

Sessions garanties disponibles

Formation Cybersécurité : synthèse et état de l'art, de la gouvernance des risques aux solutions techniques

Réf. SF34650

Acquérez une vision d'ensemble structurée de la cybersécurité d'entreprise pour identifier vos risques, dialoguer avec vos équipes et faire des choix de sécurité éclairés.

3 j Durée	2 700 € HT Inter / participant	6 150 € HT Intra (≤12 pers.)	14 Sessions à venir
--------------	-----------------------------------	---------------------------------	------------------------

Objectifs pédagogiques

- ✓ Décrire l'état de l'art des menaces et de la cybercriminalité (ransomware, APT, phishing, Kill Chain)
- ✓ Distinguer les principales solutions techniques de sécurité (filtrage, cryptographie, authentification forte, sécurisation des flux, Cloud, endpoints)
- ✓ Expliquer la gouvernance de la sécurité et le rôle des acteurs de la SSI (RSSI, direction, asset owners)
- ✓ Expliquer les dispositifs de supervision et de réaction (audits, tests d'intrusion, SIEM, SOC, réponse à incident)
- ✓ Conduire une démarche d'analyse et de maîtrise des risques (DICP, ISO 27005, EBIOS RM)
- ✓ Cadrer une politique de sécurité et construire une feuille de route adaptée à son organisation
- ✓ Identifier les normes et le cadre juridique applicables (ISO 2700x, hygiène ANSSI, RGPD, NIS2, DORA)

Public visé & prérequis

- Public visé** Architectes, Chefs de projet, DSI, Responsables de la sécurité des systèmes d'information (RSSI), Tous
- Prérequis** - Connaissance générale des systèmes d'information et des réseaux (notions d'architecture, TCP/IP) - Aucun prérequis de programmation ou d'administration système

Programme détaillé

Menaces, cybercriminalité et enjeux de sécurité

- Panorama de la menace : motivations et professionnalisation des attaquants (cybercriminalité, hacktivisme, espionnage, États)
- Typologie des attaques : ransomware, APT, phishing et spear phishing, déni de service, fraude
- Anatomie d'une cyberattaque : la Kill Chain, vulnérabilités, failles 0day et kits d'exploitation
- Tendances et statistiques : évolution des incidents, surface d'attaque (Cloud, mobilité, supply chain)
- Sources de veille et d'information : ANSSI, CERT, CLUSIF, ENISA

Activités pratiques :

- Décryptage d'une attaque par ransomware récente, étape par étape
- Construction d'une cartographie des menaces pesant sur une organisation type

Gouvernance et organisation de la sécurité

- Enjeux DICP (Disponibilité, Intégrité, Confidentialité, Preuve) et alignement avec les enjeux métiers
- Rôle et responsabilités du RSSI/CISO, relation avec la DSI et la direction générale
- La task force SSI : profils et compétences (architectes, auditeurs, pen-testeurs, superviseurs, risk managers)
- Implication de la direction et rôle des « asset owners »
- Modèle de maturité de la sécurité et structuration d'une politique de sécurité (PSSI)

Activités pratiques :

- Cartographie des acteurs et des responsabilités sécurité d'une organisation

- Auto-évaluation du niveau de maturité SSI

Analyse et maîtrise des risques

- Notions clés : actif, vulnérabilité, menace, impact, risque résiduel
- Cartographie des risques : appréciation par gravité × vraisemblance, niveaux et traitement
- Normes de gestion des risques : ISO 31000, ISO 27005
- Méthodes d'analyse : EBIOS Risk Manager (approche FR/ANSSI), aperçu NIST
- Du plan de traitement à la décision : acceptation, réduction, transfert, évitement

Activités pratiques :

- Atelier d'appréciation des risques sur un cas métier (cartographie gravité/vraisemblance)
- Élaboration d'un plan de traitement priorisé

Normes, référentiels et cadre juridique

- La série ISO 2700x : SMSI et démarche d'amélioration continue (PDCA), ISO 27001 et bonnes pratiques ISO 27002
- Règles d'hygiène et recommandations de l'ANSSI, référentiels métiers (ex. PCI DSS)
- Protection des données personnelles : RGPD, rôle de la CNIL, sanctions
- Cadre réglementaire européen : directive NIS2 (élargissement des entités concernées), règlement DORA (résilience du secteur financier), Loi de Programmation Militaire
- Responsabilités juridiques : entreprise, dirigeants, RSSI ; charte de sécurité et cybersurveillance des salariés

Activités pratiques :

- Positionnement d'une organisation vis-à-vis des obligations NIS2 / RGPD
- Revue des clauses de sécurité d'une charte informatique

Panorama des solutions techniques de sécurité

- Défense en profondeur : protection logique et physique, cloisonnement, DMZ
- Filtrage et protection réseau : firewall (UTM, NG), IPS, sécurisation du Cloud (responsabilité partagée, CASB)
- Cryptographie appliquée : chiffrement symétrique/asymétrique, fonctions de hachage, infrastructures à clés publiques (PKI)
- Authentification et habilitation : MFA, authentification forte (FIDO, OTP), gestion des identités et des accès (IAM, SSO)
- Sécurisation des flux : TLS, IPsec, VPN, SSH
- Sécurité des endpoints et des applications : durcissement des postes et serveurs, mobilité (MDM), risques OWASP, pare-feu applicatif (WAF)

Activités pratiques :

- Lecture critique d'une architecture réseau sécurisée (identification des défauts de cloisonnement)
- Atelier : choisir les mécanismes d'authentification adaptés à différents cas d'usage

Supervision, audits et réaction aux incidents

- Audits de sécurité : audit organisationnel, audit de configuration, tests d'intrusion (black/grey/white box), bug bounty
- Détection et supervision : indicateurs et tableaux de bord, journalisation, SIEM, SOC (et SOC 2.0 : EDR, UEBA, SOAR)
- Réponse à incident : organisation, CERT, forensics, référentiels ISO 27035 et NIST SP 800-61
- Continuité d'activité : PCA/PRA, RTO/RPO, gestion de crise cyber
- Sensibilisation et facteur humain : programmes de sensibilisation, serious games, charte

Activités pratiques :

- Simulation de gestion d'un incident de sécurité (de la détection à la communication)
- Construction d'un tableau de bord d'indicateurs de sécurité

Prochaines sessions

DATE	LIEU	STATUT
14/10/2026	à distance	Sur confirmation
07/12/2026	à distance	Sur confirmation
16/03/2027	Lyon	Sur confirmation

DATE	LIEU	STATUT
16/03/2027	Lille	Sur confirmation
16/03/2027	Nantes	Sur confirmation
16/03/2027	à distance	Sur confirmation

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

4,8/5 — 5 avis

Claire T. — Très bonne formation pour avoir une connaissance basique de l'IA. Le formateur est clair dans ses explications et a su répondre à toutes nos questions.

Julien G. — Très bonne formation dispensée par Pierre. Il maîtrise son sujet, il fait participer les personnes de manière à récolter leur besoin et le projette dans les principes abordés...

Ils nous font confiance

Cette année notre filière Décryptage & Tendances IT a accompagné plus de 11 entreprises dont :

THALES GLOBAL SERVICES AVEM MFP MICHELIN ALTECA COURBON SAS DOCAPOSTE GROUPAMA SUPPORTS & SERVICES ITRON FRANCE
NUMIH FRANCE SEB DEVELOPPEMENT +1 autre

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com