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

Updated on 08/26/2026

Sign Up

CNAPP Training with Prisma Cloud

2 days (14 hours)

Overview

Prisma Cloud is a CNAPP platform designed to secure applications, identities, and workloads across multicloud environments. With end-to-end visibility, risk control, and guided remediation, you can build a consistent cloud security framework, from code to execution.

This CNAPP training with Prisma Cloud enables you to go beyond the basics and master the operational challenges of cloud security in hybrid and multicloud environments.

You'll learn to understand Prisma Cloud's architecture, leverage its CSPM, CIEM, CWPP, and IaC security capabilities, and then organize risk detection, alert prioritization, and remediation.

The training will also guide you in securing workloads, analyzing misconfigurations, strengthening access governance, and standardizing DevSecOps practices tailored to cloud environments.

Upon completion of this course, you will be able to drive a more robust CNAPP approach, improve your overall security posture, and prepare for production- and compliance-oriented operations.

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 principles of a CNAPP approach and Prisma Cloud's positioning.

- Identify and prioritize risks related to configurations, identities, and cloud workloads.
- Leverage CSPM, CIEM, CWPP, and IaC security components in an end-to-end approach.
- Implement an operational approach to alerts, policies, and remediation.
- Apply best practices for DevSecOps security and multicloud governance.

Target Audience

- Cloud Security Engineer
- Cloud architect
- SOC Analyst
- DevSecOps
- Cloud Administrator

Prerequisites

- Knowledge of the fundamentals of cloud security and IaaS, PaaS, and SaaS concepts.
- Hands-on experience with AWS, Azure, or Google Cloud.
- Understanding of identities, roles, and permissions in the cloud.
- Basic knowledge of DevOps and cloud-native application deployment.

Technical Prerequisites

- A recent computer with an up-to-date web browser and sufficient resources for the demonstrations.
- Stable Wi-Fi or Ethernet connection for console access and hands-on exercises.
- Access to a cloud demo environment or test accounts, depending on the learning context.
- Headset and microphone recommended for remote sessions and workshop discussions.
- A standard text editor or IDE to view configuration and code snippets.

Agenda for our CNAPP training with Prisma Cloud

[Day 1 - Morning]

CNAPP Fundamentals and Prisma Cloud Architecture

- Understand the role of a CNAPP platform in securing the cloud lifecycle.
- Position Prisma Cloud within a multicloud and hybrid security strategy.
- Identify the key functional blocks, from visibility to remediation.
- Discover the concepts of CSPM, CIEM, CWPP, and IaC security.
- Understand the overall structure of assets, risks, and security policies.
- Hands-on workshop: getting started with the interface and locating the main dashboards.

[Day 1 – Afternoon]

Security Posture and Compliance

- Analyze the most common misconfigurations in cloud environments.
- Understand the principles of compliance, continuous monitoring, and gap analysis.
- Explore security policies and their impact on risk prioritization.
- Learn how to interpret alerts, scores, and severity levels.
- Link security posture, governance, and operational requirements.
- Hands-on workshop: assessing a set of findings and developing a remediation plan.

[Day 2 - Morning]

Identities, Workloads, and Detection

- Delve deeper into identity and permission management with CIEM.
- Understand the exposure of workloads, containers, and serverless environments.
- Link threat detection to visibility into cloud assets.
- Explore the uses of CWPP to strengthen runtime protection.
- Structure an investigation-oriented approach to reduce alert noise.
- Hands-on workshop: Analysis of a risk scenario combining identity, workloads, and cloud exposure.

[Day 2 – Afternoon]

Industrialization and Remediation

- Integrate security into DevSecOps chains and delivery workflows.
- Leverage IaC controls to prevent errors before deployment.
- Organize manual or guided remediation based on the level of criticality.
- Implement monitoring, reporting, and continuous improvement practices.
- Prepare for sustainable operations tailored to production and compliance constraints.
- Hands-on workshop: Designing an end-to-end security workflow, from code to the cloud.

Target Audience

This training is intended 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 methodologies.

Assessment upon enrollment

The assessment process at the start of the training program complies with Qualiopi quality standards. Upon final enrollment, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency with various types of technology, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also enables us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could

impede the monitoring and smooth running of the training session.

Teaching Methods

Hands-On Course: 60% Hands-On, 40% Theory. 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.