Programme de formation
GH-500 : La sécurité dans Github

(Publié le 23/04/2025)

DESCRIPTION DE LA FORMATION :

Cette formation explorera comment utiliser le GitHub Advanced Security (GHAS) pour maximiser l'impact sur la sécurité et comprendre le GHAS et son rôle dans l'écosystème de la sécurité.

GHAS joue un rôle crucial dans l'amélioration de la sécurité des projets de développement de logiciels sur GitHub. Il fournit un ensemble complet d'outils et de fonctionnalités conçus pour identifier et traiter les vulnérabilités de sécurité tout au long du cycle de développement. En intégrant la sécurité directement dans le processus de développement avec GHAS, votre équipe peut construire des logiciels plus sûrs et plus fiables.

OBJECTIFS PEDAGOGIQUES :

A l'issue de cette formation, les participants seront en capacité de :

- Explorer les fonctionnalités de GitHub Advanced Security
- Configurer les mises à jour de sécurité Dependabot sur un dépôt GitHub pour détecter, suivre et corriger les vulnérabilités des dépendances de manière proactive.

MÉTHODES & MODALITÉS PÉDAGOGIQUES :

- Cette formation sera principalement constituée de théorie et d'ateliers techniques qui permettront d'être rapidement opérationnel.
- Support : un support de cours officiel Microsoft sera remis aux participants au format électronique.
- Evaluation : Les acquis sont évalués tout au long de la formation par le formateur (Prérequis évalués avant la formation, questions régulières, travaux pratiques, QCM ou autres méthodes).
- Formateur : le tout animé par un consultant-formateur expérimenté, nourri d'une expérience terrain, et accrédité Microsoft Certified Trainer.
- Satisfaction : à l'issue de la formation, chaque participant répond à un questionnaire d'évaluation qui est ensuite analysé en vue de maintenir et d'améliorer la qualité de nos formations.
- Suivi : une feuille d'émargement par demi-journée de présence est signée par chacun des participants.
- Cette formation peut être dispensée en format inter-entreprises ou intra-entreprise sur demande et en mode présentiel comme en distanciel.

PROGRAMME DE FORMATION :

Découvrir GitHub Advanced Security

- Définir GHAS et l'importance des fonctionnalités intégrales comme l'analyse secrète, l'analyse du code et Dependabot
- Utiliser GHAS pour optimiser l'impact de la sécurité
- Comprendre GHAS et son rôle dans l'écosystème de sécurité

Configurer les mises à jour de sécurité Dependabot sur votre dépôt GitHub

- Décrire les outils disponibles pour la gestion des dépendances vulnérables sur GitHub.
- Activer et configurer les alertes Dependabot.
- Identifier les autorisations et les rôles nécessaires pour visualiser et activer les alertes Dependabot.
- Activer et configurer les mises à jour de sécurité Dependabot.
- Identifier, examiner et résoudre des dépendances vulnérables.
- Utiliser l'API GraphQL pour récupérer des informations sur les vulnérabilités.
- Configurer des notifications pour les dépendances vulnérables.

Configurer et utiliser l'analyse des secrets dans votre dépôt GitHub

- Décrire l'analyse des secrets.
- Configurer l'analyse des secrets.
- Utiliser l'analyse des secrets.

Configurer l'analyse du code sur GitHub

- Décrire l'analyse de code.
- Lister les étapes pour activer l'analyse de code dans un référentiel.
- Lister les étapes pour activer l'analyse de code avec une analyse tierce.
- Comparer l'implémentation de l'analyse CodeQL dans un workflow GitHub Actions ou dans un outil d'intégration continue (CI) tiers.
- Configurer l'analyse de code sur un référentiel à l'aide d'événements déclencheurs.
- Comparer la fréquence des workflows d'analyse de code (planifiée ou déclenchée par des événements).

Identifier les vulnérabilités de sécurité dans votre base de code en utilisant CodeQL

- Créer une base de données en utilisant CodeQL pour extraire d'abord une seule représentation relationnelle de chaque fichier source dans le codebase.
- Exécuter CodeQL dans une base de données pour identifier les problèmes dans votre code source et détecter les failles de sécurité potentielles.
- Comprendre les résultats de l'analyse CodeQL en utilisant des requêtes créées par GitHub ou de vos propres requêtes personnalisées.

Analyser du code avec GitHub CodeQL

- Comprendre CodeQL et comment il analyse le code.
- Comprendre QL, un langage de programmation logique unique.
- Configurer l'analyse du code basée sur CodeQL dans un dépôt GitHub.
- Référencer une requête CodeQL personnalisée.
- Configurer la matrice de langages dans un workflow CodeQL.
- Utiliser l'interface CLI de CodeQL pour générer des résultats d'analyse du code et les charger sur GitHub.
- Implémenter des étapes de génération personnalisées.

Administrer GitHub pour GitHub Advanced Security

- Comprendre le fonctionnement de GitHub Advanced Security et comment l'utiliser dans le cycle de vie du développement logiciel.
- Identifier les fonctionnalités de GitHub Advanced Security qui sont disponibles pour les projets open source et les produits d'entreprise.
- Activer les différentes fonctionnalités de GitHub Advanced Security sur différents produits d'entreprise.
- Déterminer qui doit avoir accès aux fonctionnalités de GitHub Advanced Security au sein d'une organisation et accordez les autorisations adéquates.
- Définir des stratégies de sécurité au niveau de l'organisation et du référentiel.
- Répondre à une alerte de sécurité.
- Utiliser la vue d'ensemble de la sécurité pour surveiller les alertes de sécurité.
- Utiliser les points de terminaison de l'API GitHub Advanced Security pour gérer les fonctionnalités et les alertes de GitHub Advanced Security.

Gérer les données sensibles et les stratégies de sécurité dans GitHub

- Créer une documentation détaillant les recommandations de sécurité et des informations utiles pour les collaborateurs.
- Définir des autorisations et d'autres règles.
- Automatiser les processus qui empêchent les violations de sécurité.
- Répondre aux violations de sécurité.

Identifier les vulnérabilités de sécurité dans votre base de code en utilisant CodeQL

- Créer une base de données en utilisant CodeQL pour extraire d'abord une seule représentation relationnelle de chaque fichier source dans le codebase.
- Exécuter CodeQL dans une base de données pour identifier les problèmes dans votre code source et détecter les failles de sécurité potentielles.
- Comprendre les résultats de l'analyse CodeQL en utilisant des requêtes créées par GitHub ou de vos propres requêtes personnalisées.

Analyser du code avec GitHub CodeQL

- Comprendre CodeQL et comment il analyse le code.
- Comprendre QL, un langage de programmation logique unique.
- Configurer l'analyse du code basée sur CodeQL dans un dépôt GitHub.
- Référencer une requête CodeQL personnalisée.
- Configurer la matrice de langages dans un workflow CodeQL.
- Découvrir comment utiliser l'interface CLI de CodeQL pour générer des résultats d'analyse du code et les charger sur GitHub.
- Implémenter des étapes de génération personnalisées.

PRÉREQUIS :

Pour suivre cette formation, vous devez avoir suivi la formation « GH-900 : Github Fundamentals » ou avoir un niveau équivalent.

Un niveau d'anglais B1 est recommandé, retrouvez les niveaux sur ce lien : Classification des niveaux de langue.

DUREE : 1 jour (7 heures)
INTERLOCUTEURS : Développeurs, Administrateur, Ingénieurs DevOps.
NIVEAU : Débutant