Parcours introductif à la Cybersécurité

Durée: 10 Jours Réf de cours: GKCYBER Version: 1 Méthodes d'apprentissage: Intra-entreprise & sur-mesure

Résumé:

Ce cursus intensif de 10 jours constitue une première immersion dans l'univers de la cybersécurité. Il vise à offrir aux participants une compréhension opérationnelle et stratégique des grands concepts et outils utilisés pour protéger les systèmes d'information. Alternant apports théoriques, cas pratiques, démonstrations techniques et travaux dirigés, la formation permet de maîtriser les fondamentaux de la cybersécurité et de préparer efficacement à une spécialisation future (audit, gestion des incidents, risques, gouvernance, SOC...).
Ce programme a été conçu pour être progressif et immersif, permettant d'acquérir aussi bien les bases normatives que les compétences techniques essentielles via des labs et simulations pratiques réalisables sur machine virtuel
Mise à jour : 16.12.2025

Public visé:

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

Objectifs pédagogiques:

- A l'issue de cette formation, les participants sauront:
- 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

Pré-requis:

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

Contenu:

Journée 1

Démarrage de la formation

- Présentation des enjeux, tour de table des participants, identification des attentes, présentation du déroulé pédagogique et des modalités d'évaluation.

Module 1. Introduction à la cybersécurité

- Enjeux de la sécurité de l'information
- Disponibilité, intégrité, confidentialité
- Terminologie : menace, vulnérabilité, risque...
- Origine et conséquences des menaces
- Sécurité en profondeur

ACTIVITÉ : LAB 1 : Étude de scénarios réels (analyse de risques à partir d'un tableau de bord simplifié)

Module 2.Famille ISO 27000

Présentation des normes ISO/CEI 27001, 27002, 27005, 27035

- Objectifs de chaque norme et complémentarité
- Processus de certification, conformité réglementaire

ACTIVITÉ : LAB 2 : Quiz interactif sur les normes + mini débat : "Une norme, à quoi ça sert ?"

Module 3. Norme ISO 27001

- Architecture de la norme
- Structure HLS
- Revue des chapitres
- Rôle de l'annexe A

ACTIVITÉ : LAB 3 : Quiz d'application sur la structure d'ISO 27001

Journées 2

Module 4. Clauses de la norme ISO 27001

- Étude détaillée des chapitres 4 à 10
- PDCA, documentation, évaluation des risques
- Contexte, leadership, analyse des risques
- Annexe A, SMSI, PDCA

ACTIVITÉ : LAB 4 : Étude de cas "Entreprise X

Journée 4

Module 6 : Gestion des risques

- Définitions, cadres ISO 27005 / 31000
- Méthodes quantitatives
- Matrice de vraisemblance/impact, criticité, scénarios

ACTIVITÉ : LAB 9 : QCM + mini atelier de modélisation de matrice de risques

Module 7 Sécurité défensive

- Traitement des risques : évitement, transfert, atténuation, acceptation
- Mesures de protection
- Mesures techniques, organisationnelles et humaines

ACTIVITÉ : LAB 10 : QCM + sélection de mesures à partir de scénarios proposés

Journée 5

Module 8. Contraintes juridiques

- Loi Godfrain, LPM, Informatique ; libertés
- Réglementation sectorielle

ACTIVITÉ : LAB 11 : QCM réglementaire (français/européen)

Module 9 RGPD et données personnelles

- Historique, définitions
- Règles d'or, DPO, traitement et sous-traitance

ACTIVITÉ : LAB 12 : Étude de cas : mise en conformité fictive d'un site web

Journée 6

Module 10. Scénarios d'attaques

- Types d'attaques (réseau, Wifi, OS, applications)
- Analyse d'attaques : DoS, Man-in-the-Middle, Ransomware, SQLi
- Attaques sur couches réseau, WiFi, OS, App LABS :
- Sniffing réseau avec Wireshark
- Simulation TCP SYN Flood
- Attaque ARP Spoofing en environnement isolé

ACTIVITÉ : LAB 15 : utilisation de OpenSSL : Commandes OpenSSL : génération de clés, encodage, déchiffrement

Module 13. Infrastructure PKI :

- Certificats, composantes, usages (SSL, VPN)

ACTIVITÉ : LAB 16 : Création PKI + Installation Apache avec certificat SSL autosigné

