corsica technologies

CYBERSECURITY SERVICES

Modern SecOps Envisioning Workshop

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

Engagement highlights

- Understand the features and benefits of Microsoft Sentinel and Unified SecOps Platform
- Gain visibility into threats across email, identity, endpoints, and non-Microsoft data
- Better understand, prioritize, and mitigate potential threat vectors
- Create a defined deployment roadmap based on your environment and goals

Uncover threats and stop them in their tracks.

Today's cyberthreats are incredibly complex, and it's hard to imagine what we'll face in the future. That's why Microsoft developed Microsoft Sentinel, a fully cloud-native SIEM.

> *"With everything running through Microsoft Sentinel, we've **reduced the time spent** on case management and resolution of alerts **by approximately 50%**."*
>
> **Stuart Gregg, Cybersecurity Operations Lead @ ASOS**

- **Get a birds-eye-view** across all data and detect threats using Microsoft's threat intelligence.
- **Investigate threats** with artificial intelligence and hunt for suspicious activities.
- **Get an overview of Microsoft Sentinel** along with insights on active threats to your Microsoft365 cloud and on premises environments.

Our workshop approach is flexible, adapting to your needs.

Let's customize your engagement to meet the specific requirements of your security operations.

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.

Remote monitoring (optional)

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 Corsica can perform remote monitoring and threat hunting for you.

Engagement objectives

- **Get hands-on experience** discovering and analyzing threats in Microsoft Sentinel and the Unified SecOps Platform. Learn how to automate your Security Operations to make them 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, prioritize, 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.

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.

Receive hands-on experience, learn how to discover and analyze threats using Microsoft Sentinel and how to automate your Security Operations to make them more effective.

Here's what we'll do:

- Analyze your requirements and priorities for a SIEM deployment and define Customer's Success Criteria
- Define scope & deploy Microsoft Sentinel in production environment integrating with Microsoft and non-Microsoft solutions
- Remote monitoring* of Microsoft Sentinel incidents and proactive threat hunting to discover attack indicators
- 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

Why Corsica Technologies?

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

Maximize the value of your Microsoft investment in M365 and reduce dependency on 3rd party platforms. The Corsica team is prepared to meet all your data security and compliance needs, ensuring a seamless and secure digital environment.