Microsoft Security

SC-200T00: Microsoft Security Operations Analyst

$2,595.00

- 4 Days

Upcoming Dates

Jul 07 - Jul 10
Oct 27 - Oct 30

Course Description

Learn how to investigate, respond to, and hunt for threats using Microsoft Sentinel, Microsoft Defender XDR and Microsoft Defender for Cloud. In this course you will learn how to mitigate cyberthreats using these technologies. Specifically, you will configure and use Microsoft 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

Course Outline

Learning Path 1: Mitigate threats using Microsoft Defender XDR

In this Learning Path we analyze threat data across domains and rapidly remediate threats with built-in orchestration and automation in Microsoft 365 Defender. This learning path aligns with exam SC-200: Microsoft Security Operations Analyst.

Modules:

- Introduction to Microsoft 365 threat protection
- Mitigate incidents using Microsoft Defender VDR
- Protect your identities with Microsoft Entra (Formerly Azure AD)
- Remediate risks with Microsoft Defender for Office 365
- Safeguard your environment with Microsoft Defender for Identity
- Secure your cloud apps and services with Microsoft Defender for Cloud Apps

Labs:

- Deploy Microsoft Defender for Endpoint
- Mitigate Attacks using Defender for Endpoint
- Describe Threat and Vulnerability Management in Microsoft Defender for Endpoint

Learning Path 2: Mitigate threats using Microsoft Copilot for Security

In this Learning Path we get started with Microsoft Copilot for Security. You're introduced to basic terminology, how Microsoft Copilot for Security processes prompts, the elements of an effective prompt, and how to enable the solution. This learning path aligns with exam SC-200: Microsoft Security Operations Analyst.

Modules:

- Fundamentals of Generative AI
- Describe Microsoft Copilot for Security
- Describe the core features of Microsoft Copilot for Security
- Describe the embedded experiences of Microsoft Copilot for Security

Lab:

- Explore Microsoft Security Copilot

Learning Path 3: Mitigate threats using Microsoft Purview

In this Learning Path we focus on Microsoft Purview's risk and compliance solutions that assist security operations analysts detect threats to organizations and identify, classify, and protect sensitive data, as well as monitor and report on compliance. This learning path aligns with exam SC-200: Microsoft Security Operations Analyst.

Modules:

- Microsoft Purview Compliance Solutions
- Respond to data loss prevention alerts using Microsoft 365
- Manage insider risk in Microsoft Purview
- Investigate threats with Content search in Microsoft Purview
- Search and investigate with Microsoft Purview Audit

Lab:

- Explore Microsoft Purview Audit logs

Learning Path 4: Mitigate threats using Microsoft Defender for Endpoint

In this Learning Path we implement the Microsoft Defender for Endpoint platform to detect, investigate, and respond to advanced threats. This learning path aligns with exam SC-200: Microsoft Security Operations Analyst.

Modules:

- Protect against threats with Microsoft Defender for Endpoint
- Deploy the Microsoft Defender for Endpoint environment
- Implement Windows security enhancements
- Perform device investigations
- Perform actions on a device
- Perform evidence and entities investigations
- Configure and manage automation
- Configure for alerts and detections
- Utilize Threat and Vulnerability Management

Lab:

- Mitigate threats using Microsoft Defender for Endpoint

Learning Path 5: Mitigate threats using Microsoft Defender for Cloud

In this learning path we use Microsoft Defender for Cloud, for Azure, hybrid cloud, and on-premises workload protection and security. This learning path aligns with exam SC-200: Microsoft Security Operations Analyst.

