DAYMARK
Navigate information technology

Microsoft Azure Sentinel Proof of Concept

HIGHLIGHTS

- **Centralize Security Monitoring:** Seamlessly unify security operations across on-premises and cloud environments for streamlined oversight and faster threat response.
- **Scalable and Cost-Effective:** Leverage a flexible, cloud-native SIEM solution that adapts to your business while offering budget-friendly, pay-as-you-go pricing.
- **Simplified Compliance:** Reduce audit preparation time with built-in tools and customizable reports, making it easier to adhere to regulatory requirements and maintain industry standards.

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.

Build a robust event management strategy with a unified approach, real-time insights, and advanced threat detection.

OVERVIEW

Transform your event management strategy with a powerful, unified approach to 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 Azure Sentinel with Azure Event Hubs. Designed to provide both strategic guidance and practical application, this POC by Daymark Solutions will support you in deploying Azure Sentinel within your current environment. The integration is tailored to safeguard your digital landscape, leveraging Microsoft Azure to create a scalable, robust security framework.

The POC consists of two sessions designed to build expertise with hands-on experience. The first session focuses on planning and deployment of Azure 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, cost-effective security operation tailored to your unique needs. Integrating Azure Sentinel with Azure Event Hubs transforms your security approach, enabling you to respond quickly to emerging threats and insights to continually strengthen your security posture.

LEARNING OBJECTIVES

At the engagement, participants will learn how to:

- Enable Azure Sentinel in your environment.
- 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 complete Azure Sentinel implementation with Azure Event Hubs integration.
- **Activities:**
  - Review Azure Sentinel capabilities.
  - Explain Azure Event Hubs integration with Azure Sentinel.
  - Assess required roles and permissions.
  - Review cost estimates based on requirements.
  - Enable and configure Azure Sentinel in the environment.
  - Activate User and Entity Behavior Analytics (UEBA).
  - Integrate Microsoft Defender Threat Intelligence with Azure Sentinel.

Workstream 2: Sentinel Review & Threat Analysis

- **Objective:** Provide hands-on training for Azure Sentinel for detection, hunting, and investigation activities.
- **Activities:**
  - Use Azure Sentinel's data collection to monitor and manage cybersecurity posture.
  - Manage Azure Sentinel dashboards and workbooks.
  - Visualize data through collected dashboards.
  - Oversee and respond to incidents within Azure Sentinel.
  - Configure alerting in Azure 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

© 2024 Daymark Solutions, Inc. All rights reserved. Other brands, products or service names are or may be trademarks or service marks of their respective owners.