

# Formation Sécurité des systèmes d'exploitation et des réseaux

## Présentation

Cette formation couvre les points critiques des systèmes d'information, la sécurité des données et des réseaux, ainsi que la sécurisation des systèmes et la recherche de failles. Elle combine théorie et pratique pour une compréhension approfondie et appliquée.

Durée : 35,00 heures (5 jours)

Tarif INTRA : Nous consulter

## Objectifs de la formation

- Pouvoir évaluer les risques internes et externes liés à l'utilisation d'Internet.
- Comprendre les mécanismes garantissant la fiabilité et la confidentialité des données grâce aux solutions sécurisantes.
- Disposer d'une première approche des concepts techniques pour comprendre la sécurité des systèmes d'information.

## Prérequis

Bonne connaissance générale des réseaux et des systèmes d'exploitation courants.

## Public

Cette formation s'adresse aux professionnels de l'informatique et de la cybersécurité, aux administrateurs réseau, aux ingénieurs systèmes, ainsi qu'aux étudiants en informatique souhaitant se spécialiser dans la sécurité des systèmes d'information.

## Programme de la formation

### J1 : Comprendre les Points Critiques d'un Environnement SI

#### Architecture des systèmes d'information

- Les composants critiques : serveurs, bases de données, réseaux, endpoints.
- Les interconnexions et zones sensibles (DMZ, VLAN, Cloud).



### **Menaces principales sur les SI**

- Intrusions, attaques par déni de service (DDoS), ransomwares.
- Menaces internes : erreurs humaines et actes malveillants.

### **Approches de sécurisation globales**

- Modèle Zero Trust.
- Sécurisation multi-couches.

### **Travaux Pratiques Contextualisés**

- Assistance : Identification des zones sensibles dans un réseau multisite.

## **J2 : Sécurité des Données**

### **Criticité et classification des données**

- Identifier les données sensibles et critiques (DICP : Disponibilité, Intégrité, Confidentialité, Preuves).

### **Techniques de sécurisation des données**

- Chiffrement symétrique, asymétrique, et hashing.
- Gestion des droits d'accès et solutions DLP (Data Loss Prevention).

### **Protection contre les menaces sur les données**

- Exfiltration, vol de données, ransomware.

### **Travaux Pratiques sous forme d'activité à corriger avec le tuteur**

- Configuration d'un chiffrement de données sensibles sur un serveur de sinistres.

## **J3 : Sécurité des Réseaux**

### **Principes de la sécurité réseau**

- Pare-feu, VPN, et segmentations réseau (VLAN).
- Surveillance réseau avec IDS et IPS.

### **Protection des protocoles et services critiques**

- Sécurisation des communications (SSL, TLS, IPsec).
- Surveillance et filtrage des flux réseau.

### **Scénarios d'attaques et parades**

- DDoS, spoofing, man-in-the-middle.

### **Travaux Pratiques Contextualisés sous forme d'activité à corriger avec le tuteur**

- Assurance : Configuration d'un pare-feu pour sécuriser les échanges entre agences.
- Conseil : Analyse d'un incident réseau à l'aide d'IDS.

## **J4 : Sécurité des Systèmes et Recherche des Failles**

### **Sécurisation des systèmes d'exploitation**

- Hardening : Windows, Linux/Unix, Mac.
- Sécurisation des environnements nomades : Android, iOS.

### **Recherche d'informations sur les failles**

- Sources fiables (ANSSI, CVE).
- Outils d'évaluation : Nessus, OpenVAS.

### **Travaux Pratiques Contextualisés**

- Analyse des configurations système pour identifier des failles potentielles.
- Application des bonnes pratiques de hardening sur un serveur Linux.

## Organisation

### Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

### Moyens pédagogiques et techniques

- Apports des connaissances communes.
- Mises en situation sur le thème de la formation et des cas concrets.
- Méthodologie d'apprentissage attractive, interactive et participative.
- Equilibre théorie / pratique : 60 % / 40 %.
- Supports de cours fournis au format papier et/ou numérique.
- Ressources documentaires en ligne et références mises à disposition par le formateur.
- Pour les formations en présentiel dans les locaux mis à disposition, les apprenants sont accueillis dans une salle de cours équipée d'un réseau Wi-Fi, d'un tableau blanc ou paperboard. Un ordinateur avec les logiciels appropriés est mis à disposition (le cas échéant).

### Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation :

- Recueil des besoins des apprenants afin de disposer des informations essentielles au bon déroulé de la formation (profil, niveau, attentes particulières...).
- Auto-positionnement des apprenants afin de mesurer le niveau de départ.

Tout au long de la formation :

- Évaluation continue des acquis avec des questions orales, des exercices, des QCM, des cas pratiques ou mises en situation...

A la fin de la formation :

- Auto-positionnement des apprenants afin de mesurer l'acquisition des compétences.
- Evaluation par le formateur des compétences acquises par les apprenants.
- Questionnaire de satisfaction à chaud afin de recueillir la satisfaction des apprenants à l'issue de la formation.
- Questionnaire de satisfaction à froid afin d'évaluer les apports ancrés de la formation et leurs mises en application au quotidien.

### **Accessibilité**

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.