SC-5004: Defend against cyberthreats with Microsoft Defender XDR

Course ID #: 7000-1091-ZZ-Z
Hours: 7

Course Content

Description:

In this course, you will cover: 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.

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

Target Audience:

Security Operations Analyst

Topics:

Lesson 1: Mitigate incidents using Microsoft Defender

- Introduction
- 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
- Module assessment
- Summary and resources

Lesson 2: Deploy the Microsoft Defender for Endpoint environment

- Introduction
- Use the Microsoft Defender porta
- Manage incidents
- Investigate incidents
- Manage and investigate alerts
- Manage automated investigations
- Use the action center14 min
- Explore advanced hunting3 min
- Investigate Microsoft Entra sign-in logs
- Understand Microsoft Secure Score
- Analyze threat analytics
- Analyze reports
- Configure the Microsoft Defender porta
- Module assessment
- Summary and resources

SC-5004: Defend against cyberthreats with Microsoft Defender XDR

Course ID #: 7000-1091-ZZ-Z
Hours: 7

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

- Introduction
- Use the Microsoft Defender porta
- 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
- Module assessment
- Summary and resources

Lesson 4: Configure and manage automation using Microsoft Defender for Endpoint

- Introduction
- Use the Microsoft Defender porta
- 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
- Module assessment
- Summary and resources

Lesson 5: Perform device investigations in Microsoft Defender for Endpoint

- Introduction
- 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
- Module assessment
- Summary and resources

Lesson 6: Defend against Cyberthreats with Microsoft Defender XDR lab exercises

- Introduction
- 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
- Module assessment
- Summary and resources

SC-5004: Defend against cyberthreats with Microsoft Defender XDR

Course ID #: 7000-1091-ZZ-Z
Hours: 7

NASBA Information

Attendance Requirement: To be awarded the full credit hours, you must sign in and attend the entire course.
Recommended Field(s) of Study:
Recommended CPEs: 7.80

Policies: Course Registration, Cancellation, Refund, and Complaint Resolution
For more information regarding administrative policies such as complaint and program cancellation policies, please contact our offices at 800-639-3535 or visit us at: **www.tcworkshop.com**

Official National Registry Statement:
The Computer Workshop is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credits. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: www.nasbaregistry.org

NOTE: Since our information is in multiple places on our website or in PDF format that is sent to clients, we have provided our normal course content with the NASBA Information added along with links to our policy page on the web. We will add our name to the Official National Registry Statement after we are approved.