Microsoft Security Operations Analyst (SC-200)

Description

Enhance Your Cybersecurity Skills

Discover how to become a cybersecurity expert by mastering Microsoft’s essential tools. The Microsoft Security Operations Analyst (SC-200) course guides you in effectively detecting, addressing, and analyzing threats. With powerful tools like Microsoft Sentinel, Microsoft Defender XDR, and Microsoft Defender for Cloud, you’ll learn to protect modern IT environments.

This course is designed for anyone looking to specialize in security incident response and proactive risk management. You’ll learn to use Kusto Query Language (KQL) for incident analysis, configure Sentinel, and enhance your security posture. Numerous hands-on demonstrations and case studies allow you to directly apply the concepts learned.

Obtain your SC-200 certification with comprehensive preparation

This comprehensive course thoroughly prepares you for the SC-200 exam, equipping you with all the essential knowledge for success. Develop your analytical skills, improve your incident response capabilities, and become a key player in cybersecurity using Microsoft solutions.

Course Content
Module 1: Introduction to Microsoft Defender XDR Threat Protection

- Explore use cases for Extended Detection and Response (XDR)
- Understand Microsoft Defender XDR in a Security Operations Center (SOC)
- Explore Microsoft Security Graph
- Review security incidents in Microsoft Defender XDR

Module 2: Reduce Incidents with Microsoft Defender

- Use the Microsoft Defender portal
- Manage incidents
- Investigate incidents
- Manage and review alerts
- Manage automated investigations
- Use the Notification Center
- Explore advanced threat hunting
- Review Microsoft Entra sign-in logs
- Understand the Microsoft Secure Score
- Analyze threats
- Analyze reports
- Configure the Microsoft Defender portal

Module 3: Mitigate Risks with Microsoft Defender for Office 365

- Introduction to Microsoft Defender for Office 365

- Automate, investigate, and remediate
- Configure, protect, and detect
- Simulate attacks

Module 4: Manage Microsoft Entra Identity Protection

- Review the fundamentals of Identity Protection
- Implement and manage a user risk policy
- Monitor, investigate, and remediate risky users
- Secure workload identities
- Explore Microsoft Defender for Identity

Module 5: Protect Your Environment with Microsoft Defender for Identity

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

Module 6: Secure Your Cloud Apps and Services with Microsoft Defender for Cloud Apps

- Understand the Microsoft Defender for Cloud Apps framework
- Discover your cloud apps with Cloud Discovery
- Protect your data and apps with Conditional Access App Control
- Navigate discovery and access control with Microsoft Defender for Cloud Apps
- Classify and protect sensitive information
- Detect threats

Module 7: Introduction to Generative AI

- What is Generative AI?
- What are language models?
- Using language models
- What are copilots?
- Microsoft Copilot
- Copilot prompt considerations
- Extending and developing copilots

Module 8: Overview of Microsoft Security Copilot

- Get familiar with Microsoft Security Copilot
- Understand Microsoft Security Copilot terminology
- How Security Copilot processes prompts
- Elements of an effective prompt
- How to activate Microsoft Security Copilot

Module 9: Core Features of Microsoft Security Copilot

- Features in the standalone Microsoft Security Copilot experience
- Features within a standalone session
- Understand workspaces
- Explore available Microsoft plugins
- Explore supported non-Microsoft plugins

- Create custom prompt sequences
- Set up knowledge base connections

Module 10: Integrated Experiences in Microsoft Security Copilot

- Copilot in Microsoft Defender XDR
- Copilot in Microsoft Purview
- Copilot in Microsoft Entra
- Copilot in Microsoft Intune
- Copilot in Microsoft Defender for Cloud (preview)

Module 11: Explore Microsoft Security Copilot Use Cases

- Explore the initial run experience
- Explore the standalone experience
- Set up the Microsoft Sentinel plugin
- Enable a custom plugin
- Use file uploads as a knowledge base
- Create a custom prompt guide
- Explore Copilot features in Microsoft Defender XDR
- Discover Copilot features in Microsoft Purview

Module 12: Respond to Data Loss Prevention Alerts Using Microsoft 365

- Understand data loss prevention (DLP) alerts
- Review DLP alerts in Microsoft Purview
- Investigate DLP alerts in Microsoft Defender for Cloud Apps

Module 13: Manage Insider Risk in Microsoft Purview

- Overview of Insider Risk Management
- Introduction to managing insider risk policies
- Create and manage insider risk policies
- Investigate insider risk alerts
- Take action on insider risk cases
- Manage insider risk forensic evidence
- Create insider risk management notice templates

Module 14: Investigate with Microsoft Purview Audit

- Overview of Microsoft Purview Audit
- Configure and manage Microsoft Purview Audit
- Conduct searches with Audit (Standard)
- Audit Microsoft Copilot interactions for Microsoft 365
- Review activities with Audit (Premium)
- Export audit log data
- Configure audit log retention with Audit (Premium)

