Microsoft Security Operations Analyst (Microsoft SC-200)

Official SC-200 course, exam preparation

Hands-on course of 4 days - 28h
Ref.: MCJ - Price 2026: CHF2 890 (excl. taxes)

With this training course, you'll learn how to detect, analyze and respond to threats using Microsoft Sentinel, Microsoft Defender XDR and Microsoft Defender for Cloud. You'll see how to use them to strengthen security, investigate incidents and reduce cyberthreats.

EDUCATIONAL OBJECTIVES

At the end of the training, the trainee will be able to:

Understand and apply the principles of security in Azure.

Manage user identities and access.

Secure networks, data and applications.

Monitor and correct threats and vulnerabilities.

Implement protection and compliance solutions.

TEACHING METHODS

Training in French. Official course material in digital format and in English. Good understanding of written English.

CERTIFICATION

Successful completion of the exam leads to certification as a "Microsoft Certified: Security Operations Analyst Associate".

PARTICIPANTS

Security professionals responsible for detecting, analyzing and responding to threats using Microsoft protection and monitoring tools.

PREREQUISITES

Basic knowledge of Microsoft, Azure and Microsoft 365 security is recommended before taking this course.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@ORSYS.fr to review your request and its feasibility.

THE PROGRAMME

last updated: 11/2025

1) Mitigate threats with Microsoft Defender XDR

- Introduction to threat protection with Microsoft Defender XDR.
- Mitigate incidents with Microsoft Defender.
- Reduce risk with Microsoft Defender for Office 365.
- Manage Microsoft Entra Identity Protection.
- Secure your environment with Microsoft Defender for Identity.
- Secure your applications and cloud services with Microsoft Defender for Cloud Apps.

2) Mitigate threats with Microsoft Security Copilot

- Introduction to the concepts of generative AI.
- Introducing Microsoft Security Copilot.
- Copilot's main safety features.
- Integrated Copilot experiences in Microsoft Security products.
- Microsoft Security Copilot use case.

3) Mitigate threats with Microsoft Purview

- Investigate and respond to Microsoft Purview Data Loss Prevention (DLP) alerts.
- Investigate internal risk alerts and related activities.
- Conduct research and investigations with Microsoft Purview Audit.
- Search content with Microsoft Purview eDiscovery.

4) Mitigate threats with Microsoft Defender for Endpoint

- Protect yourself against threats with Defender for Endpoint.
- Deploy the Defender for Endpoint environment.

- Improving Windows security with Defender for Endpoint.
- Examine devices with Defender for Endpoint.
- Act on a device via Defender for Endpoint.
- Analyze evidence and entities in Defender for Endpoint.
- Configure and manage automation with Defender for Endpoint.
- Configure alerts and detections in Defender for Endpoint.
- Using vulnerability management in Defender for Endpoint.

5) Mitigate threats with Microsoft Defender for the Cloud
- Plan the protection of cloud workloads with Defender for the Cloud.
- Connect Azure resources to Defender for the Cloud.
- Connect non-Azure resources to Defender for the Cloud.
- Managing the cloud security posture.
- Explain how to protect cloud workloads.
- Apply remediation to security alerts.

DATES

Contact us