



# Cyber-sécurité au laboratoire : mettre en place une protection proactive

**NOUVEAU**

MANAGEMENT - COMMUNICATION

**ADAPTABLE EN INTRA**

## Objectifs

- Comprendre et maîtriser l'OWASP Project & CVE
- Mettre en place une méthodologie de contrôle et développer un SMSI
- Acquérir les savoirs nécessaires pour le déploiement d'un outil de détection d'intrusions
- Découvrir et appliquer une méthodologie de pentest en toute autonomie
- Etablir un protocole d'urgence en cas d'attaque

## Prérequis

- Niveau 1 - Connaissances basiques en réseaux et systèmes
- Niveau 2 - Bonne connaissance de la sécurité informatique.

## Public

- Niveau 1 - Techniciens & Administrateurs systèmes et réseaux...
- Niveau 2 - Responsable et/ou Architecte sécurité...

## Programme

### Comprendre l'OWASP Projet & le CVE

- Appréhender le monde de la sécurité informatique
- Les notions officielles de « hacker » et de « hacking »
- La culture et l'état d'esprit des pirates informatiques
- Quels risques et quelles menaces pour le SI ?
- Développement d'un SMSI

### Déployer une méthodologie et des outils d'audits automatisés

- Les enjeux du pentest et les différentes approches
- Comment automatiser sa gestion des vulnérabilités
- HTTPCS Security, Scanner de Vulnérabilité Web & Applicatif

### Paramétrer et prendre en main un Scanner de Vulnérabilité Web

- Scan Réseau
- Analyse Système et Analyse Web
- Test d'intrusion sur une adresse IP
- Test d'intrusion par un collaborateur interne

### Créer et mettre en place un protocole d'urgence en cas d'attaque

- Comment savoir qu'une intrusion a réussi ?
- Méthode et réponse à un incident
- Nettoyage et remise en production des serveurs qui ont été piratés
- Cadre juridique et réponse aux hackers

### Application et travaux dirigés

- Planification et lancement d'un audit Grey Box
- Lecture et analyse d'un rapport de pentest
- Correction et application des contre-mesures spécifiques à chaque faille découverte (OWASP & CVE)
- Projet de développement d'un SMSI
- Création d'un protocole d'urgence en cas d'attaque

Réf.: INF.PP

### Durée

2 jours 14 h

### Coût (net)

520 €

### Intervenants

### Session

### Lieu

BIOFORMATION  
75015 PARIS

### Pédagogie

TP 50% - Théorie 50%

### Notes

- Remise d'un support de cours.
- Outils pédagogiques : Vidéoprojection.
- Validation des acquis par exercices de mises en application tout au long de la formation.
- Durée journalière habituelle de formation : 7 h.

Heure de début 1<sup>er</sup> jour : 9h30

Heure de fin dernier jour : 16h30