Module 15: Investigate Threats with Microsoft Purview Content Search

- Explore Microsoft Purview eDiscovery solutions
- Create a content search
- View search results and statistics

- Export search results and reports
- Configure search permission filtering
- Search and delete emails

Module 16: Protect Against Threats with Microsoft Defender for Endpoint

- Introduction to Microsoft Defender for Endpoint
- Practice security administration
- Hunt threats within your network

Module 17: Deploy the Microsoft Defender for Endpoint Environment

- Set up your environment
- Understand OS compatibility and capabilities
- Onboard devices
- Manage access
- Create and manage role-based access control (RBAC)
- Configure device groups
- Configure advanced environment features

Module 18: Implement Windows Security Enhancements with Microsoft Defender for Endpoint

- Understand attack surface reduction
- Enable attack surface reduction rules

Module 19: Investigate Devices in Microsoft Defender for Endpoint

- Use the device inventory list
- Investigate devices
- Use behavioral blocking and containment
- Discover devices with device discovery

Module 20: Perform Device Actions Using Microsoft Defender for Endpoint

- Understand device actions
- Run Microsoft Defender Antivirus scans on devices
- Collect investigation packages from devices
- Initiate a live response session

Module 21: Investigate Evidence and Entities Using Microsoft Defender for Endpoint

- Investigate a file
- Investigate a user account
- Investigate an IP address
- Investigate a domain

Module 22: Configure and Manage Automation Using Microsoft Defender for Endpoint

- Configure advanced features
- Manage automation upload and folder settings
- Configure automated investigation and remediation features
- Block at-risk devices

Module 23: Configure Alerts and Detections in Microsoft Defender for Endpoint

- Configure advanced features
- Configure alert notifications
- Manage alert suppression
- Manage indicators

Module 24: Use Vulnerability Management in Microsoft Defender for Endpoint

- Understand vulnerability management
- Explore vulnerabilities on your devices
- Manage remediation

Module 25: Plan Cloud Workload Protections Using Microsoft Defender for Cloud

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

Module 26: Connect Azure Resources to Microsoft Defender for Cloud

- Explore and manage your resources with Resource Inventory
- Configure automatic provisioning
- Manually provision the Log Analytics agent

Module 27: Connect Non-Azure Resources to Microsoft Defender for Cloud

- Protect non-Azure resources
- Connect non-Azure machines
- Connect your AWS accounts
- Connect your GCP accounts

Module 28: Manage Your Cloud Security Posture Management

- Explore secure score
- Explore recommendations
- Measure and enforce regulatory compliance
- Understand workbooks

Module 29: Explain Cloud Workload Protections in Microsoft Defender for Cloud

- 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 additional Microsoft Defender protections

Module 30: Remediate Security Alerts Using Microsoft Defender for Cloud

- Understand security alerts

- Remediate alerts and automate responses
- Dismiss Defender for Cloud alerts
- Generate threat intelligence reports
- Respond to alerts from Azure resources

Module 31: Build KQL Statements for Microsoft Azure Sentinel

- Understand the structure of Kusto Query Language (KQL) statements
- Use the search operator
- Use the where operator
- Use the let statement
- Use the extend operator
- Use the order by operator
- Use project operators

Module 32: Analyze Query Results Using KQL

- 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

Module 33: Generate Multi-Table Statements Using KQL

- Use the union operator
- Use the join operator

Module 34: Use Data in Microsoft Azure Sentinel with KQL

- Extract data from unstructured string fields
- Extract data from structured string data
- Incorporate external data
- Create parsers with functions

Module 35: Introduction to Microsoft Sentinel

- Overview of Microsoft Sentinel
- How Microsoft Sentinel works
- When to use Microsoft Sentinel

Module 36: Create and Manage Microsoft Sentinel Workspaces

- Organize Microsoft Sentinel workspace
- Create a Microsoft Sentinel workspace
- Manage workspaces across tenants with Azure Lighthouse
- Overview of Microsoft Sentinel permissions and roles
- Manage Microsoft Sentinel settings
- Configure logs

Module 37: Query Logs in Microsoft Azure Sentinel

- Query logs from the Logs page
- Overview of Microsoft Sentinel tables

- Understand common tables
- Understand Microsoft Defender XDR tables

Module 38: Use Watchlists in Microsoft Azure Sentinel

- Plan for watchlists
- Create a watchlist
- Manage watchlists

Module 39: Use Threat Intelligence in Microsoft Azure Sentinel

- Define threat intelligence
- Manage your threat indicators
- View threat indicators with KQL

Module 40: Integrate Microsoft Defender XDR with Microsoft Sentinel

- Understand the benefits of integrating Microsoft Sentinel with Defender XDR
- Explore capability differences between Microsoft Defender XDR and Sentinel portals
- Onboard Microsoft Sentinel to Microsoft Defender XDR
- Explore Sentinel features within Microsoft Defender XDR

