BULLETPROOF
a GLI company

MODERN SECOPS ENVISIONING WORKSHOP

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

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 with a Modern SecOps Envisioning Workshop before they cause harm

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

Microsoft Funding

Reach out to Bulletproof to check your eligibility for Microsoft funding—your organization may qualify based on program requirements.

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 deployment roadmap based on your environment and goals

An engagement designed to meet of your security operations needs

Using a modular approach, we will allow you to customize the engagement to meet your specific security operations needs.

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 Bulletproof can perform remote monitoring and threat hunting for you.

Engagement Objectives

Through this workshop (approximately 27-53 hours of delivery depending on your needs), we will work with you to:

- **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 onpremises 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 it more effective.

Analyze customer's 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

About Bulletproof

Bulletproof is a global leader in IT, security, and compliance—recognized by Microsoft as a 2024 Security Trailblazer and 2021 Global Security Partner of the Year.

As a trusted Microsoft Solutions Partner with specializations in Cloud Security, Threat Protection, Data Security, and Identity & Access Management, we deliver end-to-end protection that's proven, modern, and Microsoft-aligned.

Member of
Microsoft Intelligent Security Association

Microsoft Security

Microsoft Verified Managed XDR Solution