

# SC-200T00 Microsoft Security Operations Analyst

---

## Class Length

4 Days

---

## Overview

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.

---

## Prerequisite Comments

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.

---

## Target 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.

---

## Course Objectives

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

---

## Course Outline

### 1 - Mitigate threats using Microsoft Defender for Endpoint

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

## **2 - Mitigate threats using Microsoft 365 Defender**

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

## **3 - Mitigate threats using Azure Defender**

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

#### **4 - Create queries for Azure Sentinel using Kusto Query Language (KQL)**

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

#### **5 - Configure your Azure Sentinel environment**

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

## 6 - Connect logs to Azure Sentinel

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 Sysl