Module 41: Connect Data to Microsoft Sentinel Using Data Connectors

- Ingest log data with data connectors
- Understand data connector providers
- View connected hosts

Module 42: Connect Microsoft Services to Microsoft Sentinel

- Plan for Microsoft service connectors
- Connect the Microsoft 365 connector
- Connect the Microsoft Entra connector
- Connect the Microsoft Entra ID Protection connector
- Connect the Azure Activity connector

Module 43: Connect Microsoft Defender XDR to Microsoft Sentinel

- Plan for Microsoft Defender XDR connectors
- Connect the Microsoft Defender XDR connector
- Connect the Microsoft Defender for Cloud connector
- Connect Microsoft Defender for IoT
- Connect existing Microsoft Defender connectors

Module 44: Connect Windows Hosts to Microsoft Sentinel

- Plan for the Windows host security events connector
- Connect using the Windows Security Events connector via AMA
- Connect using the Windows Security Events connector via legacy agent
- Collect Sysmon event logs

Module 45: Connect Common Event Format Logs to Microsoft Sentinel

- Plan for Common Event Format (CEF) connector

- Connect your external solution using the CEF connector

Module 46: Connect Syslog Data Sources to Microsoft Sentinel

- Plan for Syslog data collection
- Collect data from Linux sources using Syslog
- Configure data collection rules for Syslog sources
- Analyze Syslog data with KQL

Module 47: Connect Threat Indicators to Microsoft Sentinel

- Plan for threat intelligence connectors
- Connect the TAXII threat intelligence connector
- Enable threat intelligence platform connectors
- View threat indicators with KQL

Module 48: 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 using the wizard
- Manage analytics rules

Module 49: Automate with Microsoft Sentinel

- Understand automation options
- Create automation rules

Module 50: Respond to Threats with Microsoft Sentinel Playbooks

- What are Microsoft Sentinel Playbooks?
- Trigger a playbook in real-time
- Run playbooks on demand

Module 51: Manage Security Incidents in Microsoft Sentinel

- Understand incidents
- Evidence and entities in incidents
- Incident management

Module 52: Identify Threats with Behavioral Analytics

- Understand behavioral analytics
- Explore entities
- View entity behavior insights
- Use anomaly detection analytics rule templates

Module 53: Normalize Data in Microsoft Sentinel

- Understand data normalization
- Use ASIM parsers
- Understand parameterized KQL functions
- Create an ASIM parser

- Configure Azure Monitor data collection rules

Module 54: Query, Visualize, and Monitor Data in Microsoft Sentinel

- Monitor and visualize data
- Query data using Kusto Query Language (KQL)
- Use default Microsoft Sentinel workbooks
- Create a custom Microsoft Sentinel workbook

Module 55: Manage Content in Microsoft Sentinel

- Use solutions from the content hub
- Use repositories for deployment

Module 56: Explain Threat Hunting Concepts in Microsoft Sentinel

- Understand cybersecurity threat hunting
- Develop a hunting hypothesis
- Explore MITRE ATT&CK framework

Module 57: Hunt for Threats with Microsoft Sentinel

- Create and manage threat hunting queries
- Save key findings with bookmarks
- Observe threats over time with live stream

Module 58: Use Search Jobs in Microsoft Sentinel

- Hunt using search jobs
- Restore historical data

Module 59: Hunt Threats Using Notebooks in Microsoft Sentinel

- Access Azure Sentinel data with external tools
- Hunt threats with notebooks
- Create a notebook
- Explore notebook code

Lab / Exercises

- This course provides you with exclusive access to the official Microsoft lab, enabling you to practice your skills in a professional environment.

Documentation

- Access to Microsoft Learn, Microsoft's online learning platform, offering interactive resources and educational content to deepen your knowledge and develop your technical skills.

Exam

- This course prepares you to the SC-200 : Microsoft Security Operations Analyst exam

Participant profiles

- Cybersecurity analysts

- Systems technicians and engineers
- IT security consultants
- Cloud and network administrators
- IT risk management professionals

Prerequisites

- Understand the fundamental concepts of cybersecurity and incident management
- Master the basics of Microsoft Azure and cloud environments
- Know how to use IT administration and monitoring tools

Objectives

- Configure and use Microsoft Sentinel to detect and respond to threats
- Analyze and remediate incidents with Microsoft Defender XDR
- Automate attack responses with Microsoft Defender for Office 365
- Manage and secure identities with Microsoft Entra Identity Protection
- Explore cloud applications and protect data with Microsoft Defender for Cloud Apps
- Use Microsoft Security Copilot to strengthen security operations
- Deploy and manage Microsoft Defender for Endpoint
- Analyze and remediate security alerts with Microsoft Defender for Cloud

Description
Microsoft Security Operations Analyst (SC-200)
Niveau
Intermédiaire
Classroom Registration Price (CHF)
3200
Virtual Classroom Registration Price (CHF)
3000
Duration (in Days)
4
Reference
SC-200T00