SF FORMATIONS | SAS, société par actions simplifiée au capital social de 1 000,00 € |
N° SIRET 892.767.617.00012 | N° de TVA FR70892767617 ·
Certification Qualiopi n° ATA 135 2024 |Enregistré sous le numéro 768 200 998 82
Cet enregistrement ne vaut pas agrément de l'Etat.

PROGRAMME DE LA FORMATION

PARCOURS INTRODUCTIF À LA CYBERSÉCURITÉ

Format : Classe virtuelle synchrone – 70 h sur 10 jours

Public cible : Toute personne souhaitant s'orienter vers les métiers de la cybersécurité, notamment les techniciens et administrateurs systèmes et réseaux.

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

Objectifs finaux :

- Détenir une vision globale de la cybersécurité et de 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.

Méthodologie pédagogique

Formation construite selon le cycle de Kolb :
1. Expérience concrète : immersion dans un scénario fil rouge où les participants endossent le rôle d'une équipe cybersécurité.
2. Observation réfléchie : analyse des écarts et identification des besoins.
3. Conceptualisation : apports théoriques et cadrage réglementaire.
4. Expérimentation : mise en œuvre dans des ateliers collaboratifs et simulations.

Modalités : classe virtuelle interactive, outils collaboratifs gratuits (Miro, Google Workspace, Padlet, Kahoot), sous-groupes, démos techniques en partage d'écran.

SF FORMATIONS | SAS, société par actions simplifiée au capital social de 1 000,00 € |
N° SIRET 892.767.617.00012 | N° de TVA FR70892767617 ·
Certification Qualiopi n° ATA 135 2024 |Enregistré sous le numéro 768 200 998 82
Cet enregistrement ne vaut pas agrément de l'Etat.

Programme détaillé

Découvrir l'écosystème de la cybersécurité (3h30)
● Enjeux et acteurs majeurs
● Panorama des cybermenaces
● Introduction au scénario fil rouge
Modalités : Brise-glace (Kahoot), analyse guidée d'un incident réel, présentation interactive
Evaluation par Quiz interactif + restitution orale

Connaître les fondamentaux techniques (3h30)
● Systèmes d'information et réseaux
● Principes de sécurité (CIA : Confidentialité, Intégrité, Disponibilité)
Modalités : Schéma collaboratif sur Miro, étude de cas réseau simplifié
Evaluation par QCM en ligne + feedback collectif

Référentiels et normes en cybersécurité (3h30)
● ISO 27001, ANSSI, RGPD
● Bonnes pratiques reconnues
Modalités : Atelier Miro : cartographie des obligations appliquées au fil rouge
Evaluation par restitution orale

Cadre juridique et obligations (3h30)
● Lois et responsabilités
● Impacts pour les entreprises
Modalités : Simulation d'un contrôle réglementaire
Evaluation par grille d'évaluation de conformité

Identifier les menaces et vulnérabilités (3h30)
●Types d'attaques (phishing, ransomware…)
● Failles techniques et humaines
Modalités : Jeu de rôle : identification des failles dans un scénario
Evaluation par tableau de synthèse validé par le formateur

Analyse de risques (3h)
● Méthodes (EBIOS, ISO 27005)
● Priorisation des risques
Modalités : Atelier Excel collaboratif pour hiérarchiser les risques
Evaluation par présentation du plan de priorisation

Outils et solutions de protection (3h30)
● Antivirus, pare-feu, IDS/IPS
● Sauvegardes et chiffrement
Modalités : Démonstration en partage d'écran + exercice de choix d'outils
Evaluation par validation par l'expert

Sécurité des réseaux et systèmes (4h)
● Segmentation réseau
● Supervision et journalisation
Modalités : Atelier de configuration simulée
Evaluation par checklist validée par le formateur

Gestion des accès et authentification (3h30)
● Politiques de mot de passe
● MFA et contrôle d'accès
Modalités : Mise en place d'une politique d'accès dans le scénario
Evaluation par validation de la conformité

Sécurité du poste de travail et mobilité (3h30)
● BYOD, VPN
● Sensibilisation utilisateurs
Modalités : Création d'une fiche de bonnes pratiques
Evaluation par correction collective

Plan de continuité et reprise d'activité (3h30)
● PCA/PRA
● Tests et mises à jour
Modalités : Travail en sous-groupe sur Google Docs
Evaluation par restitution et feedback

Scénario fil rouge

Contexte : "DataSecure Services", PME opérant des services numériques pour des clients B2B, souhaite professionnaliser sa cybersécurité après une série d'incidents (phishing ciblé, exfiltration de données, arrêt de service). Les participants incarnent l'équipe en charge de la mise à niveau du dispositif de sécurité, de la gestion des incidents et de la conformité aux référentiels et obligations applicables. Le scénario se déroule en continu tout au long des 10 jours, avec des jalons quotidiens et des livrables progressifs.

Modalités d'évaluation et livrables

Évaluations formatives :

- Quiz courts (Kahoot/Wooclap) en fin de séquence pour vérifier les acquis.
- Restitutions orales en sous-groupes avec feedback structuré du formateur.
- "Exit tickets" (formulaires rapides) pour vérifier la compréhension des notions clés.
- Observation en situation (jeux de rôle, démos guidées) avec grille critériée.
- Feedback entre pairs lors des ateliers collaboratifs.

Évaluations sommatives :

- Projet fil rouge (60 %) : dossier complet comprenant le tableau de bord cybersécurité, le registre des risques priorisés, un playbook incident et 3 procédures opérationnelles clés.
- Soutenance finale (30 %) : présentation de 10 minutes par groupe, suivie de 5 minutes de questions.
- Quiz de validation (10 %) : vérification des connaissances essentielles (référentiels, risques, outils).

Critères d'évaluation (grille) :

- Exactitude technique et conformité aux référentiels.
- Applicabilité opérationnelle dans un contexte PME/ETI.
- Clarté, structuration et pertinence des priorités.
- Qualité de la communication (orale et écrite) et travail collaboratif.

Livrables fournis (modèles éditables) :

- Cartographie des actifs & dépendances (modèle tableur).
- Registre des risques (trame EBIOS/ISO 27005 simplifiée) avec priorisation.
- Politique de mots de passe et procédure MFA (modèles .docx).
- Procédure de gestion des correctifs (patch management) et calendrier type.
- Procédure de sauvegarde + canevas PRA/PCA (schéma décisionnel).
- Playbook de réponse à incident (phishing et ransomware) + journal de notification (canevas ANSSI).
- Charte utilisateur & bonnes pratiques (version 2 pages + version affichable).
- Kit de sensibilisation (jeu de 6 diapositives, 1 e-mail type, 5 micro-messages).
- Tableau de bord cybersécurité (KPI : taux d'équipements durcis, couverture MFA, MTTD/MTTR, taux de patchs >30j, incidents ouverts/clos, sauvegardes testées).
- Plan de veille (sources, fréquence, responsabilités et critères d'alerte).
- Checklists : durcissement poste (Windows/Linux), sécurité réseau de base, revue périodique des

accès.
- Glossaire des termes clés (niveau introductif).

Dispositifs d'engagement en classe virtuelle :

- Alternance toutes les 15–20 minutes (poll/quiz ↔ apport ↔ atelier).
- Travail en sous-groupes (breakouts) avec rôles tournants (leader, rapporteur, timekeeper).
- Tableaux blancs collaboratifs (Miro) et co-édition (Docs/Sheets) pour produire les livrables.
- Démos courtes en partage d'écran, micro-défis techniques et études de cas fil rouge.
- Rituels d'énergie (icebreakers, checkpoints) et canaux de chat dédiés Q/R.