MICROSOFT SECURITY OPERATIONS ANALYST

SC-200T00

Duration: 4 days; Instructor-led

WHAT WILL YOU LEARN

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

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.

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 CONTENTS

Module 1: 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
- Remediate risks with Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Protect your identities with Azure AD Identity Protection
- Microsoft Defender for Cloud Apps
- Respond to data loss prevention alerts using Microsoft 365
- Manage insider risk in Microsoft 365

- Lab : Mitigate threats using Microsoft 365 Defender
- Explore 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
- Investigate alerts in Microsoft 365 Defender
- Describe the investigation and remediation features of Azure Active Directory Identity Protection
- Explain how Cloud Discovery helps you see what's going on in your organization

Module 2: 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 Endpoint. 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 security enhancements
- Perform device investigations
- Perform actions on a device
- Perform evidence and entities investigations
- Configure and manage automation
- Configure for alerts and detections
- Utilize Threat and Vulnerability Management

Lab : Mitigate threats using Microsoft 365 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 devices
- 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 3: Mitigate threats using Microsoft Defender for Cloud

Use Microsoft Defender for Cloud, for Azure, hybrid cloud, and on-premises workload protection and security. Learn the purpose of Microsoft Defender for Cloud and how to enable it. You will also learn about the protections and detections provided by Microsoft Defender for Cloud for each cloud workload. Learn how you can add Microsoft Defender for Cloud capabilities to your hybrid environment.

Lessons
- Plan for cloud workload protections using Microsoft Defender for Cloud
- Workload protections in Microsoft Defender for Cloud
- Connect Azure assets to Microsoft Defender for Cloud
- Connect non-Azure resources to Microsoft Defender for Cloud
- Remediate security alerts using Microsoft Defender for Cloud

Lab : Mitigate threats using Microsoft Defender for Cloud
- Deploy Microsoft Defender for Cloud
- Mitigate Attacks with Microsoft Defender for Cloud

After completing this module, students will be able to:
- Describe Microsoft Defender for Cloud features
- Explain which workloads are protected by Microsoft Defender for Cloud
- Explain how Microsoft Defender for Cloud protections function
- Configure auto-provisioning in Microsoft Defender for Cloud
- Describe manual provisioning in Microsoft Defender for Cloud
- Connect non-Azure machines to Microsoft Defender for Cloud
- Describe alerts in Microsoft Defender for Cloud
- Remediate alerts in Microsoft Defender for Cloud
- Automate responses in Microsoft Defender for Cloud

Module 4: Create queries for Microsoft Sentinel using Kusto Query Language (KQL)

Write Kusto Query Language (KQL) statements to query log data to perform detections, analysis, and reporting in Microsoft 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 Microsoft 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 Microsoft Sentinel. Learn how to use the Kusto Query Language (KQL) to manipulate string data ingested from log sources.

Lessons
- Construct KQL statements for Microsoft Sentinel
- Analyze query results using KQL
- Build multi-table statements using KQL
- Work with string data using KQL statements

Lab : Create queries for Microsoft Sentinel using Kusto Query Language (KQL)
- Create queries for Microsoft Sentinel using Kusto Query Language (KQL)
- 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 Microsoft Sentinel environment

Get started with Microsoft Sentinel by properly configuring the Microsoft 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. Microsoft 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 Microsoft 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 Microsoft Sentinel.

Lessons
- 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

Lab : Configure your Microsoft Sentinel environment
- Configure your Microsoft Sentinel environment

After completing this module, students will be able to:
- Identify the various components and functionality of Microsoft Sentinel.
- Identify use cases where Microsoft Sentinel would be a good solution.
- Describe Microsoft Sentinel workspace architecture
- Install Microsoft Sentinel workspace
- Manage an Microsoft Sentinel workspace
- Create a watchlist in Microsoft Sentinel
- Use KQL to access the watchlist in Microsoft Sentinel
- Manage threat indicators in Microsoft Sentinel
- Use KQL to access threat indicators in Microsoft Sentinel

Module 6: Connect logs to Microsoft Sentinel

Connect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds to Microsoft Sentinel. The primary approach to connect log data is using the Microsoft 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 Microsoft Sentinel connectors for Microsoft 365 Defender.

Lessons
- Connect data to Microsoft Sentinel using data connectors
- Connect Microsoft services to Microsoft Sentinel
- Connect Microsoft 365 Defender 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

Lab : Connect logs to Microsoft Sentinel
- Connect data to Microsoft Sentinel using data connectors
- Connect Windows devices to Microsoft Sentinel using data connectors
- Connect Linux hosts to Microsoft Sentinel using data connectors
- Connect Threat intelligence to Microsoft Sentinel using data connectors

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

Module 7: Create detections and perform investigations using Microsoft Sentinel

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

Lessons
- Threat detection with Microsoft Sentinel analytics
- Security incident management in Microsoft Sentinel
- Threat response with Microsoft Sentinel playbooks
- User and entity behavior analytics in Microsoft Sentinel
- Query, visualize, and monitor data in Microsoft Sentinel

Lab : Create detections and perform investigations using Microsoft Sentinel
- Activate a Microsoft Security rule
- Create a Playbook
- Create a Scheduled Query
- Understand Detection Modeling
- Conduct attacks
- Create detections
- Investigate incidents
- Create workbooks

After completing this module, students will be able to:

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

Module 8: Perform threat hunting in Microsoft 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 concepts in Microsoft Sentinel
- Threat hunting with Microsoft Sentinel
- Hunt for threats using notebooks in Microsoft Sentinel

Lab : Threat hunting in Microsoft Sentinel

- Perform threat hunting in Microsoft Sentinel
- Threat hunting using notebooks with Microsoft Sentinel

After completing this module, students will be able to:

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