

Microsoft Sentinel Value Insights

We are a Microsoft GSI partner, Azure Expert MSP, and a Microsoft Cloud Solutions Partner with all six Solution Partner Designations in Microsoft's Cloud Partner Program supported by multiple Microsoft Specializations.

As IT assumes a more strategic role, the significance of security is escalating daily. Our customers face the problem that SIEM (Security Information and Event Management) solutions are designed for past environments and struggle to keep up with today's challenges, let alone manage tomorrow's unforeseen risks.

See and stop threats before they cause harm with Microsoft Sentinel Value Insights.

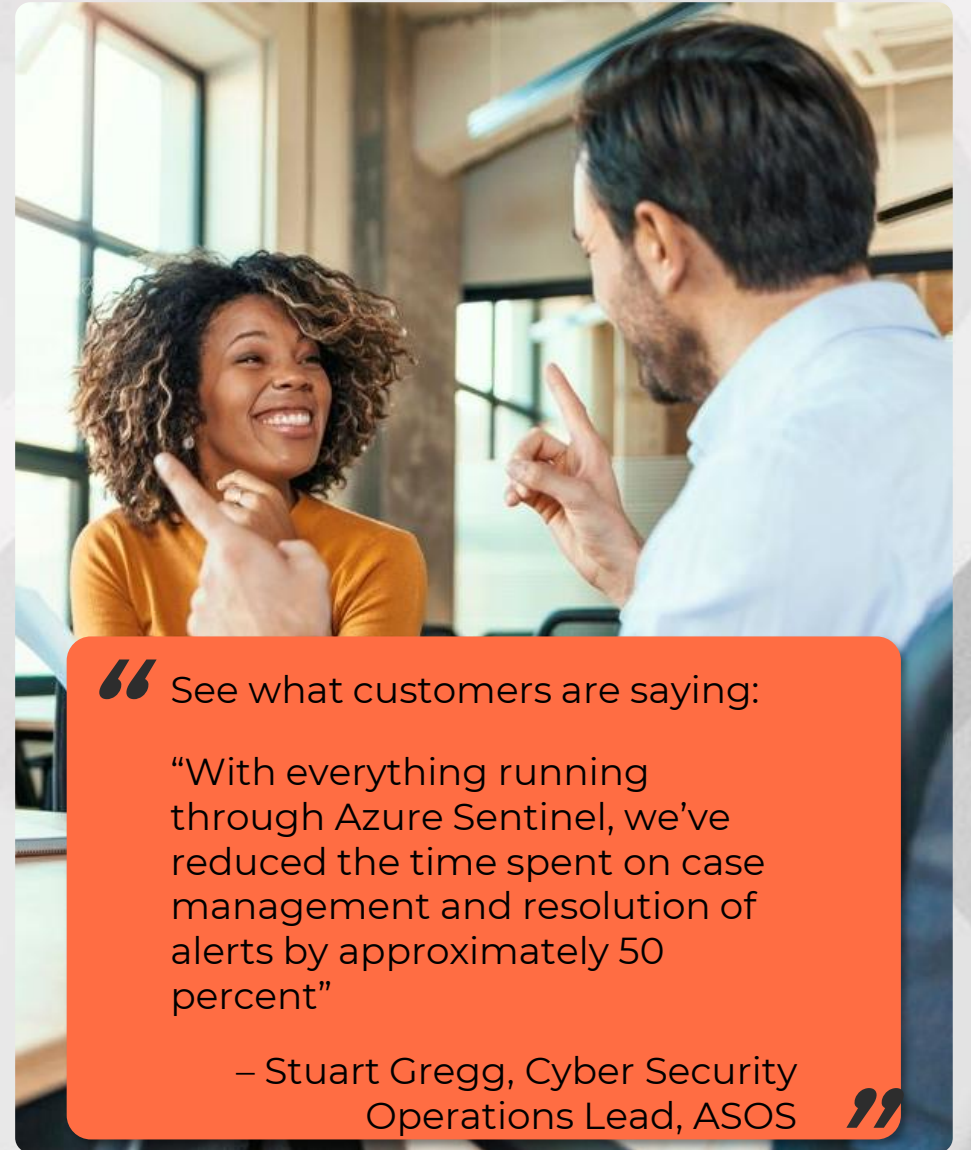
What We Offer

In Scope:

- Deployment of M365 trial licenses
- Configuration of M365 Security tools according to the delivery guide for Value Insights
- Threat exploration to discover threats actively attacking the customer
- Mapping threats discovered to a recommended method of mitigation

Out of Scope:

- Incident Response
- PoC or Lab Deployment
- Deep analysis
- Configuration of M365 Security tools beyond the guidance of Value Insights
- Forensic Analysis



“ See what customers are saying:

“With everything running through Azure Sentinel, we've reduced the time spent on case management and resolution of alerts by approximately 50 percent”

– Stuart Gregg, Cyber Security Operations Lead, ASOS”

