Atech

Microsoft Sentinel Engagement

Gain a bird's eye view across your enterprise with SIEM for a modern world

"With everything running through Azure Sentinel, we've reduced the time spent on case management and resolution of alerts by approximately 50 percent"
-Stuart Gregg, Cyber Security Operations Lead, ASOS

As IT becomes more strategic, the importance of security grows daily. Security information and event management (SIEM) solutions built for yesterday's environments struggle to keep pace with today's challenges—let alone tomorrow's unimagined risks.

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

Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Get an overview of Microsoft Sentinel along with insights on active threats to your Microsoft 365 cloud and on-premises environments with a Microsoft Sentinel Workshop.

CHOOSE THE APPROACH THAT'S BEST FOR YOU

Every organization is different, so this workshop can be customized to fit your environment and goals. We can provide either of two scenarios:

Remote monitoring

If your organization doesn't have its own security operations center (SOC) or if you want to offload some monitoring tasks, we will demonstrate how Atech can perform remote monitoring and threat hunting for you.

Joint threat exploration

If your organization is interested in learning how to integrate Microsoft Sentinel in your existing SOC by replacing or augmenting an existing SIEM, we will work with your SecOps team and provide additional readiness to bring them up to speed.

Engagement highlights

 Understand the features and benefits of Microsoft Sentinel

 Gain visibility into threats across email, identity, and data

 Better understand, prioritize, and mitigate potential threat vectors

 Create a defined deployment roadmap based on your environment and goals

 Develop joint plans and next steps

See and stop threats before they cause harm with a Microsoft Sentinel Engagement

What we'll do

Analyze your requirements and priorities for a SIEM deployment

Define scope & deploy Microsoft Sentinel in your production environment

Remote monitoring* and proactive threat hunting to discover attack indicators *optional component

Discover threats and demonstrate how to automate responses

Recommend next steps on how to proceed with a Production implementation of Microsoft Sentinel

Engagement objectives

Discover threats to your Microsoft 365 cloud and on-premises environments across email, identity and data.

Understand how to mitigate threats by showing how Microsoft 365 and Azure security products can help mitigate and protect against threats that are found.

Plan next steps and provide information to build a business case for a production deployment of Microsoft Sentinel including a technical deployment roadmap.
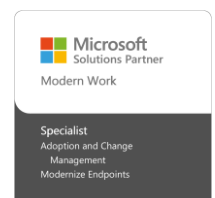
AZURE ARC: SIMPLIFYING HYBRID AND CLOUD MANAGEMENT

As part of this workshop Atech will share the benefits of the Azure Arc solution. Learn more regarding:

- Extending the Azure management experience into on-premises infrastructure
- Arc Resource Bridge (Preview) to provide VM lifecycle management in VMWare or Hyper-V
- Onboarding infrastructure and core management features for no additional cost
- Additional functionality billable through either add-on licenses or consumption cost
  - Such as Azure Monitor consumption or SQL Management
- Defender for Cloud integration for security posture monitoring and management

Why Atech?

Atech specialises in Microsoft Modern work and Security with more than a decade of experience in Microsoft 365 Business Solutions. We manage deployment, licensing and migration to the cloud, so that you can focus on growing your business.

Atech delivers tailored Microsoft 365 solutions to thousands of companies in the UK and worldwide. We couple out-of-the-box thinking with proven strategy to create a unique cloud-based solution for every one of our clients.

Microsoft Solutions Partner
Security
Specialist
Cloud Security
Identity and Access Management
Information Protection and Governance
Threat Protection

Microsoft Solutions Partner
Infrastructure Azure
Specialist
Networking Services
Infra and Database Migration
Azure Virtual Desktop

Microsoft Solutions Partner
Modern Work
Specialist
Adoption and Change Management
Modernize Endpoints

Microsoft Solutions Partner
Digital & App Innovation Azure

Microsoft Partner
Microsoft

2022 Partner of the Year Finalist
Modern Endpoint Management Award

ISO 27001   CREST

ACM
ISO 27001:2013 REGISTERED

UKAS
MANAGEMENT SYSTEMS
24

Microsoft Partner
Microsoft

Data & AI Azure
Digital & App Innovation Azure
Infrastructure Azure
Modern Work
Security

2022 Partner of the Year Finalist
Modern Endpoint Management Award

Explore More