Course Outline

Microsoft Security Operations Analyst

Course SC-200T00: 4 days Instructor Led

About this course

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.

Audience profile

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.

- Basic understanding of Microsoft 365
- Fundamental understanding of Microsoft security, compliance, and identity products
- Intermediate understanding of Microsoft Windows
- Familiarity with Azure services, specifically Azure SQL Database and Azure Storage
- Familiarity with Azure virtual machines and virtual networking
- Basic understanding of scripting concepts.

At course completion

After completing this course, students will be able to:

- Introduction to Microsoft 365 threat protection
- 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 Defender for Cloud Apps
- Respond to data loss prevention alerts using Microsoft 365
- Manage insider risk in Microsoft Purview
- Protect against threats with Microsoft Defender for Endpoint
- Deploy the Microsoft Defender for Endpoint environment
- Implement Windows security enhancements with 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 Vulnerability Management in Microsoft Defender for Endpoint
- Plan for cloud workload protections using Microsoft Defender for Cloud
- Connect Azure assets to Microsoft Defender for Cloud

Course Outline

- Connect non-Azure resources to Microsoft Defender for Cloud
- Manage your cloud security posture management
- Explain cloud workload protections in Microsoft Defender for Cloud
- Remediate security alerts using Microsoft Defender for Cloud
- Construct KQL statements for Microsoft Sentinel
- Analyze query results using KQL
- Build multi-table statements using KQL
- Work with data in Microsoft Sentinel using Kusto Query Language
- 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
- 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
- Threat detection with Microsoft Sentinel analytics
- Automation in Microsoft Sentinel
- Threat response with Microsoft Sentinel playbooks
- Security incident management in Microsoft Sentinel
- Identify threats with Behavioral Analytics
- Data normalization in Microsoft Sentinel
- Query, visualize, and monitor data in Microsoft Sentinel
- Manage content in Microsoft Sentinel
- Explain threat hunting concepts in Microsoft Sentinel
- Threat hunting with Microsoft Sentinel
- Use Search jobs in Microsoft Sentinel
- Hunt for threats using notebooks in Microsoft Sentinel

Course Outline

Module 1: Introduction to Microsoft 365 threat protection

- Understand Microsoft 365 Defender solution by domain
- Understand Microsoft 365 Defender role in a Modern SOC

Module 2: Mitigate incidents using Microsoft 365 Defender

- Manage incidents in Microsoft 365 Defender
- Investigate incidents in Microsoft 365 Defender
- Conduct advanced hunting in Microsoft 365 Defender

Course Outline

Module 3: Protect your identities with Azure AD Identity Protection

- Describe the features of Azure Active Directory Identity Protection.
- Describe the investigation and remediation features of Azure Active Directory Identity Protection.

Module 4: Remediate risks with Microsoft Defender for Office 365

- Define the capabilities of Microsoft Defender for Office 365.
- Understand how to simulate attacks within your network.
- Explain how Microsoft Defender for Office 365 can remediate risks in your environment.

Module 5: Safeguard your environment with Microsoft Defender for Identity

- Define the capabilities of Microsoft Defender for Identity.
- Understand how to configure Microsoft Defender for Identity sensors.
- Explain how Microsoft Defender for Identity can remediate risks in your environment.

Module 6: Secure your cloud apps and services with Microsoft Defender for Cloud Apps

- Define the Defender for Cloud Apps framework
- Explain how Cloud Discovery helps you see what's going on in your organization
- Understand how to use Conditional Access App Control policies to control access to the apps in your organization

Module 7: Respond to data loss prevention alerts using Microsoft 365

- Describe data loss prevention (DLP) components in Microsoft 365
- Investigate DLP alerts in the Microsoft Purview compliance portal
- Investigate DLP alerts in Microsoft Defender for Cloud Apps

Module 8: Manage insider risk in Microsoft Purview

- Explain how Microsoft Purview Insider Risk Management can help prevent, detect, and contain internal risks in an organization.
- Describe the types of built-in, pre-defined policy templates.
- List the prerequisites that need to be met before creating insider risk policies.
- Explain the types of actions you can take on an insider risk management case.

Module 9: Protect against threats with Microsoft Defender for Endpoint

- Define the capabilities of Microsoft Defender for Endpoint.
- Understand how to hunt threats within your network.
- Explain how Microsoft Defender for Endpoint can remediate risks in your environment.

