SC 5004- Defend Against Cyberthreats With Microsoft Defender XDR

Days: 1

Prerequisites: Experience using the Microsoft Defender portal. Basic understanding of Microsoft Defender for Endpoint. Basic understanding of Microsoft Sentinel. Experience using Kusto Query Language (KQL) in Microsoft Sentinel.

Audience: Security Operations Analyst

Description: Implement the Microsoft Defender for Endpoint environment to manage devices, perform investigations on endpoints, manage incidents in Defender XDR, and use Advanced Hunting with Kusto Query Language (KQL) to detect unique threats.

OUTLINE:

LESSON 1 - MITIGATE INCIDENTS USING MICROSOFT DEFENDER

- Use the Microsoft Defender portal
- Manage incidents
- Investigate incidents
- Manage and investigate alerts
- Manage automated investigations
- Use the action center
- Explore advanced hunting
- Investigate Microsoft Entra sign-in logs
- Understand Microsoft Secure Score
- Analyze threat analytics
- Analyze reports
- Configure the Microsoft Defender portal

LESSON 2 - DEPLOY THE MICROSOFT DEFENDER FOR ENDPOINT ENVIRONMENT

- Create your environment
- Understand operating systems compatibility and features
- Onboard devices
- Manage access
- Create and manage roles for role-based access control
- Configure device groups
- Configure environment advanced features

LESSON 3 - CONFIGURE FOR ALERTS AND DETECTIONS IN MICROSOFT DEFENDER FOR ENDPOINT

- Configure advanced features
- Configure alert notifications
- Manage alert suppression
- Manage indicators

LESSON 4 - CONFIGURE AND MANAGE AUTOMATION USING MICROSOFT DEFENDER FOR ENDPOINT

- Configure advanced features
- Manage automation upload and folder settings
- Configure automated investigation and remediation capabilities
- Block at risk devices

LESSON 5 - PERFORM DEVICE INVESTIGATIONS IN MICROSOFT DEFENDER FOR ENDPOINT

- Use the device inventory list
- Investigate the device
- Use behavioral blocking
- Detect devices with device discovery

LESSON 6 - DEFEND AGAINST CYBERTHREATS WITH MICROSOFT DEFENDER XDR LAB EXERCISES

- Configure the Microsoft Defender XDR environment
- Deploy Microsoft Defender for Endpoint
- Mitigate Attacks with Microsoft Defender for Endpoint

SC 5004- Defend Against Cyberthreats With Microsoft Defender XDR