SC 5001- Configure SIEM Security Operations Using Microsoft Sentinel

Days: 1

Prerequisites: Fundamental understanding of Microsoft Azure. Basic understanding of Microsoft Sentinel. Experience using Kusto Query Language (KQL) in Microsoft Sentinel

Audience: The Microsoft Security Operations Analyst collaborates with organizational stakeholders to secure the organization's information technology systems. Their goal is to reduce organizational risk by rapidly remediating active attacks in the environment, advising on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders. Responsibilities include threat management, monitoring, and response by using a variety of security solutions across their environment. The role primarily investigates, responds to, and hunts for threats using Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft Defender XDR, and third-party security products. Since the Security Operations Analyst consumes the operational output of these tools, they are also a critical stakeholder in their configuration and deployment.

Description: Get started with Microsoft Sentinel security operations by configuring the Microsoft Sentinel workspace, connecting Microsoft services and Windows security events to Microsoft Sentinel, configuring Microsoft Sentinel analytics rules, and responding to threats with automated responses.

Course Objectives: After completing this course, students will be able to:

- Create and configure a Microsoft Sentinel workspace
- Deploy a Microsoft Sentinel content hub solution
- Connect Windows hosts to Microsoft Sentinel
- Configure analytics rules in Microsoft Sentinel
- Configure automation in Microsoft Sentinel

OUTLINE:

LESSON 1 - CREATE AND MANAGE MICROSOFT SENTINEL WORKSPACES

- Plan for the Microsoft Sentinel workspace
- Create a Microsoft Sentinel workspace
- Manage workspaces across tenants using Azure Lighthouse
- Understand Microsoft Sentinel permissions and roles
- Manage Microsoft Sentinel settings
- Configure logs
- Module assessment

LESSON 2 - CONNECT MICROSOFT SERVICES TO MICROSOFT SENTINEL

- Plan for Microsoft services connectors
- Connect the Microsoft 365 connector
- Connect the Microsoft Entra connector
- Connect the Microsoft Entra ID Protection connector
- Connect the Azure Activity connector
- Module assessment

LESSON 3 - CONNECT WINDOWS HOSTS TO MICROSOFT SENTINEL

- Plan for Windows hosts security events connector
- Connect using the Windows Security Events via AMA Connector
- Connect using the Security Events via Legacy Agent Connector
- Collect Sysmon event logs
- Module assessment

LESSON 4 - THREAT DETECTION WITH MICROSOFT SENTINEL ANALYTICS

- What is Microsoft Sentinel Analytics?
- Types of analytics rules
- Create an analytics rule from templates
- Create an analytics rule from wizard
- Manage analytics rules

SC 5001- Configure SIEM Security Operations Using Microsoft Sentinel

LESSON 5 - AUTOMATION IN MICROSOFT SENTINEL

- Understand automation options
- Create automation rules
- Module assessment

LESSON 6 - CONFIGURE SIEM SECURITY OPERATIONS USING MICROSOFT SENTINEL