Module 10: Deploy the Microsoft Defender for Endpoint environment

- Create a Microsoft Defender for Endpoint environment
- Onboard devices to be monitored by Microsoft Defender for Endpoint

Course Outline

- Configure Microsoft Defender for Endpoint environment settings

Module 11: Implement Windows security enhancements with Microsoft Defender for Endpoint

- Explain Attack Surface Reduction in Windows
- Enable Attack Surface Reduction rules on Windows 10 devices
- Configure Attack Surface Reduction rules on Windows 10 devices

Module 12: Perform device investigations in Microsoft Defender for Endpoint

- Use the device page in Microsoft Defender for Endpoint
- Describe device forensics information collected by Microsoft Defender for Endpoint
- Describe behavioral blocking by Microsoft Defender for Endpoint

Module 13: Perform actions on a device using Microsoft Defender for Endpoint

- Perform actions on a device using Microsoft Defender for Endpoint
- Conduct forensics data collection using Microsoft Defender for Endpoint
- Access devices remotely using Microsoft Defender for Endpoint

Module 14: Perform evidence and entities investigations using Microsoft Defender for Endpoint

- Investigate files in Microsoft Defender for Endpoint
- Investigate domains and IP addresses in Microsoft Defender for Endpoint
- Investigate user accounts in Microsoft Defender for Endpoint

Module 15: Configure and manage automation using Microsoft Defender for Endpoint

- Configure advanced features of Microsoft Defender for Endpoint
- Manage automation settings in Microsoft Defender for Endpoint

Module 16: Configure for alerts and detections in Microsoft Defender for Endpoint

- Configure alert settings in Microsoft Defender for Endpoint
- Manage indicators in Microsoft Defender for Endpoint

Module 17: Utilize Vulnerability Management in Microsoft Defender for Endpoint

- Describe Vulnerability Management in Microsoft Defender for Endpoint
- Identify vulnerabilities on your devices with Microsoft Defender for Endpoint
- Track emerging threats in Microsoft Defender for Endpoint

Module 18: Plan for cloud workload protections using Microsoft Defender for Cloud

- Describe Microsoft Defender for Cloud features
- Microsoft Defender for Cloud workload protections
- Enable Microsoft Defender for Cloud

Course Outline

Module 19: Connect Azure assets to Microsoft Defender for Cloud

- Explore Azure assets
- Configure auto-provisioning in Microsoft Defender for Cloud
- Describe manual provisioning in Microsoft Defender for Cloud

Module 20: Connect non-Azure resources to Microsoft Defender for Cloud

- Connect non-Azure machines to Microsoft Defender for Cloud
- Connect AWS accounts to Microsoft Defender for Cloud
- Connect GCP accounts to Microsoft Defender for Cloud

Module 21: Manage your cloud security posture management

- Describe Microsoft Defender for Cloud features.
- Explain the Microsoft Defender for Cloud security posture management protections for your resources.

Module 22: Explain cloud workload protections in Microsoft Defender for Cloud

- Explain which workloads are protected by Microsoft Defender for Cloud
- Describe the benefits of the protections offered by Microsoft Defender for Cloud
- Explain how Microsoft Defender for Cloud protections function

Module 23: Remediate security alerts using 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 24: Construct KQL statements for Microsoft Sentinel

- 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

Module 25: Analyze query results using KQL

- Summarize data using KQL statements
- Render visualizations using KQL statements

Module 26: Build multi-table statements using KQL

- Create queries using unions to view results across multiple tables using KQL
- Merge two tables with the join operator using KQL

Module 27: Work with data in Microsoft Sentinel using Kusto Query Language

- Extract data from unstructured string fields using KQL
- Extract data from structured string data using KQL

- Create Functions using KQL

Module 28: Introduction to Microsoft Sentinel

- Identify the various components and functionality of Microsoft Sentinel.
- Identify use cases where Microsoft Sentinel would be a good solution.

