Microsoft
CERTIFIED
SECURITY OPERATIONS
ANALYST
ASSOCIATE

Microsoft Security Operations Analyst

Course Duration: 4 Days
Exam Reference: SC-200

Course Overview

This course trains security professionals to investigate, respond to, and hunt for threats using Microsoft's primary security tools: Microsoft Sentinel (SIEM/SOAR), Microsoft Defender XDR, and Microsoft Defender for Cloud. You will master Kusto Query Language (KQL) for detection and reporting, and learn to reduce organizational risk by rapidly remediating active attacks and advising on improvements to threat protection practices.

Prerequisites

Success is dependent on a background in security principles and the Microsoft cloud platform. This course immediately dives into implementation of advanced tools.

Course Objectives

- Mitigate threats across endpoints, identity, email, and cloud apps using the Microsoft Defender XDR suite.
- Configure and utilize Microsoft Sentinel (SIEM) for log ingestion, alert creation, and incident investigation.
- Perform advanced threat hunting using Kusto Query Language (KQL) and specialized Sentinel tools.
- Manage and mitigate risks related to information protection, data loss, and insider threats using Microsoft Purview.
- Understand and utilize Microsoft Security Copilot for faster threat analysis and response leveraging Generative AI.

ATA
APPLIED
TECHNOLOGY
ACADEMY

Contact Us

☎

800.674.3550

2151 W. Hillsboro Blvd., Ste 210
Deerfield Beach, FL 33442

Connect With Us

AppliedTechnologyAcademy.com

Microsoft Security Operations Analyst

Course Outline

Module 1: Mitigate threats using Microsoft Defender XDR

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

Module 2: Mitigate threats using Microsoft Security Copilot

- Fundamentals of 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

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

Module 4: Mitigate threats using Microsoft Defender for Endpoint

- 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

- 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)

- 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

- 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 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

- 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 10: Perform threat hunting in Microsoft Sentinel

- 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