FORMATION Analyste Forensique Niveau 1

Ref. ***CAF1-10***
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 de certification 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 forenscics investigator

Objectifs :

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

- Décrire le processus d'investigation digital
- Reproduire les bonnes pratiques liées à l'analyse forensique
- Organiser l'analyse forensique selon le contexte
- Choisir les outils et méthode à appliquer
- Construire une timeline

- Collecter des preuves

Programme :

JOUR 1

Introduction de la SSI
Le numérique en entreprise
Les risques qui pèsent sur les entreprises
Digital Forensique
Le forensique & le « Digital Forensics »
Comment est apparu le Digital Forensic
Les enjeux du forensique pour une entreprise aujourd'hui
Mener une investigation forensique : la méthodologie
Le contexte d'une investigation : Judiciaire, réponse à incident, scientifique, threat intelligence
Les standards d'une investigation forensique
Les métiers du Digital Forensic

TD QUIZZ sur le processus d'investigation

JOUR 2

L'analyse forensique réseau
Les cas d'utilisation de la forensique en réseau
Les types de sources de données
Les équipements sur lesquels collecter les sources de données
Les protocoles réseau à surveiller
Les traces laissées par une attaque sur le réseau (exemple d'une attaque)
Boîte à outils de criminalistique réseau

TP Prise en main de Wireshark et étude de pcap

L'analyse forensique des journaux
L'utilité de l'analyse des journaux
Les types de journaux
L'importance de l'horodatage
L'analyse des journaux traditionnels
Les outils de l'analyse des journaux traditionnels
L'analyse des journaux moderne : Les SIEM
Les éditeurs de SIEM
La méthodologie de l'analyse des journaux

TP Prise en main de Kibana et analyse forensique des journaux dans la pratique

JOUR 3

L'analyse forensique mémoire
Qu'est-ce que l'analyse mémoire
Pourquoi faire une analyse mémoire ?
Faire un dump mémoire : Les outils
La méthodologie de l'analyse mémoire

TP Prise en main de volatility et analyse de dump de systèmes infectés. Utilisation et choix d'outils

L'analyse de disque dur
Qu'est ce que l'analyse de disque dur
Pourquoi faire une analyse du disque dur ?
Faire une copie du disque dur : Les outils
Les systèmes de de fichiers
La méthodologie de l'analyse de disque dur

TP Prise en main d'Autopsy et analyse de disque dur Windows et Linux. Utilisation et choix d'outils

JOUR 4

L’analyse de fichier
Qu’est-ce que l’analyse de fichiers
Pourquoi faire une analyse de fichiers ?
Les types de fichiers
Anatomie d’un des types de fichiers
La méthodologie de l’analyse de fichier
Les outils

TP Final : Analyser un environnement compromis

JOUR 5

Examen blanc : préparation examen final
Réalisation d'une analyse forensique selon situation, évolution et choix d'outils, réalisation timeline, collecte de preuves

Examen Final:
QCM sur processus d’analyse, bonnes pratiques. Etudes de cas sur divers contextes. Analyse d’un système compromis. Collecte de preuves et élaboration Timeline

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 PERSONNE
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.

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