COURSE OUTLINE

MS-SC200T00: MICROSOFT SECURITY OPERATIONS ANALYST

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
4 Days	Intermediate	Security	Instructor-led	NA

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.

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 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.

PREREQUISITES

Before attending this course, students must have:

- 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 OBJECTIVES

After completing this course, students will be able to:

- 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

COURSE CONTENT

Module 1: Introduction to Microsoft Defender XDR threat protection

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

Lessons

- Introduction
- Explore Extended Detection & Response (XDR) response use cases
- Understand Microsoft Defender XDR in a Security Operations Center (SOC)
- Explore Microsoft Security Graph
- Investigate security incidents in Microsoft Defender XDR
- Knowledge check
- Summary and resources

Learning objectives

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

Module 2: Mitigate incidents using Microsoft Defender

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

Lessons

- Introduction
- Use the Microsoft Defender portal
- Manage incidents
- Investigate incidents
- Manage and investigate alerts
- Manage automated investigations
- Use the action center
- Explore advanced hunting
- Investigate Microsoft Entra sign-in logs
- Understand Microsoft Secure Score
- Analyse threat analytics
- Analyse reports
- Configure the Microsoft Defender portal
- Knowledge check
- Summary and resources

Learning Objectives

- Manage incidents in Microsoft 365 Defender
- Investigate incidents in Microsoft 365 Defender

- Conduct advanced hunting in Microsoft 365 Defender

Module 3: Remediate risks with Microsoft Defender for Office 365

Learn about the Microsoft Defender for Office 365 component of Microsoft Defender XDR.

Lessons

- Introduction to Microsoft Defender for Office 365
- Automate, investigate, and remediate
- Configure, protect, and detect
- Simulate attacks
- Summary and knowledge check

Learning objectives

- 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 4: Manage Microsoft Entra Identity Protection

Protecting a user's identity by monitoring their usage and sign-in patterns ensure a secure cloud solution. Explore how to design and implement Microsoft Entra Identity protection.

Lessons

- Introduction
- Review identity protection basics
- Implement and manage user risk policy
- Exercise enable sign-in risk policy
- Exercise configure Microsoft Entra multifactor authentication registration policy
- Monitor, investigate, and remediate elevated risky users
- Implement security for workload identities
- Explore Microsoft Defender for Identity
- Knowledge check
- Summary and resources

Learning objectives

- Implement and manage a user risk policy.
- Implement and manage sign-in risk policies.
- Implement and manage MFA registration policy.
- Monitor, investigate, and remediate elevated risky users.

Module 5: Safeguard your environment with Microsoft Defender for Identity

Learn about the Microsoft Defender for Identity component of Microsoft Defender XDR.

Lessons

- Introduction to Microsoft Defender for Identity
- Configure Microsoft Defender for Identity sensors
- Review compromised accounts or data
- Integrate with other Microsoft tools
- Summary and knowledge check

Learning objectives

- 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

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.

Lessons

- Introduction
- Understand the Defender for Cloud Apps Framework
- Explore your cloud apps with Cloud Discovery
- Protect your data and apps with Conditional Access App Control
- Walk through discovery and access control with Microsoft Defender for Cloud Apps
- Classify and protect sensitive information
- Detect Threats
- Knowledge check
- Summary

Learning objectives

- 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: Introduction to generative AI concepts

In this module, you explore the way in which language models enable AI applications and services to generate original content based on natural language input.

Lessons

- Introduction
- What is generative AI?
- How do language models work?
- Understand how transformers advance language models
- Understand differences in language models
- Improve prompt results
- Create responsible generative AI solutions
- Module assessment
- Summary

Learning Objectives

- Understand what generative AI can do and how it appears in today's applications.
- Understand how language models can understand and generate language.
- Describe ways you can engineer good prompts and quality responses.
- Describe responsible generative AI concepts.

Module 8: Describe Microsoft Security Copilot

Get acquainted with Microsoft Copilot for Security. You are introduced to some basic terminology, how Microsoft Copilot for Security processes prompts, the elements of an effective prompt, and how to enable the solution.

