

Mis à jour le 16/10/2026

S'inscrire

Formation Certification GitLab Security Essentials Associate

2 jours (14 heures)

Présentation

Préparez votre certification en sécurité applicative avec une approche concrète du DevSecOps et des contrôles intégrés aux pipelines. Du SAST au DAST, en passant par la détection des secrets et la gestion des vulnérabilités, développez les réflexes nécessaires pour sécuriser vos projets et aborder les évaluations avec méthode.

Notre Formation Certification GitLab Security Essentials Associate vous permettra de préparer les compétences de sécurité visées par le parcours officiel, en associant révisions ciblées et mises en situation sur une application de démonstration.

Vous apprendrez à configurer les analyses de sécurité dans vos pipelines, à examiner les dépendances et les images de conteneurs, puis à interpréter les résultats pour identifier les corrections prioritaires.

À l'issue de la formation, vous serez en mesure de traiter les vulnérabilités détectées, de définir des politiques de sécurité et de contrôler les approbations des demandes de fusion selon les risques identifiés.

Cette préparation aborde également les cas pratiques de certification, les questions de connaissances et les erreurs de configuration fréquentes. Des exercices progressifs vous permettront de consolider vos acquis et de préparer votre passage de l'examen, proposé en complément du parcours pédagogique.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Identifier les contrôles de sécurité adaptés aux différents composants d'une application
- Configurer les analyses statiques, dynamiques et de détection des secrets dans un pipeline
- Analyser les dépendances, les images de conteneurs et les configurations d'infrastructure
- Prioriser les vulnérabilités et vérifier les corrections apportées
- Mettre en place des politiques de sécurité et des règles d'approbation
- Préparer les évaluations de connaissances et les mises en situation du parcours de certification

Public visé

- Ingénieur DevSecOps
- Ingénieur DevOps
- Développeur logiciel
- Ingénieur sécurité applicative
- Ingénieur plateforme

Pré-requis

- Pratique de Git pour les branches, les commits et les fusions
- Utilisation courante de GitLab pour les projets et les demandes de fusion
- Connaissance des pipelines GitLab CI/CD et de la syntaxe YAML pour leur configuration
- Notions de sécurité applicative et de gestion des dépendances
- Compréhension des images et registres de conteneurs avec Docker ou un outil équivalent

Pré-requis techniques

- Ordinateur avec 8 Go de mémoire vive recommandés et un navigateur Firefox ou Chrome dans une version maintenue
- Connexion Internet stable autorisant les accès aux plateformes pédagogiques et aux registres nécessaires aux ateliers
- Compte GitLab avec accès à un groupe de laboratoire et droits de configuration des projets et des politiques
- Environnement GitLab Ultimate ou environnement pédagogique équivalent donnant accès aux fonctions de sécurité étudiées
- Accès à un GitLab Runner compatible avec les analyseurs et à une application de test isolée pour les analyses dynamiques

Programme de notre formation GitLab Security Essentials Associate

[Jour 1 - Matin]

Fondamentaux de sécurité et analyses du code

- Cadrage de la Formation Certification GitLab Security Essentials Associate, compétences visées et diagnostic initial
- Principes DevSecOps, approche shift left et responsabilités des équipes
- Choix des analyseurs, périmètres de détection et fonctionnalités selon les niveaux de licence
- Configuration du SAST et de la détection des secrets dans un pipeline
- Lecture des résultats dans les demandes de fusion, rapports et journaux des tâches
- Atelier pratique : activer les analyses du code et des secrets sur un projet de laboratoire, puis interpréter les résultats obtenus.

[Jour 1 - Après-midi]

Dépendances, conteneurs et infrastructure

- Configuration du Dependency Scanning et identification des composants vulnérables
- Lecture d'une SBOM, inventaire des dépendances et identification des licences
- Activation du Container Scanning et analyse des vulnérabilités d'une image
- Analyse des configurations Infrastructure as Code et repérage des paramètres à risque
- Diagnostic des analyses incomplètes, prérequis des analyseurs et erreurs de pipeline
- Atelier pratique : analyser les dépendances, une image de conteneur et une configuration d'infrastructure, puis corriger une anomalie et relancer les contrôles.

[Jour 2 - Matin]

Analyses dynamiques et traitement des vulnérabilités

- Principes du DAST, différences avec le SAST et choix des cibles autorisées
- Configuration des analyses d'une application web et introduction aux analyses d'API
- Exploitation des rapports de vulnérabilités et des tableaux de bord de sécurité
- Qualification des résultats, sévérité, contexte métier et justification des faux positifs
- Cycle de remédiation, création de tickets et vérification des corrections
- Atelier pratique : lancer une analyse dynamique sur une application isolée, qualifier les résultats et suivre une correction jusqu'à sa vérification.

[Jour 2 - Après-midi]

Politiques de sécurité et préparation à l'examen

- Organisation d'un projet de politiques de sécurité, périmètres et droits associés
- Configuration des politiques d'exécution des analyses et contrôle de leur application
- Définition des politiques d'approbation selon les vulnérabilités et les licences détectées
- Révision transversale des compétences de certification et résolution de scénarios de configuration
- Questionnaire blanc pédagogique, analyse des erreurs et plan de révision individuel
- Atelier pratique : réaliser un cas de synthèse chronométré combinant analyses, traitement des vulnérabilités et politique d'approbation, puis justifier les choix effectués.

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.