SECURE DEV LINUX IOT

Développez des programmes sécurisés sous Linux pour les objets connectés

Objectif

Former les développeurs à l'intégration des bonnes pratiques cyber pour une programmation sécurisée en environnement Linux et IOT.

Destinataires

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

Prérequis

La connaissance du langage de programmation système C ou C++ 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 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 contremesures existantes dans les mécanismes intégrés aux noyaux spécifiques du développement
- Tester le logiciel ou l'application pour éviter les intrusions et limiter les failles dans les Systèmes d'Information en mettant en oeuvre 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
- Utiliser les mécanismes de sécurité offerts par Linux pour éviter les intrusions et limiter les failles dans les Systèmes d'Information en étant capable de gérer les contrôles d'accès, les privilèges et les restrictions sur les fichiers

Formateurs

Consultants-Formateurs spécialistes de la sécurité informatique.

DURÉE
3 jours
21 heures

TARIF INTER
2 250 € HT
par stagiaire

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.

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
- Intégration de la sécurité dans les projets

Spécificités des systèmes embarqués et IOT

CONCEPTION

Spécifications fonctionnelles
- Principe de sécurité par défaut
- Transparence vs sécurité par l'obscurité
- Protection des données sensibles
- Modèles DAC et MAC
- Concepts cryptographiques
- Traçabilité
- Fonctionnalités dangereuses
- Gestion des mises à jour

Spécifications techniques et implémentation des fonctions de sécurité
- Authentification
- Gestion des mots de passe
- Gestion des sessions
- Autorisation / Gestion des droits
- Cryptographie appliquée
- Gestion des erreurs

PROGRAMME (IN)SÉCURISÉE

Problèmes spécifiques aux langages C et C++
- Buffer overflow
- String format bug
- Interger overflow
- Gestion des pointeurs et use-after-free

Problèmes liés aux systèmes
- Race conditions
- Shatter attacks

Outils et recette sécurité
- Protections offertes par les systèmes d'exploitation
- Options de compilation et configuration des interpréteurs
- Tests manuels de sécurité
- Tests unitaires, audit statique de code
- Tests automatisés de sécurité
- Fuzzing et tests d'intrusion applicatifs

MÉCANISMES DE SÉCURITÉ OFFERTS PAR LINUX

Contrôle d'accès
- ACL POSIX
- Pare-feu iptables et nftables

Gestion des privilèges élevés
- Niveaux de droits
- Programmes privilégiés : Bits SetUID/SetGID Identifiants utilisateurs d'un processus
- Capabilities

Fonctionnalités avancées sur systèmes Linux
- Restrictions sur les Fichiers (Chroot)
- Espace de nommage (UTS, réseau, IPC, points de montage, processus, utilisateurs et cgroup)
- Cgroups et isolation de processus Seccomp (modes, filtres BPF et eBPF)
- Conteneurs : Docker - LXC - sVirt

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.

01/2026