

Formation : GitHub Advanced Security (Microsoft GH-500)

Cours officiel GH-500, préparation à l'examen

Formation pratique - 1j - 7h00 - Réf. GHS

Prix : 850 € H.T.

NEW

Avec cette formation, vous découvrirez comment GitHub Advanced Security (GHAS) renforce la sécurité de vos projets en identifiant et corrigeant les vulnérabilités tout au long du cycle de développement. Vous apprendrez à l'exploiter efficacement et à comprendre son rôle dans l'écosystème de la sécurité.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- ✓ Comprendre les fonctionnalités et avantages de GitHub Advanced Security (GHAS)
- ✓ Activer et configurer l'analyse de code pour détecter les vulnérabilités
- ✓ Utiliser l'analyse des secrets pour prévenir les fuites d'informations sensibles
- ✓ Mettre en œuvre la gestion des dépendances avec Dependabot pour sécuriser la supply chain
- ✓ Interpréter et agir sur les alertes de sécurité générées par GHAS

Public concerné

Toute personne souhaitant utiliser GitHub Advanced Security (GHAS) pour renforcer la sécurité du code, de la supply chain et des secrets.

Prérequis

Connaissances de base en développement et en sécurité, et bonne compréhension de l'anglais à l'écrit

Méthodes et moyens pédagogiques

Méthodes pédagogiques

Animation de la formation en français. Support de cours officiel au format numérique et en anglais.

PARTICIPANTS

Toute personne souhaitant utiliser GitHub Advanced Security (GHAS) pour renforcer la sécurité du code, de la supply chain et des secrets.

PRÉREQUIS

Connaissances de base en développement et en sécurité, et bonne compréhension de l'anglais à l'écrit

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.
Évaluation par le participant, à l'issue de la formation, des compétences acquises durant la formation.
Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation...

À l'issue de chaque formation, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur. Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques...

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Programme de la formation

1 Sécurité avancée GitHub (partie 1/2)

- Présentation de GitHub Advanced Security.
- Configurer les mises à jour de sécurité Dependabot sur votre dépôt GitHub.
- Configurer et utiliser l'analyse des secrets dans votre dépôt GitHub.
- Configurer l'analyse du code sur GitHub.

2 Sécurité avancée GitHub (partie 2/2)

- Identifier les vulnérabilités de sécurité dans votre code avec CodeQL.
- Identifier les vulnérabilités de sécurité dans votre code avec CodeQL.
- Administration de GitHub pour la sécurité avancée.
- Gérer les données sensibles et les stratégies de sécurité dans GitHub.

Options

Certification : 200 € H.T.

Ce programme est une création originale, conçu par les équipes pédagogiques d'ORSYS Formation. Toute reproduction, représentation, adaptation ou exploitation, totale ou partielle, sans autorisation préalable écrite d'ORSYS, est strictement interdite. ORSYS se réserve le droit d'engager toute action nécessaire à la protection de ses droits de propriété intellectuelle.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.