# Microsoft Security Operations Analyst

### Course SC-200T00-A: 3 days; Instructor-Led

## Introduction

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.

## Skills gained

- 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

## 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.

 

Job role: Security Engineer, Security Operations Analyst
Preparation for exam: SC-200

## 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.

## Course Outline

**Module 1: 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.

**Lessons**

- Protect against threats with Microsoft Defender for Endpoint
- Deploy the Microsoft Defender for Endpoint environment
- Implement Windows 10 security enhancements with Microsoft Defender for Endpoint
- Manage alerts and incidents in 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 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

After completing this module, students will be able to:

- Define the capabilities of Microsoft Defender for Endpoint
- Configure Microsoft Defender for Endpoint environment settings
- Configure Attack Surface Reduction rules on Windows 10 devices
- Investigate alerts in Microsoft Defender for Endpoint
- Describe device forensics information collected by Microsoft Defender for Endpoint
- Conduct forensics data collection using Microsoft Defender for Endpoint
- Investigate user accounts in Microsoft Defender for Endpoint
- Manage automation settings in Microsoft Defender for Endpoint
- Manage indicators in Microsoft Defender for Endpoint
- Describe Threat and Vulnerability Management in Microsoft Defender for Endpoint

**Module 2: 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.

**Lessons**

- Introduction to threat protection with Microsoft 365
- Mitigate incidents using Microsoft 365 Defender
- Protect your identities with Azure AD Identity Protection

 

- Remediate risks with Microsoft Defender for Office 365
- Safeguard your environment with Microsoft Defender for Identity
- Secure your cloud apps and services with Microsoft Cloud App Security
- Respond to data loss prevention alerts using Microsoft 365
- Manage insider risk in Microsoft 365

**Lab : Mitigate threats using Microsoft 365 Defender**

- Mitigate Attacks with Microsoft 365 Defender

After completing this module, students will be able to:

- Explain how the threat landscape is evolving.
- Manage incidents in Microsoft 365 Defender
- Conduct advanced hunting in Microsoft 365 Defender
- Describe the investigation and remediation features of Azure Active Directory Identity Protection.
- Define the capabilities of Microsoft Defender for Endpoint.
- Explain how Microsoft Defender for Endpoint can remediate risks in your environment.
- Define the Cloud App Security framework
- Explain how Cloud Discovery helps you see what's going on in your organization

**Module 3: 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.

**Lessons**

- Plan for cloud workload protections using Azure Defender
- Explain cloud workload protections in Azure Defender
- Connect Azure assets to Azure Defender
- Connect non-Azure resources to Azure Defender
- Remediate security alerts using Azure Defender

**Lab : Mitigate threats using Azure Defender**

- Deploy Azure Defender
- Mitigate Attacks with Azure Defender

After completing this module, students will be able to:

- Describe Azure Defender features
- Explain Azure Security Center features
- Explain which workloads are protected by Azure Defender
- Explain how Azure Defender protections function
- Configure auto-provisioning in Azure Defender
- Describe manual provisioning in Azure Defender
- Connect non-Azure machines to Azure Defender
- Describe alerts in Azure Defender
- Remediate alerts in Azure Defender
- Automate responses in Azure Defender

**Module 4: 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.

**Lessons**

- Construct KQL statements for Azure Sentinel
- Analyze query results using KQL
- Build multi-table statements using KQL

 

- 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

After completing this module, students will be able to:

- Construct KQL statements
- Search log files for security events using KQL
- Filter searches based on event time, severity, domain, and other relevant data using KQL
- Summarize data using KQL statements
- Render visualizations using KQL statements
- Extract data from unstructured string fields using KQL
- Extract data from structured string data using KQL
- Create Functions using KQL

**Module 5: 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.

**Lessons**

- Introduction to Azure Sentinel
- Create and manage Azure Sentinel workspaces
- Query logs in Azure Sentinel
- Use watchlists in Azure Sentinel
- Utilize threat intelligence in Azure Sentinel

**Lab : Configure your Azure Sentinel environment**

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

After completing this module, students will be able to:

- Identify the various components and functionality of Azure Sentinel.
- Identify use cases where Azure Sentinel would be a good solution.
- Describe Azure Sentinel workspace architecture
- Install Azure Sentinel workspace
- Manage an Azure Sentinel workspace
- Create a watchlist in Azure Sentinel
- Use KQL to access the watchlist in Azure Sentinel
- Manage threat indicators in Azure Sentinel
- Use KQL to access threat indicators in Azure Sentinel

**Module 6: 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.

**Lessons**

- Connect data to Azure Sentinel using data connectors
- Connect Microsoft services to Azure Sentinel
- Connect Microsoft 365 Defender to Azure Sentinel
- Connect Windows hosts to Azure Sentinel

 

- Connect Common Event Format logs to Azure Sentinel
- Connect syslog data sources to Azure Sentinel
- 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

After completing this module, students will be able to:

- Explain the use of data connectors in Azure Sentinel
- Explain the Common Event Format and Syslog connector differences in Azure Sentinel
- Connect Microsoft service connectors
- Explain how connectors auto-create incidents in Azure Sentinel
- Activate the Microsoft 365 Defender connector in Azure Sentinel
- Connect Azure Windows Virtual Machines to Azure Sentinel
- Connect non-Azure Windows hosts to Azure Sentinel
- Configure Log Analytics agent to collect Sysmon events
- Explain the Common Event Format connector deployment options in Azure Sentinel
- Configure the TAXII connector in Azure Sentinel
- View threat indicators in Azure Sentinel

**Module 7: 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.

**Lessons**

- Threat detection with Azure Sentinel analytics
- Threat response with Azure Sentinel playbooks
- Security incident management in Azure Sentinel
- Use entity behavior analytics in Azure Sentinel
- 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

After completing this module, students will be able to:

- Explain the importance of Azure Sentinel Analytics.
- Create rules from templates.
- Manage rules with modifications.
- Explain Azure Sentinel SOAR capabilities.
- Create a playbook to automate an incident response.
- Investigate and manage incident resolution.
- Explain User and Entity Behavior Analytics in Azure Sentinel
- Explore entities in Azure Sentinel
- Visualize security data using Azure Sentinel Workbooks.

**Module 8: 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.

**Lessons**

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

 

**Lab : Threat hunting in Azure Sentinel**

- Threat Hunting in Azure Sentinel
- Threat Hunting using Notebooks

After completing this module, students will be able to:

- Describe threat hunting concepts for use with Azure Sentinel
- Define a threat hunting hypothesis for use in Azure Sentinel
- Use queries to hunt for threats.
- Observe threats over time with livestream.
- Explore API libraries for advanced threat hunting in Azure Sentinel
- Create and use notebooks in Azure Sentinel

 