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

Updated 01/23/2025

Sign up

Zeek training

3 days (21 hours)

Presentation

Our Zeek training will teach you the skills you need to detect, identify and contain all intrusions. Our program covers all the tool's functionalities, so you can effectively analyze and deal with cyber attacks.

In this course, you'll learn how to identify intrusions with Zeek and secure your IT environment. Through a hands-on demonstration, you'll learn how to optimize, integrate and manage Zeek in production.

You'll learn about best practices, role management, logs and . Threat response automation and orchestration with Zeek.

As with all our training courses, we will introduce you to the latest version of the software: Zeek V7.1.0

Objectives

- Understanding Zeek's role in cybersecurity
- Logs generated by Zeek
- Zeek scripting language
- Optimizing performance in high-traffic environments
- malicious domains
- Create scripts to customize alerts and analyses

Target audience

- **Cybersecurity Analysts**
- SOC Analysts
- Safety engineer

- Network Administrator

Prerequisites

Basic knowledge of networks and systems.

Zeek training program

INTRODUCTION TO ZEEK

- Understanding Zeek's role in cybersecurity
- How Zeek works: architecture and components
- Differences between Zeek and other IDSs such as Snot or Suricata
- Basic concepts: events, logs, scripts
- Network monitoring, threat detection

Installing and configuring Zeek

- System and hardware requirements
- Linux installation and network deployment
- Zeek initial configuration and main files
- Passive monitoring: network interface settings
- Post-installation verification and testing

Analysis of logs generated by Zeek

- Logs generated by Zeek
  - HTTP
  - DNS
  - SSL
  - Connection logs
- Understanding important fields in logs
- Extraction of safety-critical information
- Methods for identifying anomalies in logs
- Log volume management

Scripting with Zeek

- Zeek scripting language
- Scripting syntax and logic for Zeek
- Create scripts to customize alerts and analyses
- Event management and detection of specific threats
- Integrated frameworks
  - Notice
  - Intel

Advanced threat detection

- Advanced network protocol monitoring
- Detection of network anomalies and data exfiltration
- Threat identification via SSL/TLS encrypted connections
- Use of IP blacklists
- malicious domains
- Detection of port scans and suspicious activity

Zeek optimization and integration

- Optimizing performance in high-traffic environments
- Tuning network parameters to improve efficiency
- Integration with third-party tools
  - Elastic Stack
  - Splunk
  - SIEMs
- Automation with external scripts
  - Python
  - Make
- Export Zeek data for external analysis

Securing and managing Zeek in production

- Update and maintenance management
- Monitor the availability and health of Zeek instances
- Implementing a configuration backup strategy
- GDPR and ISO 27001 compliance

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.