SC-200T00: Microsoft Security Operations Analyst

Course Details

Course Code: SC-200T00

Duration: 4 days

Notes:

- This course syllabus should be used to determine whether the course is appropriate for the students, based on their current skills and technical training needs.
- Course content, prices, and availability are subject to change without notice.
- Terms and Conditions apply

Elements of this syllabus are subject to change.

About this course

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.

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.

Academy IT Pty Ltd
Level 4, 45 Grenfell Street
ADELAIDE 5000

Email: sales@academyit.com.au
Web: www.academyit.com.au

Phone: 08 7324 9800
Brian: 0400 112 083

Academy IT

Table of Contents

Introduction to Microsoft 365 threat protection
In this module, you'll learn how to use the Microsoft Defender XDR integrated threat protection suite.

Learning objectives
In this module, you learned the role that Microsoft Defender XDR plays in a modern SOC. You should now be able to:

- Understand Microsoft Defender XDR solutions by domain
- Understand the Microsoft Defender XDR role in a Modern SOC

Mitigate incidents using Microsoft 365 Defender
Learn how the Microsoft 365 Defender portal provides a unified view of incidents from the Microsoft 365 Defender family of products.

Learning objectives
Upon completion of this module, the learner will be able to:

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

Protect your identities with Microsoft Entra ID Protection
Use the advanced detection and remediation of identity-based threats to protect your Microsoft Entra identities and applications from compromise.

Learning objectives
In this module, you will:

- Describe the features of Microsoft Entra ID Protection.
- Describe the investigation and remediation features of Microsoft Entra ID Protection.

Remediate risks with Microsoft Defender for Office 365
Learn about the Microsoft Defender for Office 365 component of Microsoft 365 Defender.

Learning objectives
In this module, you will learn how to:

- 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.

Safeguard your environment with Microsoft Defender for Identity
Learn about the Microsoft Defender for Identity component of Microsoft 365 Defender.

Learning objectives
Upon completion of this module, you should be able to:

- 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.

Secure your cloud apps and services with Microsoft Defender for Cloud Apps
Microsoft Defender for Cloud Apps is a cloud access security broker (CASB) that operates on multiple clouds. It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your cloud services. Learn how to use Defender for Cloud Apps in your organization.

Learning objectives
At the end of this module, you should be able to:

- 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

Respond to data loss prevention alerts using Microsoft 365
As a Security Operations Analyst, you need to understand compliance related terminology and alerts. Learn how the data loss prevention alerts will help in your investigation to find the full scope of the incident.

Learning objectives
Upon completion of this module, the learner will be able to:

- 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

Manage insider risk in Microsoft Purview
Microsoft Purview Insider Risk Management helps organizations address internal risks, such as IP theft, fraud, and sabotage. Learn about insider risk management and how Microsoft technologies can help you detect, investigate, and take action on risky activities in your organization.

Learning objectives
Upon completion of this module, you should be able to:

- 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.

Investigate threats by using audit features in Microsoft Defender XDR and Microsoft Purview Standard
This module examines how to search for audited activities using the Microsoft Purview Audit (UAL) solution, including how to export, configure, and view the audit log records that were retrieved from an audit log search.

Learning objectives
By the end of this module, you'll be able to:

- Describe the differences between Audit (Standard) and Audit (Premium).
- Start recording user and admin activity in the Unified Audit Log (UAL).
- Identify the core features of the Audit (Standard) solution.
- Set up and implement audit log searching using the Audit (Standard) solution.
- Export, configure, and view audit log records.
- Use audit log searching to troubleshoot common support issues.

Investigate threats using audit in Microsoft Defender XDR and Microsoft Purview (Premium)
This module explores the differences between Microsoft Purview Audit (Standard) and Audit (Premium), plus the key functionality in Audit (Premium), including setup requirements, enabling audit logging, creating audit log retention policies, and performing forensics investigations.

Learning objectives
By the end of this module, you'll be able to:

- Describe the differences between Audit (Standard) and Audit (Premium).
- Set up and implement Microsoft Purview Audit (Premium).
- Create audit log retention policies.
- Perform forensic investigations of compromised user accounts.

Investigate threats with Content search in Microsoft Purview
This module examines how to search for content in the Microsoft Purview compliance portal using Content Search functionality, including how to view and export the search results, and configure search permissions filtering.

Learning objectives
By the end of this module, you'll be able to:

- Describe how to use content search in the Microsoft Purview compliance portal.
- Design and create a content search.
- Preview the search results.
- View the search statistics.
- Export the search results and search report.
- Configure search permission filtering.

Protect against threats with Microsoft Defender for Endpoint
Learn how Microsoft Defender for Endpoint can help your organization stay secure.

Learning objectives
In this module, you will learn how to:

- 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.

Deploy the Microsoft Defender for Endpoint environment
Learn how to deploy the Microsoft Defender for Endpoint environment, including onboarding devices and configuring security.

