FORMATION ANALYSTE FORENSIQUE RESEAUX

Ref. ***CAFRX-10***
Durée : 5.0 jour(s) / 35.0 heures

Les cyber attaques font parties du lot quotidien du monde de l'entreprise et du numérique. Il devient alors vital de pouvoir investiguer sur le cyber crime et retrouver tous les éléments utiles pour réagir et être recevable devant la loi.

Cette formation s'inscrit dans un shéma visant à valider les savoirs requis pour les fiches métiers de l'ANSSI suivantes : Responsable du SOC, Opérateur Analyste SOC, Responsable du CSIRT, Analyste réponse aux incidents de sécurité, Analyste de la menace cybersécurité, Consultant cybersécurité, Formateur en cybersécurité.

Pré-requis :

Connaissances des bases des réseaux.
Connaissances des bases systèmes Linux et Windows.
Connaissances des bases de la SSI.
Quelques connaissances en développement peuvent être un plus.

Personnes concernées :

Administrateurs système et réseau.
Ingénieurs système et réseau.
Développeur ayant des bases.
Responsable Sécurité.
Responsable Gestion des incidents.
Analyste Incident de sécurité.

ECSF Metiers associés:
Cyber Incident Responder, Digital Forensics Investigators, Cybersecurity Architect

Objectifs :

À l'issue de la formation, le participant sera en mesure de :

- Reproduire les bonnes pratiques d'investigations numériques
- Sélectionner les outils d'analyse adéquats au contexte
- Interpréter un rapport d'investigation
- Démontrer un scénario d'attaque
- Classifier les types de menaces

- Analyser différents types de données
- Collaborer à la rédaction d'un rapport d'investigation
- Determiner sur la timeline
- Déterminer les axes d'amélioration

Programme :

JOUR 1

Introduction au forensique réseau

Relation avec les autres domaines de la forensique.
Les différents types de preuves
Relation avec les NIDS/IPS
Collecte de preuves
Outils

Evaluation : sélection d'outils.
Analyse scénarios d'attaques avec wirershark, Règles NIDS/IPS, Collecte de preuves

JOUR 2

Journalisation et surveillance

Principes
Conditions préalables pour l'analyse
Analyse de la chronologie
Agrégation et corrélation des sources
Collecte et stockage du trafic
Principes juridiques

Evaluation : collecte et analyse de logs, réalisation de timelines

JOUR 3

Détection

Distinguer le trafic malveillant
Détecter les intrusions
Threat intellingence

Evaluation : mise en situation d'intrusions, détection et mise en place de modèles

JOUR 4

Analyse / Interprétation des données

Méthodologie
Vue d'ensemble
Chaine de contrôle
Rapports
Lessons apprises

Amélioration continue

Evaluation : Analyser un environnement compromis. Rapport, analyse et amélioration continue
Questions ouvertes sur les bonnes pratiques

JOUR 5

Préparation certification

Démarche pédagogique :

Formation orientée sur la pratique
70% de pratique et 30% de théorie
Cybersecurity Educator ECSF

Evaluation et validation :

EXAMEN : PASSAGE DE LA CERTIFICATION DE PERSONNES

Partie théorique et pratique
Le temps destiné au passage de la certification est de 3H.
L'examen est composé de 3 parties :

- QCM,
- Mise en situation sur points spécifiques,
- Mise en situation sur cas concrets.

Bureau Veritas Certification assure l'examen final de ce programme de formation.

L'examen valide des domaines de compétences en relation avec les profils métiers identifiés par l'Europpean union agency for cybersecurity via l'European Cybersecurity Skills Framework