Modules:

- Plan for cloud workload protections using Microsoft Defender for Cloud
- Connect Azure assets to Microsoft Defender for Cloud
- Connect non-Azure resources to Microsoft Defender for Cloud
- Manage your cloud security posture management
- Workload protections in Microsoft Defender for Cloud
- Remediate security alerts using Microsoft Defender for Cloud

Labs:

- Deploy Microsoft Defender for Cloud
- Mitigate Attacks with Microsoft Defender for Cloud

Learning Path 6: Create queries for Microsoft Sentinel using Kusto Query Language (KQL)

In this Learning Path we will write Kusto Query Language (KQL) statements to query log data to perform detections, analysis, and reporting in Microsoft Sentinel. This learning path will focus on the most used operators. The example KQL statements will showcase security related table queries.

Modules:

- Construct KQL statements for Azure Sentinel
- Analyze query results using KQL
- Build multi-table statements using KQL
- Work with data in Microsoft Sentinel using Kusto Query Language

Labs:

- Construct Basic KQL Statements
- Analyze query results using KQL
- Build multi-table statements using KQL
- Work with string data using KQL statements

Learning Path 7: Configure your Microsoft Sentinel environment

In this Learning Path we get started with Microsoft Sentinel by properly configuring the Microsoft Sentinel workspace. This learning path aligns with exam SC-200: Microsoft Security Operations Analyst.

Modules:

- Introduction to Microsoft Sentinel
- Create and manage Microsoft Sentinel workspaces
- Query logs in Microsoft Sentinel
- Use watchlists in Microsoft Sentinel
- Utilize threat intelligence in Microsoft Sentinel
- Integrate Microsoft Defender XDR

Labs:

- Create a Microsoft Sentinel Workspace
- Create a Watchlist
- Create a Threat Indicator

Learning Path 8: Connect logs to Microsoft Sentinel

In this Learning Path we connect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds to Microsoft Sentinel. This learning path aligns with exam SC-200: Microsoft Security Operations Analyst.

Modules:

- Connect data to Microsoft Sentinel using data connectors
- Connect Microsoft services to Microsoft Sentinel
- Connect Microsoft XDR Defender to Microsoft Sentinel
- Connect Windows hosts to Microsoft Sentinel
- Connect Common Event Format logs to Microsoft Sentinel
- Connect syslog data sources to Microsoft Sentinel
- Connect threat indicators to Microsoft Sentinel

Labs:

- Connect Microsoft services to Microsoft Sentinel
- Connect Windows hosts to Microsoft Sentinel
- Connect Linux hosts to Microsoft Sentinel
- Connect Threat intelligence to Microsoft Sentinel

Learning Path 9: Create detections and perform investigations using Microsoft Sentinel

In this Learning Path we detect previously uncovered threats and rapidly remediate threats with built-in orchestration and automation in Microsoft Sentinel. This learning path aligns with exam SC-200: Microsoft Security Operations Analyst.

Modules:

- Threat detection with Microsoft Sentinel analytics
- Automation In Microsoft Sentinel
- Threat response with Microsoft Sentinel playbooks
- Security incident management in Microsoft Sentinel
- Identify threats with Entity behavioral analytics in Microsoft Sentinel
- Data normalization in Microsoft Sentinel
- Query, visualize, and monitor data in Microsoft Sentinel
- Manage content in Microsoft Sentinel

Labs:

- Create Analytical Rules
- Model Attacks to Define Rule Logic
- Mitigate Attacks using Microsoft Sentinel
- Create Workbooks in Microsoft Sentinel

Learning Path 10: Perform threat hunting in Azure Sentinel

In this Learning Path we proactively hunt for security threats using the Microsoft Sentinel powerful threat hunting tools. This learning path aligns with exam SC-200: Microsoft Security Operations Analyst.

Modules

- Explain threat hunting concepts in Microsoft Sentinel
- Threat hunting with Microsoft Sentinel
- Using search jobs in Microsoft Sentinel
- Hunt for threats using notebooks in Microsoft Sentinel

Labs:

- Threat Hunting in Microsoft Sentinel
- Threat Hunting using Notebooks

Audience

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, advise 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 Sentinel, Microsoft Defender for Cloud, Microsoft Defender XDR, 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.

Prerequisites

Before attending this course, students must have:

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

What You Will Learn