



ORGANISME DE FORMATION AUX TECHNOLOGIES ET METIERS DE L'INFORMATIQUE

Formation Découvrez les solutions techniques pour sécuriser votre SI *Cryptographie, Zero Trust, sécurité des endpoints, réseaux et applications*

N° ACTIVITÉ : 11 92 18558 92

TÉLÉPHONE : 01 85 77 07 07

E-MAIL : inscription@hubformation.com

Objectifs

- | Décrire les cyberattaques modernes, y compris les usages offensifs de l'IA : kill chain, MITRE ATT&CK, APT, attaques via la supply chain et ransomware
- | Appliquer une démarche de cybersécurité structurée par les risques, la conformité et les référentiels clés, notamment ISO 2700x, EBIOS RM et les bonnes pratiques d'hygiène numérique
- | Identifier les principales mesures de protection des architectures réseau on-premise et dans le Cloud avec le Zero Trust et en intégrant la cryptographie, l'authentification forte et la sécurisation des communications
- | Évaluer les risques liés aux terminaux, applications, systèmes d'IA et dispositifs de supervision afin de choisir les contrôles adaptés de prévention, détection et réponse aux incidents

Public

| DSI et leurs collaborateurs directs, RSSI, DPO, décideurs informatiques, consultants, ingénieurs, chefs de projets et responsables fonctionnels

Prérequis

| Aucun

Programme de la formation

Cybercriminalité et principes fondamentaux de cybersécurité

- | La cybercriminalité : définition et enjeux
- | Analyse de la menace cyber (CTI) et techniques d'attaque (framework MITRE ATT&CK)
- | Panorama des cyberattaques contre les entreprises et les infrastructures critiques
- | Les attaques via la chaîne d'approvisionnement
- | L'IA au service du cybercrime : deepfake phishing, voice cloning, AI-Powered social engineering, automated spear phishing, AI-Generated Scam websites
- | Les principes fondamentaux de cybersécurité : défense en profondeur, moindre privilège, besoin d'en connaître, ...
- | La double approche de la cybersécurité : conformité vs gestion des risques
- | Analyse de risque : ISO 27005 vs EBIOS RM
- | Panorama des normes ISO 2700x et focus sur l'ISO 27001 & 27002

Architectures sécurisées et sécurité du cloud computing

- | La protection périmétrique via une architecture classique : Firewall, DMZ, Proxy...
- | Evolution de la sécurité des infrastructures : Firewall NG, SASE, Zero Trust (ZTA), ...
- | L'apport des solutions NDR & framework Mitre ATT&CK
- | La sécurité en périphérie (SSE) et des accès au Cloud (CASB)
- | La sécurité dans le Cloud : modèle de responsabilité partagé
- | Les référentiels de Cloud Security Alliance : Security guidance, CCM, CAIQ
- | Les solutions de sécurité spécifiques au Cloud : CASB, CWPP, CNAPP, CSPM et SSPM

Référence	SRXC
Durée	3 jours (21h)
Tarif	2 995 €HT
Repas	repas inclus

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 5 au 7 juillet 2027

du 22 au 24 novembre 2027

PARIS

du 23 au 25 novembre 2026

du 24 au 26 mai 2027

du 20 au 22 septembre 2027

[VOIR TOUTES LES DATES](#)

Notions fondamentales de cryptographie

- | Définitions et principes fondamentaux (cryptologie, cryptanalyse, principe de Kerckhoffs, ...)
- | Le chiffrement symétrique avec AES et le chiffrement asymétrique avec RSA, DH et ECDSA
- | Les fonctions de hachage : séries SHA2 et SHA3 du NIST et HMAC
- | Les différentes techniques de cryptanalyse. Qu'en est-il de la cryptanalyse quantique ?
- | Les infrastructures PKI et les certificats électroniques X509 v3
- | Les certifications de sécurité : critères communs (ISO 15408), FIPS 140 & Cybersecurity Act

La sécurité des Endpoints

- | Anatomie d'une cyberattaque moderne : de la compromission d'un Endpoint au contrôle de l'AD
- | Le panorama des logiciels malveillants : ver, trojan, backdoor, spyware, scareware, rootkit...
- | Les logiciels antivirus (EPP) et les solutions EDR / XDR
- | Les failles dans les navigateurs et les attaques de type « drive-by compromise »
- | Ransomware (rançongiciel) : la menace cyber numéro 1 dans le monde

Authentification des utilisateurs

- | Panorama des attaques sur les mots de passe : sniffing, keylogger, credential stuffing...
- | Authentification MFA : mot de passe, code PIN, soft token (HOTP, TOTP), FIDO U2F...
- | Authentification via la biométrie et focus sur les aspects juridiques
- | Les gestionnaires de mots de passe : quelle confiance, quelles alternatives ?
- | L'authentification password-less avec l'initiative « Passkey »
- | Synthèse des attaques sur l'authentification et contre-mesures associées

Sécurité des flux réseaux

- | Le standard IPsec, protocoles AH, ESP, IKE et la gestion des clés
- | Le protocole SSL/TLS (de SSL v2 à TLS v1.3)
- | Le protocole HTTPS : mise en œuvre et description détaillée des échanges
- | La sécurité des réseaux Wi-Fi (WPA2 et WPA3) et authentification (IEEE 802.1X, EAP-TLS,...)

La sécurité des logiciels et des applications

- | Les vulnérabilités logicielles : identification (CVE) et cycle de vie
- | Evaluer la criticité des failles (CVSS et SSVC) et prédiction d'exploitation (EPSS)
- | Les principaux risques des applications Web (Top Ten OWASP)
- | Le principe de défense en profondeur appliqué à la sécurité applicative
- | Les méthodes de développement sécurisé (Microsoft SDL, SAMM) et de maturité (BSIMM)
- | Les différentes activités de sécurité dans un Secure-SDLC
- | Le DevSecOps pour une intégration en continu de la sécurité des applications dans le Cloud

Audit, tests d'intrusion et supervision de la sécurité

- | Les centres de gestion des vulnérabilités (VOC)
- | Identification et gestion de la surface d'attaque (ASM)
- | Les tests de sécurité applicative (SAST, DAST, IAST)
- | Test d'intrusion vs Exercice red team
- | Le SIEM (Security Information and Event Management) et la détection des incidents de sécurité
- | Le SOC (Security Operation Center) et technologies associées (IA/ML, deceptive security, CTI...)
- | L'automatisation de la réponse à incident (SOAR)

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

- | Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
 - | Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
 - | Privilégier une connexion filaire plutôt que le Wifi.
 - | Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
 - | Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
 - | Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
 - | Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
 - | Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
 - | Horaires identiques au présentiel.
-

Accessibilité



Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.