MS-SC5004: DEFEND AGAINST CYBERTHREATS WITH MICROSOFT DEFENDER XDR

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
1 Day	Intermediate	Security	Instructor-led	NA

INTRODUCTION

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 will need to have access to a Microsoft 365 Tenant with a Microsoft Defender for Endpoint P2 license to perform the exercises.

AUDIENCE PROFILE

This course is aimed at Security Operations Analysts.

PREREQUISITES

Before attending this course, students should have:

- 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

COURSE OBJECTIVES

After completing this course, students will be able to:

- Configure a Microsoft Defender XDR environment
- Manage devices using Microsoft Defender for Endpoint
- Handle incidents in Microsoft Defender XDR
- Perform investigations on endpoints
- Use Advanced Hunting with Kusto Query Language (KQL) to detect unique threats

COURSE CONTENT

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.

Lessons

- 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

Upon completion of this module, you should be able to:

- 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.

Lessons

- 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
- Summary and resources

Upon completion of this module, you should be able to:

- 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.

Lessons

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

Upon completion of this module, you should be able to:

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

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

Learn how to configure automation in Microsoft Defender for Endpoint by managing environmental settings.

Lessons

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

Upon completion of this module, you should be able to:

- Configure advanced features of Microsoft Defender for Endpoint
- Manage automation settings in Microsoft Defender for Endpoint

Module 5: 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.

Lessons

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

Upon completion of this module, you should be able to:

- 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 6: 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.

Lessons

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

Upon completion of this module, you should be able to:

- 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

ASSOCIATED CERTIFICATIONS & EXAM

There is no Associated Certification or Exam for this course, however, there is an assessment to achieve your Applied Skills credential. (Assessment Link)