Hacking

CONDUITE ET COORDINATION D'UN PROJET DE TEST D'INTRUSION

Objectifs

- Comprendre et évaluer la menace ambiante
- Maîtriser l'évaluation automatisée de la sécurité des infrastructures
- Les bonnes méthodes pour apprendre à anticiper un test d'intrusion
- Réagir lorsqu'un TI se passe mal

Publics

- DSI
- Auditeur interne
- Risk Manager
- Analyste sécurité des SI

Formation(s) complémentaire(s)

- Techniques d'intrusion informatique et hacking

DURÉE : 1 JOUR
PRIX : 990€ HT
DATES : 4 JUIN / 24 SEPTEMBRE / 20 NOVEMBRE / 10 DÉCEMBRE

Programme

Le rôle des tests d'intrusion dans la gestion des risques IT

- Les TI et les autres formes d'évaluation de la sécurité
- Cadre réglementaire et déontologie des TI
- Démarche générale des TI
- Les normes et standards (OWASP, OSSTMM, etc.)

Risques spécifiques aux tests d'intrusion

- Objectifs des TI
- Ce qui peut mal se passer et la gestion des risques

La nécessité d'un mécanisme de scoring

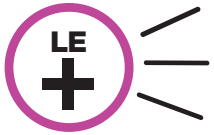
- Scoring des vulnérabilités (CVSS)
- Catégorie des outils
- Limites des outils

Préparer et conduire les TI

- Identifier les risques
- Préparer son entreprise à un TI
- Réagir en cas d'incidents
- Coordonner les équipes
- Corriger les failles et vulnérabilités

Choisir un prestataire

- Mesure de son expertise
- Les 10 questions à poser
- Les pièges à éviter



Coaching en test d'intrusion