Learning objectives
Upon completion of this module, the learner will be able to:

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

Implement Windows security enhancements with Microsoft Defender for Endpoint
Microsoft Defender for Endpoint gives you various tools to eliminate risks by reducing the surface area for attacks without blocking user productivity. Learn about Attack Surface Reduction (ASR) with Microsoft Defender for Endpoint.

Learning objectives
Upon completion of this module, the learner will be able to:

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

Perform device investigations in Microsoft Defender for Endpoint
Microsoft Defender for Endpoint provides detailed device information, including forensics information. Learn about information available to you through Microsoft Defender for Endpoint that will aid in your investigations.

Learning objectives
Upon completion of this module, the learner will be able to:

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

Perform actions on a device using Microsoft Defender for Endpoint
Learn how Microsoft Defender for Endpoint provides the remote capability to contain devices and collect forensics data.

Learning objectives
Upon completion of this module, the learner will be able to:

- 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

Configure and manage automation using Microsoft Defender for Endpoint
Learn how to configure automation in Microsoft Defender for Endpoint by managing environmental settings.

Learning objectives
Upon completion of this module, the learner will be able to:

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

Perform evidence and entities investigations using Microsoft Defender for Endpoint
Learn about the artifacts in your environment and how they relate to other artifacts and alerts that will provide you with insight to understand the overall impact to your environment.

Learning objectives
Upon completion of this module, the learner will be able to:

- 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

Configure and manage automation using Microsoft Defender for Endpoint
Learn how to configure automation in Microsoft Defender for Endpoint by managing environmental settings.

Learning objectives
Upon completion of this module, the learner will be able to:

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

Configure for alerts and detections in Microsoft Defender for Endpoint
Learn how to configure settings to manage alerts and notifications. You'll also learn to enable indicators as part of the detection process.

Learning objectives
After completion of this module, you'll be able to:

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

Utilize Vulnerability Management in Microsoft Defender for Endpoint
Learn about your environment's weaknesses by using Vulnerability Management in Microsoft Defender for Endpoint.

Learning objectives
Upon completion of this module, the learner will be able to:

- 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

Plan for cloud workload protections using Microsoft Defender for Cloud
Learn the purpose of Microsoft Defender for Cloud and how to enable the system.

Learning objectives
Upon completion of this module, the learner will be able to:

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

Connect Azure assets to Microsoft Defender for Cloud
Learn how to connect your various Azure assets to Microsoft Defender for Cloud to detect threats.

Learning objectives
Upon completion of this module, the learner will be able to:

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

Connect non-Azure resources to Microsoft Defender for Cloud
Learn how you can add Microsoft Defender for Cloud capabilities to your hybrid environment.

Learning objectives
Upon completion of this module, the learner will be able to:

- 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

Manage your cloud security posture management
Microsoft Defender for Cloud, Cloud Security Posture Management (CSPM) provides visibility

into vulnerable resources and provides hardening guidance.

Learning objectives

- In this module, you'll learn how Microsoft Defender for Cloud provides security posture management. Upon completion you'll be able to:
- Describe Microsoft Defender for Cloud features.
- Explain the Microsoft Defender for Cloud security posture management protections for your resources.

Explain cloud workload protections in Microsoft Defender for Cloud

Learn about the protections and detections provided by Microsoft Defender for Cloud with each cloud workload.

Learning objectives

Upon completion of this module, the learner will be able to:

- 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

Remediate security alerts using Microsoft Defender for Cloud

Learn how to remediate security alerts in Microsoft Defender for Cloud.

Learning objectives

Upon completion of this module, the learner will be able to:

- Describe alerts in Microsoft Defender for Cloud
- Remediate alerts in Microsoft Defender for Cloud
- Automate responses in Microsoft Defender for Cloud

Construct KQL statements for Microsoft Sentinel

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.

Learning objectives

Upon completion of this module, the learner 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

Analyze query results using KQL

Learn how to summarize and visualize data with a KQL statement provides the foundation to build detections in Microsoft Sentinel.

Learning objectives

Upon completion of this module, the learner will be able to:

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

Build multi-table statements using KQL

Learn how to work with multiple tables using KQL.

Learning objectives

Upon completion of this module, the learner will be able to:

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

Work with data in Microsoft Sentinel using Kusto Query Language

Learn how to use the Kusto Query Language (KQL) to manipulate string data ingested from log sources.

Learning objectives

Upon completion of this module, the learner will be able to:

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

Academy IT

Table of Contents

Introduction to Microsoft Sentinel
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.

Learning objectives
By the end of this module, you'll be able to:

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

Create and manage Microsoft Sentinel workspaces
Learn about the architecture of Microsoft Sentinel workspaces to ensure you configure your system to meet your organization's security operations requirements.

Learning objectives
Upon completion of this module, the learner will be able to:

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

Query logs in Microsoft Sentinel
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.

Learning objectives
Upon completion of this module, the learner will be able to:

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

Use watchlists in Microsoft Sentinel
Learn how to create Microsoft Sentinel watchlists that are a named list of imported data. Once created, you can easily use the named watchlist in KQL queries.

Learning objectives
Upon completion of this module, the learner will be able to:

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

Utilize threat intelligence in Microsoft Sentinel
Learn how the Microsoft Sentinel Threat Intelligence page enables you to manage threat indicators.