Journée 9

Module 14. Le SOC :

- Rôle, architecture, besoins
- Le SIEM
- Centralisation des logs

ACTIVITÉ : LAB 17 : QCM

Module 15 Gestion d'un SOC :

- Incidents : détection, priorisation, gestion
- CERT, coordination, cadre juridique

Module 16 Gestion des vulnérabilités :

- Processus, responsabilités
- Outils : OpenVAS, Nessus, Qualys
- Plan de remédiation

ACTIVITÉ : LAB 18 : Scan OpenVAS

Module 17. Gestion des menaces (MITRE ATT;CK) :

- Prévention structurée
- Tactiques, techniques, mappage des menaces

ACTIVITÉ : LAB 19 : QCM + étude de scénarios MITRE

Journée 10

Module 18. Plan de continuité d'activité (PCA) :

- Analyse, stratégies, responsabilités
- Analyse d'impact
- Continuité et reprise
- Solutions techniques

: analyse du contexte et des parties intéressées”

ACTIVITÉ : LAB 5 : Comparaison de politiques de sécurité types

ACTIVITÉ : LAB 6 : Matching : relier mesures de l’annexe A à des scénarios de risque

Module 5. Amélioration continue (ISO 27001)

Journée 3

- Indicateurs, journalisation, tableaux de bord
- Audit interne, gestion des non-conformités, actions correctives

ACTIVITÉ : LAB 7 : Simulation d’audit sur un jeu de documentation fictif

ACTIVITÉ : LAB 8 : Correction d’un cas de non-conformité (débrief collectif)

- Injection SQL sur VM vulnérable (DVWA / bWAPP)

ACTIVITÉ : LAB13 : Wireshark, TCP SYN, ARP Spoofing, SQLi

Journée 7

Module 11 Équipements de sécurité

- Firewall, NAT, Proxy, VLAN, DMZ, WAF, IDS
- Analyse de logs, segmentation, audit réseau TP :
- Configuration de VLAN avec Packet Tracer / GNS3
- Tour d’horizon Fortigate (Web demo ou VM)

ACTIVITÉ : LAB 14 : Sécurité avec (Cisco ou Fortigate)

Journée 8

Module 12. Cryptographie :

- Types de chiffrement (Symétrique, asymétrique, hachage)
- Chiffrement symétrique : AES, DES
- Asymétrique : RSA, DSA
- Fonctions de hachage : MD5, SHA-2

ACTIVITÉ : LAB 20 : Cas pratique de plan de continuité (tableau de stratégie + BIA simplifié)

Cas pratique PCA

Module 19. Sécurité applicative (OWASP) :

- OWASP Top 10 : Injection, XSS, CSRF, RCE...
- Burp Suite / ZAP : interception, injection, découverte de vulnérabilités

ACTIVITÉ : LAB 21 : Tests d’injection sur environnement DVWA via Burp / ZAP

- Evaluation finale de fin de parcours
- Clôture de la formation

Méthodes pédagogiques :

Compétences du formateur
Nos formateurs disposent d’au moins 3 ans d’expérience en sécurité informatique, support technique ou administration système/réseau. Leur double compétence professionnelle et pédagogique permet une montée en compétence progressive et concrète sur les fondamentaux de la cybersécurité.
Répartition théorie/pratique Théorie : 50 %Concepts et normes (ISO 27001, RGPD, PCA…) Terminologie cybersécurité, réglementations, gouvernancePrésentation des architectures de sécurité et des cadres de menaces Pratique : 50 %21 labs & TP : scan de vulnérabilités, filtrage réseau, chiffrement, injection SQL, analyse de logs, etc. Mise en œuvre de PKI, audit de conformité, tests d’attaques simulées Études de cas, débats, QCM et restitutions collectives
Méthodes pédagogiques
Animation participative via des outils collaboratifs, partages d’écran, analyses d’études de cas, exercices collaboratifs et activités de groupe simulant des contextes réels.
Matériel fourni : Support de cours au format digital Documentations et outils Les QCM d’entraînement Les fichiers d’exercices et corrigés Les modèles de documents utilisés dans les travaux pratiques

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s’auto-évaluer sur l’atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d’inscription :

• Vous pouvez vous inscrire sur l’une de nos sessions planifiées en inter-entreprises jusqu’à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non