Microsoft Sentinel Value Insights

How it Works

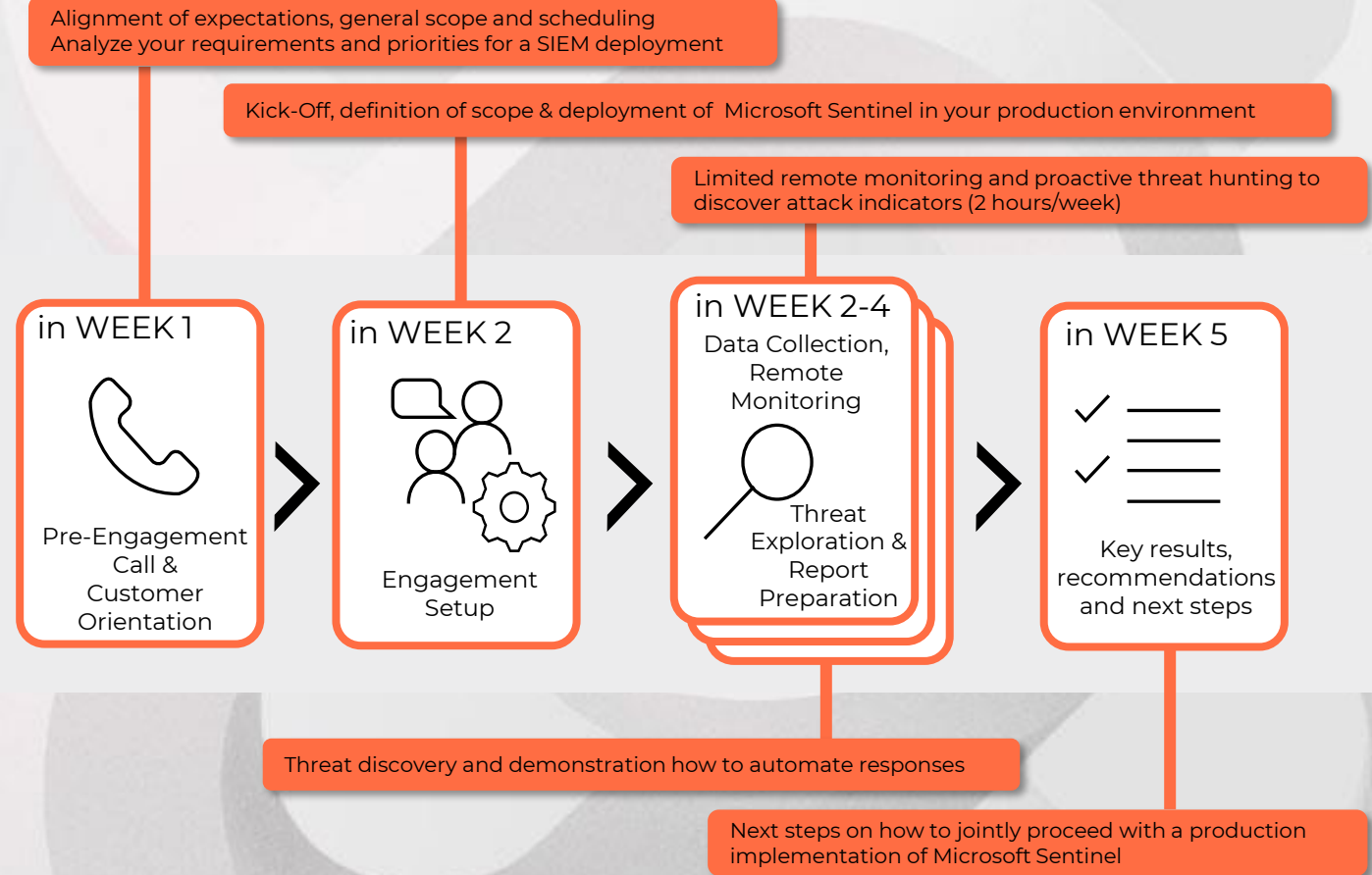
Identify active identity, email, and data threats in both on-premises and cloud environments.

As IT becomes more strategic, the importance of security grows daily. Security information and event management (SIEM) solutions built for yesterday's environments struggle to keep pace with today's challenges—let alone tomorrow's unimagined risks.

See and stop threats before they cause harm with Microsoft Sentinel Value Insights.

Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Execution Strategies and Solutions



Microsoft Sentinel Value Insights

Customer Outcomes

Discovering threats to your Microsoft 365 cloud and on-premises environments across email, identity, and data.

Understanding how to mitigate threats by showing how Microsoft 365 and Azure security products can help mitigate and protect against threats that are found.

Planning the next steps and providing information to build a business case for a production deployment of Microsoft Sentinel, including a technical deployment roadmap.

Customer Success

Company:

The Autobahn GmbH des Bundes is a federal government limited liability company under the responsibility of the Bundesministerium für Digitales und Verkehr.

It oversees the planning, construction, operation, maintenance, financing, and asset management of Germany's highways.

The definition of a strategy and the management of partners play a central role here.

Solution:

- With the selection of the Microsoft Sentinel platform, the detection infrastructure was embedded in the IT strategy of Autobahn GmbH des Bundes.
- The IT landscape is monitored 24/7 in order to detect any attacks at an early stage and respond to them accordingly and quickly.
- The success of the project is based on consistent project management - both on the customer's side and ours. The organizational challenges posed by the constantly changing IT landscape were successfully mastered by this project management.

Outcome:

With the Microsoft Sentinel platform and the Security Operation Center (SOC), the Autobahn GmbH des Bundes will receive a future-proof solution for monitoring IT.

With the introduction of security monitoring, Autobahn GmbH des Bundes will achieve compliance with the KRITIS requirements of the federal government from 2023. In detail:

- Fast response to safety-relevant incidents and thus avoidance of failures
- Future-oriented solution through high flexibility