EduGroupe
Accompagner pour réussir

Parcours introductif à la Cybersécurité

Référence : **SECINTROC** Durée : **10 jours (70 heures)** Certification : **Aucune**

Connaissances préalables

- Avoir des connaissances générales dans les systèmes d'information et connaître le guide d'hygiène sécurité de l'ANSSI

Profil des stagiaires

- Toutes personnes souhaitant s'orienter vers les métiers de la cybersécurité, notamment les techniciens et administrateurs systèmes et réseaux

Objectifs

- Détenir une vision globale de la cybersécurité et son environnement (enjeux, écosystème…)
- Connaître les différents référentiels, normes et outils de la cybersécurité
- Appréhender les métiers liés à la cybersécurité
- Connaître les obligations juridiques liées à la cybersécurité
- Comprendre les principaux risques et menaces ainsi que les mesures de protection
- Identifier les bonnes pratiques en matière de sécurité informatique

Certification préparée

- Aucune

Méthodes pédagogiques

- Groupes de 4 à 12 personnes
- Présentations interactives avec échanges constants pour contextualiser les concepts et illustrer les enjeux
- Accès à des environnements virtualisés et hébergés dans le cloud
- Etudes de cas réels, exercices en sous-groupes (salles virtuelles)
- Tableau blanc collaboratif
- Sondages/quiz
- Retours d'expérience
- Trames et modèles opérationnels
- Signature d'une feuille d'émargement pour attester de la présence à chaque demi-journée de formation
- Possibilité de choisir entre 10 jours consécutifs ou un découpage (4+3+3) incluant des intersessions d'une à deux semaines

Formateur

- Consultant-formateur expert en Cybersécurité

Méthodes d'évaluation des acquis

- Participation et réalisation d'exercices tout au long de la formation
- Auto-évaluation des acquis par le stagiaire via un questionnaire

- Attestations des compétences acquises et de fin de stage adressée à chaque participant

Contenu du cours

JOUR 1 – Enjeux et panorama de la cybersécurité (7 heures)

• Les enjeux stratégiques et économiques de la cybersécurité
• Profils et motivations des attaquants, cybercriminalité et APT
• Panorama des menaces et cyberattaques récentes
• Les piliers de la cybersécurité : CIDT (Confidentialité, Intégrité, Disponibilité, Traçabilité)
• Organisation de la cybersécurité en France et acteurs clés (ANSSI, CERT-FR, CNIL)
• 🛠 Exercice : cartographie des acteurs et des menaces pour une entreprise fictive

JOUR 2 – Architecture du SI et bonnes pratiques de sécurité (7 heures)

• Connaître son SI et ses points de vulnérabilité
• Réseaux, interconnexions, accès distants, WiFi
• Gestion des identités et des privilèges
• Sécurité physique et contrats
• Supervision et gestion des incidents
• 🛠 TP : mise en place de bonnes pratiques d'hygiène numérique (authentification, MFA, gestion des privilèges)

JOUR 3 - Risques, attaques et cycle offensif (7 heures)

• Outils et méthodes de l'attaquant
• Typologie des attaques (physiques, systèmes, réseaux, applicatives)
• Méthodologies de pentest et cycle offensif
• Unified Kill Chain et MITRE ATT&CK
• 🛠 Quiz interactif : reconnaître le type d'attaque à partir d'un scénario

JOUR 4 - Reconnaissance et collecte d'informations (7 heures)

• Reconnaissance passive (OSINT, veille ouverte)
• Reconnaissance active (scans réseaux & ports)
• Introduction aux outils : Nmap, Metasploit
• 🛠 TP : investigation passive (Google dorking, WHOIS, Shodan) et scan actif contrôlé

JOUR 5 - Exploitation et tests pratiques d'attaques (7 heures)

• Attaques Man-in-the-Middle
• Exploitation de vulnérabilités (CVE)
• Attaques applicatives (SQLi, XSS)
• Post-exploitation et maintien d'accès
• 🛠 Activités : TP exploitation guidée d'une faille, TP Man In the Middle, TP attaques applicatives, TP mise en place d'une backd
un environnement de test

JOUR 6 - Défenses réseau et systèmes (7 heures)

• Sécurité du réseau : pare-feu, segmentation, proxy
• Protection : antivirus, IDS/IPS
• Exemple pratique de sécurisation d'un réseau
• 🛠 TP : mise en place d'une politique de filtrage (firewall) et analyse du trafic

JOUR 7 - Cryptographie et protocoles sécurisés (7 heures)

• Fondamentaux : chiffrement symétrique et asymétrique, signatures numériques
• Autorités de certification et IGC
• Protocoles sécurisés (TLS, SSH, VPN)
• 🛠 TP : mise en œuvre d'un chiffrement et d'un tunnel sécurisé (VPN)

JOUR 8 - Hardening et sécurisation avancée (7 heures)

• Durcissement Linux et Windows
• Sécurisation des équipements réseaux
• Bonnes pratiques de configuration et de supervision
• 🛠 TP : mise en œuvre d'un durcissement système (check-list ANSSI)

JOUR 9 - Gouvernance, référentiels et métiers de la cybersécurité (7 heures)

• Introduction aux normes ISO 27000, ISO 27005 (gestion des risques), ISO 22301 (PCA/PRA)
• Référentiels ANSSI, CIS Controls, NIST Cybersecurity Framework
• Gouvernance de la sécurité, PSSI, chartes utilisateurs et administrateurs
• Les métiers et rôles de la cybersécurité (RSSI, analyste SOC, pentester, auditeur, DPO)
• 🛠 Étude de cas : audit simplifié d'une entreprise fictive avec analyse des écarts

JOUR 10 - Aspects juridiques, veille et prospective (7 heures)

• Obligations légales : CNIL, RGPD, NIS2, LPM, eIDAS
• Les responsabilités en cas d'incident (juridiques et contractuelles)
• La veille cyber : sources (CERT, ANSSI, MITRE, IOC feeds, OSINT)
• L'avenir de la cybersécurité : tendances (cloud, IA, IoT, souveraineté numérique)
• 🛠 Atelier fil rouge : mise en situation finale avec analyse d'incident, recommandations, restitution devant le groupe

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