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

Mis à jour le 05/06/2026

S'inscrire

Formation GitHub Advanced Security

2 jours (14 heures)

Présentation

GitHub Advanced Security (GHAS) permet de sécuriser le cycle de développement logiciel directement dans GitHub grâce au Code Scanning, au Secret Scanning, à Dependabot et aux tableaux de bord de sécurité.

Notre formation GitHub Advanced Security vous permettra de mettre en place une démarche DevSecOps concrète afin d'identifier, prioriser et corriger les vulnérabilités au plus tôt dans vos projets logiciels.

Vous apprendrez à analyser vos dépôts GitHub, configurer le Code Scanning, exploiter CodeQL, détecter les secrets exposés, traiter les alertes de dépendances et réduire les risques liés à la supply chain logicielle.

Vous serez en mesure de renforcer la sécurité de vos repositories, de structurer un processus de remédiation, de configurer les bonnes pratiques de gouvernance et de suivre les indicateurs de sécurité avec Security Overview.

À l'issue de cette formation, vous serez capable d'exploiter GitHub Advanced Security pour sécuriser vos développements, vos dépendances, vos secrets et vos workflows dans une organisation DevOps.

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

Objectifs

- Comprendre le rôle de GitHub Advanced Security dans une démarche DevSecOps.
- Configurer le Code Scanning et analyser les vulnérabilités applicatives.

- Exploiter CodeQL pour détecter des failles de sécurité dans le code.
- Mettre en place le Secret Scanning et gérer les alertes associées.
- Sécuriser les dépendances avec Dependabot.
- Renforcer la sécurité de la supply chain logicielle.
- Piloter la posture sécurité d’une organisation avec les tableaux de bord GitHub.

Public visé

- Ingénieurs DevOps
- Ingénieurs DevSecOps
- Développeurs
- Lead Developers
- Architectes logiciels
- RSSI techniques
- Responsables sécurité applicative
- Platform Engineers

Pré-requis

- Connaissances de base de Git et GitHub.
- Compréhension des workflows de développement logiciel.
- Notions de CI/CD appréciées.
- Notions de sécurité applicative ou DevSecOps recommandées.

Pré-requis techniques

- Ordinateur portable avec connexion Internet stable.
- Compte GitHub actif.
- Accès à une organisation ou un dépôt GitHub de test.
- Navigateur web récent.
- Éditeur de code installé, comme Visual Studio Code.

Programme de notre formation GitHub Advanced Security (GHAS)

[Jour 1 - Matin]

Introduction à GitHub Advanced Security et sécurisation du code

- Présentation de GitHub Advanced Security
- Les enjeux de sécurité du cycle de développement logiciel
- Positionner GHAS dans une démarche DevSecOps
- Comprendre les risques liés aux secrets, dépendances et vulnérabilités applicatives
- Présentation des fonctionnalités GitHub Advanced Security

- Présentation du Code Scanning
- Comprendre les vulnérabilités applicatives courantes
- Configurer et exécuter une analyse de sécurité
- Interpréter les résultats et prioriser les corrections
- Atelier pratique : Analyser un dépôt GitHub et mettre en œuvre une première stratégie de détection des vulnérabilités.

[Jour 1 - Après-midi]

CodeQL et analyse avancée des vulnérabilités

- Présentation de CodeQL
- Comprendre le modèle d'analyse sémantique du code
- Configurer des règles d'analyse
- Personnaliser les requêtes CodeQL
- Identifier les vulnérabilités complexes
- Intégrer CodeQL dans les workflows CI/CD

Secret Scanning et protection des secrets

- Comprendre les risques liés aux secrets exposés dans le code
- Fonctionnement de Secret Scanning
- Détection des clés, tokens et identifiants sensibles
- Gestion des alertes et processus de remédiation
- Bonnes pratiques de gestion des secrets dans GitHub
- Prévenir les fuites de secrets dans les projets collaboratifs
- Atelier pratique : Détecter et corriger des secrets exposés dans un dépôt GitHub.

[Jour 2 - Matin]

Dependabot et sécurisation des dépendances

- Comprendre les risques liés aux dépendances logicielles
- Présentation de Dependabot Alerts
- Gestion des mises à jour automatiques
- Analyse des vulnérabilités des bibliothèques
- Gestion des correctifs et validation des mises à jour
- Réduire les risques liés à la supply chain logicielle
- Atelier pratique : Configurer Dependabot et traiter plusieurs vulnérabilités détectées.

[Jour 2 - Après-midi]

Supply Chain Security et gouvernance GitHub

- Comprendre les enjeux de la sécurité de la supply chain logicielle

- Identifier les risques liés aux composants tiers
- Mettre en place une gouvernance sécurité dans GitHub
- Appliquer les bonnes pratiques DevSecOps
- Renforcer la sécurité des dépôts et des workflows

Pilotage de la sécurité et amélioration continue

- Security Overview et tableaux de bord GitHub
- Suivre les indicateurs de sécurité d’une organisation
- Prioriser les actions de remédiation
- Mesurer l’efficacité des pratiques DevSecOps
- Construire une démarche d’amélioration continue
- Atelier pratique : Construire un tableau de bord sécurité et présenter les indicateurs clés d’un projet.

Pour aller plus loin

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.