FORMATION COURTE

INFORMATIQUE, SÉCURITÉ, SI

DÉFENSE : DÉFENDRE UN SYSTÈME INFORMATIQUE

inter/intra entreprise

Dates : consulter le calendrier
Durée : 4 jours ; 28 heures
Lieu : Compiègne
Tarif : consulter le dépliant « Tarifs »
Prérequis : avoir des connaissances de base en Linux et avoir suivi la formation Risque : prévenir et assurer la protection des systèmes informatiques (CYBERISK) ou avoir les compétences associées à la formation.
Référence produit : CYBERDEF

LES POINTS FORTS

- Entraînement sur des situations réelles ; pédagogie tournée vers la pratique ; formation partagée avec des étudiants ingénieurs
- Un temps réservé aux questions propres aux spécificités des activités de l'organisation

EN SAVOIR +
www.utc.fr
→ Formation continue et VAE

Ce module s'intéresse à la défense des systèmes informatiques. Il permet de comprendre les attaques informatiques et de mettre en œuvre la détection d'intrusion, la détection de vulnérabilité, les tests de pénétration et la surveillance des systèmes.

Objectifs

- Comprendre les attaques informatiques ;
- Savoir détecter les intrusions ;
- Pratiquer le test de pénétration ;
- Surveiller les systèmes.

Public

Informaticiens (niveau en sécurité intermédiaire à avancé).

Modalités pédagogiques

Cours ; exercices ; ateliers-projets et études de cas pour un SI d'entreprise.

Modalités d'évaluation

Évaluation effectuée à l'occasion des tests de connaissances ; travaux de mise en application ; étude.

Programme

Comprendre les attaques informatiques

- Principes des attaques (reproduction d'attaques classiques) ;
- Analyse d'attaques à partir de traces ;
- Attaques des canaux auxiliaires.

Savoir détecter les intrusions

- Principes de la détection d'intrusion ; KIDS, HIDS, NIDS ;
- Utilisation du NIDS (snort).

Pratiquer le test de pénétration

- Méthodologie du test de pénétration ;
- Scanners de vulnérabilité (Openvas) ;
- Pratique du test d'intrusion sur machines virtuelles.

Surveiller les systèmes
- Principes de l'exploitation des logs ; outils (Syslog, SNMP, Nagios...) ;
- Security Information and Event Manager (OSSIM) ;
- Pratique de ELK (Elastic search, Logstash, Kibana).

Intervenants

Nos intervenants sont issus des secteurs économiques publics, privés, académiques et professionnels. Ils comptent généralement plus de 10 ans d'expérience professionnelle dans leur domaine d'expertise.