
Programme de Formation

Sécurité des Systèmes d'Information (SSI) : panorama des menaces et tendances clés

Organisation

Durée : 14 heures

Mode d'organisation : Présentiel

Contenu pédagogique



Public visé

Directeurs des systèmes d'information, responsables de la sécurité des systèmes d'information, chefs de projets IT, architectes réseaux ou sécurité, consultants en cybersécurité, ou toute personne impliquée dans la protection et la gouvernance des systèmes d'information.



Objectifs pédagogiques

- Identifier les domaines fondamentaux de la SSI et la gestion des risques associés.
- Présenter les normes et référentiels majeurs en matière de sécurité informatique.
- Décrire les menaces actuelles et les principales solutions techniques de protection.
- Comprendre les enjeux de la sécurité dans les environnements Cloud, mobiles et virtualisés.
- Approfondir la supervision de la sécurité et anticiper les tendances futures.



Description

Jour 1

Matin : Introduction à la SSI et cadres de référence

Définitions clés : intégrité, disponibilité, confidentialité, authentification, traçabilité.

Typologie des cybermenaces et profils d'attaquants.

Principaux acteurs et organisations : ANSSI, CNIL, ENISA, NIST.

Exigences légales et contextes juridiques : RGPD, LCEN, RGS, eIDAS.

Normes ISO 27001, ISO 27002, ISO 31000, ISO 27005.

Gouvernance SSI : politique, sensibilisation, charte informatique.

Introduction aux démarches de gestion des risques : EBIOS RM, PSSI.

Après-midi : Cryptographie et protection, malwares et attaques

Bases du chiffrement : symétrique, asymétrique, PKI.

Protocoles essentiels : SSL/TLS, SSH, certificats numériques.

Typologie des malwares : virus, ransomwares, spyware, rootkits.

Stratégies d'attaque : phishing, DDoS, injection SQL, XSS, CSRF.

Défenses : antivirus, EDR (Endpoint Detection and Response), sensibilisation aux menaces.

Travaux pratiques : Analyse d'exemples d'incidents et évaluation du niveau de sécurité d'un SI.

Jour 2

Matin : Technologies et infrastructures de sécurisation

Gestion des mots de passe, durcissement des systèmes.
Sécurité réseau : VLAN, VPN SSL/IPSec, NAC, RBAC, IAM.
Sécurisation des infrastructures Wi-Fi : WPA3, modes personnel et entreprise.
Sécurisation des flux : proxy, firewalls, WAF, DLP, IDS/IPS.
Sécurité de la mobilité et du cloud : BYOD, télétravail sécurisé, sécurité Cloud.

Après-midi : Supervision, gestion des incidents et tendances

Introduction au SIEM, SOAR, SOC.
Surveillance des événements et réponse automatisée.
Intelligence Artificielle, Machine Learning appliqués à la sécurité.
Cyber-résilience : self-healing systems.
Blockchain et Software Defined Security (SDS).
Travaux pratiques : Atelier de construction d'une feuille de route SSI pour une organisation fictive.



Prérequis

Avoir une bonne connaissance générale des systèmes d'information.



Modalités pédagogiques

- Notre approche pédagogique repose sur une alternance entre apports théoriques opérationnels et mises en pratique directement issues du contexte professionnel des participants.
- Chaque thème traité s'appuie sur des études de cas concrets et des exercices pratiques, conçus spécifiquement à partir des situations réelles rencontrées dans l'environnement professionnel des stagiaires.
- Nos méthodes favorisent l'adaptation aux besoins de chaque participant afin d'optimiser leur engagement et leur apprentissage.
- L'animation privilégie une pédagogie active, favorisant les échanges, l'analyse réflexive des pratiques et une adaptation continue aux réalités professionnelles des participants.



Moyens et supports pédagogiques

- Des supports pédagogiques numériques adaptés au contexte professionnel sont remis aux participants.
- Dispositifs pédagogiques variés sont mobilisés tout au long de la formation (études de cas, exercices pratiques, travaux en sous-groupes, mises en situation, jeux pédagogiques) favorisant l'apprentissage actif, collaboratif et l'appropriation des contenus.



Modalités d'évaluation et de suivi

- Un QCM est réalisé en début et en fin de formation afin d'évaluer l'évolution des connaissances.
- Le suivi des stagiaires est assuré tout au long de la formation à travers des ateliers pratiques, des mises en situation et des échanges permettant d'évaluer leur participation et leur progression.

Une attestation individuelle de formation sera remise à chaque participant à l'issue de la formation.



Informations sur l'accessibilité

Si vous êtes en situation de handicap, ou si vous rencontrez une difficulté pouvant impacter votre participation à la formation, n'hésitez pas à nous contacter. Nous étudierons ensemble les aménagements ou adaptations pédagogiques, matérielles ou organisationnelles à mettre en place pour vous accompagner dans les meilleures conditions.