Formation

Référent Sécurité

Durée : 3 jours – 21h

Cette formation donne les connaissances suffisantes théoriques et pratiques en cybersécurité à ceux qui en portent la responsabilité.

L'objectif de la formation est d'entraîner aux gestes clés en matière de cybersécurité.

Celle-ci place l'apprenant dans la peau d'un hacker pour mieux percevoir les conséquences d'une attaque cyber et acquérir les bons réflexes pour s'en protéger.

Une formation pratique qui alterne théorie et mises en situation, grâce à des démonstrations d'attaques réelles.

Public visé : Profils techniques, responsables de projets techniques

Prérequis : Connaissance de la structuration d'un système d'information

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation, le stagiaire est en capacité de :

- Evaluer les enjeux et impacts d'une attaque cyber sur un système d'information
- Identifier les attaques cybersécurité
- Déceler les vulnérabilités sur les serveurs
- Déceler les vulnérabilités sur les applications WEB
- Mettre en place une stratégie d'automatisation de la sécurité

PROGRAMME

1. Maitriser les enjeux de la cybersécurité

- Connaitre les enjeux juridiques (RGPD, NIS2)
- Identifier les attaques et bonnes pratiques des attaques contre les utilisateurs
- Identifier les principaux types d'attaques sur un SI
- Identifier les différents niveaux de gestion de la sécurité
- Connaître les principes et domaines de la SSI afin de sécuriser son SI
- Connaitre les basiques de la sécurité pour un SI

Travaux pratiques :

Approche offensive : Attaque de serveurs ; Attaque par clé USB ; bruteforce de mots de passe, deepfake

Approche défensive : Scanner automatique les vulnérabilités ; les basiques de sécurité

Informations pratiques

Durée : 3 jours – 21h

Ressources
Supports de cours
70% d'exercices pratiques

Tarifs 2024
En inter : 1990€ HT/stagiaire
En intra : contactez-nous pour un devis

Modalités
Sur inscription
Contact et information par mail
Session de 8 stagiaires minimum

Lieu
Sur site Client, LUPISE
ou distanciel

Accessibilité aux personnes en situation de handicap
Contactez-nous pour étudier la faisabilité de votre demande.

Taux de satisfaction

★ ★ ★ ★ ★

Compétences des formateurs
Nos formateurs sont des spécialistes certifiés de la cybersécurité avec une expérience terrain dans la sécurité des systèmes d'information. Ils ont été validés par notre équipe pédagogique sur le plan des connaissances métiers et sur celui de la pédagogie, et sont évalués régulièrement. Une veille permanente ainsi qu'une pratique régulière dans leur domaine garantit leur niveau d'expertise.

Modalités d'évaluation des stagiaires
Les objectifs sont régulièrement évalués tout au long de la formation moyen de quizz, de mises en situation et de travaux pratiques et formalisés sous forme de grille d'évaluation des compétences en fin de module par le formateur
Le participant complète un test de positionnement en amont et en aval de la formation pour valider les compétences acquises.

Moyens techniques et pédagogiques
Aides audiovisuelles, environnement de formation en ligne, support de cours et exercices, études de cas ou présentation de cas réels, sessions de questions-réponses.

LUPISE

contact@lupise.fr

2. Maitriser la gouvernance de la sécurité

- Conduire une évaluation d'un actif de l'entreprise et des objectifs de sécurité
- Superviser et gérer les incidents cyber
- Identifier les différences entre continuité de l'activité et reprise de activité, plan de gestion de crise
- Mettre en place une organisation SSI dans l'entreprise
- Identifier les différents guides de l'ANSSI, CNIL et Cybermalveillance

Travaux pratiques :

Approche offensive : Gérer une crise Cyber ; Observer les attaques en live sur un serveur compromis

Approche défensive : Appliquer un Business Impact Analysis

3. Appliquer la sécurité dans les systèmes et serveurs

- Sécuriser les composants
- Contrôler, gérer et superviser les accès techniques
- Identifier les services vulnérables dans un environnement cloud
- Sécuriser les flux

Travaux pratiques :

Approche offensive : Hacking de serveurs

Approche défensive : Renforcer les configurations par défaut ; Analyser post mortem

4. Appliquer la sécurité dans les développements applicatifs WEB

- Connaître risques majeurs de la sécurité dans les développements
- Détecter les principales failles applicatives (TOP10 OWASP)
- Savoir appliquer le maintien en sécurité dans le cycle de vie
- Implémenter des coffres forts numériques

Travaux pratiques :

Approche offensive : Exploiter les principales vulnérabilités WEB

Approche défensive : Mettre en place une approche défensive automatisée (DevSecOps)

Informations complémentaires

- **Matériel nécessaire**

Les stagiaires devront être munis d'un PC pendant la formation.

- **Evaluation et validation de la formation**

À la fin de chaque formation, les participants complètent un questionnaire d'évaluation qui est analysé par nos équipes pédagogiques.

Une feuille d'émargement par demi-journée de présence est signée par le stagiaire. A l'issue de la formation, un certificat de réalisation de formation est remis au stagiaire si celui-ci a bien assisté à la totalité de la session.

contact@lupise.fr