Réaliser une investigation numérique (sécurité inforensic)

La certification « Réaliser une investigation numérique (Sécurité Inforensic) permet aux apprenants d'acquérir les compétences pour identifier et évaluer l'ensemble des méthodes de rétrospection faisant suite à une menace de sécurité afin de préconiser les mesures d'urgences pour en limiter la propagation.

Prérequis : spécialiste en sécurité informatique, systèmes, réseaux et infrastructure globale. Avoir une appétence pour les différents systèmes d'exploitation.
Public cible : Ingénieur cybersécurité, Consultant forensic, administrateur sécurité
Niveau d'expériences : Une première expérience dans la sécurité informatique.

REFERENTIEL DE COMPETENCES	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
C.1.1 *Utiliser des méthodologies d'investigations numériques dans l'objectif d'une information judiciaire futur en s'appuyant sur les éléments recueillis.*	**E.1- Etude de cas** *Lors de cette mise en situation professionnelle, le/la candidat(e) doit :* *En un temps limité de 4H, à partir d'un besoin exprimé ou généré* *Préparer la méthodologie à appliquer* - *Identifier les différents éléments présents sur la scène d'investigation* - *Conserver les éléments recueillis de la scène d'investigation* - *Analyser à froid* - *Analyser les résultats post mortem* - *Produire un rapport d'investigation* **E.2 Mener une investigation** *Lors de cette mise en situation professionnelle, le/la candidat(e) doit :* - *Identifier la bonne méthode d'investigation en utilisant les outils adaptés (phase de collecte, préparation à l'investigation et choix des outils)* - *Réaliser une investigation à travers différents scénarios* - *Identifier les artefacts d'intérêt de l'étude de cas.* **E.3 Analyser les traces recueillies** *Lors de cette mise en situation professionnelle, le/la candidate doit :* - Produire un rapport des artefacts correspondant à l'étude de cas - Une timeline devra être déduite des artefacts	CRIT 1.1 Les objectifs de l'investigation ont été identifiés Une méthodologie d'investigation numérique a été sélectionnée Le processus retenu permet l'atteinte des objectifs
C.1.2 *Mener une investigation numérique au sein d'un système d'information afin d'en identifier les différents artefacts* d'intérêt.		CRIT 1.2 Les différents artefacts recueillis présent au sein du système d'information ont été relevés et sont investigués
C.1.3 *Discriminer les traces recueillies dans l'objectif de pouvoir les produisent lors d'une information judiciaire.*		CRIT 1.3 Des artefacts correspondant aux scénarios sont recueillis et modélisés et permettent de produire un rapport et le présenter au jury .

Dérouler de l'examen

Après l'étude cas de 4h le candidat présentera un rapport au jury qu'il défendra à l'oral pendant 1h en justifiant la méthode et les outils sélectionnés.

1) *Analyse du rapport par le jury sans candidat*
2) *Présentation du rapport par le candidat devant le jury = 30min*
3) *Question du jury au candidat = 30min*
    a. *Rapport*
    b. *L'étude de cas*
    c. *Technique*
    d. *Qualité oratoire*

Jury de certification

Grille d'évaluation complétée par le jury avec un score minimal de 70/100 pour la validation de l'ensemble des compétences de la certification.

Le jury de certification analysera les éléments de l'étude de cas et de la mise en situation afin de valider la certification.

Grilles de notations

Nom du candidat	***Date***	***Numéro de certification***
Enquête à chaud	*Note sur 20*	*Commentaire du jury*
Conserver les preuves	*Note sur 10*	*Commentaire du jury*
Rapport post mortem ***Qualité*** ***Pertinence*** ***Timeline***	*Note sur 40*	*Commentaire du jury*
Oral ***Expression*** ***Explication*** ***Méthode***	*Note sur 30*	*Commentaire du jury*

Résulta du candidat	***Total sur 100***	***Commentaire du jury***