

Cybersécurité réseaux / Internet : la synthèse

Référence : **SECRES001**

Durée : **3 jours (21 heures)**

Certification : **Aucune**

Connaissances préalables

- Des connaissances générales sur l'informatique et le réseau Internet sont nécessaires

Profil des stagiaires

- RSSI, DSI, architectes, développeurs, chefs de projets, commerciaux avant-vente, administrateurs système et réseau

Objectifs

- Connaître l'évolution de la cybercriminalité et de ses enjeux
- Maîtriser la sécurité du Cloud, des applications, des postes clients
- Comprendre les principes de la cryptographie
- Gérer les processus de supervision de la sécurité SI

Certification préparée

- Aucune

Méthodes pédagogiques

- 6 à 12 personnes maximum par cours, 1 poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions

Formateur·rice

- Consultant-Formateur expert Cybersécurité

Méthodes d'évaluation des acquis

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

Contenu du cours

1. Sécurité de l'information et cybercriminalité

- Principes de sécurité : défense en profondeur, modélisation du risque Cyber
- Les méthodes de gestion de risques (ISO 27005, EBIOS RM)
- Panorama des normes ISO 2700x
- Évolution de la cybercriminalité
- Les nouvelles menaces (APT, spear phishing, watering hole, Crypto-jacking,...)
- Les failles de sécurité dans les logiciels
- Le déroulement d'une cyberattaque (Kill Chain)
- Les failles 0day, 0day Exploit et kit d'exploitation

2. Firewall, virtualisation et Cloud Computing

- La protection périmétrique basée sur les firewalls et les zones DMZ
- Différences entre firewalls UTM, entreprise, NG et NG-v2
- Produits IPS (Intrusion Prevention System) et IPS NG
- Les vulnérabilités dans la virtualisation
- Les risques associés au Cloud Computing selon le CESIN, l'ENISA et la CSA
- Les solutions CASB pour sécuriser les données et applications dans le Cloud
- Le Cloud Controls Matrix et son utilisation pour l'évaluation des fournisseurs de Cloud

3. Sécurité des postes clients

- Comprendre les menaces orientées postes clients
- Les logiciels anti-virus/anti-spyware
- Comment gérer les correctifs de sécurité sur les postes clients ?
- Ransomware : mesures préventives et correctives
- Comment sécuriser les périphériques amovibles ?
- Les vulnérabilités des navigateurs et des plug-ins
- L'attaque Drive-by download
- Les menaces via les clés USB (BadUSB, rubber ducky,...)

4. Fondamentaux de la cryptographie

- Les techniques cryptographiques
- Les algorithmes à clé publique et symétriques
- Les fonctions de hachage simple, avec sel et avec clé (HMAC)
- Les architectures à clés publiques (PKI)
- Certification CC et qualification ANSSI des produits cryptographiques

5. Authentification et habilitation des utilisateurs

- L'authentification biométrique et les aspects juridiques
- L'authentification par challenge/response
- Les différentes techniques d'attaque (brute force, keylogger, credential stuffing,...)
- L'authentification forte à facteurs multiples (MFA)
- Authentification carte à puce et certificat client X509
- Les standards HOTP et TOTP de l'OATH
- Les standards UAF et U2F de l'alliance FIDO (Fast ID Online)

6. La sécurité des flux réseaux

- Crypto API SSL et évolutions de SSL v2 à TLS v1.3
- Les attaques sur les protocoles SSL/TLS
- Les attaques sur les flux HTTPS
- Le confinement hardware des clés, certifications FIPS-140-2
- Évaluer facilement la sécurité d'un serveur HTTPS
- Le standard IPsec, les modes AH et ESP, IKE et la gestion des clés
- Surmonter les problèmes entre IPsec et NAT
- Les VPN SSL. Quel intérêt par rapport à IPsec ?
- Utilisation de SSH et OpenSSH pour l'administration distante sécurisée
- Déchiffrement des flux à la volée : aspects juridiques

7. Sécurité Wi-Fi

- Attaques spécifiques Wi-Fi
- Comment détecter les Rogue AP ?
- Mécanismes de sécurité des bornes
- Description des risques
- Le standard de sécurité IEEE 802.11i
- Attaque KRACK sur WPA et WPA2
- Les apports de WPA3 et les vulnérabilités DragonBlood
- Authentification des utilisateurs et des terminaux
- L'authentification Wi-Fi dans l'entreprise
- Outils d'audit, logiciels libres, aircrack-ng, Netstumbler, WiFiScanner...

8. Sécurité des Smartphones

- Les menaces et attaques sur la mobilité
- iOS et Android : forces et faiblesses
- Virus et codes malveillants sur mobile
- Les solutions de MDM et EMM pour la gestion de flotte

9. Sécurité des applications

- Application du principe de défense en profondeur
- Applications Web et mobiles : quelles différences en matière de sécurité ?
- Les principaux risques selon l'OWASP
- Focus sur les attaques XSS, CSRF, SQL injection et session hijacking
- Les principales méthodes de développement sécurisé
- Quelle clause de sécurité dans les contrats de développement ?
- Le pare-feu applicatif ou WAF
- Evaluer le niveau de sécurité d'une application

10. Gestion et supervision active de la sécurité

- Les audits de sécurité (scope et référentiels : ISO 27001, RGPD,)
- Les tests d'intrusion (black box, gray box et white box)
- Les plateformes de "bug Bounty"
- Comment répondre efficacement aux attaques ?
- Mettre en place une solution de SIEM
- Mettre en œuvre ou externaliser son Security Operation Center (SOC) ?
- Les technologies du SOC 2.0 (CASB, UEBA, Deceptive Security, EDR, SOAR, machine learning, ...)
- Les labels ANSSI (PASSI, PDIS & PRIS) pour l'externalisation
- Les procédures de réponse à incident (ISO 27035 et NIST SP 800-61 R2)

Notre référent handicap se tient à votre disposition au [01.71.19.70.30](tel:01.71.19.70.30) ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.