+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 XSIAM Training

2 days (14 hours)

Overview

Cortex XSIAM is an AI-driven operational security platform that unifies XDR, SIEM, SOAR, and automation to transform the SOC. This training provides you with the keys to leveraging an architecture designed for detection, investigation, and response, with production-oriented use cases.

Our Cortex XSIAM training will enable you to go beyond basic usage and master the essential functions found in a modern security operations center.

You'll learn to understand the platform's architecture, leverage data collection and normalization, conduct faster investigations with XQL, and structure automation workflows tailored to the SOC's needs.

Upon completion of the training, you will be able to analyze alerts more effectively, prioritize incidents, reduce operational noise, and better standardize your detection and response activities.

This training also covers dashboards, metrics, event contextualization, best practices for management, and the reflexes needed to use Cortex XSIAM 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 how Cortex XSIAM fits into a modern SOC strategy.

- Master the platform’s main components, data collection, and normalization logic.
- Use XQL to search for, correlate, and analyze security events.
- Structure faster, better-prioritized investigations based on alerts and cases.
- Implement automation measures to accelerate incident response.
- Use dashboards and management reports to monitor security activity.

Target Audience

- SOC Analyst
- SOC Engineer
- Operational Security Manager
- Cybersecurity Consultant
- Detection and Response Engineer

Prerequisites

- Basic knowledge of cybersecurity and how a SOC operates.
- Practical experience with alert investigation and event analysis.
- Understanding of SIEM, XDR, or SOAR principles.
- Ability to easily interpret logs, indicators, and technical security data.
- Prior experience with a monitoring or incident response platform.

Technical Prerequisites

- A recent laptop with an up-to-date web browser and sufficient resources for the exercises.
- A stable Wi-Fi or Ethernet connection to follow the demonstrations and workshops.
- Access to a lab environment or a Cortex XSIAM demo account, if provided.
- Headphones and a microphone for remote sessions, if the training is conducted via videoconference.
- A work environment that allows you to open multiple tabs, consoles, and dashboards simultaneously.

Cortex XSIAM Training Program

[Day 1 - Morning]

Platform Fundamentals

- Cortex XSIAM’s role in the SecOps ecosystem.
- Functional architecture, unified platform logic, and operational benefits.
- The role of data in detection, investigation, and response.
- Overview of XDR, SIEM, SOAR, and automation components.
- Overview of key objects, views, and workspaces.

- Hands-on workshop: getting familiar with the interface, identifying key areas, and locating monitoring objects.

[Day 1 - Afternoon]

Data Collection and Analysis

- Supported data sources and ingestion logic.
- Standardization, enrichment, and contextualization of events.
- Managing alerts, signals, and cases in the analysis workflow.
- Data quality principles to improve detection.
- Organizing monitoring views for the SOC’s daily operations.
- Hands-on workshop: Analyzing an event stream, extracting relevant data, and qualifying an alert.

[Day 2 - Morning]

Investigation with XQL

- Basic XQL syntax and query logic.
- Filtering, aggregating, and sorting analysis results.
- Correlating events to reconstruct an attack sequence.
- Searching for indicators, anomalies, and suspicious behavior.
- Methods for speeding up triage and reducing noise.
- Hands-on workshop: writing XQL queries to investigate an incident scenario.

[Day 2 - Afternoon] SOC

Automation and Management

- Logic behind automation workflows and guided actions.
- Triggering responses based on severity level.
- Dashboards, metrics, and operational monitoring.
- Best practices for prioritization and reducing turnaround time.
- Standardization of repetitive tasks in the SOC.
- Hands-on workshop: Design an automated response scenario and validate it using a use case.

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 business knowledge or modern methods.

Assessment at the Start of Training

The assessment at the start of the training program 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 technology, 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 (in-house or virtual classroom) that could pose challenges for monitoring and ensuring the smooth operation 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.