Best-of

Ref. SEC-ESS

# Sécurité des systèmes et services réseaux

4 jours (28 heures) | Initiation | Présentiel ou classe à distance

à partir de
**2 780 € HT** par personne (TVA en vigueur)

Repas inclus en présentiel

*Contenu mis à jour le 25/09/2026. Document téléchargé le 07/10/2026.*

## Objectifs

A l'issue de cette formation, vous serez capable de :

- Identifier les enjeux de la sécurité des systèmes d'information, ainsi que ses acteurs et ses limites
- Proposer des solutions pour pouvoir faire transiter et stocker des données sur un réseau d'entreprise de façon sécurisée
- Installer et paramétrer un pare-feu approprié au réseau d'une entreprise
- Installer et configurer un proxy
- Mettre en place un filtrage
- Utiliser différents outils permettant de prévenir et détecter une intrusion sur un réseau.

Les compétences visées par cette formation font l'objet d'une évaluation.

## À qui s'adresse cette formation ?

Responsables de la sécurité des systèmes d'information (RSSI), directeurs des systèmes d'information (DSI), administrateurs système et réseau, techniciens de maintenance système et réseau, consultants en sécurité informatique.

### Prérequis

Avoir des connaissances en réseau et système.

# Programme

1 Pendant votre formation

## Sécurité des systèmes et services réseaux

Jour 1 - Matin

### Les fondamentaux de la sécurité système et réseau

- Définition de la cybersécurité et terminologie de base
- Aperçu des menaces, vulnérabilités et attaques courantes
- L'importance de la sécurité pour les entreprises et les organisations gouvernementales
- Le pilotage et la maîtrise des risques
- Les normes et règlements de la sécurité
- Les méthodologies appliquées
- Les documentations essentielles
- Les architectures réseaux et leurs évolutions
- Les systèmes d'exploitation modernes et leur sécurité
- La conception d'application et ses évolutions en cybersécurité

Jour 1 - Après-midi

### Principes de sécurité des réseaux

- Rappels sur le modèle OSI
- Les composants d'un réseau (routeurs, switches, hubs, firewalls...)
- La sécurité des protocoles réseau (TCP/IP, DNS, DHCP, HTTP...)
- Les forces et faiblesses d'un commutateur
- Les faiblesses de l'accès réseau
- Les faiblesses de la couche d'interconnexions des réseaux
- Les faiblesses de la couche transport
- Les principales faiblesses de la pile TCP/IP
- Les faiblesses de la couche application
- La démarche de sécurisation des réseaux
- Les techniques de sécurisation des réseaux (pare-feu, VPN, IDS/IPS...)
- Maîtriser l'interprétation des flux réseaux
- Panorama des solutions du marché

*Exemples de travaux pratiques (à titre indicatif)*

- *Réaliser une attaque d'ARP Cache Poisoning et proposer des mesures de prévention*
- *Déterminer l'ensemble des ports TCP/IP ouverts sur la machine jouant le rôle de routeur*
- *Réaliser une attaque MITM entre deux machines du réseau*

- *Evader la sécurité IPS d'une machine du réseau*

Jour 2 - Matin

### Intégrer et gérer un firewall

- Le rôle et le positionnement d'un firewall
- Les différents types de firewalls et leurs avantages
- Les composantes d'une règle de filtrage
- ACL (Access Control List)
- Eviter les faux positifs
- Les bonnes pratiques
- La gestion de la journalisation
- L'utilisation des agents SNMP (Simple Network Management Protocol)

*Exemples de travaux pratiques (à titre indicatif)*

- *Déployer un firewall stateful*
- *Créer des règles pour n'autoriser que la station à communiquer avec la machine de formation, sauf pour le DNS et l'HTTP / HTTPS*
- *Réaliser une attaque de SYN Flood et proposer des mesures de prévention*

Jour 2 - Après-midi

### Mise en place d'un proxy

- Le rôle et le positionnement d'un proxy
- Les différents types de proxies et leurs avantages
- Les étapes de déploiement d'un proxy
- La création de règles et de listes
- Les bonnes pratiques

*Exemples de travaux pratiques (à titre indicatif)*

- *Déploiement d'un proxy et paramétrage d'un filtrage utilisateur par Blacklist*

### Les IDS (Intrusion Detection System) et IPS (Intrusion Prevention System)

- Le rôle et le positionnement des IPS et des IDS
- Les différents types d'IPS et d'IDS (HIDS, NHIDS, HIPS...)
- Les composantes d'une règle de détection et de filtrage
- Les bonnes pratiques
- La gestion de la journalisation
- La remontée des alertes

*Exemples de travaux pratiques (à titre indicatif)*

- *Déploiement d'un NIDS et paramétrage des remontées de logs*
- *Déploiement d'un HIPS et paramétrage des remontées de logs*