Lessons

- Introduction
- Get acquainted with Microsoft Security Copilot
- Describe Microsoft Security Copilot terminology
- Describe how Microsoft Security Copilot processes prompt requests
- Describe the elements of an effective prompt
- Describe how to enable Microsoft Security Copilot
- Knowledge check
- Summary and resources

Learning Objectives

- Describe what Microsoft Security Copilot is.
- Describe the terminology of Microsoft Security Copilot.
- Describe how Microsoft Security Copilot processes prompt requests.
- Describe the elements of an effective prompt
- Describe how to enable Microsoft Security Copilot.

Module 9: Describe the core features of Microsoft Security Copilot

Microsoft Security Copilot has a rich set of features. Learn about available plugins, promptbooks, the ways you can export and share information from Copilot, and much more.

Lessons

- Introduction
- Describe the features available in the standalone experience of Microsoft Copilot for Security
- Describe the features available in a session of the standalone experience
- Describe the Microsoft plugins available in Microsoft Copilot for Security
- Describe the non-Microsoft plugins supported by Microsoft Copilot for Security
- Describe custom promptbooks
- Describe knowledge base connections
- Knowledge check
- Summary and resources

Learning Objectives

- Describe the features available in the standalone Copilot experience.
- Describe the plugins available in Copilot.
- Describe custom promptbooks.
- Describe knowledge base connections.

Module 10: Describe the embedded experiences of Microsoft Copilot for Security

Microsoft Security Copilot is accessible directly from some Microsoft security products. This is referred to as the embedded experience. Learn about the scenarios supported by the Copilot embedded experience in Microsoft's security solutions.

Lessons

- Introduction
- Describe Microsoft Copilot in Microsoft Defender XDR
- Microsoft Copilot in Microsoft Purview
- Microsoft Copilot in Microsoft Entra
- Microsoft Copilot in Microsoft Intune
- Microsoft Copilot in Microsoft Defender for Cloud (Preview)
- Knowledge check
- Summary and resources

Learning Objectives

- Describe Microsoft Copilot in Microsoft Defender XDR.
- Describe Microsoft Copilot in Microsoft Purview.
- Describe Microsoft Copilot in Microsoft Entra.
- Describe Microsoft Copilot in Microsoft Intune.
- Describe Microsoft Copilot in Microsoft Defender for Cloud.

Module 11: Explore use cases of Microsoft Security Copilot

Explore use cases of Microsoft Security Copilot in the standalone and embedded experiences, through lab-like exercises.

Lessons

- Introduction
- Explore the first run experience
- Explore the standalone experience
- Explore Security Copilot workspaces
- Configure the Microsoft Sentinel plugin
- Enable a custom plugin
- Explore file uploads as a knowledge base
- Create a custom promptbook
- Explore the capabilities of Copilot in Microsoft Defender XDR
- Explore the capabilities of Copilot in Microsoft Purview
- Explore the capabilities of Copilot in Microsoft Entra
- Module assessment
- Summary and resources

Learning Objectives

- "Set up Microsoft Security Copilot."
- "Work with sources in Copilot."
- "Create a custom promptbook."
- "Use the capabilities of Copilot embedded within our security solutions, including Microsoft Purview, Microsoft Entra, and Microsoft Defender for Cloud."

Module 12: Investigate and respond to Microsoft Purview Data Loss Prevention alerts

Microsoft Purview and Microsoft Defender XDR help organizations detect potential data loss risks and respond quickly to protect sensitive information. Investigation and response activities include reviewing DLP alerts, applying appropriate remediation actions, and documenting findings in a structured and consistent way.

Lessons

- Introduction
- Understand data loss prevention (DLP) alerts
- Understand the DLP alert lifecycle
- Configure DLP policies to generate alerts
- Investigate DLP alerts in Microsoft Purview
- Investigate DLP alerts in Microsoft Defender XDR
- Respond to DLP alerts
- Module assessment
- Summary

In this module you learn to:

- Investigate DLP alerts in Microsoft Purview and Microsoft Defender XDR
- Review alert details, related user activities, and matched events
- Apply remediation actions and update alert or incident statuses
- Assign ownership, document decisions, and support accountability
- Recognize when DLP policies might need adjustments based on investigation outcomes

Module 13: Investigate insider risk alerts and related activity

Investigate insider risk alerts and manage related cases in Microsoft Purview to assess user behavior, take appropriate action, and coordinate deeper reviews across teams.

