# Microsoft Security Operations Analyst

## Description

This training offered by Microsoft will allow you to discover how to investigate, respond to, and research threats using Microsoft Azure Sentinel, Azure Defender, and Microsoft 365 Defender. Throughout this program, you will learn how to mitigate cybersecurity threats using these technologies. Specifically, you will configure and utilize Azure Sentinel along with the query language Kusto (KQL) to perform detection, analysis, and reporting tasks.

**Classroom Registration Price (CHF)**
3200
**Virtual Classroom Registration Price (CHF)**
3000
**Course Content**
**Module 1: Introduction to Microsoft 365 threat protection**

- Explore Extended Detection & Response (XDR) response use cases
- Understand Microsoft 365 Defender in a Security Operations Center (SOC)
- Investigate security incident in Microsoft 365 Defender

**Module 2: Mitigate incidents using Microsoft 365 Defender**

- Use the Microsoft 365 Defender portal
- Manage incidents
- Investigate incidents
- Manage and investigate alerts
- Manage automated investigations
- Use the action center
- Explore advanced hunting
- Investigate Azure AD sign-in logs
- Understand Microsoft Secure Score
- Analyze threat analytics
- Analyze reports
- Configure the Microsoft 365 Defender portal

**Module 3: Protect your identities with Azure AD Identity Protection**

- Azure AD Identity Protection overview
- Detect risks with Azure AD Identity Protection policies
- Investigate and remediate risks detected by Azure AD Identity Protection

**Module 4: Remediate risks with Microsoft Defender for Office 365**

- Introduction to Microsoft Defender for Office 365
- Automate, investigate, and remediate
- Configure, protect, and detect

**Module 5: Safeguard your environment with Microsoft Defender for Identity**

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

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

- 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

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

- Describe data loss prevention alerts
- Investigate data loss prevention alerts in Microsoft Purview
- Investigate data loss prevention alerts in Microsoft Defender for Cloud Apps

**Module 8: Manage insider risk in Microsoft Purview**

- Insider risk management overview
- Introduction to managing insider risk policies
- Create and manage insider risk policies
- Knowledge check
- Investigate insider risk alerts
- Take action on insider risk alerts through cases

**Module 9: Protect against threats with Microsoft Defender for Endpoint**

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

**Module 10: Deploy the Microsoft Defender for Endpoint environment**

- 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

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

- Understand attack surface reduction
- Enable attack surface reduction rules

**Module 12: Perform device investigations in Microsoft Defender for Endpoint**

- Use the device inventory list

- Investigate the device
- Use behavioral blocking
- Detect devices with device discovery

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

- Explain device actions
- Run Microsoft Defender antivirus scan on devices
- Collect investigation package from devices
- Initiate live response session

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

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

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

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

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

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

**Module 17: Utilize Vulnerability Management in Microsoft Defender for Endpoint**

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

**Module 18: Plan for 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 19: Connect Azure assets to Microsoft Defender for Cloud**

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

**Module 20: 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 21: Manage your cloud security posture management**

- Explore Secure Score
- Explore Recommendations
- Measure and enforce regulatory compliance
- Understand Workbooks

**Module 22: 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 Microsoft Defender additional protections

**Module 23: Remediate security alerts using Microsoft Defender for Cloud**

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

**Module 24: Construct KQL statements for Microsoft Sentinel**

- 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

**Module 25: 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 26: Build multi-table statements using KQL**

- Use the union operator
- Use the join operator

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

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

**Module 28: Introduction to Microsoft Sentinel**

- What is Microsoft Sentinel?
- How Microsoft Sentinel works
- When to use Microsoft Sentinel

**Module 29: Create and manage Microsoft Sentinel workspaces**

- 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

**Module 30: Query logs in Microsoft Sentinel**

- Query logs in the logs page
- Understand Microsoft Sentinel tables
- Understand common tables
- Understand Microsoft 365 Defender tables

**Module 31: Use watchlists in Microsoft Sentinel**

- Plan for watchlists
- Create a watchlist
- Manage watchlists

**Module 32: Utilize threat intelligence in Microsoft Sentinel**

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

**Module 33: Connect data to Microsoft Sentinel using data connectors**

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

**Module 34: Connect Microsoft services to Microsoft Sentinel**

- Plan for Microsoft services connectors
- Connect the Microsoft Office 365 connector
- Connect the Azure Active Directory connector
- Connect the Azure Active Directory identity protection connector
- Connect the Azure Activity connector

**Module 35: Connect Microsoft 365 Defender to Microsoft Sentinel**

- Plan for Microsoft 365 Defender connectors
- Connect the Microsoft 365 Defender connector
- Connect Microsoft Defender for Cloud connector
- Connect Microsoft Defender for IoT
- Connect Microsoft Defender legacy connectors

**Module 36: Connect Windows hosts to Microsoft Sentinel**

- 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

**Module 37: Connect Common Event Format logs to Microsoft Sentinel**

- Plan for Common Event Format connector
- Connect your external solution using the Common Event Format connector

**Module 38: Connect syslog data sources to Microsoft Sentinel**

- Plan for the syslog connector
- Collect data from Linux-based sources using syslog
- Configure the log analytics agent
- Parse syslog data with KQL

**Module 39: Connect threat indicators to Microsoft Sentinel**

- Plan for threat intelligence connectors
- Connect the threat intelligence TAXII connector
- Connect the threat intelligence platforms connector
- View your threat indicators with KQL

**Module 40: Threat detection 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

**Module 41: Automation in Microsoft Sentinel**

- Understand automation options
- Create automation rules

**Module 42: Threat response with Microsoft Sentinel playbooks**

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

**Module 43: Security incident management in Microsoft Sentinel**

- Describe incident management
- Understand evidence and entities
- Manage incidents

**Module 44: Identify threats with Behavioral Analytics**

- Understand behavioral analytics
- Explore entities
- Display entity behavior information
- Use Anomaly detection analytical rule templates

**Module 45: Data normalization in Microsoft Sentinel**

- Understand data normalization
- Use ASIM Parsers
- Understand parameterized KQL functions
- Create an ASIM Parser
- Configure Azure Monitor Data Collection Rules

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

- Monitor and visualize data
- Query data using Kusto Query Language
- Use default Microsoft Sentinel Workbooks
- Create a new Microsoft Sentinel Workbook

**Module 47: Manage content in Microsoft Sentinel**

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

**Module 48: Explain threat hunting concepts in Microsoft Sentinel**

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

**Module 49: Threat hunting with Microsoft Sentinel**

- Explore creation and management of Microsoft Sentinel threat-hunting queries
- Save key findings with bookmarks
- Observe threats over time with livestream

**Module 50: Use Search jobs in Microsoft Sentinel**

- Hunt with a Search Job
- Restore historical data

**Module 51: Hunt for threats using notebooks in Microsoft Sentinel**

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

**Lab / Exercises**

- Official Microsoft Labs

**Documentation**

- Access to Microsoft Learn (online learning content)

**Exam**

- This course prepares you to the **SC-200 : Microsoft Security Operations Analyst** exam
- If you wish to take this exam, please select it when you add the course to your basket

**Participant profiles**

- Security Analysts
- Security engineers

**Prerequisites**

- 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

**Objectives**

- Mitigate threats by using Microsoft 365 Defender
- Mitigate threats by using Defender for Cloud
- Mitigate threats by using Microsoft Sentinel

**Niveau**
Intermédiaire
**Duration (in Days)**
4
**Reference**
SC-200T00