AMBIENT-IT

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

Updated on 03/10/2024

Sign up

OpenCTI training

2 days (14 hours)

Presentation

OpenCTI is an open-source platform dedicated to cyber threat intelligence. It enables the collection, analysis and visualization of threats. Thanks to this technology, organizations can understand and anticipate cyberattacks.

During this course, you'll learn how to use OpenCTI to centralize and structure information on cyber threats, create links between different sources, visualize relationships between threats and automate integration with other security tools.

You'll also discover the key concepts of Threat Intelligence, such as indicators of compromise (IoCs), tactics, techniques and procedures (TTPs), and incident management using OpenCTI. You'll see how to structure and enrich threat data.

With this training, you'll master cyber threat intelligence management, security process automation and cyber attack analysis. You'll develop skills in data visualization, cross-team collaboration and risk anticipation.

This training course will bring you up to date with the latest developments in OpenCTI.

Objectives

- Understanding the basics of Cyber Threat Intelligence (CTI) with OpenCTI
- Using OpenCTI's dashboards and search functions
- Analyze and pivot between data to uncover threats and relationships
- Manage and configure OpenCTI for high availability and performance
- Apply troubleshooting techniques to solve problems

Target audience

- Network administrators
- **Developers**
- IT security professionals

Prerequisites

- Knowledge of Linux
- A good understanding of network concepts (TCP/IP, DNS, DHCP, etc.) is required.
- Knowledge of languages such as Python, Bash or PowerShell
- Experience in IT security

our opencti training program

INTRODUCTION to OpenCTI

- What is OpenCTI?
- Introduction to the basics of CTI (Cyber Threat Intelligence)
- Approach and use
- Data model
- Discussion on the importance of cyber threat intelligence

PLATFORM HEADER

- Search for specific information
- Customized dashboards
- Survey overview
- User profile and subscriptions

DATA MINING AND PIVOTS

- Organization dashboard
- Analysis
  - Reports
  - Grouping
- Events
  - Relationships and pivots of knowledge
  - Comments
  - Observed data
- Comments
  - Observables
  - Artifacts
  - Infrastructure

- Threats
  - Threat actors
  - Knowledge deductions
  - Intrusion sets
  - Campaigns
- Arsenal
  - Malware
  - Tools
  - Vulnerabilities

ADVANCED PLATFORM MANAGEMENT

- Advanced techniques for OpenCTI management and monitoring
- Configuring and managing a clustered environment for high availability
- Elasticsearch index optimization and rollover management
- Installation and configuration of a local map server for geospatial data
- Performance monitoring and real-time adjustments

PROBLEM SOLVING

- Troubleshooting methodologies to identify and solve common problems
- Incident management and error recovery
- Log analysis for problem diagnosis
- Tips for maintaining platform stability and performance
- Use OpenCTI forums, documentation and support to solve problems

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, with 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.