Learning objectives
Upon completion of this module, the learner will be able to:

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

Connect data to Microsoft Sentinel using data connectors
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.

Learning objectives
Upon completion of this module, the learner will be able to:

- Describe how to install Content Hub Solutions to provision Microsoft Sentinel 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

Connect Microsoft services to Microsoft Sentinel
Learn how to connect Microsoft 365 and Azure service logs to Microsoft Sentinel.

Learning objectives
Upon completion of this module, the learner will be able to:

- Connect Microsoft service connectors

- Explain how connectors auto-create incidents in Microsoft Sentinel

Connect Microsoft Defender XDR to Microsoft Sentinel

Learn about the configuration options and data provided by Microsoft Sentinel connectors for Microsoft Defender XDR.

Learning objectives

Upon completion of this module, the learner will be able to:

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

Connect Windows hosts to Microsoft Sentinel

One of the most common logs to collect is Windows security events. Learn how Microsoft Sentinel makes this easy with the Security Events connector.

Learning objectives

Upon completion of this module, the learner will be able to:

- Connect Azure Windows Virtual Machines to Microsoft Sentinel
- Connect non-Azure Windows hosts to Microsoft Sentinel
- Configure Log Analytics agent to collect Sysmon events

Connect Common Event Format logs to Microsoft Sentinel

Most vendor-provided connectors utilize the CEF connector. Learn about the Common Event Format (CEF) connector's configuration options.

Learning objectives

Upon completion of this module, the learner will be able to:

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

Connect syslog data sources to Microsoft Sentinel

Learn about the Azure Monitor Agent Linux Syslog Data Collection Rule configuration options, which enable you to parse Syslog data.

Learning objectives

Upon completion of this module, the learner is able to:

- Describe the Azure Monitor Agent Data Collection Rule (DCR) for Syslog
- Install and Configure the Azure Monitor Linux Agent extension with the Syslog DCR
- Run the Azure Arc Linux deployment and connection scripts
- Verify Syslog log data is available in Microsoft Sentinel
- Create a parser using KQL in Microsoft Sentinel

Connect threat indicators to Microsoft Sentinel

Learn how to connect Threat Intelligence Indicators to the Microsoft Sentinel workspace using the provided data connectors.

Learning objectives

Upon completion of this module, the learner will be able to:

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

Threat detection with Microsoft Sentinel analytics

In this module, you learned how Microsoft Sentinel Analytics can help the SecOps team identify and stop cyber-attacks.

Learning objectives

In this module, you will:

- Explain the importance of Microsoft Sentinel Analytics.
- Explain different types of analytics rules.
- Create rules from templates.

Automation in Microsoft Sentinel

By the end of this module, you'll be able to use automation rules in Microsoft Sentinel to automated incident management.

Learning objectives

After completing this module, you'll be able to:

- Explain automation options in Microsoft Sentinel
- Create automation rules in Microsoft Sentinel
- Create new analytics rules and queries using the analytics rule wizard.
- Manage rules with modifications.

Security incident management in Microsoft Sentinel

Learn about security incidents, incident evidence and entities, incident management, and how to use Microsoft Sentinel to handle incidents.

Learning objectives

- Learn about security incidents and Microsoft Sentinel incident management.
- Explore Microsoft Sentinel incident evidence and entities.
- Use Microsoft Sentinel to investigate security incidents and manage incident resolution.

Identify threats with Behavioural Analytics

Learn how to use entity behaviour analytics in Microsoft Sentinel to identify threats inside your organization.

Learning objectives

Upon completion of this module, the learner will be able to:

- Explain User and Entity Behaviour Analytics in Azure Sentinel
- Explore entities in Microsoft Sentinel

Data normalization in Microsoft Sentinel

By the end of this module, you'll be able to use ASIM parsers to identify threats inside your organization.

Learning objectives

After completing this module, you will be able to:

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

Query, visualize, and monitor data in Microsoft Sentinel

This module describes how to query, visualize, and monitor data in Microsoft Sentinel.

Learning objectives

In this module you will:

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

Manage content in Microsoft Sentinel

By the end of this module, you'll be able to manage content in Microsoft Sentinel.

Learning objectives

After completing this module, you'll be able to:

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

Explain threat hunting concepts in Microsoft Sentinel

Learn the threat hunting process in Microsoft Sentinel.

Learning objectives

Upon completion of this module, the learner will be able to:

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

Threat hunting with Microsoft Sentinel

In this module, you'll learn to proactively identify threat behaviours by using Microsoft Sentinel queries. You'll also learn to use bookmarks and livestream to hunt threats.

Learning objectives

In this module, you will:

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

Use Search jobs in Microsoft Sentinel

In Microsoft Sentinel, you can search across long time periods in large datasets by using a search job.

Learning objectives

After completing this module, you'll be able to:

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

Hunt for threats using notebooks in Microsoft Sentinel

Learn how to use notebooks in Microsoft Sentinel for advanced hunting.

Learning objectives

Upon completion of this module, the learner will be able to:

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