Solution Brief

Services for Microsoft Sentinel

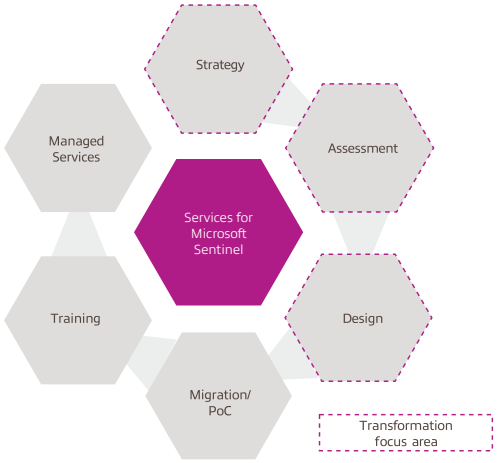
Modernize your security operations with an intelligent platform.

The data center — and threatscape — is evolving. And re-engineering the Security Operations Center (SOC) is more critical than ever. IT assets are sprawling and diverse, and multi-vendor security environments are notorious for management and visibility challenges. Traditional tools for Security Information and Events Management (SIEM) have limitations such as integration difficulties. As manual processes, skills shortages, and reactive models persist, security becomes less of a strategic business function.

Our **Services for Microsoft Sentinel** help you take advantage of cutting-edge technology from Microsoft to strengthen and simplify your security environment. During an engagement, our consultants address all major areas of your SOC, including new tools or processes that would be beneficial to adopt.

Services scope:

- Log analytics and management
- SOC tools
- Orchestration and automation
- Cloud access
- Endpoint protection
- Threat intelligence
- Event/case management
- Data sources
- Operational controls and governance
- Vulnerability assessment
- Integrations and support



Achieve your goals.

We understand that strengthening your security program doesn't happen overnight. That's why our services are designed to help you make meaningful changes that drive systematic transformation.

- Assess strengths, gaps, and opportunities of existing security infrastructure.
- Evaluate security policies and requirements in light of business needs and industry best practices.
- Design your ideal future SOC, inclusive of next-generation approaches and tool sets.
- Plan for key SIEM changes to drive modernization and reduce manual efforts.
- Develop a deployment roadmap for implementing advanced solutions from Microsoft.

Why Insight for Microsoft

Microsoft Azure

Largest
Azure partner

Dedicated team
of Azure technical solution advisors

Microsoft partner with
18 Gold & Silver competencies including:

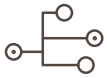
- Cloud Customer Relationship Management
- Cloud Platform and Cloud Productivity
- Datacenter and Data Platform

Microsoft award winner

- Azure Security Deployment Partner of the Year
- Microsoft Worldwide Artificial Intelligence Partner of the Year
- Microsoft U.S. Partner Award for Data & AI — Internet of Things
- Microsoft U.S. Partner Award for Apps and Infrastructure — Open Source on Azure

About Microsoft Sentinel

Microsoft Sentinel™ is a cloud-native SIEM service with built-in Artificial Intelligence (AI) analytics from Microsoft that allow you to see and stop threats to your enterprise before they cause harm. Unrestricted to hardware and easy to scale, Microsoft® Sentinel flexes to support your organizational agility.



Collect data at cloud scale — across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.

Detect previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence from Microsoft.

Investigate threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft.

Respond to incidents rapidly with built-in orchestration and automation of common tasks.

Our approach

We begin by evaluating your current security environment based on best practices, as well as how it aligns with your business needs and objectives. Together, we develop plans for deploying Microsoft Sentinel, considering cost, sizing, and other factors. Walk away with a detailed roadmap and other deliverables, including cost analysis, SOC current state and Microsoft Sentinel future readiness assessment, design requirements and architectural analysis, and next step recommendations.

Services may be delivered remotely, on-site, or a combination of both.

Assess

- Existing platforms and SOC tools
- Security policies and procedures
- Use cases, rules, and alerts
- Data sources discovery
- Business and IT requirements

Design

- Design Microsoft Sentinel solution
- Determine sizing and pricing
- Changes to access, penetration testing, integration, etc.
- Non-Microsoft product integration

Recommend

- Microsoft Sentinel deployment roadmap
- Replacement or migration of existing SOC
- Augmentation of existing SOC solutions
- Financial estimates

Insight Managed Security Services (MSS)

Insight Managed Security Services allows you to build on the strengths and capabilities of Microsoft Sentinel, combining industry-hardened best practices with cutting-edge risk mitigation. Insight MSS helps clients offload the heavy burden of caring for a complex and dynamic security environment.

Managed Security outcomes:

Faster response times

Stronger governance and compliance

Richer context and visibility

Improved threat detection

Reduced security team burden

20+ years
of support services delivery

175+
support services engineers

Three
24/7/365 U.S. support centers

Insight.

Driving innovation with digital transformation

At Insight, we help clients enable innovation with an approach that spans people, processes, and technologies. We believe the best path to digital transformation is integrative, responsive, and proactively aligned to industry demands. Our client-focused approach delivers best-fit solutions across a scope of services, including the modern workplace, modern applications, modern infrastructures, the intelligent edge, cybersecurity, and data and AI.

Learn more at:

solutions.insight.com | insight.com

Getting started is easy.

Visit solutions.insight.com/contact-us to connect with our team.