Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS, Woluwedal 30, 1932 Sint-Stevens-Woluwe

Email: education.ecs.benelux@arrow.com
Phone: +32 2 332 19 57

Microsoft Security Operations Analyst

CODE:	LENGTH:	PRICE:
MCS_SC-200T00	32 Hours (4 days)	€2,295.00

Description

Learn how to investigate, respond to, and hunt for threats using Microsoft Sentinel, Microsoft Defender XDR and Microsoft Defender for Cloud. 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

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 XDR, Microsoft Defender for Cloud, 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

- Fundamental understanding of Microsoft security, compliance, and identity products
- Basic understanding of Microsoft Defender XDR

- Working knowledge of Microsoft security, compliance, and identity products
- Working knowledge of security operations and incident response
- Working knowledge of Microsoft Defender XDR

- Basic understanding of Microsoft 365
- Intermediate understanding of Microsoft Windows 10 and 11 devices
- Understanding of Microsoft Defender by completing learning path SC-200: Mitigate threats using Microsoft Defender

- Familiarity with Azure services, specifically Azure SQL Database and Azure Storage
- Familiarity with Azure virtual machines and virtual networking
- Foundational knowledge of computer networking

Programme

Introduction to Microsoft Defender XDR threat protection
• 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
• Module assessment
• Summary and resources
Mitigate incidents using Microsoft Defender
• 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
• Analyze threat analytics with the Security Copilot Threat Intelligence Briefing Agent
• Analyze reports
• Configure the Microsoft Defender portal
• Module assessment
• Summary and resources

Remediate threats using Microsoft Defender
• Introduction to Microsoft Defender for Office 365
• Automate, investigate, and remediate
• Configure, protect, and detect
• Microsoft Security Copilot Phishing Triage Agent in Microsoft Defender
• Simulate attacks
• Summary and knowledge check

Manage Microsoft Entra Identity Protection
• 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
• Explore the Identity Risk Management Agent
• Module assessment
• Summary and resources

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
• Summary and knowledge check

Secure your cloud apps and services with Microsoft Defender for Cloud Apps
• 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
• Module assessment
• Summary

Introduction to generative AI and agents
• Introduction
• Large language models (LLMs)
• Prompts
• AI agents
• Exercise - Explore generative AI
• Module assessment
• Summary

Describe Microsoft Security Copilot
• 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
• Module assessment
• Summary and resources

Describe the core features of Microsoft Security Copilot
• Introduction
• Describe the features available in the standalone experience of Microsoft Security Copilot
• Describe the features available in a session of the standalone experience
• Describe workspaces

• Describe Security Copilot plugins
• Describe custom promptbooks
• Describe knowledge base connections
• Module assessment
• Summary and resources

Describe the embedded experiences of Microsoft Security Copilot
• Introduction
• Describe Copilot in Microsoft Defender XDR
• Copilot in Microsoft Purview
• Copilot in Microsoft Entra
• Copilot in Microsoft Intune
• Copilot in Microsoft Defender for Cloud
• Module assessment
• Summary and resources

Experience Security Copilot through guided simulations
• Introduction
• Explore owner settings in Security Copilot
• Use prompts and promptbooks in Security Copilot
• Create a custom promptbook in Security Copilot
• Investigate data protection activity in Microsoft Purview
• Investigate insider risks and compliance in Microsoft Purview
• Investigate security incidents in Microsoft Defender XDR
• Explore and create an agent in Security Copilot
• Explore the Conditional Access Optimization Agent
• Module assessment
• Summary

Protect against threats with Microsoft Defender for Endpoint
• Introduction to Microsoft Defender for Endpoint
• Practice security administration
• Hunt threats within your network
• Summary and knowledge check

Deploy the Microsoft Defender for Endpoint environment
• 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
• Module assessment
• Summary and resources

Implement Windows security enhancements with Microsoft Defender for Endpoint
• Introduction
• Understand attack surface reduction
• Enable attack surface reduction rules
• Module assessment
• Summary and resources

Perform device investigations in Microsoft Defender for Endpoint
• Introduction
• Use the device inventory list
• Investigate the device
• Use behavioral blocking
• Detect devices with device discovery
• Module assessment
• Summary and resources

Perform actions on a device using Microsoft Defender for Endpoint
• Introduction
• Explain device actions
• Run Microsoft Defender antivirus scan on devices
• Collect investigation package from devices
• Initiate live response session
• Module assessment
• Summary and resources

Perform evidence and entities investigations using Microsoft Defender for Endpoint
• Introduction
• Investigate a file
• Investigate a user account
• Investigate an IP address

• Investigate a domain
• Module assessment
• Summary and resources

Configure and manage automation using Microsoft Defender for Endpoint
• Introduction
• Configure advanced features
• Manage automation upload and folder settings
• Configure automated investigation and remediation capabilities
• Block at risk devices
• Module assessment
• Summary and resources

Configure for alerts and detections in Microsoft Defender for Endpoint
• Introduction
• Configure advanced features
• Configure alert notifications
• Manage alert suppression
• Manage indicators
• Module assessment
• Summary and resources

Utilize Vulnerability Management in Microsoft Defender for Endpoint
• Introduction
• Understand vulnerability management
• Explore vulnerabilities on your devices
• Manage remediation
• Module assessment
• Summary and resources

Plan for cloud workload protections using Microsoft Defender for Cloud
• 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
• Module assessment
• Summary and resources

Connect Azure assets to Microsoft Defender for Cloud
• Introduction
• Explore and manage your resources with asset inventory
• Configure auto provisioning
• Manual agent provisioning
• Module assessment
• Summary and resources

Connect non-Azure resources to Microsoft Defender for Cloud
• Introduction
• Protect non-Azure resources
• Connect non-Azure machines
• Connect your AWS accounts
• Connect your GCP accounts
• Module assessment
• Summary and resources

Manage your cloud security posture management
• Introduction
• Explore Secure Score
• Explore Recommendations
• Measure and enforce regulatory compliance
• Understand Workbooks
• Module assessment
• Summary and resources

Explain cloud workload protections in Microsoft Defender for Cloud
• 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
• Module assessment
• Summary and resources
Remediate security alerts using Microsoft Defender for Cloud
• 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
• Module assessment
• Summary and resources

Session Dates

Date	Location	Time Zone	Language	Type	Guaranteed	PRICE
22 Feb 2027	Virtual Classroom (CET / UTC +1)	CET	English	Instructor Led Online		€2,295.00
26 Apr 2027	Virtual Classroom (CET / UTC +1)	CEDT	English	Instructor Led Online		€2,295.00
28 Jun 2027	Virtual Classroom (CET / UTC +1)	CEDT	English	Instructor Led Online		€2,295.00

Additional Information

This training is also available as onsite training. Please contact us to find out more.