

GitLab Security Essentials Training

OEM: GitLab • Code: GITLAB_SECURITY_ESSENTIALS_TRAINING

COURSE DESCRIPTION

This class covers all of the essential security capabilities of GitLab, including Static Application Security Testing, secret detection, Dynamic Application Security Testing, dependency scanning, container scanning, API security, and compliance. Since most of these features are only available for customers with an Ultimate license, this course is intended for Ultimate customers only.

AUDIENCE PROFILE

- Project managers, developers, DevSecOps engineers, and security specialists who are using GitLab with the Ultimate license

PREREQUISITES

- GitLab Fundamentals course or equivalent knowledge
- GitLab CI/CD course or equivalent knowledge
- Knowledge of GitLab Duo and Duo Agent Platform (DAP) is beneficial to have for this course, but is not mandatory.
- This class is not appropriate for students without any Git, GitLab, or GitLab CI/CD knowledge

COURSE OBJECTIVES

By the end of this course, participants will be able to:

- This section doesn't contain any content.

COURSE OUTLINE

Module 1: Security in the Software Delivery Life Cycle

- Shift security left and right
- Choose security scanners
- Leverage vulnerability management and vulnerability reports
- Use security best practices

Module 2: Static Application Security Detection (SAST) and secret detection

- Solve problems with SAST
- Use best practices for implementing SAST scanners
- Solve problems with secret detection
- Use best practices for implementing secret detection scanners

Module 3: Addressing vulnerabilities

- View vulnerabilities in merge requests, vulnerability reports, and pipeline reports
- Use best practices for triaging vulnerabilities
- Use Duo Agent Platform to remediate vulnerabilities and check for false positives

Module 4: Dependency scanning and Infrastructure as Code (IaC) scanning

- Solve problems with dependency scanning
- Use best practices for implementing dependency scanners
- Solve problems with IaC scanning
- Use best practices for implementing IaC scanners

Module 5: Container scanning

- Solve problems with container scanning
- Use best practices for implementing container scanners

Module 6: API security and Dynamic Application Security Testing (DAST)

- Solve problems with API security
- Use best practices for implementing API security
- Solve problems with DAST
- Use best practices for implementing DAST scanners

Module 7: Operational container scanning

- Solve problems with operational container scanning
- Use best practices for implementing operational container scanners

Module 8: Compliance

- Align with common compliance standards
- Identify and enforce compliance requirements
- Track security-related actions
- Gather audit events for processing
- Control what can be pushed to a repository