Lessons

- Introduction
- Understand insider risk alerts and investigations
- Manage alert volume in insider risk management
- Investigate and triage insider risk alerts in Microsoft Purview
- Analyze alert context with the All risk factors tab
- Investigate activity details with the Activity explorer tab
- Review patterns over time with the User activity tab
- Investigate insider risk alerts in Microsoft Defender XDR
- Manage and take action on insider risk cases
- Module assessment
- Summary

Learning objectives

- Understand how alerts are generated and prioritized in Insider Risk Management.
- Tune policies and thresholds to manage alert volume effectively.
- Use the Alerts dashboard and alert details to triage and respond to risky activity.
- Investigate behavior using tabs like All risk factors, Activity explorer, and User activity.
- Integrate with Microsoft Defender XDR for broader threat investigation.
- Create, manage, and resolve Insider Risk Management cases.

Module 14: Search and investigate with Microsoft Purview Audit

Enhance data security and compliance with Microsoft Purview Audit by configuring detailed audits, managing logs, and analyzing access patterns.

Lessons
- Introduction
- Microsoft Purview Audit overview
- Configure and manage Microsoft Purview Audit
- Conduct searches with Audit (Standard)
- Audit Microsoft Copilot for Microsoft 365 interactions
- Investigate activities with Audit (Premium)
- Export audit log data
- Configure audit retention with Audit (Premium)
- Knowledge check
- Summary

Learning Objectives
- Identify the differences between Microsoft Purview Audit (Standard) and Audit (Premium).
- Configure Microsoft Purview Audit for optimal log management.
- Perform audits to assess compliance and security measures.
- Analyze irregular access patterns using advanced tools in Purview Audit (Premium) and PowerShell.
- Ensure regulatory compliance through strategic data management.

Module 15: Search for content with Microsoft Purview eDiscovery

Use Microsoft Purview eDiscovery to search for content across Microsoft 365. This module covers how to configure cases, define search criteria, and locate messages, files, and other organizational data.

Lessons
- Introduction
- Understand eDiscovery and content search capabilities
- Prerequisites for using eDiscovery in Microsoft Purview
- Create an eDiscovery search
- Conduct an eDiscovery search
- Export eDiscovery search results
- Module assessment
- Summary and resources

In this module you learn how to:
- Assign the roles and permissions to access Microsoft Purview eDiscovery
- Create and manage cases used to run eDiscovery searches
- Define search scope and build queries using conditions, keywords, and Copilot-generated prompts
- Run searches and validate results using statistics or random samples

Module 16: Protect against threats with Microsoft Defender for Endpoint

Learn how Microsoft Defender for Endpoint can help your organization stay secure.

Lessons
- Introduction to Microsoft Defender for Endpoint
- Practice security administration
- Hunt threats within your network
- Summary and knowledge check

Learning objectives
- 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 17: Deploy the Microsoft Defender for Endpoint environment

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

Lessons
- Introduction
- Create your environment
- Understand operating systems compatibility and features
- Onboard devices
- Manage access
- Create and manage roles for role-based access control
- Configure device groups
- Configure environment advanced features
- Knowledge check
- Summary and resources

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

Module 18: 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.

Lessons
- Introduction
- Understand attack surface reduction
- Enable attack surface reduction
- Knowledge Check
- Summary and resources

Learning objectives
- 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 19: 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.

Lessons
- Introduction
- Use the device inventory list
- Investigate the device
- Use behavioral blocking
- Detect devices with device discovery
- Knowledge check
- Summary and resources

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 behavioral blocking by Microsoft Defender for Endpoint

Module 20: 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.

Lessons
- Introduction
- Explain device actions
- Run Microsoft Defender antivirus scan on devices
- Collect investigation package from devices
- Initiate live response session
- Knowledge check
- Summary and resources

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

Module 21: 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.

Lessons

- Introduction
- Investigate a file
- Investigate a user account
- Investigate an IP address
- Investigate a domain
- Knowledge check
- Summary and resources

Learning objectives

- 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 22: Configure and manage automation using Microsoft Defender for Endpoint

Learn how to configure automation in Microsoft Defender for Endpoint by managing environmental settings.

