DAYMARK
Navigate information technology

Enhance Security and Event Management with Microsoft Azure Sentinel

HIGHLIGHTS

- Seamlessly integrate Microsoft Sentinel with Azure Event Hubs to centralize and unify security monitoring across on-premises and cloud environments.
- Benefit from a scalable, cloud-native SIEM solution that grows with your business needs, offering flexible, pay-as-you-go pricing.
- Simplify regulatory compliance with built-in tools and customizable reporting features, ensuring adherence to industry standards and reducing the burden of audit preparations.

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.

Leverage Microsoft Azure Sentinel to build a robust event management strategy.

OVERVIEW

Transform your security strategy with a powerful, unified approach—integrate Microsoft Sentinel and Azure Event Hubs to proactively safeguard your digital environment with real-time insights and advanced threat detection. This Proof of Concept (POC) offers your organization the opportunity to enhance security by integrating Microsoft Sentinel with Azure Event Hubs. Designed to provide both strategic guidance and practical application, this POC by Daymark Solutions will support you in deploying Sentinel within your current environment. The integration is tailored to safeguard your digital landscape, leveraging Azure to create a scalable, robust security framework.

The POC consists of two sessions, each designed to build expertise and hands-on experience. The first session focuses on the planning and deployment of Microsoft Sentinel according to industry best practices, including enabling Defender threat analytics for real-time monitoring and threat detection. The second session is dedicated to threat analysis, allowing your team to practice threat hunting, detection, and investigation using Sentinel tools within your environment.

With this POC, your organization will develop a proactive, efficient, and cost-effective security operation, tailored to meet your unique needs. Integrating Microsoft Sentinel with Azure Event Hubs transforms your security approach, enabling you to respond quickly to emerging threats and gain insights to continuously enhance your security posture.

LEARNING OBJECTIVES

At the completion of the engagement, participants will:

- Learn to enable Microsoft Sentinel in your environment
- Learn how to integrate Azure Event Hubs into your Sentinel deployment
- Develop workbooks, playbooks, and automation rules to enhance cybersecurity
- Review detection, hunting, and investigation of threats

AGENDA

Workstream 1: Plan & Deploy Sentinel

- **Objective:** Design a Proof of Concept (POC) to assess and gather client-specific requirements for a full Microsoft Sentinel implementation with Azure Event Hub integration.
- **Activities:**
  - Review Sentinel capabilities.
  - Explain Azure Event Hubs integration with Sentinel.
  - Assess required roles and permissions.
  - Reveiw cost estimates based on requirements.
  - Enable and Configure Sentinel in the environment.
  - Activate User and Entity Behavior Analytics (UEBA).
  - Integrate Microsoft Defender Threat Intelligence with Sentinel.

Workstream 2: Sentinel Review & Threat Analysis

- **Objective:** Provide hands-on learning for customer staff to use Microsoft Sentinel for detection, hunting, and investigation activities.
- **Activities:**
  - Use Microsoft Sentinel's data collection to monitor and manage cybersecurity posture.
  - Manage Sentinel dashboards and workbooks.
  - Visualize data through collected dashboards.
  - Oversee and respond to incidents within Sentinel.
  - Configure alerting in Microsoft Sentinel.
  - Use notebooks to assist in investigations.
  - Examine incident timelines and correlate alerts to incidents.
  - Conduct remediation steps while investigating threats.

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

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

+1.781.359.3000
info@daymarksi.com
www.daymarksi.com

DAYMARK
Navigate information technology