
SC-200T00: Microsoft Security Operations Analyst

Learn how to investigate, respond to, and hunt for threats using Microsoft Sentinel, Microsoft Defender for Cloud, and Microsoft 365 Defender. 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.

Objectives

- Explain how Microsoft Defender for Endpoint can remediate risks in your environment
- Administer a Microsoft Defender for Endpoint environment
- Configure Attack Surface Reduction rules on Windows devices
- Perform actions on a device using Microsoft Defender for Endpoint
- Investigate domains and IP addresses in Microsoft Defender for Endpoint
- Investigate user accounts in Microsoft Defender for Endpoint
- Configure alert settings in Microsoft 365 Defender
- Explain how the threat landscape is evolving
- Conduct advanced hunting in Microsoft 365 Defender
- Manage incidents in Microsoft 365 Defender
- Explain how Microsoft Defender for Identity can remediate risks in your environment
- Investigate DLP alerts in Microsoft Defender for Cloud Apps
- Explain the types of actions you can take on an insider risk management case

- Configure auto-provisioning in Microsoft Defender for Cloud Apps
- Remediate alerts in Microsoft Defender for Cloud Apps
- Construct KQL statements
- Filter searches based on event time, severity, domain, and other relevant data using KQL
- Extract data from unstructured string fields using KQL
- Manage a Microsoft Sentinel workspace
- Use KQL to access the watchlist in Microsoft Sentinel
- Manage threat indicators in Microsoft Sentinel
- Explain the Common Event Format and Syslog connector differences in Microsoft Sentinel
- Connect Azure Windows Virtual Machines to Microsoft Sentinel
- Configure Log Analytics agent to collect Sysmon events
- Create new analytics rules and queries using the analytics rule wizard
- Create a playbook to automate an incident response
- Use queries to hunt for threats
- Observe threats over time with livestream

Prerequisites

- 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.

Intended 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, 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 Sentinel, Microsoft Defender for Cloud, 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.

Topics

- Mitigate threats using Microsoft Defender for Endpoint
- Mitigate threats using Microsoft 365 Defender
- Mitigate threats using Azure Defender
- Create queries for Azure Sentinel using Kusto Query Language (KQL)
- Configure your Azure Sentinel environment
- Connect logs to Azure Sentinel
- Create detections and perform investigations using Azure Sentinel
- Perform threat hunting in Azure Sentinel