Microsoft Sentinel PoC

USA TOP 10
Microsoft Security

Value proposition

Modern security operations needs to be intelligent, adaptive and make best use of automation and machine learning to keep pace with today's threats. Traditional SIEM solutions gather and present security alerts but the increasingly frequent and sophisticated attacks, volume of alerts and need for rapid detection and remediation has led to a shift to more modern solutions. Microsoft Sentinel is a cloud native SIEM and SOAR solution backed by Microsoft's advanced telemetry, providing a single solution for alert detection, investigation, remediation, and proactive hunting across Microsoft and 3rd party signals through a vast ecosystem of native connectors & integrations.

Workloads

- Microsoft Sentinel
- Azure Logic Apps (Playbooks)
- First & third-party workload native connectors

Engagement Outcomes

- Review your security goals and objectives
- Identify real threats in your cloud or PoC environment
- Map identified threats to specific solution recommendations
- Automate incident response to reduce mean time to detect (MTTD) and mean time to respond (MTTR)
- Showcase security scenarios with product demos
- Develop joint plans and next steps

Who should participate

- CISO, CIO, CSO, IT Security, IT Security Operations
- 11 hours of collaborative sessions scheduled over 2-3 weeks

Assessment offers

- Microsoft funding for Invoke-led Assessment may be available upon request
- Engagement length and cost will vary, depending upon scenarios explored

Timeline & Scope – Customer customizable (**minimal customer effort**)

Stage 1

Engagement Setup

- Pre-Engagement Call
- Pre-Requisites and Scope
- Align on SIEM use cases
- Microsoft Sentinel Overview
- Technical Setup

Stage 2

Monitoring & Response

- Remote incident monitoring
- Automated Incident Response
- Threat Exploration
- Integration with Defender (Optional)

Stage 3

Exploration and Report Generation

- Report Generation
- Results Presentation
- Customer Conversation
- Build the Plan & Next Steps Discussion

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