SC-5004 Defend against cyberthreats with Microsoft Defender XDR

Overview

Course Duration: 1 Days

About This Course

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

Audience Profile

Suited for Security Operations Analysts.

Course Outline

Module 1: Mitigate incidents using Microsoft Defender

Learn how the Microsoft Defender portal provides a unified view of incidents from the Microsoft Defender family of products.

Lesson

- Manage incidents in Microsoft Defender
- Investigate incidents in Microsoft Defender
- Conduct advanced hunting in Microsoft Defender

Module 2: Deploy the Microsoft Defender for Endpoint environment

Learn how to deploy the Microsoft Defender for Endpoint environment, including onboarding devices and configuring security.

Lesson

- Create a Microsoft Defender for Endpoint environment
- Onboard devices to be monitored by Microsoft Defender for Endpoint
- Configure Microsoft Defender for Endpoint environment settings

Module 3: Configure for alerts and detections in Microsoft Defender for Endpoint

Learn how to configure settings to manage alerts and notifications. You'll also learn to enable indicators as part of the detection process.

Lesson

- Configure alert settings in Microsoft Defender for Endpoint
- Manage indicators in Microsoft Defender for Endpoint

Module 4: Perform device investigations in Microsoft Defender for Endpoint

Microsoft Defender for Endpoint provides detailed device information, including forensics information. Learn about information available to you through Microsoft Defender for Endpoint that aids in your investigations.

Lesson

- Use the device page in Microsoft Defender for Endpoint
- Describe device forensics information collected by Microsoft Defender for Endpoint
- Describe behavioral blocking by Microsoft Defender for Endpoint

Module 5: Defend against Cyberthreats with Microsoft Defender XDR lab exercises

In this module, you learned how to configure Microsoft Defender XDR, deploy Microsoft Defender for Endpoint, and onboard devices. You also configured policies, mitigated threats and responded to incidents with Defender XDR.

Lesson

- Configure the Microsoft Defender XDR environment
- Deploy Microsoft Defender for Endpoint
- Mitigate threats using Microsoft Defender for Endpoint
- Investigate and respond to incidents using Microsoft Defender XDR

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