Lessons

- Introduction
- Configure advanced features
- Manage automation upload and folder settings
- Configure automated investigation and remediation capabilities
- Block at risk devices
- Knowledge check
- Summary and resources

Learning objectives

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

Module 23: 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.

Lessons

- Introduction
- Configure advanced features
- Configure alert notifications
- Manage alert suppression
- Manage indicators
- Knowledge check
- Summary and resources

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

Module 24: Utilize Vulnerability Management in Microsoft Defender for Endpoint

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

Lessons

- Introduction
- Understand vulnerability management
- Explore vulnerabilities on your devices
- Manage remediation
- Knowledge check
- Summary and resources

Learning objectives

- 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 25: Plan for cloud workload protections using Microsoft Defender for Cloud

Learn the purpose of Microsoft Defender for Cloud and how to enable the system.

Lessons

- Introduction
- Explain Microsoft Defender for Cloud
- Describe Microsoft Defender for Cloud workload protections
- Exercise - Microsoft Defender for Cloud interactive guide
- Enable Microsoft Defender for Cloud
- Knowledge check
- Summary and resources

Learning objectives

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

Module 26: Connect Azure assets to Microsoft Defender for Cloud

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

Lessons

- Introduction
- Explore and manage your resources with asset inventory
- Configure auto provisioning
- Manual log analytics agent provisioning
- Knowledge check
- Summary and resources

Learning objectives

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

Module 27: Connect non-Azure resources to Microsoft Defender for Cloud

Learn how you can add Microsoft Defender for Cloud capabilities to your hybrid environment.

Lessons

- Introduction
- Protect non-Azure resources
- Connect non-Azure machines
- Connect your AWS accounts
- Connect your GCP accounts
- Knowledge check
- Summary and resources

Learning objectives

- 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 28: Manage your cloud security posture management

Microsoft Defender for Cloud, Cloud Security Posture Management (CSPM) provides visibility into vulnerable resources and provides hardening guidance.

Lessons

- Introduction
- Explore Secure Score
- Explore Recommendations
- Measure and enforce regulatory compliance
- Understand Workbooks
- Knowledge check
- Summary and resources

Learning objectives

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

Module 29: 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.

Lessons

- Introduction
- Understand Microsoft Defender for servers

- Understand Microsoft Defender for App Service
- Understand Microsoft Defender for Storage
- Understand Microsoft Defender for SQL
- Understand Microsoft Defender for open-source databases
- Understand Microsoft Defender for Key Vault
- Understand Microsoft Defender for Resource Manager
- Understand Microsoft Defender for DNS
- Understand Microsoft Defender for Containers
- Understand Microsoft Defender additional protections
- Knowledge check
- Summary and resources

Learning objectives

- 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 protection functions

Module 30: Remediate security alerts using Microsoft Defender for Cloud

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

Lessons

- Introduction
- Understand security alerts
- Remediate alerts and automate responses
- Suppress alerts from Defender for Cloud
- Generate threat intelligence reports
- Respond to alerts from Azure resources
- Knowledge check
- Summary and resources

Learning objectives

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

Module 31: 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.

Lessons

- Introduction
- Understand the Kusto Query Language statement structure
- Use the search operator
- Use the where operator
- Use the let statement
- Use the extend operator
- Use the order by operator
- Use the project operators
- Knowledge check
- Summary and resources

Learning objectives

- 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 32: Analyse query results using KQL

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

Lessons

- Introduction
- Use the summarize operator
- Use the summarize operator to filter results
- Use the summarize operator to prepare data
- Use the render operator to create visualizations
- Knowledge check
- Summary and resources

Learning objectives

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

Modules 33: Build multi-table statements using KQL

Learn how to work with multiple tables using KQL.

Lessons

- Introduction
- Use the union operator
- Use the join operator
- Knowledge check
- Summary and resources

Learning objectives

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

Module 34: 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.

Lessons

- Introduction
- Extract data from unstructured string fields
- Extract data from structured string data
- Integrate external data
- Create parsers with functions
- Knowledge check
- Summary and resources

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

Module 35: 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.

