DEFEND AGAINST CYBERTHREATS WITH MICROSOFT DEFENDER XDR (SC-5004)

Course Code: 834084

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. You'll need to have access to a Microsoft 365 E5 Tenant with a Microsoft Defender for Endpoint P2 license to perform the exercises.

What You'll Learn

In this course you will learn:

- How the Microsoft Defender portal provides a unified view of incidents from the Microsoft Defender family of products.
- How to eploy the Microsoft Defender for Endpoint environment, including onboarding devices and configuring security.
- How to configure settings to manage alerts and notifications. You'll also learn to enable indicators as part of the detection process.
- How to configure automation in Microsoft Defender for Endpoint by managing environmental settings.
- 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.

Who Needs to Attend

Suited for Security Operations Analysts

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

DEFEND AGAINST CYBERTHREATS WITH MICROSOFT DEFENDER XDR (SC-5004)

Course Code: 834084

CLASSROOM LIVE	$675 CAD	1 Day

Classroom Live Outline

Module 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
- Knowledge check
- Summary and resources

Module 2: Deploy the Microsoft Defender for Endpoint environment

- Introduction
- 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
- Knowledge check

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

- Introduction
- Configure advanced features
- Configure alert notifications
- Manage alert suppression
- Manage indicators
- Knowledge check
- Summary and resources

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

- Introduction
- Configure advanced features
- Manage automation upload and folder settings
- Configure automated investigation and remediation capabilities
- Block at risk devices
- Knowledge check
- Summary and resources

Module 5: Perform device investigations in Microsoft Defender for Endpoint

- Introduction
- Use the device inventory list
- Investigate the device
- Use behavioral blocking
- Detect devices with device discovery
- Knowledge check
- Summary and resources

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

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

DEFEND AGAINST CYBERTHREATS WITH MICROSOFT DEFENDER XDR (SC-5004)

Course Code: 834084

VIRTUAL CLASSROOM LIVE	$675 CAD	1 Day

Virtual Classroom Live Outline

Module 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
- Knowledge check
- Summary and resources

Module 2: Deploy the Microsoft Defender for Endpoint environment

- Introduction
- 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
- Knowledge check

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

- Introduction
- Configure advanced features
- Configure alert notifications
- Manage alert suppression
- Manage indicators
- Knowledge check
- Summary and resources

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

- Introduction
- Configure advanced features
- Manage automation upload and folder settings
- Configure automated investigation and remediation capabilities
- Block at risk devices
- Knowledge check
- Summary and resources

Module 5: Perform device investigations in Microsoft Defender for Endpoint

- Introduction
- Use the device inventory list
- Investigate the device
- Use behavioral blocking
- Detect devices with device discovery
- Knowledge check
- Summary and resources

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

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

Sep 8 - 8, 2025 | 9:00 AM - 5:00 PM EDT

DEFEND AGAINST CYBERTHREATS WITH MICROSOFT DEFENDER XDR (SC-5004)

Course Code: 834084

PRIVATE GROUP TRAINING	1 Day

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 5/9/2025 2:27:51 AM