G-echo
6 Avenue de la Gare - C24
31380 Garidech
+33.6.03.62.14.40
contact@g-echo.fr

Programme de formation

Fortify Security Solutions (Microfocus)

But de la formation

La formation "Fortify Security Solutions" consiste en une introduction de deux jours à la sécurité des applications lors du développement et du test des vulnérabilités de sécurité de votre logiciel avec la suite de produits Fortify.
En tant qu'étudiant, vous en apprendrez davantage sur les menaces pesant sur les applications, ainsi que sur l'architecture et le fonctionnement de la solution Fortify.
Grâce à des activités pratiques, vous apprendrez à mettre en œuvre Fortify SCA (analyseur de code statique), Fortify SSC (Centre de sécurité logicielle) et WebInspect.

Après avoir réussi ce cours, vous devriez être capable de:

- Identifier la sécurité de votre application (selon le Top 10 OWASP) et référentiels de gouvernance avec OpenSAMM,
- Exécuter des analyses à l'aide de Fortify Static Code Analyzer (SCA) et WebInspect (WI),
- Reporter, gérer les projets et résoudre les vulnérabilités de vos applications à l'aide de SSC.

Pré-requis

- Compétences de base en programmation (i.e. lire du code Java, C / C ++ ou .NET),
- Compréhension de base des technologies Web: requêtes et réponses HTTP, balises HTML, JavaScript, et serveur contenu dynamique côté utilisateur (JSP, ASP ou similaire),
- La connaissance du codage d'applications web, du développement en général et des bonnes pratiques de sécurité.

Type de public

- Développeurs de logiciels,
- Gestionnaires de produits,
- Gestionnaires de développement,
- Gestionnaires Q / A,
- Analystes Q / A,
- Analystes de la sécurité des applications.

Moyens pédagogiques

- Outils informatiques, supports papier et cloud pour les tests.

Sanction de la formation

- Attestation de suivi de formation.

G-echo
6 Avenue de la Gare - C24
31380 Garidech
+33.6.03.62.14.40
contact@g-echo.fr

Méthodes pédagogiques

- Supports de cours et présentation magistrale,
- Exercices pratiques via des plateformes virtuelles ou vos équipements.

Durée

14 heures (2 jours).

Programme

Module 1: Vue générale de OpenSAMM

- Appliquer le modèle SAMM (Software Assurance Maturity Model) à l'infrastructure de sécurité d'une organisation,
- Utilisez les directives SAMM pour évaluer les objectifs de sécurité de votre logiciel,
- Aligner le paramétrage SAMM de Fortify avec les pratiques de sécurité de votre organisation.

Module 2: Scan des vulnérabilités

- Énumérer le Top 10 des risques de sécurité des applications de l'OWASP,
- Effectuer un modèle de menace de base et une évaluation des risques,
- Intégrer les activités de sécurité dans un SDLC de base.

Module 3: Utilisation des produits Fortify

- Identifier le produit Fortify selon la ligne de repère de l'initiative OpenSAMM,
- Décrire les rapports et l'analyse des incidents ou vulnérabilités détectés,
- Décrire l'architecture et la structure des produits Fortify et leur intégration dans l'entreprise,
- Exigences de mise en œuvre de la suite Fortify.

Module 4: Fortifier SCA (Analyseur de code statique - Static Code Analyser)

- Navigation dans "Audit Workbench",
- Audit et suppression des faux positif,
- Identification et classification des informations sur les vulnérabilités découvertes.

Module 5: WebInspect (WI) / Agent WI

- Définition sur les capacités opérationnelles de WebInspect,
- Licence et activation de WebInspect,
- Naviguation dans les écrans opérationnels de WebInspect.

Module 6: Fority SSC (Centre de sécurité logicielle)

- Inspection et ajustement des résultats d'analyse,
- Création de projets dans SSC,
- Connexion à SSC à partir de AWB,
- Transfert et téléchargement des analyses dans SSC,
- Génération des rapports pour montrer les problèmes en suspens et les progrès accomplis par rapport aux objectifs de sécurité,
- Intégration des activités de sécurité dans votre SDLC.