Microsoft 365 Threat Protection Workshop

OBJECTIVES

- Identify the customer's key security objectives and challenges
- Perform a guided discovery of threats and vulnerabilities
- Demonstrate Microsoft Threat Protection capabilities using the customer's existing or trial licenses
- Provide recommendations and a strategic roadmap for improving threat protection and response

ABOUT DAYMARK

Daymark Solutions excels in creating sophisticated technology solutions, specializing in addressing complex business challenges through expertly designed systems. Their highly skilled architects are adept at crafting well-architected solutions that seamlessly integrate cloud and data center technologies. By combining these technologies, they create robust, scalable and secure systems tailored to meet their clients' unique needs.

OVERVIEW

In the Daymark Microsoft 365 Threat Protection Workshop, Daymark will assess the organization's current security posture, identify key threats and vulnerabilities, and demonstrate how Microsoft 365 Threat Protection solutions can enhance security across identities, endpoints, email, and cloud applications.

Scope - The workshop is delivered over three (3) days. The agenda includes:

Day 1: Discovery & Foundations

- Workshop kickoff and introductions
- Identification of security priorities and goals
- Review of Microsoft licensing and deployed solutions
- Environment discovery and security assessment
- Microsoft Threat Protection overview
- Demonstration of Microsoft Defender Portal (XDR)
    - Demonstrate incident queue and alert correlation
    - Explain advanced hunting and investigation capabilities
    - Review built-in reporting and analytics
    - Integration with Sentinel

Day 2: Training & Demonstrations

- **Cloud Identity Protection**
    - Overview of Entra ID Protection and Conditional Access
    - Explore identity risk levels and real-world attack techniques (token replay, MFA fatigue)
    - Demonstrate policy creation, risky detection logs, and remediation

DELIVERABLES

After the engagement, Workshop participants will receive:

- Executive summary
- Recommendations and next steps roadmap
- Licensing guidance

Day 2: Training & Demonstrations Continued

- **Microsoft Defender for Office 365**
  - Review types of threats stopped by Defender for O365
  - Review anti-phishing, anti-malware, Safe Links, and Safe Attachments features
  - Explore Threat Explorer and Attack Simulation Training
- **Microsoft Defender for Endpoint**
  - Explore risk-based vulnerability management and secure score integration
  - Explore attack surface reduction rules
  - Review incident correlation and device timeline for investigation
- **Microsoft Defender for Cloud Apps**
  - Discover and assess usage of unsanctioned or shadow IT apps
  - Review app governance and data loss prevention (DLP) policies
  - Monitor user behavior for anomalies and risky actions across cloud services
- **Microsoft Security Copilot demonstration**
  - Demonstrate natural language queries for incident analysis
  - Show example threat summaries and contextual data generation
  - Explore how Copilot can assist analysts with playbook automation and recommendations

Day 3: Review & Recommendations

- Recap of key findings
- Threat discovery and gap review
- Remediation and improvement roadmap
- Executive summary and deliverables review
- Feedback and next steps

Learn more about Daymark Solutions, visit **www.daymarksi.com**

Daymark Solutions, Inc.
131 Middlesex Turnpike
Burlington, Massachusetts 01803

📞 +1.781.359.3000
✉ info@daymarksi.com
🌐 www.daymarksi.com

DAYMARK
Navigate information technology