Association Des Neticiens

# CYBERSÉCURITÉ AVANCÉE

**Durée :**
3 jours

**Format :**
Cours
Travaux Dirigés

**Coût :**
2400€ / stagiaire

**Effectif minimum :**
Formation mise en place à partir de 5 participants


**Contact :**

Anna TEA
anna.tea@neticien.net
07 61 11 64 69

Michel TABOURET
michel.tabouret@neticien.net
07 66 07 20 38

www.formations-neticiens.net

@ADN-Association des Neticiens


## Objectifs :

**Savoir mettre en oeuvre la Cybersécurité :**

- Comprendre les vulnérabilités inhérentes aux mécanismes réseaux et applicatifs couramment utilisés
- Connaitre le panorama des solutions techniques de sécurité
- Appréhender les méthodes et normes de prise en compte de la sécurité :
- Comprendre et anticiper les difficultés couramment rencontrées
- dans la gestion de la sécurité dans une organisation
- Présenter les filières métiers de la cybersécurité dans l'environnement d'exercice de leur fonction au sein des organisations
- Repérer les attaques sur les couches hautes et savoir mettre en place des mesures pour limiter l'impact des attaques

## Prérequis :

Module Cybersécurite Initiation (2 jours)

Connaissances fondamentales en réseaux informatiques : structures d'un réseau local, dispositifs sur le réseau (routeur, concentrateur, commutateur) ainsi que les protocoles TCP/IP

Connaissances fondamentales en systèmes d'exploitation : permissions sur les fichiers, protection mémoire, principes de sécurisation d'un OS (operating system, ou système d'exploitation en français), analyse de Windows et virtualisation.

## Contenu de la formation :

### CYBERSÉCURITÉ : LES ASPECTS RÉSEAUX ET APPLICATIFS

#### La sécurité des protocoles IP, ICMP, TCP, UDP

Présentation synthétique des faiblesses inhérentes à ces protocoles

#### Revue d'architectures réseaux (sécurisation)

Pare-feu
Répartiteur de charge
Anti-virus
IDS/IPS (Intrusion Detection & Prevention Systems)
VPN (Virtual Private Network) IPsec et SSL
Segmentation
Exemple pratique de sécurisation d'un réseau

6h

#### Cryptographie

Vocabulaire relatif à la cryptographie
Un peu d'histoire (Chiffrement de César, Machine Enigma)
Présentation des concepts de chiffrement (symétrique, asymétrique, chiffrement, hashage, signature électronique, certificats et tokens)
Présentation des applications pratiques de la cryptographie dans les services et usages quotidiens

#### La sécurité des applications Web

Usurpation d'identité via les cookies
Injection SQL

#### Quizz (mécanismes techniques à connaitre) et évaluation de la formation

## CYBERSÉCURITÉ : LA GESTION OPÉRATIONNELLE DE LA CYBERSÉCURITÉ AU SEIN D'UNE ORGANISATION

6h

### Intégrer la sécurité au sein d'une organisation à travers une présentation synthétique de la famille des normes ISO/IEC 27000, notamment

Préambule de présentation du chapitre
Panorama des normes ISO 27000
Système de Management de la Sécurité de l'Information (27001)
Code de bonnes pratiques (27002)
Gestion des risques (27005)
Classification des informations
Gestion des ressources humaines

### Intégrer la sécurité dans les projets

Préambule de présentation du chapitre
Prise en compte de la sécurité dans le cycle de vie d'un projet
Contre-exemple de prise en compte en fin de développement
Approche par l'analyse et le traitement du risque
Plan d'action SSI : la défense en profondeur

### Les difficultés couramment rencontrées dans la prise en compte de sécurité

Compréhension insuffisante des enjeux
Implication nécessaire de la direction
Difficulté de faire des choix en toute confiance
Arbitrage délicat entre commodité et sécurité
Suivre l'évolution des technologies
Frontières floues entre sphères professionnelle, publique et privée

### Présentation de métiers liés à la cybersécurité

Positionnement des métiers au sein des organisations
Cartographie des métiers et compétences
Profils et carrières
Perspectives d'embauche

### Quizz (l'organisation de la sécurité) et évaluation de la formation

## CYBERSÉCURITÉ : LA SÉCURITÉ DES RÉSEAUX

3h

### Capture de données sur un réseau

### Attaques sur un réseau

Déni de service
Usurpation d'identité
Vol de session

### Pare-feux et proxys

Notions fondamentales
Règles de filtrage
Architectures des pare-feux

### Systèmes de détection d'intrusion

### IPsec

### SSH

Authentification du serveur
Protocoles cryptographiques
Authentification du client
Redirections de ports

### SSL/TLS

Fondements de SSL/TLS
Mécanismes cryptographiques

### Quizz (la sécurité des réseaux) et évaluation de la formation

## CYBERSÉCURITÉ : LA SÉCURITÉ DES SYSTÈMES D'EXPLOITATION

3h

### Protections mémoire

### Droits spéciaux sur les fichiers Unix

### Sécuriser Unix

### Évolution des solutions de sécurité Windows

### Sécurité Windows au niveau de l'AD, de la base des registres et de la base SAM

### Sécurité au niveau de l'architecture des systèmes d'exploitation Windows

### Gestion des comptes et des utilisateurs Windows Virtualisation des OS

### Quizz (la sécurité des systèmes d'exploitation) et évaluation de la formation