Formation Concevoir et déployer la sécurité du SI

Code : SEC-STRATEGY-100 Durée : 3 jours (21 heures)

Public visé

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

{{< formation-prerequis >}}

Objectifs pédagogiques

À 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
- Améliorer la communication entre la maîtrise d'ouvrage, la maîtrise d'oeuvre et la SSI
- Effectuer des choix techniques

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, NIS 2

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

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 (MITM), Applications (phishing, DoS, spoofing)
- Attaques sur les mots de passe, injection SQL, CSRF, XSS, injection de commandes, interceptions couche 2 et 3, Hijacking
- Bonnes pratiques de développement
- Évaluer 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, DKIM, SPF, DMARC, S/MIME
- Durcissement des systèmes Windows, Linux et des serveurs Web
- Séparation des flux par VLAN
- Cryptage des données en ligne (VPN SSL et 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
- WAF (Web Access Firewall)
- DLP (Data Lost Prevention) - Data Masking
- IDS/IPS, honeypots

Virtualisation et conteneurisation

- Hyperviseur, Emulateur, Isolation de contexte

BYOD

- Utilisation des équipements personnels
- Enjeux et Risques
- MDM, App Wrapping

Télétravail et Cloud

- TS Web Access, VDI
- 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

- SNMP, Netconf
- SIEM (Security Information and Event Management)
- SOAR (Security Orchestration, Automation and Response)
- SOC (Security Operation Center)
- EMM (Entreprise Mobility Management)
- SecaaS (Security as a Service)

Tendances actuelles

- Intelligence Artificielle et Machine Learning
- Security Self Healing System
- Software Defined Security
- Blockchain

Modalités d'évaluation des acquis

- En début et en fin de formation, une auto-évaluation des connaissances au regard des objectifs pédagogiques du séminaire suivi

{{< formation-require >}}

{{< formation-seealso >}}