Jour 3 - Matin

### La sécurité du routage

- Le rôle et le fonctionnement des routeurs
- Les attaques sur les routeurs
- Les attaques sur les protocoles de routage
  - RIP (Routing Information Protocol)
  - OSPF (Open Shortest Path First)
  - EIGRP (Enhanced Interior Gateway Routing Protocol)
  - HSRP (Hot Standby Router Protocol)
  - IS-IS
  - BGP (Border Gateway Protocol)
  - Les "Appliances" de sécurité

*Exemples de travaux pratiques (à titre indicatif)*

- *Mise en place d'un routeur et sécurisation de la couche de routage*

Jour 3 - Après-midi

### La virtualisation et son durcissement

- Rappel sur la virtualisation
- Les composantes principales d'un système de virtualisation
- Les risques et faiblesses inhérents à la virtualisation
- Les éléments de sécurisation
- Les nouveaux concepts de virtualisation (NFV...)
- Les autres solutions d'abstraction (conteneurisation, isolation...)

### Durcissement Windows

- La politique de mises à jour et de patchs
- La sécurité des comptes utilisateurs
  - Politique de gestion des mots de passe
  - Désactivation des comptes utilisateurs inutilisés
- La politique de gestion du contrôle d'accès aux fichiers et au registre
- La sécurité des données et de l'exécution
  - Les antivirus et antimalwares (Microsoft Defender, Device Guard, Credential Guard, AMSI)
  - Le chiffrement des disques durs (Bitlocker, TPM, agent de récupération)
  - La prévention de l'exécution (Applocker, DEP, ASLR, CFG, SEHOP...)
- La sécurité des contenus Web (Smartscreen)
- La sécurité du démarrage (Secure Boot - UEFI)
- Le pare-feu Windows (configuration et règles)
- Le contrôle de l'élévation de privilèges (UAC)

- La politique d'audit et de logs
- Les Group Policies

Jour 4 - Matin

### Durcissement Windows - Suite

*Exemples de travaux pratiques (à titre indicatif)*

- *Déploiement d'Applocker et paramétrage d'une interdiction d'exécution d'application en dehors de "Program Files" et "Windows"*
- *Création d'une exception dans Applocker pour Teams*
- *Modification de l'élévation de privilèges pour mettre l'accès aux privilèges avec ou sans UAC*
- *Création de règles de firewall pour durcir l'accès aux protocoles d'infrastructure*
- *Mise en place d'IPSec pour l'administration du poste Windows*

### Durcissement Linux

- La politique de mises à jour et de patchs
- La sécurité des comptes utilisateurs
  - Gestion de comptes d'accès
  - Politique de gestion des mots de passe
  - Désactivation des comptes utilisateurs inutilisés
  - Délai d'expiration de sessions utilisateurs
  - PAM et NSS
- La minimisation des services
  - Services exposés à des flux non maîtrisés
  - Services réseau résidents
  - Configuration des services avec sysctl

Jour 4 - Après-midi

### Durcissement Linux - Suite

- La gestion des privilèges
  - Vérification du système de fichiers et des droits
  - Gestion des droits d'accès
  - L'Umask
  - Les fichiers sans utilisateur ou groupe propriétaire
  - Les fichiers et répertoires accessibles à tous en écriture
  - Les fichiers IPC nommés, sockets ou pipes
  - Les fichiers à contenu sensible
- Le pare-feu et sa configuration de base
- La prévention et la sécurisation de l'exécution
  - Le chiffrement des partitions

- Les fichiers exécutables setuid ou setgid
- Les systèmes de contrôle d'accès mandataire (SELinux, AppArmor, Smack…)
- Les systèmes de jails et de conteneurs (chroot, schroot, docker, LXC, firejail…)
- Protection contre les buffer-overflows (PaX, Grsecurity, GCC avec SSP, ASan, Valgrind…)

- La configuration d'outils et services de monitoring
  - Surveillance du système par auditd
  - Utilisation et gestion de Syslogd
- La sécurisation des mails système et root
- Le Kernel Hardening

*Exemples de travaux pratiques (à titre indicatif)*

- *Création d'un script système de surveillance des configurations dans /etc et sécurisation de son exécution*
- *Création d'un script de surveillance de l'activité du système de fichiers et sécurisation de son exécution*
- *Configuration du firewall pour limiter l'accès à SSH à votre poste*

## Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.
Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

Nous contacter pour en savoir plus →

## Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne

- Supports de cours et exercices

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

** nous consulter pour la faisabilité en distanciel*

*** ratio variable selon le cours suivi*

Accessibilité aux personnes en situation de handicap

## Détails de la session

### Du 1 décembre 2026 au 4 décembre 2026 (4 jours / 28 heures)

Metz

Du 1 décembre 2026 au 4 décembre 2026 Metz

- 1 décembre 2026 ---------- 9h00 - 15h30
- 2 décembre 2026 ---------- 9h00 - 15h30
- 3 décembre 2026 ---------- 9h00 - 15h30
- 4 décembre 2026 ---------- 9h00 - 15h30