Analyste SOC (Security Operations Center)

Description de la formation

A l'issue de la formation, le stagiaire sera capable d'assurer les fonctions d'analyste d'un Security Operations Center (SOC). Cette formation vous permettra d'apprendre diverses techniques telles que l'ingénierie sociale, la détection et l'analyse des intrusions (configurer l'analyse de vulnérabilité, configurer les mises à jour de signature, comprendre l'analyse des logs), l'anticipation et la mise en place des protections nécessaires à travers le durcissement des systèmes d'exploitation et les défenses du périmètre pour analyser et attaquer ses propres réseaux.

Objectifs pédagogiques

- Connaître l'organisation d'un SOC.
- Comprendre le métier d'analyste SOC.
- Appréhender les outils utilisés par les analystes SOC.
- Identifier les principales problématiques à travers des cas d'usage.
- Apprendre à détecter des intrusions.
- Savoir gérer différents incidents.
- Optimiser la sécurité d'un système d'information.

Prérequis

- Connaître le guide sécurité de l'ANSSI.
- Avoir des connaissances en réseau.
- Avoir suivi le parcours introductif à la cybersécurité ou posséder des connaissances équivalentes.

Modalités pédagogiques

- **Modalité :** Formation réalisée en présentiel ou en distanciel selon la formule retenue.
- **Méthode :** La formation se déroule entre 50% de théorie et 50% de pratique. Le formateur partage des points théoriques et des cas concrets, lance des discussions et échanges entre les stagiaires et propose des jeux / outils en relation avec le contenu et des mises en pratique.
- **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.
- 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 et d'outils collaboratifs numériques.
- 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

CYB020

Durée

8 jours (56 heures)

Nombre de participants

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

Profil des stagiaires

Techniciens, Administrateurs Systèmes et Réseaux, Responsables informatiques, Consultants en sécurité, Ingénieurs, Responsables techniques, Architectes réseaux, Chefs de projets…

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 : 3 600,00 € HT
- Intra-entreprise : sur demande

Contenu de la formation

JOUR 01

DEFINITION ET OBJECTIF D'UN SOC

- Les métiers du SOC
- Catalogue de services et fonctions d'un SOC
  - Fonction de prévention de sécurité
  - Fonction de détection
  - Fonction de réaction
- Structure et fonctionnement d'un SOC
  - Processus du SOC
  - Ressource humaine
  - Structure de pilotage
- Les moyens
  - Humain
  - Logistique
  - Applicatif

JOURS 02, 03 & 04

COMPOSANTS ET ARCHITECTURE TECHNIQUE D'UN SOC

- Firewall / Proxy
- IPS/IDS
- Scan de vulnérabilités
- SIEM
- Les différents systèmes

JOUR 05

ASPECTS JURIDIQUES D'UNE MOE D'UN SOC & MISE EN PLACE D'UN SOC

- Phase de conception : DESIGN
- Phase de construction : BUILD
- Phase de démarrage : RUN
- Premier bilan

JOUR 06

GESTION D'UN SOC

- Le contrôle et les indicateurs
- L'amélioration continue
- Le PCA PRA du SOC
- Relation avec les clients et les fournisseurs
- Externaliser le SOC

JOURS 07 & 08

ETUDE SUR UN SOC EXISTANT

Les stagiaires participent à une étude de cas basée sur un SOC existant. L'objectif est de faire découvrir par la pratique et mettant en œuvre les compétences acquises durant la formation.