

Updated on 27/11/2024

Sign up

## Tracecat training

2 days (14 hours)

### Presentation

Tracecat is an open-source technology designed to automate security and personalize it infinitely through integration with Workflow. It enables engineers and security professionals to understand and control the automation of their playbooks.

This course covers Tracecat features, such as installing and configuring the tool, integrating with Docker Compose to create your first playbooks. We'll cover best practices for deploying playbooks securely, taking advantage of YAML to simplify the creation process.

You'll learn how to use control flow via workflow conditions, how to activate workflows via schedules and webhooks, and how to manage data migrations safely.

By the end of the course, you'll have mastered the creation of Playbooks, the advanced use of Tracecat for workflow management, and the management and security of sensitive data.

Our training will be based on the latest version of the technology: [Tracecat v 0.13](#).

### Objectives

- Master the fundamentals and advantages of Tracecat for workflow management
- Deploy Tracecat in Docker with Docker Compose following security best practices
- Integrate Tracecat and use Workflow to manage playbooks
- Customize playbooks and integrate them into Workflow
- Configure Tracecat to automate playbook management

### Target audience

- Developers
- Safety engineer
- Network administrators
- System administrators
- DevOps

## Prerequisites

- Basic knowledge of Docker and Docker Compose
- Familiarity with the Ansible playbook system
- Python and YAML programming language skills
- Access to a Docker environment to install Tracecat

# TRACECAT TRAINING PROGRAM

## INTRODUCTION TO TRACECAT

- What is Tracecat?
- Why use it?
- Basic features
  - Actions
  - Secrets
  - Expressions
  - Functions

## INSTALLATION AND CONFIGURATION

- Detailed steps for installing Tracecat
- Initial configuration and integration with Docker
- Using Docker Compose to simplify Tracecat deployment
- Setting up the Tracecat development environment
- Good safety practices during installation and configuration

## INTEGRATION WITH DOCKER

- Introducing DOCKER and the role of Tracecat
- Configuring Tracecat to work with Docker
- Understanding the key metrics provided by Tracecat
- Creating more complex playbooks with YAML
- Practical configuration and visualization exercises

## USING THE USER INTERFACE

- Navigating the Tracecat user interface
- Understanding the different tools and their uses in Tracecat
- Creation of different playbooks according to specific needs
- modification and integration with python and YAML
- Alert and notification management

## USING TRACECAT

- Learn how to use CONTROL FLOW under WORKFLOW conditions
- Using Tracecat to combine a Smaller-WORKFLOW with a Single-WORKFLOW
- Understand how to activate WORKFLOW through schedules and webhooks
- Customized additions and integration into the action register
- Discover how to update and manage data migrations securely

## UNDERSTAND THE MAIN FEATURES OF TRACECAT

- Building blocks for improved workflow automation
- Store and retrieve sensitive data
- Referencing action and result metadata in Workflow

## 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 enabling 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 with regard to 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.