

Etat de l'art de la sécurité des systèmes d'information (SSI)

3 jours (21 heures)

Initiation

Présentiel ou classe à distance

à partir de

2 655 € 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 différents domaines de la sécurité et de la maîtrise des risques liés aux informations
- Présenter les principes et les normes de chaque domaine de la SSI
- Décrire les tendances actuelles au niveau des menaces et des solutions à notre disposition
- Améliorer la communication entre la maîtrise d'ouvrage, la maîtrise d'oeuvre et la SSI
- Effectuer des choix techniques.

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

À qui s'adresse cette formation ?

Directeurs des systèmes d'information ou responsables informatiques, RSSI, chefs de projets sécurité, architectes informatiques.

Prérequis

Avoir une bonne connaissance générale des systèmes d'information.

Programme

1 Pendant votre formation

Etat de l'art de la sécurité des systèmes d'information (SSI)

Jour 1

Introduction

- Généralités
- Statistiques
- Définitions
- Les critères de sécurité
- Les profils des hackers...

Organisation de la SSI et référentiels

- Organisation au niveau étatique
- Les principaux acteurs au plan international
- Les services spécialisés en cybercriminalité
- Les référentiels (ANSSI, NIST, CVE, MITRE...)

Exigences légales et contexte juridique

- Le corpus juridique de la sphère du numérique aux niveaux national, européen et international
- Focus sur les directives et les règlements impactants
- La jurisprudence
- La cybersurveillance...

Démarche globale, conformité et bonnes pratiques

- De la gouvernance à la sensibilisation
- Assurabilité du risque cyber
- Les principales normes dédiées au management de la sécurité IT, à la gestion des risques et à l'audit (ISO27xxx, Ebios RM...)

Jour 2

Cryptographie

- Chiffrement symétrique, chiffrement asymétrique, signature, algorithmes (DES, 3DES, AES...)
- Protocoles SSL, SSH
- Public Key Infrastructure (PKI), gestion des certificats TLS, rupture protocolaire...

Notions complémentaires

- Authentification forte, multi-facteurs, politique de mot de passe
- Network Address Translation

- Défense en profondeur
- Continuité et reprise d'activités
- Performance du SI
- Certification, qualification, visas...

Malwares, antivirus, attaques

- Panorama des malwares
- Antivirus, anti-malwares
- Les technologies de remédiation "Detection and Response"
- Etude des principales attaques cyber (MITM, hijacking, injections...)
- Focus sur l'Intelligence Artificielle (IA)
- Bonnes pratiques de développement logiciel
- Evaluer votre sécurité informatique, réagir en cas d'attaque...

Jour 3

Techniques, technologies et équipements

- Solutions de gestion des mots de passe
- Sécurisation des infrastructures de messagerie :
 - Blacklistage
 - Chiffrement réseau
 - Domain Key Identified Mail (DKIM)
 - Sender Policy Framework (SPF)
 - DMARC
 - Chiffrement
 - Signature des messages
- Durcissement des systèmes Windows, Linux et des serveurs Web
- Isolation des flux par la formation des réseaux virtuels (VLAN)
- Chiffrement des données réseau (tunneling, VPN)
- Les différents types de contrôle d'accès aux données et aux applications
- IAM (Identity et Access Management)
- Le contrôle d'accès réseau : 802.1x / EAP, Network Access Control (NAC)
- Sécurité des réseaux WiFi :
 - Technologies radio
 - Protocoles
 - Architecture...
- Sécurité périmétrique :
 - Proxy
 - Reverse proxy
 - Firewalls

- DLP...
- Protection des applications Web : WAF (Web Application Firewall)
- Surveillance du trafic réseau, blocage des flux
- Virtualisation et conteneurisation
- Segmentation interne
- Gestion des flottes mobiles :
 - Utilisation des équipements personnels dans le cadre professionnel
 - Technologies associées
- Télétravail (TS Web Access, VDI...)
- La sécurité du Cloud :
 - Normalisation
 - Sécurisation des flux et des données
 - Authentification, contrôle d'accès, serveur metadataire, deep inspection, conformité
 - Architecture de sécurité unifiée en mode Cloud, les briques fonctionnelles, Cloud hybride, multi-Cloud...

Supervision, gestion et plateformes spécialisées

- Protocoles de gestion des équipements réseau
- Gestion des informations de sécurité, corrélation, orchestration, automatisation et réponse
- Organisation de la sécurité défensive
- Organisation de la sécurité proactive
- Externalisation de la cybersécurité...

Tendances

- Intelligence Artificielle et Machine Learning
- Security Self Healing System
- Software Defined Security
- Blockchain...

Synthèse des actuelles cybermenaces

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 apports théoriques et démonstrations concrètes.

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

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*

[Accessibilité aux personnes en situation de handicap](#)

Détails de la session

Du 1 décembre 2026 au 3 décembre 2026 (3 jours / 21 heures)

Paris La Défense

Du 1 décembre 2026 au 3 décembre 2026

Paris La Défense

- 1 décembre 2026 9h00 – 16h00
- 2 décembre 2026 9h00 – 16h00
- 3 décembre 2026 9h00 – 16h00