Gouvernance

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

3 jours (21h00) | ★★★★½ 4,6/5 | SEMI-SSI | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel



*Contenu mis à jour le 18/10/2024. Document téléchargé le 08/12/2024.*

## Objectifs de formation

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.

## Modalités, méthodes et moyens 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*

## Prérequis

Avoir une bonne connaissance générale des systèmes d'information.

## Public concerné

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

## Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

# Programme

## Jour 1

### Introduction

- Statistiques
- Définitions
- Domaines concernés
  - Intégrité
  - Disponibilité
  - Confidentialité
  - Authentification
  - Imputation
  - Traçabilité...
- Les profils des hackers

### Organisation de la SSI et référentiels

- Organigramme état
  - SGDSN
  - ANSSI
  - HFDS...
- Acteurs
  - CNIL
  - ENISA
  - NIST
  - CSA...
- Services spécialisés en cybercriminalité
  - C3N
  - BL2C...

### Exigences légales et contexte juridique

- Lois
  - Godfrain
  - CPI
  - LCEN
  - LSQ
  - Hadopi...
- Jurisprudence
  - Courriels
  - Fichiers personnels...

- Cybersurveillance, RGPD, RGS, eIDAS, PCI-DSS

### Démarche globale et normes

- Maturité des processus, gouvernance, PSI, sensibilisation des utilisateurs...
- Normalisation, ISO 13335, ISO 31000, certifications ISO 27001
- SMSI ISO 27001 (phases PDCA), analyse de risques ISO 20005/EBIOS, assurabilité du risque, EBIOS RM...
- PSSI, ISO 27002
- Sensibilisation, charte informatique

## Jour 2

### Cryptographie

- Chiffrement symétrique, chiffrement asymétrique, algorithmes (DES, 3DES, AES...)
- Public Key Infrastructure (PKI), architecture AE/AC/OC, CSR, PKCS#12, génération de certificats, norme X509, OCSP...
- Handshake SSL, SSH, protocoles de hachage...

### Notions complémentaires

- Authentification simple / forte, zéro trust, DSP2, OTP
- Stockage des mots de passe, politique de mot de passe
- Défense en profondeur, PCA/PRA, translation, classification
- Performance du SI, Critères Communs / ISO 15408
- Certification, qualification, visas
- Intégration de la SSI dans les projets

### Malwares, antivirus, attaques

- Malwares
  - Cheval de Troie
  - Virus
  - Rootkit
  - Spyware
  - Robot
  - Cryptovirus, ransomwares
- Antivirus, anti-malwares
  - Analyse comportementale
  - Heuristique
  - Signatures
  - Endpoint Detection and Response...
- Attaques
  - Terminal
  - Réseaux
  - Applications (phishing, DoS, spoofing...)
- Attaques sur les mots de passe, injection SQL, CSRF, XSS, injection de commandes, interceptions couche 2 et 3, Hijacking...
- Evaluer votre sécurité informatique, réagir en cas d'attaque

## Jour 3

### Techniques, technologies et équipements

- Solutions de gestion des mots de passe
- Infrastructure de messagerie
  - Open Relay, Spam, StartTLS, Domain Key Identified Mail (DKIM), Sender Policy Framework (SPF), DMARC
- Durcissement des systèmes Windows, Linux et des serveurs Web
- Séparation des flux par la formation des réseaux virtuels (VLAN)
- Cryptage des données en ligne (VPN SSL et VPN IPsec)

- Mandatory Access Control (MAC), Discretionary Access Control (DAC)
- Contrôle d'accès
  - 802.1x / EAP Networks Access Control (NAC)
  - Role Based Access Control (RBAC)
  - IAM (Identity et Access Management)
- Protocoles Wi-Fi
  - Technologies radio
  - Personal mode
  - Mode enterprise
  - WPA3...
- Filtrage
  - Proxy, mode coupure SSL
  - Reverse-proxy
  - Firewalls protocolaires, de contenus, d'applications, d'identité
  - FWNG
  - DMZ, matrice des flux
- Filtrage des applications Web : WAF (Web Access Firewall)
- DLP (Data Lost Prevention) - Data Masking
- IDS/IPS, honeypots
- Virtualisation et conteneurisation
  - Hyperviseur
  - Emulateur
  - Isolation de contexte...
- Le BYOD
  - Utilisation des équipements personnels dans le cadre professionnel
  - Enjeux
  - Risques
  - MDM
  - App Wrapping
- Télétravail (TS Web Access, VDI...)
- La sécurité dans le Cloud
  - Modèle de responsabilités
  - ISO 27017
  - ISO 27018
  - Encryptions
  - Vol de données
  - Flux de données
  - Cloud Access Security Broker
  - SWG
  - Zero Trust Network Access
  - Secured Service Edge...

## Supervision gestion et plateformes spécialisées

- SIEM (Security Information and Event Management)
- SOAR (Security Orchestration, Automation and Response)
- SOC (Security Operation Center)
- Plateforme de gestion et de sécurité des mobiles EMM (Entreprise Mobility Management)
- Plateforme de Cloud de sécurité (SecaaS : Security as a Service)

## Tendances actuelles

- Recours à l'Intelligence Artificielle et à la Machine Learning
- Security Self Healing System
- Software Defined Security
- Blockchain

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

## Modalités d’évaluation des acquis

– Les participants réalisent, en début et en fin de formation, une auto-évaluation de leurs connaissances au regard des objectifs pédagogiques du séminaire suivi

## Accessibilité de la formation

Le groupe M2i s'engage pour faciliter l'accessibilité de ses formations. Toutes nos formations sont accessibles aux personnes en situation de handicap : les détails de l'accueil des personnes sont consultables sur la page Accueil PSH.

## Modalités et délais d’accès à la formation

Les formations M2i sont disponibles selon les modalités proposées sur la page programme.
Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation.
Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.