Modern SecOps Engagement

See and stop threats before they cause harm with a Modern SecOps Engagement

As IT becomes more strategic, the importance of security grows daily.

SIEM solutions built for yesterday's environments struggle to keep pace with today's challenges.

That's why Microsoft developed Microsoft Sentinel, a fully cloud-native SIEM.

Get an overview of Microsoft Sentinel, along with insights on active threats to your Microsoft 365 cloud and on-premises environments across email, identity, endpoints, and third-party data.

Get a birds-eye view across all data ingested and detect threats using Microsoft's analytics and threat intelligence. Investigate threats with artificial intelligence and hunt for suspicious activities.

Key engagement deliverables:

Get hands-on experience and learn how to discover and analyze threats using Microsoft Sentinel and the Unified SecOps Platform. Learn how to automate your Security Operations to make it more effective.

Gain visibility into threats to your Microsoft 365 and Azure clouds and on-premises environments across email, identity, endpoints, and third-party data to better understand, prioritise and mitigate potential cyberattack vectors.

Help you understand how Microsoft Sentinel and Defender XDR security products can help you mitigate and protect against the threats found during the period of this engagement.

Experience the benefits of a managed monitoring and incident response service (optional). Experience the benefits of a true cloud native SIEM, monitored by your cybersecurity experts.

Create a roadmap for improvements and deployments, based on your environment and goals.

Develop joint plans and next steps to improve threat detection and remediation.

Our approach:

Analyse: Analyse customer's requirements and priorities for a SIEM deployment and define Customer's Success Criteria.

Define and deploy: Define scope and deploy Microsoft Sentinel in production environment integrating with Microsoft and non-Microsoft solutions.

Monitor (optional): Remote monitoring of Microsoft Sentinel incidents and proactive threat hunting to discover attack indicators.

Discover: Discover threats to on-premises and cloud environments across email, identity, endpoints, and third-party data.

Recommend: Next steps on how to proceed with a production implementation of Microsoft Sentinel and the Unified SecOps Platform.

Length of engagement approx. 2-3 weeks.

Who should be involved:

The engagement is intended for security decision-makers such as:

- Chief Information Security Officer (CISO)
- Chief Information Officer (CIO)
- Chief Security Officer (CSO)
- IT Security Architects
- IT Security Administrators
- IT Security Operations (Sec Ops)

Our modular approach:

Mandatory Modules

- Microsoft Defender XDR / Unified SecOps
- Identity Threat Detection
- Communication and Collaboration Threat Detection
- Azure Threat Detection
- Threat Intelligence

All mandatory modules are included in the engagement.

Selectable Modules

- Server Threat Detection
- Third-party Alert/Logs
- SOC Automation

At least one (1) selectable module must be included in the engagement.

Kocho

Become greater with Kocho

Our mission is to take your organisation on a journey of secure transformation.

Are you ready to get started? Talk to us today.

→ Contact us

About Kocho

At Kocho, we connect users and devices securely to Microsoft cloud services.

We believe greatness lies in everyone, and we offer a unique blend of professional, and managed IT solutions, to help ambitious companies realise their full potential.

Kocho. Become greater.

1 of 7 Microsoft global partners with all Security Accreditations

Member of Microsoft Intelligent Security Association

Microsoft Security

Microsoft Verified Managed XDR Solution

Microsoft Solutions Partner
Security

Microsoft Solutions Partner
Modern Work

Microsoft Solutions Partner
Data & AI (Azure)

Microsoft Solutions Partner
Infrastructure (Azure)

Microsoft Solutions Partner
Digital & App Innovation (Azure)

Microsoft Specialisation
- Cloud Security
- Threat Protection
- Modernise Endpoints
- Infra & Database Migration
- Identity & Access Management
- Information Protection & Governance

CISSP

Cyber Essentials Certified Plus

ISO 9001 Certified

bsi. ISO/IEC 27001 Information Security Management