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

Updated on 10/16/2026

Sign Up

GitLab Security Essentials Associate Certification Training

2 days (14 hours)

Overview

Prepare for your application security certification with a hands-on approach to DevSecOps and controls integrated into pipelines. From SAST to DAST, including secret detection and vulnerability management, develop the skills needed to secure your projects and approach assessments systematically.

Our GitLab Security Essentials Associate Certification Training will help you develop the security skills required by the official certification track, combining targeted reviews with hands-on exercises using a demo application.

You'll learn how to configure security scans in your pipelines, examine dependencies and container images, and then interpret the results to identify priority fixes.

By the end of the training, you'll be able to address detected vulnerabilities, define security policies, and manage merge request approvals based on identified risks.

This preparation also covers practical certification scenarios, knowledge-based questions, and common configuration errors. Progressive exercises will help you reinforce what you've learned and prepare for the exam, which is offered as a supplement to the course.

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

Objectives

- Identify security controls appropriate for the various components of an application
- Configure static, dynamic, and secret detection analyses within a pipeline
- Analyze dependencies, container images, and infrastructure configurations
- Prioritize vulnerabilities and verify that fixes have been applied
- Implement security policies and approval rules
- Prepare knowledge assessments and practical exercises for the certification track

Target Audience

- DevSecOps Engineer
- DevOps Engineer
- Software Developer
- Application Security Engineer
- Platform Engineer

Prerequisites

- Experience with Git for branches, commits, and merges
- Proficiency in using GitLab for projects and merge requests
- Knowledge of GitLab CI/CD pipelines and YAML syntax for configuring them
- Basic understanding of application security and dependency management
- Understanding of container images and registries using Docker or an equivalent tool

Technical Prerequisites

- Computer with 8 GB of RAM recommended and a supported version of Firefox or Chrome
- Stable internet connection allowing access to the learning platforms and registries required for the workshops
- GitLab account with access to a lab group and permissions to configure projects and policies
- GitLab Ultimate environment or equivalent educational environment providing access to the security features being studied
- Access to a GitLab Runner compatible with the scanners and to an isolated test application for dynamic scans

Our GitLab Security Essentials Associate Training Curriculum

[Day 1 - Morning]

Security Fundamentals and Code Analysis

- Overview of the GitLab Security Essentials Associate Certification Training, targeted skills, and initial assessment
- DevSecOps principles, the “shift left” approach, and team responsibilities
- Selection of scanners, detection scopes, and features based on license levels
- Configuring SAST and secret detection in a pipeline
- Interpreting results in merge requests, reports, and task logs
- Hands-on Workshop: Enable code and secret scans on a lab project, then interpret the results.

[Day 1 - Afternoon]

Dependencies, containers, and infrastructure

- Configuring Dependency Scanning and identifying vulnerable components
- Reading an SBOM, taking inventory of dependencies, and identifying licenses
- Enabling Container Scanning and analyzing vulnerabilities in an image
- Analyzing Infrastructure as Code configurations and identifying risky settings
- Diagnosing Incomplete Scans, Scanner Prerequisites, and Pipeline Errors
- Hands-on workshop: Analyze dependencies, a container image, and an infrastructure configuration, then correct an issue and rerun the checks.

[Day 2 - Morning]

Dynamic analysis and vulnerability handling

- Principles of DAST, differences from SAST, and selection of authorized targets
- Configuring web application scans and an introduction to API scans
- Utilizing vulnerability reports and security dashboards
- Qualifying results, severity, business context, and justifying false positives
- Remediation cycle, ticket creation, and verification of fixes
- Hands-on workshop: Run a dynamic scan on an isolated application, qualify the results, and track a fix through to verification.

[Day 2 - Afternoon]

Security Policies and Exam Preparation

- Organizing a security policy project, scopes, and associated permissions
- Configuring scan execution policies and monitoring their enforcement
- Defining approval policies based on detected vulnerabilities and licenses
- Comprehensive Review of Certification Skills and Solving Configuration Scenarios
- Educational practice quiz, error analysis, and individual study plan
- Hands-on workshop: Complete a timed synthesis exercise combining analysis, vulnerability handling, and approval policies, then justify the choices made.

Target Audience

This training is intended for both individuals and companies—large or small—seeking to train their teams in new, advanced IT technologies or to acquire specific industry knowledge or modern methodologies.

Entry-Level Assessment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency level across various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. 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.

Training organization registered under number 11 75 54743 75. This registration does not constitute state accreditation.
© Ambient IT 2015-2026. All rights reserved. Paris, France - Switzerland - Belgium - Luxembourg