SC 200T00-A: Defend Against Cyberthreats with Microsoft's Security Operations Platform

Days: 4

Description: Learn how to investigate, respond to, and hunt for threats using Microsoft Azure Sentinel, Azure Defender, and Microsoft 365 Defender. In this course, students will learn how to mitigate cyberthreats using these technologies. Specifically, students will configure and use Azure Sentinel as well as utilize Kusto Query Language (KQL) to perform detection, analysis, and reporting. The course was designed for people who work in a Security Operations job role and helps learners prepare for the exam SC-200: Microsoft Security Operations Analyst.

Prerequisites:

- Basic Understanding of Microsoft 365
- Fundamental Understanding of Microsoft Security, Compliance, and Identity Products
- Intermediate Understanding of Windows 10
- Familiarity with Azure Services, Specifically Azure SQL Database and Azure Storage
- Familiarity with Azure Virtual Machines and Virtual Networking
- Basic Understanding of Scripting Concepts

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 XDR, Microsoft Defender for Cloud, 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.

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

- Manage threat mitigation using Microsoft Defender XDR, Microsoft Purview, Microsoft Defender for Endpoint and Microsoft Defender for Cloud
- Create KQL queries for Microsoft Sentinel
- Configure your environment in Microsoft Sentinel
- Manage log connection to Microsoft Sentinel
- Detect and remediate threats using Microsoft Sentinel
- Manage threat hunting in Microsoft Sentinel

OUTLINE:

MODULE 1: MITIGATE THREATS USING MICROSOFT DEFENDER XDR

MODULE 2: MITIGATE THREATS USING MICROSOFT SECURITY COPILOT

MODULE 3: MITIGATE THREATS USING MICROSOFT PURVIEW

MODULE 4: MITIGATE THREATS USING MICROSOFT DEFENDER FOR ENDPOINT

MODULE 5: MITIGATE THREATS USING MICROSOFT DEFENDER FOR CLOUD

MODULE 6: CREATE QUERIES FOR MICROSOFT SENTINEL USING KUSTO QUERY LANGUAGE (KQL)

SC 200T00-A: Defend Against Cyberthreats with Microsoft's Security Operations Platform

MODULE 7: CONFIGURE YOUR MICROSOFT SENTINEL ENVIRONMENT

MODULE 8: CONNECT LOGS TO MICROSOFT SENTINEL

MODULE 9: CREATE DETECTIONS AND PERFORM INVESTIGATIONS USING MICROSOFT SENTINEL

MODULE 10: PERFORM THREAT HUNTING IN MICROSOFT SENTINEL