Course : Microsoft Security Operations Analyst (Microsoft SC-200)

Official SC-200 course, exam preparation

Practical course - 4d - 28h00 - Ref. MCJ
Price : 2890 € E.T.

3,8 / 5

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.

Teaching objectives

At the end of the training, the participant 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.

Intended audience

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.

Practical details

Teaching methods

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

Course schedule

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 who lead the training courses are specialists in the subjects covered. They are approved by the publisher and certified for the course. They have also been validated by our teaching teams in terms of both professional knowledge and teaching skills for each course they teach. They have at least three to ten years of experience in their field and hold or have held positions of responsibility in companies.

ASSESSMENT TERMS

Assessment of targeted skills prior to training.
Assessment by the participant, at the end of the training course, of the skills acquired during the training course.
Validation by the trainer of the participant's learning outcomes, specifying the tools used: multiple-choice questions, role-playing exercises, etc.
At the end of each training course, ITTCERT provides participants with a course evaluation questionnaire, which is then analysed by our teaching teams. Participants also complete an official evaluation of the publisher.
An attendance sheet for each half-day of attendance is provided at the end of the training course, along with a certificate of completion if the participant has attended the entire session.

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.

Options

Certification : 200 € HT

Successful completion of the exam leads to certification as a "Microsoft Certified: Security Operations Analyst Associate".
Comment passer votre examen ?

The certification option comes in the form of a voucher and practice tests that will allow you to practise and take the exam at the end of the training course.

Dates and locations

TEACHING AIDS AND TECHNICAL RESOURCES

The teaching resources used are the publisher's official materials and practical exercises.

TERMS AND DEADLINES

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

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you have specific accessibility requirements? Contact Ms FOSSE, disability advisor, at the following address: psh-accueil@orsys.fr so that we can assess your request and its feasibility.

REMOTE CLASS
2026 : 23 June, 6 Oct., 15 Dec.

LYON
2026 : 23 June, 15 Dec.

PARIS LA DÉFENSE
2026 : 23 June, 6 Oct., 15 Dec.