DAYMARK
Navigate information technology

Microsoft Defender XDR Implementation & Enablement

HIGHLIGHTS

- **End to End Defender XDR Deployment:** Rapid implementation and integration of all Microsoft 365 Defender workloads into a single, unified detection and response platform.
- **Built on Industry Leading Standards:** Configured using proven Microsoft and security best practices to ensure a hardened, scalable, and supportable security foundation from day one.
- **Immediate SOC Readiness:** Defender XDR is operational at go live, with correlated incidents, automated investigation and actionable detections.

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.

Accelerate your Extended Detection & Response (XDR) capabilities leveraging Microsoft Defender.

OVERVIEW

Daymark accelerates adoption of Microsoft Defender XDR by rapidly deploying and integrating all Microsoft 365 Defender workloads into a single, operational detection and response platform. We implement Microsoft Defender for Endpoint to secure devices across Windows, macOS, Linux, and mobile platforms using industry best practices, enabling EDR, attack surface reduction, and automated investigation and response from day one. Microsoft Defender for Office 365 is configured to protect email and collaboration workloads from phishing, malware, and impersonation attacks, with policies tuned to deliver high fidelity detections directly within the Defender XDR incident experience.

To address identity centric threats, Daymark deploys Microsoft Defender for Identity to surface attacks such as lateral movement, credential theft, and privilege abuse across on premises and hybrid Active Directory environments. We extend detection and control into SaaS applications using Microsoft Defender for Cloud Apps, providing visibility into risky user behavior, data exfiltration, and OAuth misuse, fully correlated with endpoint, email, and identity signals. As an optional extension, Daymark implements a lightweight Microsoft Sentinel configuration to ingest Defender XDR data for extended retention, advanced investigation, and compliance driven analysis—without introducing full SIEM complexity.

Together, these capabilities deliver a unified, SOC ready Microsoft Defender XDR platform for organizations starting from zero. Daymark applies proven standards and deep Microsoft security expertise to ensure the environment is implemented quickly, integrated correctly, and ready to support real world detection and response operations immediately.

BUSINESS OUTCOMES

At the completion of the engagement, you will receive:

- **Unified Visibility Across the Attack Surface:** Consolidated visibility across endpoints, identity, email, and SaaS apps in a single incident and alert experience—so teams see the full kill chain, not disconnected events.
- **Comprehensive, Integrated Security Platform (XDR First):** A fully integrated Microsoft 365 Defender XDR stack that correlates signals across workloads to improve detection quality and reduce blind spots created by siloed tools.
- **Faster Detection, Investigation, and Response:** SOC ready operations with prioritized incidents, automated investigation and response, and consistent workflows—reducing time to triage and speeding containment and remediation.
- **License and Tooling Optimization Using Microsoft Capabilities:** Maximizes the value of existing Microsoft licensing by implementing native security features and reducing the need for overlapping third party point solutions, simplifying vendor and platform sprawl.

AGENDA

Workstream 1: Overview & Objectives

- Review engagement goals, scope, and success criteria.
- Align on Defender XDR outcomes, timelines, and operational expectations.

Workstream 2: Current State & Readiness Assessment

- Review existing Microsoft 365 licensing, tenant configuration, and identity posture.
- Identify gaps, dependencies, and prerequisites for Defender XDR deployment.
- Confirm assumptions for environments starting from zero.

Workstream 3: Defender XDR Architecture & Integration Approach

- Overview of Microsoft Defender XDR and how Endpoint, Identity, Office 365, and Cloud Apps integrate into a single detection and response platform.
- Review Daymark's standards based deployment approach and integration patterns.

Workstream 4: Defender Workload Configuration

- Deploy Defender for Endpoint across all devices to ensure comprehensive device coverage, activate Endpoint Detection and Response (EDR) capabilities, and implement attack surface reduction rules to minimize vulnerabilities.
- Configure Defender for Office 365 by enabling anti-phishing, safe attachments, and safe links for email and collaboration.
- Integrate Defender for Identity with on-premises and cloud identity infrastructure to provide hybrid visibility; set up detection alerts for suspicious activities.
- Enable Defender for Cloud Apps to monitor SaaS usage, enforce security policies, and detect risky behaviors.

Workstream 5: Microsoft Sentinel Configuration

- Purpose and scope of a lightweight Sentinel deployment.
- Extended retention, advanced hunting, and compliance investigation use cases.

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