Lessons

- Introduction to the Unified Security Operations Platform
- What is Microsoft Sentinel?
- How Microsoft Sentinel works
- When to use Microsoft Sentinel
- Knowledge check
- Summary

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.

Module 36: 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.

Lessons

- Introduction
- Plan for the Microsoft Sentinel workspace
- Create a Microsoft Sentinel workspace
- Manage workspaces across tenants using Azure Lighthouse
- Understand Microsoft Sentinel permissions and roles
- Manage Microsoft Sentinel settings
- Configure logs
- Knowledge check
- Summary and resources

Learning objectives

- Describe Microsoft Sentinel workspace architecture
- Install Microsoft Sentinel workspace

- Manage a Microsoft Sentinel workspace

Module 37: 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.

Lessons

- Introduction
- Query logs in the logs page
- Understand Microsoft Sentinel tables
- Understand common tables
- Understand Microsoft Defender XDR tables
- Knowledge check
- Summary and resources

Learning objectives

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

Module 38: 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.

Lessons

- Introduction
- Plan for watchlists
- Create a watchlist
- Manage watchlists
- Knowledge check
- Summary and resources

Learning objectives

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

Module 39: Utilize threat intelligence in Microsoft Sentinel

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

Lessons

- Introduction
- Define threat intelligence
- Manage your threat indicators
- View your threat indicators with KQL
- Knowledge check
- Summary and resources

Learning objectives

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

Module 40: Integrate Microsoft Defender XDR with Microsoft Sentinel

In this module, you learn about the Unified Security Operations Platform that integrates Microsoft Defender XDR with Microsoft Sentinel.

Lessons

- Introduction
- Understand the benefits of integrating Microsoft Sentinel with Defender XDR
- Explore the capability differences between Microsoft Defender XDR and Microsoft
- Sentinel portals
- Onboarding Microsoft Sentinel to Microsoft Defender XDR
- Explore Microsoft Sentinel features in Microsoft Defender XDR
- Knowledge check
- Summary

Learning Objectives

- Understand the differences between Microsoft Sentinel capabilities in Azure and Defender portals
- Know the prerequisites for integrating Microsoft Defender XDR with Microsoft Sentinel
- Connect a Microsoft Sentinel workspace to Microsoft Defender XDR

Module 41: 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.

Lessons

- Introduction
- Ingest log data with data connectors
- Understand data connector providers
- View connected hosts
- Knowledge check
- Summary and resources

Learning Objectives

- 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

Module 42: Connect Microsoft services to Microsoft Sentinel

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

Lessons

- Introduction
- Plan for Microsoft services connectors
- Connect the Microsoft Office 365 connector
- Connect the Microsoft Entra connector
- Connect the Microsoft Entra ID Protection connector
- Connect the Azure Activity connector
- Knowledge check
- Summary and resources

Learning Objectives

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

Module 43: Connect Microsoft Defender XDR to Microsoft Sentinel

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

Lessons

- Introduction
- Plan for Microsoft Defender XDR connectors
- Connect the Microsoft Defender XDR connector
- Connect Microsoft Defender for Cloud connector
- Connect Microsoft Defender for IoT
- Connect Microsoft Defender legacy connectors
- Knowledge check
- Summary and resources

Learning Objectives

- 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

Module 44: Connect Windows hosts to Microsoft Sentinel

Two of the most common logs to collect are Windows security events and Sysmon. Learn how Microsoft Sentinel makes this easy with the Security Events connector.

Lessons

- Introduction
- Plan for Windows hosts security events connector
- Connect using the Windows Security Events via AMA Connector

- Connect using the Security Events via Legacy Agent Connector
- Collect Sysmon event logs
- Knowledge check
- Summary and resources

Learning Objectives

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

Module 45: 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.

Lessons

- Introduction
- Plan for Common Event Format connector
- Connect your external solution using the Common Event Format connector
- Knowledge check
- Summary and resources

Learning Objectives

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

Module 46: 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.

Lessons

- Introduction
- Plan for syslog data collection
- Collect data from Linux-based sources using syslog
- Configure the Data Collection Rule for Syslog Data Sources
- Parse syslog data with KQL
- Knowledge check
- Summary and resources

Learning Objectives

- 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

Module 47: Connect threat indicators to Microsoft Sentinel

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

Lessons

- Introduction
- Plan for threat intelligence connectors
- Connect the threat intelligence TAXII connector
- Connect the threat intelligence platforms connector
- View your threat indicators with KQL
- Knowledge check
- Summary and resources

Learning Objectives

- Configure the Defender Threat Intelligence connector in 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 48: 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.

