GitHub sécurité avancée (GH-500T00)

Durée: 1 jour
Public cible: Professionnel TI

À qui s'adresse cette formation ?

Cette formation s’adresse aux personnes souhaitant comprendre et mettre en œuvre des pratiques avancées de sécurité à l’aide de GitHub Advanced Security (GHAS).

Les participants apprendront à renforcer considérablement leurs processus de développement logiciel et à bâtir un écosystème de développement plus résilient et plus sécuritaire grâce à des solutions axées sur les développeurs permettant de protéger le code, la chaîne d’approvisionnement logicielle et les secrets avant la mise en production.

Ils découvriront également comment GHAS procure aux équipes de sécurité une visibilité accrue sur la posture de sécurité organisationnelle et sur la chaîne d’approvisionnement logicielle, tout en leur donnant accès à une veille de sécurité unique alimentée par des millions de développeurs et de chercheurs en sécurité à travers le monde.

Objectifs de la formation

À la fin de ce cours, les participants seront en mesure de:

- Définir GitHub Advanced Security (GHAS) et comprendre l’importance de fonctionnalités essentielles telles que l’analyse des secrets (Secret Scanning), l’analyse du code (Code Scanning) et Dependabot.
- Utiliser efficacement GHAS afin de maximiser l’impact des mécanismes de sécurité intégrés.
- Comprendre le rôle de GHAS dans l’écosystème de sécurité et son intégration dans les processus de sécurité organisationnels.
- Activer et configurer les alertes Dependabot ainsi que les mises à jour de sécurité automatisées.
- Mettre en œuvre l’analyse des secrets afin de prévenir les fuites d’informations sensibles.
- Configurer et utiliser l’analyse du code à l’aide de CodeQL et d’autres outils compatibles.

Description sommaire

GitHub Advanced Security (GHAS) joue un rôle essentiel dans le renforcement de la posture de sécurité des projets de développement logiciel hébergés sur GitHub. Il offre un ensemble complet d’outils et de fonctionnalités conçus pour détecter et corriger les vulnérabilités de sécurité tout au long du cycle de développement.

En intégrant directement la sécurité au processus de développement grâce à GHAS, les équipes peuvent concevoir des logiciels plus sécuritaires et plus fiables. Ce cours explore les différentes façons d’utiliser GHAS afin de maximiser son impact sur la sécurité et de comprendre son rôle dans l’écosystème de sécurité moderne.

Contenu du plan de cours

Parcours d'apprentissage : GitHub Advanced Security

- Module 1 : Introduction à GitHub Advanced Security
- Module 2 : Configurer les mises à jour de sécurité Dependabot dans votre dépôt GitHub
- Module 3 : Configurer et utiliser l’analyse des secrets (Secret Scanning) dans votre dépôt GitHub
- Module 4 : Configurer l’analyse du code (Code Scanning) sur GitHub
- Module 5 : Identifier les vulnérabilités de sécurité dans votre base de code à l’aide de CodeQL
- Module 6 : Effectuer l’analyse du code avec GitHub CodeQL
- Module 7 : Administration GitHub pour GitHub Advanced Security

  Module 8 : Gérer les données sensibles et les politiques de sécurité dans GitHub
- Module 8 : Gérer les données sensibles et les politiques de sécurité dans GitHub

Approche et méthode pédagogique

Cette formation adopte une approche pratique et structurée combinant des exposés théoriques ciblés et des ateliers guidés.

Les participants découvrent progressivement les fondements de GitHub Advanced Security à travers des exercices concrets inspirés de situations réelles de développement logiciel, favorisant une mise en application immédiate des apprentissages.

Ils apprennent à identifier les vulnérabilités, à sécuriser le code, à protéger les renseignements sensibles et à renforcer la sécurité de la chaîne d'approvisionnement logicielle grâce aux mécanismes de sécurité intégrés à GitHub.

Animée par un formateur certifié Microsoft (MCT), la formation met l'accent sur l'interactivité et le développement de compétences directement transférables afin d'aider les équipes à concevoir et à maintenir des logiciels sécuritaires tout au long du cycle de développement.

Prérequis

Les participants doivent posséder les connaissances et l'expérience suivantes avant de suivre ce cours:

- Les participants devraient également posséder :
- Une expérience d'utilisation et d'administration de dépôts GitHub.
- Une expérience de travail avec les services Microsoft Azure.
- Des compétences techniques en analyse de code, gestion des dépendances et analyse des secrets.
- Une familiarité avec des outils tels que CodeQL et Dependabot.

Recommandations

- Connaissances de base de GitHub et du contrôle de version Git.
- Connaissance des concepts de développement logiciel et de l'intégration continue/déploiement continu (CI/CD).
- Compréhension des concepts de sécurité applicative (vulnérabilités, dépendances).
- Familiarité avec les principes DevSecOps.
- Notions de gestion des identités et des accès

Notes légales