

SC-200T00-A: Microsoft Security Operations Analyst

Course Summary

Description

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.

Objectives

At the end of this course, students will be able to:

- Explain how Microsoft Defender for Endpoint can remediate risks in your environment
- Create a Microsoft Defender for Endpoint environment
- Configure Attack Surface Reduction rules on Windows 10 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 Defender for Endpoint
- 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 Cloud App Security
- Explain the types of actions you can take on an insider risk management case.
- Configure auto-provisioning in Azure Defender
- Remediate alerts in Azure Defender
- 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 an Azure Sentinel workspace
- Use KQL to access the watchlist in Azure Sentinel
- Manage threat indicators in Azure Sentinel
- Explain the Common Event Format and Syslog connector differences in Azure Sentinel
- Connect Azure Windows Virtual Machines to Azure 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

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

SC-200T00-A: Microsoft Security Operations Analyst

Course Summary (cont'd)

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 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.

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.

Duration

Four days

SC-200T00-A: Microsoft Security Operations Analyst

Course Outline

I. Mitigate threats using Microsoft Defender for Endpoint

Implement the Microsoft Defender for Endpoint platform to detect, investigate, and respond to advanced threats. Learn how Microsoft Defender for Endpoint can help your organization stay secure. Learn how to deploy the Microsoft Defender for Endpoint environment, including onboarding devices and configuring security. Learn how to investigate incidents and alerts using Microsoft Defender for Endpoints. Perform advanced hunting and consult with threat experts. You will also learn how to configure automation in Microsoft Defender for Endpoint by managing environmental settings.. Lastly, you will learn about your environment's weaknesses by using Threat and Vulnerability Management in Microsoft Defender for Endpoint.

- A. Protect against threats with Microsoft Defender for Endpoint
- B. Deploy the Microsoft Defender for Endpoint environment
- C. Implement Windows 10 security enhancements with Microsoft Defender for Endpoint
- D. Manage alerts and incidents in Microsoft Defender for Endpoint
- E. Perform device investigations in Microsoft Defender for Endpoint
- F. Perform actions on a device using Microsoft Defender for Endpoint
- G. Perform evidence and entities investigations using Microsoft Defender for Endpoint
- H. Configure and manage automation using Microsoft Defender for Endpoint
- I. Configure for alerts and detections in Microsoft Defender for Endpoint
- J. Utilize Threat and Vulnerability Management in Microsoft Defender for Endpoint

Lab : Mitigate threats using Microsoft Defender for Endpoint

- Deploy Microsoft Defender for Endpoint
- Mitigate Attacks using Defender for Endpoint

II. Mitigate threats using Microsoft 365 Defender

Analyze threat data across domains and rapidly remediate threats with built-in orchestration and automation in Microsoft 365 Defender. Learn about

cybersecurity threats and how the new threat protection tools from Microsoft protect your organization's users, devices, and data. Use the advanced detection and remediation of identity-based threats to protect your Azure Active Directory identities and applications from compromise.

- A. Introduction to threat protection with Microsoft 365
 - B. Mitigate incidents using Microsoft 365 Defender
 - C. Protect your identities with Azure AD Identity Protection
 - D. Remediate risks with Microsoft Defender for Office 365
 - E. Safeguard your environment with Microsoft Defender for Identity
 - F. Secure your cloud apps and services with Microsoft Cloud App Security
 - G. Respond to data loss prevention alerts using Microsoft 365
 - H. Manage insider risk in Microsoft 365
- Lab : Mitigate threats using Microsoft 365 Defender
- Mitigate Attacks with Microsoft 365 Defender

III. Mitigate threats using Azure Defender

Use Azure Defender integrated with Azure Security Center, for Azure, hybrid cloud, and on-premises workload protection and security. Learn the purpose of Azure Defender, Azure Defender's relationship to Azure Security Center, and how to enable Azure Defender. You will also learn about the protections and detections provided by Azure Defender for each cloud workload. Learn how you can add Azure Defender capabilities to your hybrid environment.

