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

Référence	SECCG23
Durée	3 jours (21h)
Tarif	2 960 €HT
Repas	repas inclus

Objectifs

| Maîtriser la cryptographie : pierre angulaire de la cybersécurité
| Identifier le fonctionnement des principales solutions de cybersécurité
| Assurer la sécurité des réseaux et des communications
| Identifier les risques dans les logiciels et applications et les activités de sécurité applicative

Public

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

Prérequis

| Connaissances de base en Systèmes d'Information

Programme de la formation

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. QUID 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
| 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 download »
| Le chiffrement des disques durs et des périphériques amovibles (disques externes, clés USB, ...)

Authentification des utilisateurs
| Panorama des attaques sur les mots de passe : sniffing, keylogger, credential stuffing,...
| Authentification Type I (ce que je sais) : mot de passe, code PIN, passphrase, ...
| Authentification Type II (ce que je possède) : carte à puce, soft token (HOTP, TOTP), FIDO U2F, ...
| Authentification Type III (ce que je suis) : biométrie et focus sur les aspects juridiques
| Synthèse des attaques sur l'authentification et contre-mesures associées

Sécurité des réseaux et des communications
| La sécurité des réseaux : Firewall NG, UTM, WAF, SSE, NDR, ...
| Architecture Zero Trust (ZTA)

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
du 15 au 17 septembre 2025

PARIS
du 11 au 13 juin 2025
du 17 au 19 novembre 2025

VOIR TOUTES LES DATES

| Le standard IPsec, protocoles AH, ESP, IKE et la gestion des clés
| Le protocole SSL/TLS (de SSL v2 à TLS v1.3) et mise en oeuvre avec HTTPS
| La sécurité de l'accès au Cloud (CASB) et le chiffrement des données (BYOK, HYOK, BYOE)
| 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), criticité (CVSS) et cycle de vie
| Les faiblesses dans les applications (CWE)
| 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.

Test et supervision de la sécurité
| Les scanners de vulnérabilités et de configuration
| Les différentes techniques de tests applicatifs (SAST, DAST et IAST).
| Les 7 étapes d'un test d'intrusion : de la préparation de la mission à la remise du rapport
| Le Security Information and Event Management (SIEM) et la gestion centralisée des logs
| Le SOC (Security Operation Center) et technologies associées (UEBA, Deceptive Security, 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.