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 from Microsoft Industry Solutions customizes our cloud-native Security Information & Event Management (SIEM) and Extended Detection and Response (XDR) services to your organization’s security strategies & business goals—understanding your environment, improving your security posture, and modernizing how your 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 design/redesign challenges:

- **Developing Cybersecurity Strategies** that align with specific organizational goals, strategies, and risks.
- **Leveraging agile and iterative approaches** to identifying the foundational aspects that are important in implementing comprehensive SIEM/XDR solutions.
- **Aligning and optimizing business processes** with new technologies for full detect, respond, and recover lifecycles for a more secure enterprise.
- **Driving adoption and change management** that mitigates impact to people, aligns with business goals, and considers cultural implications.

Outcomes

- **Transform**
  Align Security Assets to combat modern threats; reduce Detect, Respond, and Recover lifecycle time while demonstrating compliance and service levels.

- **Extend**
  Deliver enhanced protection across identities, endpoints, applications, and email; cover systems and services across on-premises and multi-cloud.

- **Optimize**
  Respond to real and potential security concerns using actionable insights from a “single pane of glass” 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 & 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’ rapid remediation abilities.

**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

**Cybersecurity Strategy** Modernize your cybersecurity strategy to today’s threat landscape, reduce exposure, identify priority security investments, and realize value from your security investments.

**Extended Detection & Response** Azure Active Directory (AD) Identity Protection, and Microsoft Defender for Identity, Endpoint, Office 365, Cloud, Cloud Apps, and IoT.

**Security Information and Event Management (SIEM)** Microsoft Sentinel, SIEM Migration to Microsoft Sentinel, and third-party SIEM integration.

**System Management** Privileged Access Workstations and Intune Device Management.

**Security Operations Transformation** Harden tools and practices to limit risk exposure, define measures and metrics for compliance and service levels, and align skills, roles, processes to reduce the detect, respond, and recover lifecycle.

### Duration: 26 weeks

**Not sure if you need Security Operations?**

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 representative or visit microsoft.com/industrysolutions to learn how you can protect your organization with Security Operations.