Microsoft Security

Microsoft Sentinel Engagement

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

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

"With everything running through Microsoft 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.

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

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 Engagement.

Choose the approach that's best for you

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

Remote monitoring

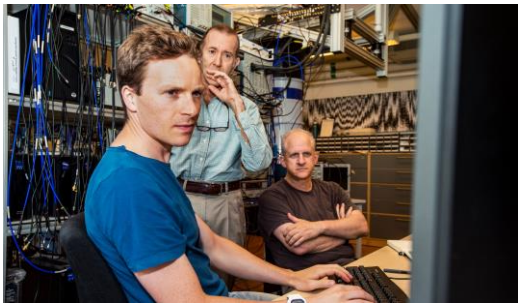
If your organization doesn't have its own security operations center (SOC) or if you want to offload some monitoring tasks, we will demonstrate how [Partner Name] can perform remote monitoring and threat hunting for you.

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 objectives

Through this engagement, we will work with you to:



- 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.

In addition, depending on the selected scenario, you will also:

Experience the benefits of a managed SIEM with a true cloud native SIEM, managed and monitored by our cybersecurity experts.
(Remote Monitoring scenario)

Receive hands-on experience, learn how to discover and analyze threats using Microsoft Sentinel and how to automate your Security Operations to make it more effective.
(Joint Threat Exploration scenario)

What we'll do

Analyze your requirements and priorities for a SIEM deployment

Define scope & deploy Microsoft Sentinel in your production environment

Remote monitoring* of Microsoft Sentinel incidents and proactive threat hunting to discover attack indicators
*optional component

Explore threats and demonstrate how to automate responses and perform threat hunting

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

Why Partner Name?

When it comes to security, you need an experienced partner.

Partner to insert their personalized information on value proposition, experience, Microsoft 365 security features knowledge, and/or services.

Include any engagement components you have added to customize the engagement, such as:

- Additional Microsoft products such as Microsoft Defender for Endpoint or Microsoft Defender for Identity
- Additional data sources such as cloud firewall or proxy servers, Windows or Linux servers and CEF/Syslog capable devices
- Integration with an existing SIEM
- Any incident response services

Sentinel360

Contact us today to get started!

Sentinel 360 | Nadeem Yusufaly | Sentinel360.io