FORMATION Sécurité du Développement Niveau 1

Ref. **CSD01-10**
Durée : 5.0 jour(s) / 35.0 heures

La forte digitalisation de notre société voit une profonde évolution du WEB et de l'Industrie. Tout est connecté et controlé via une application web, mobile ou non. Le développement web, applicatif est omniprésent et nécessite d'avoir une matrise des techniques et méthodologies de développement mais également une maitrise des moyens de sécurisation de cet ensemble.

Cette Formation permet de valider un socle de compétences et savoir pour pouvoir aborder efficacement le développement sécurisé.
Elle valide un ensemble de savoirs requis dans les fiches métiers de l'ANSSI suivantes : Spécialiste en développement sécurisé, Auditeur de sécurité technique, Développeur de solutions de sécurité, Consultant en cybersécurité, Formateur en cybersécurité, Responsble de projet de sécurité.

Pré-requis :

Connaissances de base en systèmes, réseaux et d'Internet.
Maitrisé les fondamentaux de la programmation.
Connaissances d'un langage de programmation.

Personnes concernées :

Administrateurs réseaux, systèmes, Webmaster.
Auditeur sécurité
Chef de projet développement sécurité

ECSF METIERS ASSOCIES :
CISO, Cybersecurity Auditor, Cybersecurity Architect, Cybersecurity implementor, Penetration tester, Cybersecurity risk manager

Objectifs :

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

- Lister les vulnérabilités liées au web
- Sélectionner la méthodologie adaptée au développement à réaliser
- Appliquer les bonnes pratiques et méthodologies de développement sécurisé
- Tester la sécurité d'applications Web
- Modéliser les risques associés au développement
- Choisir les mesures à adopter
- Développer de façon sécurisée et adaptée au contexte

Programme :

JOUR 1

Introduction
Présentation des normes et efforts de standardisation
Importance de la sécurité du développement
Rgpd et sécurité du développement
Security by design
Security by default
Les acteurs

Quizz sur bonnes pratiques et fondamentaux du processus de développement sécurisé

Méthodologies

Principes SecDevOps
Architectures associées
DREAD et STRIDE
SSDLC
BSSIM
OWASP
Analyse de risques

Tds : réalisation d'une analyse de risques
Quizz méthodologies

JOUR 2

Compréhension des vulnérabilités et exploitations associées

Typologie des menaces le top 10 OWASP
Failles applicatives
Attaques côté client
gestion de session et authentification
Failles de configuration
Attaques de type DDOS
Attaque Buffer-Overflow, XXE

Tds : étude top 10 owasp

JOUR 3

Sécuriser son architecture

Firewalls n-tier, outils Filtres des requêtes HTTP Rappel algorithmique Autorités de certification
Chiffrement de données
Protocoles

TP : Sécurisation d'un serveur, certificat, waf, authentification.

Sécuriser son code

Protections basiques
Usurpation d'identité
Se protéger des attaques client
Se protéger contre CSRF
Sécurité d'accès au SGBD
Protections contre les attaques de force brute, Liste de contrôle d'accès
Cheat cheat

TPs : Protection d'un code vulnérable, mise ne œuvre des bonnes pratiques de sécurisation

JOUR 4

Audits et tests de sécurité

Les types d'audits
Tester la robustesse
Apprendre à connaitre son architecture
Organiser une veille technologique
Tests statique vs dynamique

TPs exercice audit, étude rapports d'audit.

Sécurité du code et des applications dans le cloud
Les architectures
Les bonnes pratiques de sécurité à adopter
les outils de protection en SaaS

Tds : Etude de cas d'architecture SecDevOps, Quizz sur bonnes pratiques

JOUR 5

Examen blanc : préparation examen final. Quizz sur bonnes pratiques, mise en situation sur du code vulnérable à sécuriser, mise en situation sur recherche de vulnérabilités, Etude de cas sur analyse des rsiques

Examen final : QCM sur les bonnes pratiques de sécurisation du code, sur les principes du SecDevOps, sur les méthodologies à appliquer ainsi que sur le développement et le cloud.
Mise en situation sur une analyse des risques,
Mise en situation sur de la recherche de vulnérabilité et sécurisation associée.

Démarche pédagogique :

Formation orientée sur la pratique
70% de pratique et 30% de théorie
Cybersecurity Educator ECSF

Evaluation et validation :

CERTIFICATION DE PERSONNE
Partie théorique et pratique
Le temps destiné au passage de la certification est de 3H.
L'examen est composé de 3 parties : QCM, mise en situation sur points spécifiques, mise en situation sur cas concrets.
Il peut se dérouler à distance.

Bureau Veritas Certification assure l'examen final de ce programme de formation.

L'examen valide des domaines de compétences en relation avec les profils métiers identifiés par l'Europpean union agency for cybersecurity via l'European Cybersecurity Skills Framework