Insight. Cloud + Data Center Transformation

Solution Brief

Services for Azure Sentinel

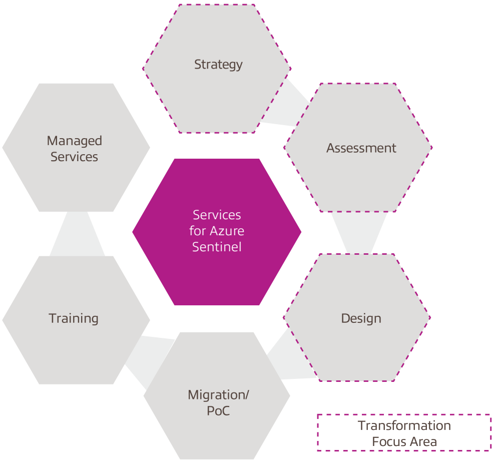
Modernize your security operations with a truly intelligent platform

Changes in the data center and overall threatscape suggest it might be high time to re-engineer the Security Operations Center (SOC). IT assets are sprawling and diverse, creating new vectors of attack. There are clear limitations with traditional tools for Security Information and Events Management (SIEM), as well as difficulties with integration. Manual processes, skills shortages, and reactive models prevail, making security resemble more a cat-and-mouse game than a strategic business function.

Our **Services for Azure 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

Although better security doesn't happen overnight, our services help you make the meaningful changes that comprise a systematic transformation.

- Assess existing security infrastructure, its strengths and shortcomings
- 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 Azure Sentinel

Azure Sentinel™ is a cloud-native SIEM service with built-in Artificial Intelligence (AI) analytics from Microsoft that allows you to see and stop threats to your enterprise before they cause harm. Unrestricted to hardware and easy to scale, Azure 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 Azure Sentinel, considering cost, sizing, and other factors. Walk away with a detailed roadmap ready to execute.

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

Recommend

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

Deliverables include

Cost analysis

SOC current state and Azure Sentinel future readiness assessment

Design requirements and architectural analysis

Next step recommendations and high-level roadmap

Insight Cloud + Data Center Transformation

Meaningful solutions driving business outcomes

We help our clients modernize and secure critical platforms to transform IT. We believe data is a key driver, hybrid models are accelerators, and secure networks are well integrated. Our end-to-end services empower companies to effectively leverage technology solutions to overcome challenges, support growth and innovation, reduce risk, and transform the business.

Learn more at:

insightCDCT.com | insight.com