analyst context-switching by consolidating Microsoft Defender, Sentinel, and Security Copilot into a single coherent operational model.
- Achieve clear resilience outcomes so your organization can respond more effectively when incidents occur.
- Reduce mean time-to-respond with agentic AI-powered alert triage and autonomous enrichment, freeing analysts to investigate incidents that require human judgment.

- Gain elastic coverage (no additional staff necessary) with 24/7 SOC operations backed by a global analyst workforce and AI automation that scales to demand peaks.
- Support NIS2, DORA, and GDPR obligations with discernible evidence since every detection, investigation, and response action is logged and auditable.
- Give leaders and senior operations staff continuous visibility into service performance with executive dashboards, SLA/KPI reporting, and incident timelines.

How Unisys works

Unisys delivers managed detection and response in three phases:

Design	Assessment of your environment, telemetry scope definition, and detection objectives alignment to your risk posture
Build	Configuration of Sentinel workspaces, playbook deployment, onboarding of Security Copilot agents, and integration of IT service management workflows
Run	Continuous 24/7 monitoring and incident response, supported by structured threat hunting, service reviews, and ongoing detection engineering

Why Unisys?

Unisys brings decades of experience overseeing global managed security services, with security operations center teams experienced in enterprise-scale security information and event management, endpoint threat detection, and incident management. Our managed detection and response capability is built natively on the Microsoft security stack, meaning our analysts, processes, and tooling are designed and optimized for Defender, Sentinel, and Security Copilot.

Ready to increase your organization's cybersecurity? Visit us online or contact us today to learn more.

unisys

unisys.com

06/26 6809-12457