Security Champion : Mettre en Œuvre un Programme de Sécurité Applicative en Environnement DevSecOps

Lien : https://innov-systems.com/formation/security-champion-mettre-en-uvre-un-programme-de-securite-applicative-en-environnement-devsecops

DURÉE
8 jours (56h)

RÉFÉRENCE
SEC267

CATÉGORIE
Cycles Métiers Sécurité Informatique

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre les principes fondamentaux de la sécurité applicative dans un contexte agile et DevOps
- Identifier et prévenir les vulnérabilités courantes du code et des infrastructures cloud
- Intégrer la sécurité dès les phases de conception et de développement logiciel
- Mettre en place un rôle de « Security Champion » au sein des équipes de développement
- Utiliser les outils et bonnes pratiques DevSecOps pour automatiser les contrôles de sécurité
- Auditer et renforcer la sécurité des applications web et API

POUR QUI ?

- Développeurs et ingénieurs logiciels
- Ingénieurs DevOps et responsables techniques
- Chefs de projets agiles et responsables produits
- Architectes logiciels
- Responsables qualité ou sécurité des systèmes d’information

Programme détaillé

1 / FONDAMENTAUX DE LA SÉCURITÉ LOGICIELLE

- Principes de la sécurité applicative dans le cycle de vie du logiciel (SDLC)
- Rôles et responsabilités du Security Champion
- Introduction au modèle DevSecOps et à la culture « shift-left »

2 / CONTEXTE ET MENACES ACTUELLES

- Panorama des cybermenaces et études de cas réels
- Vulnérabilités critiques et typologies d’attaques
- Introduction à l’OWASP Top 10 et à son évolution

3 / INTRODUCTION AUX NORMES ET RÉFÉRENTIELS

- OWASP, NIST, ISO 27034, PCI DSS
- Principes de conformité et de gouvernance en sécurité applicative

4 / ANALYSE DES RISQUES ET GESTION DES VULNÉRABILITÉS

- Méthodologie d’évaluation des risques (OWASP SAMM)
- Outils et indicateurs de suivi de la sécurité
- Classification CVE et scoring CVSS

5 / CONCEPTION D’APPLICATIONS SÉCURISÉES

- Intégrer la sécurité dès la phase de conception
- Principes de sécurité par défaut et par conception (secure by design)
- Gestion des dépendances et des bibliothèques open source

6 / POLITIQUES ET CONTRÔLES DE SÉCURITÉ

- Bonnes pratiques d’accès et d’autorisation
- Confidentialité, intégrité et disponibilité des données
- Intégration de la sécurité dans les user stories et les pipelines DevOps

7 / PROTECTION DES DONNÉES SENSIBLES

- Gestion et chiffrement des données au repos et en transit
- Gestion des clés et certificats
- Sécurisation des secrets (HashiCorp Vault, AWS Secrets Manager, etc.)

8 / CRYPTOGRAPHIE APPLIQUÉE AUX APPLICATIONS

- Chiffrement symétrique et asymétrique
- Signatures, hachages et certificats numériques
- Bonnes pratiques et erreurs courantes en implémentation

9 / TRAÇABILITÉ ET SURVEILLANCE DES APPLICATIONS

- Mise en place des journaux d’audit et logs de sécurité
- Corrélation et analyse des événements
- Détection d’anomalies et de comportements suspects

10 / AUTHENTIFICATION ET GESTION DES IDENTITÉS

- Standards modernes : OAuth2, OpenID Connect, SAML
- MFA, gestion des sessions et expiration
- Sécurisation du stockage des identifiants

11 / AUTORISATION ET GESTION DES RÔLES

- RBAC, ABAC et politiques dynamiques
- Gestion granulaire des droits d’accès

- Revue des accès et traçabilité

12 / BONNES PRATIQUES DE GESTION DES ERREURS ET ALERTES

- Gestion sécurisée des exceptions et messages d’erreurs
- Prévention des fuites d’informations sensibles
- Conception d’un plan de réponse aux incidents applicatifs

13 / ATTAQUES PAR INJECTION

- Injections SQL, LDAP, et système
- Prévention via ORM, requêtes préparées et validation d’entrées
- Cas pratiques et exercices sur code vulnérable

14 / FAILLES DE SÉRIALISATION ET REQUÊTES MALICIEUSES

- Désérialisation non sécurisée et vecteurs d’exploitation
- Protection contre les attaques CSRF
- Bonnes pratiques d’utilisation des frameworks sécurisés

15 / VULNÉRABILITÉS LIEES AUX FICHIERS ET AUX INPUTS UTILISATEUR

- Directory traversal et upload de fichiers malicieux
- Validation côté serveur vs côté client
- Filtrage et normalisation des entrées

16 / FAILLES XSS ET CONTENT SECURITY POLICY

- XSS stocké, réfléchi et DOM-based
- Mitigation avec encodage, CSP et frameworks modernes

17 / VULNÉRABILITÉS XML ET API

- XXE, ReDoS, et attaques spécifiques aux API REST/GraphQL

- Bonnes pratiques d’authentification API et limitation de débit

18 / TESTS DE SÉCURITÉ ET OUTILS D’AUDIT

- OWASP ZAP, Burp Suite, Snyk, SonarQube
- Automatisation des tests de sécurité dans la CI/CD

19 / SÉCURITÉ DES ENVIRONNEMENTS CLOUD

- Risques spécifiques au cloud (SaaS, PaaS, IaaS)
- Bonnes pratiques AWS, Azure et GCP
- Gestion des identités et des permissions cloud

20 / INTÉGRATION DEVSECOPS

- Pipelines sécurisés (CI/CD)
- Automatisation des scans de vulnérabilités
- Politique de “Security as Code”

21 / SURVEILLANCE ET RÉPONSE AUX INCIDENTS

- Intégration du monitoring de sécurité
- Alertes et remédiation automatisées
- Étude de cas : incident response dans un environnement DevSecOps

22 / ÉTUDE DE CAS COMPLÈTE

- Audit d’une application existante
- Analyse des vulnérabilités détectées et plan d’action

23 / ATELIER PRATIQUE : CRÉATION D’UN PIPELINE SECURISÉ

- Déploiement d’un projet DevSecOps complet
- Mise en œuvre des contrôles automatisés

24 / ÉVALUATION ET VALIDATION DES ACQUIS

- Quiz, exercice pratique et restitution
- Validation des compétences « Security Champion »
- Plan de suivi post-formation et certification interne

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

06 au 15 Juil. 2026	Présentiel - Casablanca
31 Août au 09 Sep. 2026	Distanciel
26 Oct. au 04 Nov. 2026	Distanciel

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com