Parcours introductif à la Cybersécurité

Description de la formation
Dans un monde de plus en plus informatisé, la sécurité est devenue un enjeu majeur pour toutes les entreprises. Ce parcours de formation, orienté pratique, permettra aux candidats de comprendre les fondamentaux de la sécurité informatique, comme les risques et les menaces qui peuvent atteindre le SI, les conséquences possibles d'une attaque informatique et les mesures de protection nécessaires.
A l'issue de la formation, le stagiaire sera capable de mettre en œuvre de manière opérationnelle les principes fondamentaux, les normes et les outils de la sécurité informatique.

Objectifs pédagogiques
- 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.

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

Modalités pédagogiques
- **Modalité :** Formation réalisée en présentiel ou en distanciel selon la formule retenue.
- **Méthode :** La formation se déroule entre 40% de théorie et 60% de pratique. Le formateur partage des points théoriques et des cas concrets et retours d'expérience (implémentation ISO 27XXX, lacunes de sécurité chez les constructeurs, expérience de Pentest, sécurité en entreprise, …), lance des discussions et échanges entre les stagiaires et propose des TPs, jeux et outils en relation avec le contenu et des mises en pratique. Des TP, non obligatoires, seront proposés et pourront être réalisés par le stagiaire en sus afin de travailler les points essentiels du cours.
- **Support de formation :** Le support de formation utilisé par le formateur est remis au stagiaire à l'issue de la formation.

Modalités techniques
- En format présentiel, le formateur dispose d'une présentation (support de formation), d'un vidéoprojecteur (ou TV), de tableaux blancs et de jeux / d'outils pédagogiques dont des TPs (exemple : scénario complet d'un attaquant puis méthode de sécurisation), d'études de cas (exemple : attaque réseaux via Wireshark pour comprendre les faiblesses réseaux et leurs moyens de sécurisation type « Man in The Middle ») et des jeux de rôle (exemple : après un TP pour définir les méthodes de sécurité et comprendre globalement le TP).
- En format présentiel, le stagiaire a besoin d'un ordinateur pouvant être connecté à internet.
- En format distanciel, le formateur dispose d'une présentation (support de formation), d'une plateforme de visioconférence, d'outils collaboratifs numériques, de TPs (exemple : scénario complet d'un attaquant puis méthode de sécurisation), d'études de cas (exemple : attaque réseaux via Wireshark pour comprendre les faiblesses réseaux et leurs moyens de sécurisation type « Man in The Middle ») et de jeux de rôle (exemple : après un TP pour définir les méthodes de sécurité et comprendre globalement le TP).
- En format distanciel, le stagiaire a besoin d'avoir une bonne connexion internet et d'un ordinateur équipé d'une webcam et d'un micro.

Code
CYB010

Durée
10 jours (70 heures)

Nombre de participants
Entre 4 (minimum) et 12 (maximum) participants.

Profil des stagiaires
Toutes personnes souhaitant apprendre les fondamentaux de la sécurité informatique et/ou souhaitant s'orienter vers les métiers de la cybersécurité, notamment les techniciens et administrateurs systèmes et réseaux.

Sanction de la formation
Attestation de fin de formation.

Accessibilité
Accessible pour les personnes en situation de handicap et aménagement possible en fonction du type de handicap (prévenir avant le début de la formation).

Modalités et délais d'accès
10 jours minimum avant la formation pour une demande de prise en charge.

Modalités de suivi et d'évaluation
- Evaluation préalable.
- Autoévaluation des acquis au cours des exercices et mises en pratiques au cours de la formation.
- Evaluation de fin de formation sous forme de test (QCM) afin de valider l'acquisition des compétences et des connaissances.
- Questionnaire d'évaluation de la satisfaction en fin de formation.
- Feuille d'émargement signée par le(s) stagiaire(s) et le formateur, par demi-journée de formation.
- Attestation de fin de formation.
- Evaluation de suivi à froid (+ 1 mois).

Intervenant
Corentin est **Consultant & Formateur en cybersécurité**. Il conseil les entreprises dans la gestion des risques liés à la sécurité de l'information, ainsi que l'implémentation et la certification d'un SMSI.

Tarifs
- Interentreprises : 4 500,00 € HT
- Intra-entreprise : sur demande

Contenu de la formation

JOUR 01

INTRODUCTION A LA SECURITE INFORMATIQUE

- Enjeux
- Appréhender les termes spécifiques à la sécurité
- Panorama 2021 de la sécurité
- Dimension géostratégique
- Les acteurs
- Les types de métiers
- Organisation de la sécurité
- Menaces risque et vulnérabilités
- Volets techniques de la sécurité
- Volets organisationnels de la sécurité
- Volets physiques de la sécurité
- Mener une veille pro active
- Manager la sécurité
- Aspects juridiques
- Aspects normatifs

JOUR 02

LES FONDAMENTAUX DE LA SECURITE DES SI

- Les volets de protection du SI
- Comprendre et agir avec le CID
- Le chiffrement
- Les droits
- L'authentification
- L'IAM
- Intégrer la mobilité
- Architecture et composants
- SIEM et SOC
- L'esprit du forensique
- Les incidents de sécurités : études et comportements

JOUR 03

LA SECURITE DANS LE CYBERESPACE

- Revue des menaces
- Les types de logiciels malveillants
- Les phases d'une attaque
- Point sur les APT
- La force du Social engineering
- Les attaques physiques
- Les attaques sur les données
- Les attaques sur le web
- Les attaques sur les mails
- Autres vecteurs d'attaques
- Risques encourus
- Réponse à incident : adopter les réflexes et comportements
- Principes de reversing

JOUR 04

SECURITE DES SYSTEMES

- Sécurité des systèmes
- Vulnérabilités du microprocesseur
- Etude des architectures systèmes
- Analyse de la mémoire
- Le BoF
- Le fuzzing
- La séparation des privilèges

JOUR 05

SECURITE DES SYSTEMES (SUITE)

- Hardening linux
- Hardening windows
- Hardening serveurs
- La sécurité dans le cloud
- Droits et devoirs au regard de la règlementation

JOUR 06

SECURITE DES RESEAUX

- Sécurité du réseau
- Tcp-ip : forces et vulnérabilités
- Les composants
- Les équipements de sécurité
- Fw et ids : comprendre, implémenter et agir sur les règles
- Les VPN
- Protocole TLS
- Protocole SSH
- HTTPS

JOUR 07

SECURITE DES RESEAUX (SUITE)

- Les communications unifiées
- Sécurité et IPV6
- Sécurité des systèmes mobiles
- Sécurité et IoT
- Les IGC
- Méthode pour appréhender la sécurisation du réseau
- Exemple d'architectures sécurisées

JOUR 08

INTRODUCTION A LA GOUVERNANCE

- Introduction NIS
- Introduction iso 27000
- Introduction RGPD
- La gouvernance de la sécurité
- La sécurité en mode projet
- Les chartes des utilisateurs
- Charte de l'administrateur système et réseau
- PSSI

JOUR 09

SECURITE DES SYSTEMES INDUSTRIELS

- Introduction aux systèmes de supervision et de contrôle industriel (SCADA)
- Composants et architectures réseau des systèmes SCADA
- Introduction à la sécurité des systèmes SCADA

JOUR 10

WARGAME CTF (CAPTURE THE FLAG)

La dernière journée de formation est dédiée à une mise en situation via un jeu de type « Capture The Flag » (CTF) et en équipe. Il s'agit d'un défi réaliste pour mettre en œuvre les compétences acquises durant cette formation.