AMBIENT-IT

+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on July 15, 2026

Sign Up

Microsoft Defender for Cloud Training

2 days (14 hours)

Overview

Microsoft Defender for Cloud is a cloud security platform designed to strengthen your security posture, prioritize risks, and protect Azure, AWS, and GCP workloads. With CSPM, CWPP, recommendations, and Secure Score, you can drive more transparent and actionable security.

Our Microsoft Defender for Cloud training goes beyond simply introducing the tool, helping you master key topics encountered in a multi-cloud and hybrid environment.

You'll learn how to structure a Cloud Security Posture Management (CSPM) approach, analyze security recommendations, interpret risk indicators, and leverage regulatory compliance dashboards.

You'll also learn how to enable and configure CWPP protection plans, understand workload coverage, track configuration discrepancies, and implement remediation actions tailored to production environments.

By the end of the training, you will be able to enhance visibility, better prioritize alerts, improve compliance, and deploy a cloud security strategy that is more robust, consistent, and actionable for operations teams.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Understand the role of Microsoft Defender for Cloud in a multicloud security strategy.
- Analyze the security posture of an environment and use the Secure Score.

- Interpret recommendations, risk levels, and remediation priorities.
- Use CSPM features to reduce misconfigurations and improve compliance.
- Configure CWPP plans to protect workloads and track their coverage.
- Implement governance, control, and monitoring practices tailored for operational use.

Target Audience

- Cloud Security Engineer
- Cloud architect
- Azure Administrator
- SOC Analyst
- Cybersecurity Consultant

Prerequisites

- Knowledge of the fundamentals of cloud architecture and shared responsibility models.
- Hands-on experience with Azure and an understanding of resources, subscriptions, and resource groups.
- Basic understanding of IT security, risk management, and access control.
- Basic experience with AWS or GCP is a plus for the multicloud environment.
- Ability to read monitoring dashboards and compliance metrics.

Technical Requirements

- A recent computer with an up-to-date browser and sufficient performance for cloud consoles.
- A stable Internet connection via Wi-Fi or Ethernet.
- Access to a Microsoft Azure environment with sufficient permissions to view security settings.
- An active Microsoft or Entra ID account to complete the exercises and log in.
- For remote training, a microphone and headset to follow along with demonstrations and workshops.

Microsoft Defender for Cloud Training Agenda

[Day 1 - Morning]

Exploring the Platform and Its Uses

- Microsoft Defender for Cloud’s role within the Microsoft security ecosystem.
- Differences between CSPM and CWPP, and how they align with business needs.
- Overview of supported environments, including Azure, AWS, and GCP.
- How to read the main dashboards, metrics, and navigation areas of the portal.
- Understanding the concepts of security posture, compliance, and prioritization.

- Hands-on workshop: getting familiar with the interface, locating key views, and identifying information useful for an initial assessment.

[Day 1 - Afternoon]

Analyzing Security Posture

- How the Secure Score works and how to interpret its changes.
- Understanding security recommendations and their prioritization.
- Analyzing risk factors related to context, configuration, and exposure.
- Using resource-based views to track discrepancies and corrective actions.
- Identifying the most common misconfigurations in a cloud environment.
- Hands-on workshop: analyzing a set of recommendations, prioritizing remediation, and proposing an action plan.

[Day 2 - Morning]

Leveraging CSPM and Compliance

- Principles of Cloud Security Posture Management in Defender for Cloud.
- Using security standards and regulatory compliance frameworks.
- Reading the compliance dashboard and interpreting discrepancies.
- Managing policies, continuous assessments, and associated remediation actions.
- Monitoring security coverage across a hybrid or multicloud environment.
- Hands-on workshop: defining a scope, reviewing its compliance, and identifying priority gaps to address.

[Day 2 - Afternoon]

Deploying workload protection

- Enabling and using CWPP policies to protect workloads.
- Overview of protections by resource type, with a focus on servers, databases, and storage.
- Understanding coverage settings, scopes, and deployment options.
- Monitoring alerts, incidents, and signals useful for operational management.
- Best practices for organizing remediation, monitoring, and long-term follow-up.
- Hands-on workshop: Configure a protection scenario, verify coverage, and prepare an actionable security report.

Target Companies

This training is designed for both individuals and companies—large or small—that wish to train their teams in new, advanced IT technologies or to acquire specific industry knowledge or modern methods.

Entry-Level Assessment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency in various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.