SECURE DEV OPS

Développez, programmez, déployez et administrez de manière cyber-sécurisée

Objectif

Former aux bonnes pratiques du développement sécurisé dans un contexte agile/DevOps.

Destinataires

Développeurs, Développeurs intégrateurs (DevOps), Développeurs intégrateurs et sécurité (DevSecOps), Éditeurs logiciels et Chefs de projets

Prérequis

La connaissance d'au moins un langage de programmation Web (Java, Node.js, PHP, Python, etc.) est nécessaire.

Des notions dans le fonctionnement des systèmes d'exploitation et en cryptographie sont un plus.

Méthode pédagogique

Une pédagogie immersive qui allie apports théoriques, retours d'expériences et cas pratiques pour un ancrage durable des compétences.

Les cas pratiques sont réalisés sur un système vulnérable fourni par SECURESPHERE.

Moyens techniques

Salle de formation équipée de postes de travail informatiques disposant de tous les logiciels nécessaires au déroulement de la formation.

Compétences acquises

- Sécuriser la conception des applications web afin d'éviter les intrusions et de limiter les failles dans les systèmes d'information en intégrant la sécurité dans les spécifications fonctionnelles et en implémentant les fonctions de sécurité dans les spécifications techniques.
- Développer des logiciels et des applications capables d'écarter les intrusions dans les systèmes d'information en caractérisant les vulnérabilités.
- Écarter les intrusions dans les systèmes d'information en développant des logiciels et des applications qui incluent les contre-mesures existantes dans les mécanismes intégrés aux noyaux spécifiques du développement web.
- Tester le logiciel ou l'application pour éviter les intrusions et limiter les failles dans les systèmes d'information en mettant en œuvre des tests de robustesse sur les éléments développés.
- Sécuriser le déploiement des applications pour éviter les intrusions et limiter les failles dans les systèmes d'information en vérifiant leur intégration dans l'environnement existant.
- Augmenter la sécurité des systèmes de production et les administrer de manière sécurisée.

Formateurs

Consultants-Formateurs spécialistes de la sécurité informatique.

DURÉE
4 jours - 28 heures

TARIF INTER
3 000 € HT

TARIF INTRA
Nous contacter

LIEU
Campus Cyber
Tour Eria,
5 rue Bellini
92800 Puteaux

ou dans vos locaux

ACCESSIBILITÉ
Cette formation est accessible aux personnes en situation de handicap.

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE

SECURESPHERE est détenteur de la certification Qualiopi au titre de la catégorie d'actions de formation.

PROGRAMME

INTRODUCTION

Concepts génériques liés aux vulnérabilités web

- Exemples réels et conséquences
- Identification des vulnérabilités (CVE)
- Criticité des vulnérabilités (CVSS) et politique de communication par les éditeurs logiciels

Gestion de projets

- Principe de l'analyse de risques (OWASP A04)
- Intégration de la sécurité dans les projets (OWASP A04)

Spécificités de l'hébergement dans le cloud et des offres software as a service (saas)

CONCEPTION

Spécifications fonctionnelles

- Principe de sécurité par défaut (OWASP A04)
- Transparence vs sécurité par l'obscurité
- Protection des données sensibles et concepts cryptographiques (OWASP A02)
- Traçabilité (OWASP A09)
- Fonctionnalités dangereuses
- Gestion des mises à jour (OWASP A06)

Spécifications techniques et implémentation des fonctions de sécurité

- Authentification (OWASP A07)
- Gestion des mots de passe
- Gestion des sessions
- Autorisation / Gestion des droits (OWASP A01)
- Cryptographie appliquée (OWASP A02)
- Gestion des erreurs

PROGRAMME (IN)SÉCURISÉE

Vulnérabilités (dont le Top 10 de l'OWASP) liées au développement et contre-mesures

- Injections (OWASP A03, OWASP A10) :

- SQL, LDAP
- Commandes système
-Arguments de commandes

- Code interprété
- Cross-site scripting – XSS
- Directory transversal
- Injections XML - XXE (OWASP A05)
- ReDoS
- Désérialisation (OWASP A08)
- Cross-site request forgery (CSRF)

OUTILS ET RECETTE SÉCURITÉ

- Tests manuels de sécurité
- Tests unitaires, audit statique de code
- Configuration de l'environnement (OWASP A05)
- Tests automatisés de sécurité
- Fuzzing et tests d'intrusion applicatifs

Vérification de la sécurité

- Filtrage réseau et NIDS
- Relais et Web Application Firewall (WAF)

DÉPLOIEMENT SÉCURISÉ

AUTOMATISATION DU DÉPLOIEMENT

- Packaging et mise à disposition d'applications
- Infrastructure As Code (exemple Ansible)
- Conteneurisation d'application sous Linux
- Gestion des secrets et bonnes pratiques liées à Docker
- Orchestration de conteneurs
- Bonnes pratiques liées à Kubernetes
- Protection de chaîne d'automatisation (CI)

PROTECTIONS RÉSEAU

- Filtrage réseau et NIDS
- Relais et Web Application Firewall (WAF)

PROTECTIONS SYSTÈME

- Durcissement des configurations
- Protections intégrées aux systèmes d'exploitation
- Administration sécurisée

ÉVALUATION
L'évaluation est réalisée tout au long de la formation, sous la forme d'exercices ou de mises en situation.

ATTESTATION
Une AACE, Attestation d'Acquisition des Compétences de l'EPITA, est délivrée aux stagiaires ayant validé l'ensemble des compétences visées par le stage.

Référent handicap : marie.moin@epita.fr

Siège Social : 14-16 rue Voltaire 94270 le Kremlin Bicêtre - Campus EPITA
RCS Créteil 809 748 635 - Déclaration d'activité N° 11 94 08975 94