Cybersécurité : élaborez votre vision stratégique

Référence : **SEACYBERST** Durée : **3 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Aucunes.

PROFIL DES STAGIAIRES

• RSSI, DSI, chefs de projet cybersécurité, responsables cellule de crise, ingénieurs d'études, concepteurs, auditeurs IT et consultants.

OBJECTIFS

• Assurer la continuité d'activité et la sécurité des données dans le cloud. • Comprendre les risques liés à la cybercriminalité et les enjeux de la cybersécurité. • Elaborer une riposte adéquate et proportionnée pour réduire les risques cyber. • Maitriser les aspects techniques, juridiques et organisationnels de la cybersécurité.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité défensive

METHODE D'EVALUATION 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

Comprendre la cybercriminalité et les enjeux

- L'impact économique de la cybercriminalité et le modèle économique du « Crime as a Service »
- Analyse de la menace cyber (CTI) et techniques d'attaque (Framework MITTRE ATT&CK)
- Ransomware (rançongiciel) : la menace cyber numéro 1 dans le monde
- Panorama des cyberattaques contre les entreprises et les infrastructures critiques
- Le rôle des crypto-monnaies (Bitcoin, Dash, Monero, Zcash,…) dans les opérations cybercriminelles

Maîtriser les principes fondamentaux de cybersécurité

- Les 7 principes fondamentaux : défense en profondeur, moindre privilège, besoin d'en connaître,…
- Assurer la cybersécurité via une approche gestion des risques ou par la conformité
- Les vulnérabilités logicielles : identification (CVE), criticité (CVSS) et cycle de vie
- Panorama des normes ISO 2700x et zoom sur l'ISO 27001 & 27002
- Les sources d'informations incontournables (ANSSI, ENISA, NIST, CIS, CSA, OWASP, CESIN, …)

Identifier le cadre juridique et règlementaire

- Les principales lois Cyber en France et la hiérarchie des normes juridiques
- La directive européenne NIS2 (Network and Information Security)
- Le règlement européen pour la protection des données personnelles (RGPD)

- Le règlement européen pour les certifications de sécurité (Cyber Security Act)
- Le règlement européen pour la sécurité de l'IoT et de la supply chain (Cyber Resilence Act)

Organiser la cybersécurité

- La politique de sécurité (PSSI) : structure, application et contrôle
- Le rôle et les responsabilités des RSSI et DPO, leurs relations avec la DSI, la DG et la CNIL
- Les métiers de la cybersécurité : auditeur, pentester, consultant, risk manager, SOC analyst, …
- Sensibilisation à la sécurité : pour qui ? pourquoi ? comment ?
- La charte de sécurité : existence légale, contenu et sanctions

Financer la cybersécurité

- Quel budget faut-il allouer à la cybersécurité ? les recommandations de l'ANSSI
- Comment définir le Return On Security Investment (ROSI) ?
- Quel est l'impact financier d'un incident de sécurité ? exemples et chiffres disponibles
- Financer le risque Cyber par une cyber-assurance : périmètre, garanties et limites

Identifier les principales solutions techniques

- Sécurité réseau : Firewall NG, UTM, WAF, SASE, Zero Trust, NDR, …
- Sécurité des « Endpoints » : antimalware (EPP) et solutions de nouvelle génération (EDR / XDR)
- Chiffrement des systèmes : Bitlocker, Luks, FileVault, Veracrypt, ...
- Protection des clés et des secrets : gestionnaires de mots de passe, TPM, HSM
- Sécurité de l'authentification : MFA, FIDO2, biométrie. Solutions « passwordless »
- Sécurité des développements logiciels : les activités de sécurité applicative d'un Secure SDLC

Sécuriser les données dans le Cloud computing

- Les principaux risques dans le Cloud et les mesures de sécurité associées
- Les solutions de sécurité spécifiques au Cloud : CASB, CWPP, CSPM et SSPM
- Le chiffrement dans le Cloud (BYOK, BYOE) et exigences dans la certification de sécurité EUCS
- Les 5 façons d'évaluer la sécurité d'un fournisseur Cloud
- L'approche française du Cloud souverain vs Cloud de confiance
- L'impact des lois américaines (Patriot Act., FISA et Cloud Act) sur la sécurité des données

Assurer la continuité d'activité

- Principes BC/DR : résilience vs continuité d'activité vs reprise d'activité
- Les fondamentaux de la gestion de la continuité d'activité (BCM)
- Réaliser un bilan d'impact sur l'activité (BIA) : différence avec l'analyse de risques
- Les métriques et exigences de la continuité : SLA, SLO, MTD, RTO, RPO, WRT
- Gestion des sauvegardes de données

Contrôler et superviser la cybersécurité

- Audits de sécurité, tests d'intrusion et programmes de Bug bounty
- Tableaux de bord de sécurité : indicateurs, KPI, KPSI, KRI et référentiels (SP 800-55, ETSI GS ISI, …)
- Agences de notation du risque Cyber (BitSight, SecurityScorecard, Cyrating, …)
- Le rôle et les activités d'un CERT / CSIRT
- Le rôle d'un SOC (Security Operation Center) et les outils SIEM / SOAR pour superviser la sécurité

*Notre **référent handicap** se tient à votre disposition au 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.*