Microsoft Security Operations Analyst

Duration: 4 Days

Who should attend:

The Microsoft Security Operations Analyst collaborates with organizational stakeholders to secure information technology systems for the organization. Their goal is to reduce organizational risk by rapidly remediating active attacks in the environment, advising on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders. Responsibilities include threat management, monitoring, and response by using a variety of security solutions across their environment. The role primarily investigates, responds to, and hunts for threats using Microsoft Azure Sentinel, Azure Defender, Microsoft 365 Defender, and third-party security products. Since the Security Operations Analyst consumes the operational output of these tools, they are also a critical stakeholder in the configuration and deployment of these technologies.

Learn how to investigate, respond to, and hunt for threats using Microsoft Azure Sentinel, Azure Defender, and Microsoft 365 Defender. In this course you will learn how to mitigate cyberthreats using these technologies. Specifically, you will configure and use Azure Sentinel as well as utilize Kusto Query Language (KQL) to perform detection, analysis, and reporting. The course was designed for people who work in a Security Operations job role and helps learners prepare for the exam SC-200: Microsoft Security Operations Analyst.

Pre-requisites:

Delegates should have:

- Basic understanding of Microsoft 365
- Fundamental understanding of Microsoft security, compliance, and identity products
- Intermediate understanding of Windows 10
- Familiarity with Azure services, specifically Azure SQL Database and Azure Storage
- Familiarity with Azure virtual machines and virtual networking
- Basic understanding of scripting concepts.

Content

Module 1: Introduction to Microsoft 365 threat protection

In this module, you'll learn how to use the Microsoft 365 Defender integrated threat protection suite.
Learning objectives
In this module, you learned the role that Microsoft 365 Defender plays in a modern SOC. You should now be able to:

- Understand Microsoft 365 Defender solution by domain
- Understand Microsoft 365 Defender role in a Modern SOC
- Introduction
- Explore Extended Detection & Response (XDR) response use cases
- Understand Microsoft 365 Defender in a Security Operations Center (SOC)
- Investigate security incident in Microsoft 365 Defender
- Knowledge check
- Summary and resources

Module 2: Mitigate incidents using Microsoft 365 Defender

Learn how the Microsoft 365 Defender portal provides a unified view of incidents from the Microsoft 365 Defender family of products.

Learning objectives

Upon completion of this module, the learner will be able to:

- Manage incidents in Microsoft 365 Defender
- Investigate incidents in Microsoft 365 Defender
- Conduct advanced hunting in Microsoft 365 Defende
- Introduction
- Use the Microsoft 365 Defender portal
- Manage incidents
- Investigate incidents
- Manage and investigate alerts
- Manage automated investigations
- Use the action center
- Explore advanced hunting
- Investigate Azure AD sign-in logs
- Understand Microsoft Secure Score
- Analyze threat analytics
- Analyze reports
- Configure the Microsoft 365 Defender portal
- Knowledge check
- Summary and resources

Module 3: Protect your identities with Azure AD Identity Protection

Use the advanced detection and remediation of identity-based threats to protect your Azure Active Directory identities and applications from compromise.

Learning objectives

In this module, you will:

- Describe the features of Azure Active Directory Identity Protection.
- Describe the investigation and remediation features of Azure Active Directory Identity Protection.
- Introduction
- Azure AD Identity Protection overview
- Detect risks with Azure AD Identity Protection policies
- Investigate and remediate risks detected by Azure AD Identity Protection
- Summary

Module 4: Remediate risks with Microsoft Defender for Office 365

Learn about the Microsoft Defender for Office 365 component of Microsoft 365 Defender.

Learning objectives

In this module, you will learn how to:

- Define the capabilities of Microsoft Defender for Office 365.
- Understand how to simulate attacks within your network.
- Explain how Microsoft Defender for Office 365 can remediate risks in your environment.
- Introduction to Microsoft Defender for Office 365

- Automate, investigate, and remediate
- Configure, protect, and detect
- Simulate attacks
- Summary and knowledge check

Module 5: Safeguard your environment with Microsoft Defender for Identity
Learn about the Microsoft Defender for Identity component of Microsoft 365 Defender.
Learning objectives
Upon completion of this module, you should be able to:

- Define the capabilities of Microsoft Defender for Identity.
- Understand how to configure Microsoft Defender for Identity sensors.
- Explain how Microsoft Defender for Identity can remediate risks in your environment.
- Introduction to Microsoft Defender for Identity
- Configure Microsoft Defender for Identity sensors
- Review compromised accounts or data
- Integrate with other Microsoft tools
- Summary and knowledge check