GitHub sécurité avancée (GH-500T00)

Durée: 1 jour
Public cible: Professionnel TI

À qui s'adresse cette formation ?

Personnes souhaitant comprendre et mettre en œuvre des pratiques de sécurité avancées à l'aide de GitHub Advanced Security (GHAS). Elles apprendront à améliorer significativement les processus de développement logiciel et à créer un écosystème de développement plus résilient et sécurisé en utilisant des solutions axées sur les personnes développant des applications, afin de garantir la sécurité du code, de la chaîne d'approvisionnement et des secrets avant la mise en production. Elles découvriront comment GHAS offre aux équipes de sécurité une visibilité sur la posture de sécurité organisationnelle et de la chaîne d'approvisionnement, ainsi qu'un accès inégalé à des renseignements issus de millions de personnes développant des applications et de personnes cherchant en sécurité dans le monde entier

Objectifs de la formation

- Comprendre les fonctionnalités et avantages de GitHub Advanced Security
- Activer et configurer l'analyse de code pour identifier les vulnérabilités
- Utiliser l'analyse de secrets pour détecter et prévenir les fuites de secrets
- Mettre en œuvre l'analyse de dépendances (Dependabot) pour les dépendances vulnérables
- Interpréter et agir sur les alertes de sécurité générées par GHAS • Intégrer les flux de sécurité dans les pipelines CI/CD
- Exploiter les options de configuration avancées pour les règles et politiques de sécurité
- Soutenir la conformité aux exigences organisationnelles et réglementaires en matière de sécurité

Description sommaire

GitHub Advanced Security (GHAS) joue un rôle crucial dans le renforcement de la posture de sécurité des projets de développement logiciel 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 vie du développement. En intégrant la sécurité directement dans le processus de développement grâce

à GHAS, votre équipe peut créer des logiciels plus sûrs et fiables. Ce cours explore comment utiliser GHAS afin de maximiser l'impact sur la sécurité et comprendre le rôle de GHAS dans l'écosystème de la sécurité.

Contenu du plan de cours

Introduction à GitHub Advanced Security

- Définir GHAS et l'importance de ses fonctionnalités principales
- Comment utiliser GHAS pour un impact maximal
- Comprendre le rôle de GHAS dans l'écosystème de la sécurité
- Évaluation du module

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

- Configurer et utiliser l'analyse de secrets dans votre dépôt GitHub
- Configurer l'analyse de code sur GitHub
- Identifier les vulnérabilités de sécurité dans votre base de code à l'aide de CodeQL
- Analyse de code avec GitHub CodeQL
- Administration GitHub pour GitHub Advanced Security
- Gérer les données sensibles et les politiques de sécurité dans GitHub

Approche et méthode pédagogique

Approche pratique et structurée combinant théorie ciblée et ateliers guidés. Les participants renforcent progressivement la sécurité des environnements GitHub à travers des exercices concrets inspirés de scénarios professionnels, favorisant une mise en application immédiate des apprentissages. Ils apprennent à identifier les vulnérabilités, protéger le code et mettre en œuvre des pratiques de sécurité avancées à l’aide des fonctionnalités GitHub Advanced Security. Animée par un formateur certifié Microsoft, la formation privilégie l’interactivité et le développement de compétences techniques directement transférables pour sécuriser efficacement les chaînes de développement en contexte professionnel.

Prérequis

Avant de suivre ce cours, les personnes participantes devraient avoir :

- Une connaissance de base de Git et GitHub (commandes essentielles, gestion des branches, fusion, etc.)
- Une expérience des flux de travail de développement logiciel (dépôts, pull requests, revues de code)
- Une compréhension des concepts fondamentaux de sécurité
- Un accès à un compte GitHub (idéalement avec des droits d'administrateur ou de sécurité sur un dépôt de test)

Recommandations

- Bases en GitHub et gestion de versions (Git)
- Connaissance des concepts de développement logiciel et CI/CD
- Compréhension des notions de sécurité applicative (vulnérabilités, dépendances)
- Familiarité avec les principes DevSecOps
- Notions de gestion des identités et des accès