Document Generated: 02/18/2026

Learning Style: Virtual Classroom

Technology: Microsoft

Difficulty: Beginner

Course Duration: 1 Day

Defend against cyberthreats with Microsoft Defender XDR (SC-5004)

About Course:

This hands-on course teaches Security Operations Analysts how to implement Microsoft Defender XDR to detect, investigate, and mitigate cyberthreats. Learn how to deploy Microsoft Defender for Endpoint, configure security settings, manage

incidents, automate responses, and use Advanced Hunting with Kusto Query Language (KQL) to identify and respond to threats in real time. Gain practical experience in securing endpoints, managing alerts, and improving your organization’s security posture.

Course Objectives:

- Mitigate incidents using Microsoft Defender
- Deploy the Microsoft Defender for Endpoint environment
- Configure for alerts and detections in Microsoft Defender for Endpoi
- Configure and manage automation using Microsoft Defender for Endpoint
- Perform device investigations in Microsoft Defender for Endpoint
- Defend against Cyberthreats with Microsoft Defender XDR lab exercises

Audience:

- IT Security Professionals & Cybersecurity Engineers
- IT / Network Administrators

Prerequisites:

- Familiarity with Microsoft Defender for Endpoint, Microsoft 365 Defender, and Microsoft Sentinel platforms.
- Knowledge of security concepts like threat detection, incident response, and security operations workflows

Course Outline:

- 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
- 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
- Configure advanced features
- Configure alert notifications
- Manage alert suppression
- Manage indicators
- Configure advanced features
- Manage automation upload and folder settings
- Configure automated investigation and remediation capabilities
- Block at risk devices
- Use the device inventory list
- Investigate the device
- Use behavioral blocking
- Detect devices with device discovery
- Configure the Microsoft Defender XDR environment
- Deploy Microsoft Defender for Endpoint
- Mitigate Attacks with Microsoft Defender for Endpoint