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

Updated on 27/05/2024

Sign up

Salt Security training: Protecting APIs

2 days (14 hours)

Presentation

Our Salt Security training will enable you to protect your APIs and prevent against the API attacks that have been evolving in recent times. You'll be able to automate this security proactively and continuously.

In this course, find out how Salt Security analyzes the behavior of a company's APIs to spot and block attacks without any prior customization or configuration.

This course is ideal for your business, as you'll study your API traffic over the short or long term, applying cloud scaling and mature algorithms.

Learn all the methods and best practices to protect your APIs effectively.

As with all our training courses, this one will feature the latest Salt Security innovations.

Objectives

- Understanding Salt Security concepts
- How to perform safety tests
- Protect your APIs
- How to use Salt Security features

Target audience

- Safety engineers

- DevOps
- Developers
- Architects

Prerequisites

Basic knowledge of computer security.

Salt Security Training Program

Secure design and development

- What is Salt Security?
- Ensure API integration
- Streamlining API threat modeling
- Business logic in design reviews
- Normative orientations of engineering teams

Discovering and cataloguing APIs

- Discovering non-production environments
- Tag and label assets
- Inclusion of API dependencies
- Using data sources to establish a basic inventory

Safety tests

- Reuse vulnerability scanning to identify API infrastructure
- Automatically analyze API code whenever possible
- Run fuzzing and dynamic tests on deployed APIs
- Check for known vulnerable code dependencies
- Test PLCs periodically or in accordance with applicable regulations
- Boost testing with bug bounties

Front-end security

- Limiting customer-side data storage
- Examine client-side protection options after server-side protection
- Providing security requirements for front-ends
- Anticipate compromised customer code and devices

Logging and monitoring

- Incorporate non-security logging requirements
- Adopt automation for logging configuration
- Adopting cloud technology

Network security

- Use encrypted transport to protect data transmitted by your APIs
- Set up IP address authorization and refusal lists for a number of API consumers
- Use dynamic flow limits and selectively define static flow limits.
- Strengthen network security through infrastructure, not code

Data security

- Use of encryption selectively or in accordance with regulations
- Use well-tested encryption algorithms and libraries
- Avoid sending massive amounts of data to API clients
- Anticipate the risks of data scraping, aggregation and inference

Companies concerned

This training 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 is used to check correct acquisition.

skills.

Sanction

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