- A. Plan for cloud workload protections using Azure Defender
- B. Explain cloud workload protections in Azure Defender
- C. Connect Azure assets to Azure Defender
- D. Connect non-Azure resources to Azure Defender
- E. Remediate security alerts using Azure Defender

Lab : Mitigate threats using Azure Defender

- Deploy Azure Defender
- Mitigate Attacks with Azure Defender

SC-200T00-A: Microsoft Security Operations Analyst

Course Outline (cont'd)

IV. Create queries for Azure Sentinel using Kusto Query Language (KQL)

Write Kusto Query Language (KQL) statements to query log data to perform detections, analysis, and reporting in Azure Sentinel. This module will focus on the most used operators. The example KQL statements will showcase security related table queries. KQL is the query language used to perform analysis on data to create analytics, workbooks, and perform hunting in Azure Sentinel. Learn how basic KQL statement structure provides the foundation to build more complex statements. Learn how to summarize and visualize data with a KQL statement provides the foundation to build detections in Azure Sentinel. Learn how to use the Kusto Query Language (KQL) to manipulate string data ingested from log sources.

- A. Construct KQL statements for Azure Sentinel
- B. Analyze query results using KQL
- C. Build multi-table statements using KQL
- D. Work with data in Azure Sentinel using Kusto Query Language

Lab : Create queries for Azure Sentinel using Kusto Query Language (KQL)

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

V. Configure your Azure Sentinel environment

Get started with Azure Sentinel by properly configuring the Azure Sentinel workspace. Traditional security information and event management (SIEM) systems typically take a long time to set up and configure. They're also not necessarily designed with cloud workloads in mind. Azure Sentinel enables you to start getting valuable security insights from your cloud and on-premises data quickly. This module helps you get started. Learn about the architecture of Azure Sentinel workspaces to ensure you configure your system to meet your organization's security operations requirements. As a Security Operations Analyst, you must understand the tables, fields, and data ingested in your workspace. Learn how to query the most used data tables in Azure Sentinel.

- A. Introduction to Azure Sentinel
- B. Create and manage Azure Sentinel workspaces

- C. Query logs in Azure Sentinel
- D. Use watchlists in Azure Sentinel
- E. Utilize threat intelligence in Azure Sentinel

Lab : Configure your Azure Sentinel environment

- Create an Azure Sentinel Workspace
- Create a Watchlist
- Create a Threat Indicator

VI. Connect logs to Azure Sentinel

Connect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds to Azure Sentinel. The primary approach to connect log data is using the Azure Sentinel provided data connectors. This module provides an overview of the available data connectors. You will get to learn about the configuration options and data provided by Azure Sentinel connectors for Microsoft 365 Defender.

- A. Connect data to Azure Sentinel using data connectors
- B. Connect Microsoft services to Azure Sentinel
- C. Connect Microsoft 365 Defender to Azure Sentinel
- D. Connect Windows hosts to Azure Sentinel
- E. Connect Common Event Format logs to Azure Sentinel
- F. Connect syslog data sources to Azure Sentinel
- G. Connect threat indicators to Azure Sentinel

Lab : Connect logs to Azure Sentinel

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

SC-200T00-A: Microsoft Security Operations Analyst

Course Outline (cont'd)

VII. Create detections and perform investigations using Azure Sentinel

Detect previously uncovered threats and rapidly remediate threats with built-in orchestration and automation in Azure Sentinel. You will learn how to create Azure Sentinel playbooks to respond to security threats. You'll investigate Azure Sentinel incident management, learn about Azure Sentinel events and entities, and discover ways to resolve incidents. You will also learn how to query, visualize, and monitor data in Azure Sentinel.

- A. Threat detection with Azure Sentinel analytics
- B. Threat response with Azure Sentinel playbooks
- C. Security incident management in Azure Sentinel
- D. Use entity behavior analytics in Azure Sentinel
- E. Query, visualize, and monitor data in Azure Sentinel

Lab : Create detections and perform investigations using Azure Sentinel

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

VIII. Perform threat hunting in Azure Sentinel

In this module, you'll learn to proactively identify threat behaviors by using Azure Sentinel queries. You'll also learn to use bookmarks and livestream to hunt threats. You will also learn how to use notebooks in Azure Sentinel for advanced hunting.

- A. Threat hunting with Azure Sentinel
- B. Hunt for threats using notebooks in Azure Sentinel

Lab : Threat hunting in Azure Sentinel

- Threat Hunting in Azure Sentinel
- Threat Hunting using Notebooks