+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

Cortex XDR Training

3 days (21 hours)

Overview

Cortex XDR centralizes the detection, investigation, and response to advanced threats by correlating signals from endpoints, the network, and the cloud. This training helps you leverage a unified security platform to gain visibility, reduce alert noise, and accelerate operational decisions.

Our Cortex XDR training will enable you to go beyond basic usage to master the key mechanisms involved in monitoring and incident handling.

You'll learn to understand the platform's architecture, analyze alerts, conduct effective investigations, and implement remediation actions tailored to the detected threats.

By the end of the training, you will be able to leverage correlation, threat hunting, triage, and response capabilities to strengthen your organization's security posture.

This training also covers best practices for deployment, configuration, monitoring, and ensuring operational reliability to make your analyses faster and more robust in a real-world environment.

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 fundamental concepts of Cortex XDR and its role in a detection and response strategy.
- Identify telemetry sources, alerts, and signals useful for security analysis.

- Investigate incidents, reconstruct an attack chain, and assess the severity of an event.
- Implement triage, investigation, and remediation actions within the interface.
- Leverage search and correlation features to accelerate threat hunting.
- Apply operational best practices to improve the SOC’s responsiveness and the quality of decisions.

Target Audience

- SOC Analyst
- Security Administrator
- Cybersecurity Engineer
- IT Security Manager
- Security Consultant

Prerequisites

- Proficiency in the fundamentals of cybersecurity and incident detection principles.
- Knowledge of Windows and Linux environments and the fundamentals of system administration.
- Understanding of network concepts, event logs, and how a SOC operates.
- Experience with a monitoring, incident management, or log analysis tool.

Technical Prerequisites

- A recent laptop with an up-to-date web browser and sufficient disk space for hands-on exercises.
- Stable Wi-Fi or Ethernet connection to access the demo environments.
- Access to a workstation with sufficient privileges to use the consoles and tools provided during the session.
- A microphone and headset are recommended for remote sessions and discussions during workshops.
- If a lab environment is provided, ensure you have a functional account and the necessary access permissions before the session begins.

Cortex XDR Training Agenda

[Day 1 - Morning]

Fundamentals and Architecture

- Understand the role of Cortex XDR in a detection and response strategy.
- Identify data sources, sensors, and multi-source correlation logic.
- Explore the overall architecture, key components, and information flows.
- Grasp the concepts of telemetry, alerts, and incidents within the platform.
- Connect SOC use cases to the solution’s native capabilities.

- Hands-on workshop: getting started with the interface, locating useful areas, and reviewing an initial incident.

[Day 1 - Afternoon] Deployment and Configuration

- Understand the logic behind deploying agents and integrations.
- Configure essential elements to set up a production-ready environment.
- Explore security profiles, policies, and basic settings.
- Analyze the impact of configuration choices on visibility and protection.
- Apply best practices for the initial structuring of a tenant.
- Hands-on workshop: Setting up a basic configuration and validating data reporting.

[Day 2 - Morning] Alert Analysis

- Interpret an alert and distinguish between useful signals, false positives, and correlated events.
- Explore the available contextual elements to characterize an incident.
- Understand the concepts of causality chains and attack scenarios.
- Use summary views to speed up triage.
- Develop a reproducible analysis method for the SOC.
- Hands-on workshop: qualifying alerts, gathering clues, and drafting an initial assessment.

[Day 2 - Afternoon] Investigation and Threat Hunting

- Delve deeper into incident investigation using data from the platform.
- Search for useful artifacts to trace the source of a compromise.
- Discover the principles of threat hunting as applied to Cortex XDR.
- Utilize filters, contextual navigation, and analysis pivots.
- Consolidate an investigation approach focused on evidence and timeline.
- Hands-on workshop: Reconstructing an attack scenario and searching for associated indicators.

[Day 3 - Morning] Response and Remediation

- Understand the response actions available in the console.
- Select appropriate measures based on criticality and confidence level.
- Manage isolation, remediation, and corrective actions in a controlled manner.
- Document decisions and ensure operational traceability.
- Integrate the response into a broader incident handling process.
- Hands-on workshop: implementing containment measures and verifying a return to a controlled state.

[Day 3 - Afternoon]

Advanced Operations and Best Practices

- Consolidate advanced practices to ensure the reliability of daily operations.
- Review methods for optimizing triage, monitoring, and follow-up.
- Identify useful metrics for managing detection activities.
- Apply best practices for governance, maintenance, and continuous improvement.
- Prepare for increased autonomy in handling the most common use cases.
- Hands-on workshop: comprehensive case study, from initial detection to final response.

Target Audience

This training is intended for both individuals and companies—large or small—that wish to train their teams in new, advanced IT technology 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 with 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.