Lessons

- Introduction
- Exercise - Detect threats with Microsoft Sentinel analytics
- What is Microsoft Sentinel Analytics?
- Types of analytics rules
- Create an analytics rule from templates
- Create an analytics rule from wizard
- Manage analytics rules
- Exercise - Detect threats with Microsoft Sentinel analytics
- Summary

Learning Objectives

- 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 49: 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.

Lessons

- Introduction
- Understand automation options
- Create automation rules
- Knowledge check
- Summary and resources

Learning Objectives

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

Module 50: Threat response with Microsoft Sentinel playbooks

This module describes how to create Microsoft Sentinel playbooks to respond to security threats.

Lessons

- Introduction
- Exercise - Create a Microsoft Sentinel playbook
- What are Microsoft Sentinel playbooks?
- Trigger a playbook in real-time
- Run playbooks on demand
- Exercise - Create a Microsoft Sentinel playbook
- Summary

Learning Objectives

- 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 51: 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.

Lessons

- Introduction
- Exercise - Set up the Azure environment
- Understand incidents
- Incident evidence and entities
- Incident management
- Exercise - Investigate an incident
- Summary

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.

Module 52: Identify threats with Behavioral Analytics

Learn how to use entity behavior analytics in Microsoft Sentinel to

identify threats inside your organization.

Lessons

- Introduction
- Understand behavioral analytics
- Explore entities
- Display entity behavior information
- Use Anomaly detection analytical rule templates
- Knowledge check
- Summary and resources

Learning Objectives

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

Module 53: Data normalization in Microsoft Sentinel

By the end of this module, you're able to use Advanced Security Information Model (ASIM) parsers to identify threats inside your organization.

Lessons

- Introduction
- Understand data normalization
- Use ASIM Parsers
- Understand parameterized KQL functions
- Create an ASIM Parser
- Configure Azure Monitor Data Collection Rules
- Knowledge check
- Summary and resources

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

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

Module 54: Query, visualize, and monitor data in Microsoft Sentinel

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

Lessons

- Introduction
- Exercise - Query and visualize data with Microsoft Sentinel Workbooks
- Monitor and visualize data
- Query data using Kusto Query Language
- Use default Microsoft Sentinel Workbooks
- Create a new Microsoft Sentinel Workbook
- Exercise - Visualize data using Microsoft Sentinel Workbooks
- Summary

Learning Objectives

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

Module 55: Manage content in Microsoft Sentinel

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

Lessons

- Introduction
- Use solutions from the content hub
- Use repositories for deployment
- Knowledge check
- Summary and resources

Learning Objectives

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

Module 56: Explain threat hunting concepts in Microsoft Sentinel

Learn the threat hunting process in Microsoft Sentinel.

Lessons

- Introduction
- Understand cybersecurity threat hunts
- Develop a hypothesis
- Explore MITRE ATT&CK
- Knowledge check
- Summary and resources

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

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

Module 57: Threat hunting with Microsoft Sentinel

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

Lessons

- Introduction
- Exercise setup
- Explore creation and management of threat-hunting queries
- Save key findings with bookmarks
- Observe threats over time with livestream
- Exercise - Hunt for threats by using Microsoft Sentinel
- Summary

Learning Objectives

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

Module 58: **Use Search jobs in Microsoft Sentinel**

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

Lessons

- Introduction
- Hunt with a Search Job
- Restore historical data
- Knowledge check
- Summary and resources

Learning Objectives

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

Module 59: **Hunt for threats using notebooks in Microsoft Sentinel**

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

Lessons

- Introduction
- Access Azure Sentinel data with external tools
- Hunt with notebooks
- Create a notebook
- Explore notebook code
- Knowledge check
- Summary and resources

Learning Objectives

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

ASSOCIATED CERTIFICATIONS & EXAMS

This course will prepare delegates to write the Microsoft Certified: Security Operations Analyst Associate Exam.