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

Updated on August 14, 2026

Sign Up

Gatewatcher Training

2 days (14 hours)

Overview

Gatewatcher is an NDR platform designed to provide comprehensive network visibility, advanced threat detection, and rapid response. With its analytics engines, alert contextualization, and decision-oriented approach, Gatewatcher helps cybersecurity teams prioritize and respond more effectively. Our Gatewatcher training course enables you to master the platform's operational fundamentals so you can effectively leverage its capabilities for detection, analysis, and incident management. You'll learn to understand the solution's architecture, interpret network events, assess alerts, and structure a coherent investigation within a SOC context. The training also covers implementing key monitoring use cases, interpreting indicators of compromise, utilizing prioritization features, and best practices for threat handling. By the end of this two-day course, you'll be able to use Gatewatcher systematically to enhance threat detection, improve your teams' responsiveness, and contribute to a more robust security posture.

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

Objectives

- Understand Gatewatcher's role within an NDR strategy.
- Identify the platform's key components and their operational uses.
- Analyze alerts and weak signals to assess a threat.
- Structure a network investigation based on the data available in the solution.
- Use prioritization features to improve incident handling.
- Apply best practices for day-to-day operations in a SOC environment.

Target Audience

- SOC Analyst
- Cybersecurity Engineer

- Information Systems Security Manager
- Security Administrator
- Cybersecurity Consultant

Prerequisites

- Basic knowledge of networks and TCP/IP addressing.
- Understanding of cybersecurity principles and security monitoring.
- Experience with a SOC, a monitoring tool, or a detection solution.
- Basic understanding of logs, events, and indicators of compromise.
- Experience operating an administration console or security analytics tool.

Technical Prerequisites

- A recent computer with an up-to-date web browser and sufficient resources for demonstrations.
- Stable Wi-Fi or Ethernet connection to access the training environments.
- Access to a workstation with login credentials that allow use of the demo console, if provided.
- Headset and microphone recommended for remote sessions and collaborative workshops.
- If a test environment is used, have the login credentials and access provided in advance.

Gatewatcher Training Program

[Day 1 - Morning]

Platform Fundamentals

- Gatewatcher’s role in an NDR and threat detection strategy.
- Understanding the functional architecture, component roles, and information flows.
- Understanding the concepts of network visibility, contextualization, and prioritization.
- Overview of the types of signals used to detect suspicious activity.
- Overview of SOC use cases and the most common applications.
- Hands-on workshop: mapping the solution’s components and linking each building block to its operational role.

[Day 1 - Afternoon]

Exploring Alerts

- Navigating the interface and identifying areas useful for analysis.
- Reading an alert, understanding the context, and identifying key elements.
- Distinguishing between noise, weak signals, and actionable events.
- Using filters, views, and search criteria to refine the analysis.
- Initial triage steps to properly guide the response.
- Hands-on workshop: Analyzing a set of alerts and classifying events according to their criticality level.

[Day 2 - Morning]

Investigation and

Correlation

- Investigation methods based on an indicator, an alert, or abnormal behavior.
- Exploring the relationships between hosts, traffic flows, and objects observed in the platform.
- Correlating signals to reconstruct a possible attack sequence.
- Interpreting clues useful for classifying a known or unknown threat.
- Organizing a reproducible investigation that can be utilized by a security team.
- Hands-on workshop: conducting a guided investigation based on a simulated attack scenario.

[Day 2 - Afternoon]

Operational Analysis

- Structuring incident handling and action priorities.
- Using management functions to accelerate decision-making.
- Best practices for tracking, documenting, and reporting analysis results.
- Integrating the solution into a daily monitoring process.
- Tips for scaling up to ensure reliable use in a production environment.
- Hands-on workshop: Building a mini incident handling process based on a business use case.

Target Audience

This training is intended for both individuals and companies—large or small—that wish to train their teams in a new advanced IT technology or to acquire specific business knowledge or modern methods.

Prerequisites for the training

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.