Comprehensive threat protection & cloud-native security management.

Security Operations & Threat Protection Services (SOTPS)

Security Operations are overwhelmed—the complexity and frequency of attacks are evolving fast, and your team is under strain from an ever-expanding range of defensive technologies, cloud adoption, and borderless networks.

Security Operations & Threat Protection (SOTPS) combines Microsoft Industry Solutions, cloud-native Security Information & Event Management (SIEM), and our Extended Detection and Response (XDR) service to improve your security posture, and modernize how the people, processes, and technology work together.

Approach

People + Process + Technology = Success

A holistic approach to support your unique business needs aligned to security Operations.

Leverage our considerable experience addressing Security Operations Center (SOC) design/redesign challenges:

Agile & Iterative, identifying the foundational aspects that are important in implementing a comprehensive SIEM/XDR solution.

Processes aligned to the new technology, optimizing the full detect, respond and recover lifecycle to realize the goal of a more secure enterprise.

Adoption and change management to support people impacts, aligned to business outcomes and cultural considerations.

Designed to achieve your business outcomes

Transform

Reduce Detect, Respond, and Recover lifecycle time while demonstrating compliance and service levels.

Extend

Deliver enhanced protection across identities, endpoints, applications, and email.

Optimize

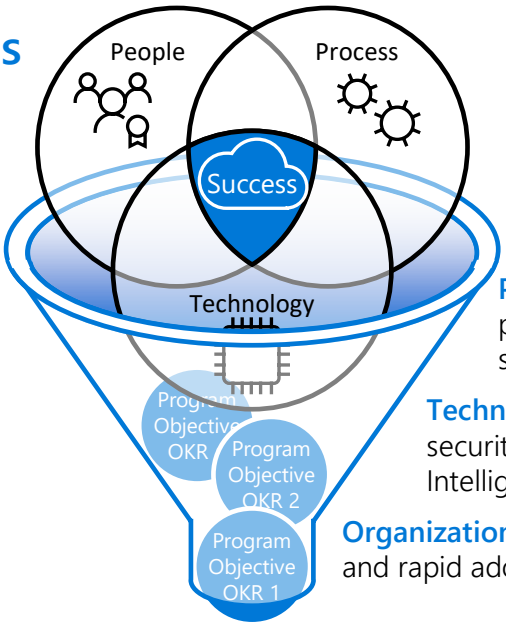
Respond to real and potential security concerns using actionable insights from a cloud-native SIEM.

Secure

Bridge security gaps between IT & OT environments by evolving network detection & response capability.

From business objectives...

We start by understanding the **objectives** and **priorities** driving your organization's change, and how they align to your *culture*, *behavior*, *operations*, and *technology strategies*.



...to a comprehensive delivery

People: Upskill and leverage your IT Pros' & Security Analysts' skills in rapid remediation.

Process: Manage governance, update processes & organizational structure to support the Modern SOC.

Technology: Deploy interconnected & modern security technologies leveraging Artificial Intelligence and Machine Learning.

Organizational Culture: Embrace continuous feedback and rapid adoption of new technologies and processes.

Capabilities

Extended Detection & Response

Azure AD Identity Protection

Microsoft Defender for
- Identity
- Endpoint
- Office 365
- Cloud
- Cloud Apps
- IoT

SIEM

Microsoft Sentinel

SIEM Migration to Microsoft Sentinel

Third-party SIEMs integration

System Management

Privileged Access Workstations

Intune Device Management

Transform Security Operations

Readiness Review

SOC
- Assessment
- Planning
- Monitoring

Adoption and Change Management

Duration: 7 to 23 weeks

Not sure if you need SOTPS?

Does your SOC struggle to keep up with the **expanding complexity and volume** of cyber threats and produce prioritized and actionable information?

Are your security analysts affected by **alert fatigue** from a **microservice architecture**?

Is the effectiveness of your SOC stalled by **outdated or incomplete organizational processes**?

Is your incident response team missing the context and processes they need to **appropriately classify and eradicate threats**?

Do your current solutions leverage **cloud native machine learning** and **auto-remediation functionality**?

Are your threat detection solutions unable to monitor **security for multiple clouds, operating systems, and platforms**?

Next Steps Contact your Microsoft Industry Solutions representative or visit https://microsoft.com/industrysolutions to learn how you can protect your organization with *Security Operations & Threat Protection*.

Microsoft