SC-200T00-AC Microsoft Security Operations Analyst

Overview

Course Duration: 4 Days

About This Course

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.

Audience Profile

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.

Course Outline

Module 1: Mitigate threats using Microsoft Defender XDR

Analyze threat data across domains and rapidly remediate threats with built-in orchestration and automation in Microsoft Defender XDR..

Lesson

- Introduction to Microsoft Defender XDR threat protection
- Mitigate incidents using Microsoft 365 Defender
- Remediate risks with Microsoft Defender for Office 365
- Manage Microsoft Entra Identity Protection
- Safeguard your environment with Microsoft Defender for Identity
- Secure your cloud apps and services with Microsoft Defender for Cloud Apps

Module 2: Mitigate threats using Microsoft Security Copilot

Get started with Microsoft Security Copilot. You're introduced to basic terminology, how Microsoft Security Copilot processes prompts, the elements of an effective prompt, and how to enable the solution**.**

Lesson

- Introduction to generative AI
- Describe Microsoft Security Copilot
- Describe the core features of Microsoft Security Copilot
- Describe the embedded experiences of Microsoft Security Copilot
- Explore use cases of Microsoft Security Copilot

Module 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.

Lesson

- Investigate and respond to Microsoft Purview Data Loss Prevention alerts
- Investigate insider risk alerts and related activity
- Search and investigate with Microsoft Purview Audit
- Investigate threats with Content search in Microsoft Purview

Module 4: Mitigate threats using Microsoft Defender for Endpoint

Implement the Microsoft Defender for Endpoint platform to detect, investigate, and respond to advanced threats..

Lesson

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

Module 5: Mitigate threats using Microsoft Defender for Cloud

Use Microsoft Defender for Cloud, for Azure, hybrid cloud, and on-premises workload protection and security.

Lesson

- 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
- Explain cloud workload protections in Microsoft Defender for Cloud
- Remediate security alerts using Microsoft Defender for Cloud

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

Write Kusto Query Language (KQL) statements to query log data to perform detections, analysis, and reporting in Microsoft Sentinel.

Lesson

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

Module 7: Configure your Microsoft Sentinel environment

Get started with Microsoft Sentinel by properly configuring the Microsoft Sentinel workspace

Lesson

- 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 with Microsoft Sentinel

Module 8: Connect logs to Microsoft Sentinel
Connect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds to Microsoft Sentinel.
Lesson

- Connect data to Microsoft Sentinel using data connectors
- Connect Microsoft services to Microsoft Sentinel
- Connect Microsoft Defender XDR 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

Module 9: Create detections and perform investigations using Microsoft Sentinel
Detect previously uncovered threats and rapidly remediate threats with built-in orchestration and automation in Microsoft Sentinel.
Lesson

- 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 Behavioral Analytics
- Data normalization in Microsoft Sentinel
- Query, visualize, and monitor data in Microsoft Sentinel
- Manage content in Microsoft Sentinel

Module 9: Perform threat hunting in Microsoft Sentinel
Proactively hunt for security threats using the Microsoft Sentinel powerful threat hunting tools
Lesson

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

Prerequisites

- Fundamental understanding of Microsoft security, compliance, and identity products
- Basic understanding of Microsoft Defender XDR