Module 29: Create and manage Microsoft Sentinel workspaces

- Describe Microsoft Sentinel workspace architecture
- Install Microsoft Sentinel workspace
- Manage a Microsoft Sentinel workspace

Module 30: Query logs in Microsoft Sentinel

- Use the Logs page to view data tables in Microsoft Sentinel
- Query the most used tables using Microsoft Sentinel

Module 31: Use watchlists in Microsoft Sentinel

- Create a watchlist in Microsoft Sentinel
- Use KQL to access the watchlist in Microsoft Sentinel

Module 32: Utilize threat intelligence in Microsoft Sentinel

- Manage threat indicators in Microsoft Sentinel
- Use KQL to access threat indicators in Microsoft Sentinel

Module 33: Connect data to Microsoft Sentinel using data connectors

- Explain the use of data connectors in Microsoft Sentinel
- Describe the Microsoft Sentinel data connector providers
- Explain the Common Event Format and Syslog connector differences in Microsoft Sentinel

Module 34: Connect Microsoft services to Microsoft Sentinel

- Connect Microsoft service connectors
- Explain how connectors auto-create incidents in Microsoft Sentinel

Module 35: Connect Microsoft 365 Defender to Microsoft Sentinel

- Activate the Microsoft 365 Defender connector in Microsoft Sentinel
- Activate the Microsoft Defender for Cloud connector in Microsoft Sentinel
- Activate the Microsoft Defender for IoT connector in Microsoft Sentinel

Module 36: Connect Windows hosts to 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

Course Outline

Module 37: Connect Common Event Format logs to Microsoft Sentinel

- Explain the Common Event Format connector deployment options in Microsoft Sentinel
- Run the deployment script for the Common Event Format connector

Module 38: Connect syslog data sources to Microsoft Sentinel

- Describe the Syslog connector deployment options in Microsoft Sentinel
- Run the connector deployment script to send data to Microsoft Sentinel
- Configure the Log Analytics agent integration for Microsoft Sentinel
- Create a parse using KQL in Microsoft Sentinel

Module 39: Connect threat indicators to Microsoft Sentinel

- Configure the TAXII connector in Microsoft Sentinel
- Configure the Threat Intelligence Platform connector in Microsoft Sentinel
- View threat indicators in Microsoft Sentinel

Module 40: Threat detection with Microsoft Sentinel analytics

- Explain the importance of Microsoft Sentinel Analytics.
- Explain different types of analytics rules.
- Create rules from templates.
- Create new analytics rules and queries using the analytics rule wizard.
- Manage rules with modifications.

Module 41: Automation in Microsoft Sentinel

- Explain automation options in Microsoft Sentinel
- Create automation rules in Microsoft Sentinel

Module 42: Threat response with Microsoft Sentinel playbooks

- Explain Microsoft Sentinel SOAR capabilities.
- Explore the Microsoft Sentinel Logic Apps connector.
- Create a playbook to automate an incident response.
- Run a playbook on demand in response to an incident.

Module 43: Security incident management in Microsoft Sentinel

- Understand Microsoft Sentinel incident management
- Explore Microsoft Sentinel evidence and entity management
- Investigate and manage incident resolution

Module 44: Identify threats with Behavioral Analytics

- Explain User and Entity Behavior Analytics in Azure Sentinel

- Explore entities in Microsoft Sentinel

Module 45: Data normalization in Microsoft Sentinel

- Use ASIM Parsers
- Create ASIM Parser
- Create parameterized KQL functions

Module 46: Query, visualize, and monitor data in Microsoft Sentinel

- Visualize security data using Microsoft Sentinel Workbooks.
- Understand how queries work.
- Explore workbook capabilities.
- Create a Microsoft Sentinel Workbook.

Module 47: Manage content in Microsoft Sentinel

- Install a content hub solution in Microsoft Sentinel
- Connect a GitHub repository to Microsoft Sentinel

Module 48: Explain threat hunting concepts in Microsoft Sentinel

- Describe threat hunting concepts for use with Microsoft Sentinel
- Define a threat hunting hypothesis for use in Microsoft Sentinel

Module 49: Threat hunting with Microsoft Sentinel

- Use queries to hunt for threats.
- Save key findings with bookmarks.
- Observe threats over time with livestream.

Module 50: Use Search jobs in Microsoft Sentinel

- Use Search Jobs in Microsoft Sentinel
- Restore archive logs in Microsoft Sentinel

Module 51: Hunt for threats using notebooks in Microsoft Sentinel

- Explore API libraries for advanced threat hunting in Microsoft Sentinel
- Describe notebooks in Microsoft Sentinel
- Create and use notebooks in Microsoft Sentinel