Investigation numérique (Computer Forensics)

Financement

Formation professionnelle continue
Non conventionnée / sans dispositif

Organisme responsable et contact

M2I FORMATION MERIGNAC
Agnès RICHIR
05.57.19.07.60
a.richir@m2iformation.fr

Accès à la formation

Publics visés :

Demandeur d'emploi
Jeune de moins de 26 ans
Personne handicapée
Salarié(e)
Actif(ve) non salarié(e)

Sélection :

Entretien

Niveau d'entrée requis :

Sans niveau spécifique

Conditions d'accès :

être majeur

Prérequis pédagogiques :

Connaissances généralistes en programmation, réseau et système

Contrat de professionnalisation possible ?

Non

Objectif de la formation

Acquérir des compétences générales sur l'investigation numérique

Contenu et modalités d'organisation

Jour 1 Introduction Qu'est-ce que le Forensic ? Qu'est-ce que le Forensic numérique ? Les cas d'utilisation du Forensic dans une organisation Forensic et réponse à incident Obligations légales et limitations CERT (Computer Emergency Response Team) / CSIRT (Computer Security Incident Response Team) Méthodologie Méthodologie d'investigation légale Audit préalable Enregistrements des preuves (chain of custody) Collecte des preuves Matériels d'investigation Logiciels d'investigation Protection de la collecte Calculs des empreintes de fichiers Rédaction du rapport Investigation numérique "live" Méthodologie live Forensic Pourquoi le live ? Qu'est-il possible de faire ? Présentation de la suite Sysinternals Investigation réseau Enregistrement et surveillance Les différents types de données Acquisition des preuves et sondes Rappel des bases du réseau Présentation des outils connus Identifier une erreur de type ARP (Address Resolution Protocol) Storm Identifier une attaque DHCP (Dynamic Host Configuration Protocol) Starvation Identifier une attaque ARP Spoofing Identifier un scan réseau Identifier une exfiltration de données Identifier un téléchargement via Torrent Exemple de travaux pratiques (à titre indicatif) Trouver des attaques de types ARP Spoofing Jour 2 Forensic Windows Analyse des systèmes de fichiers FAT (File Allocation Table) / exFAT (Extended File Allocation Table) (court) NTFS (New Technology File System) Timeline (MFT) Artefacts Système EVTX (Windows XML Event Log) Analyse base de registre Analyse VSC (Volume Shadow Copies) Autres (Jumplist, prefetch, AMcache) Artefacts applicatifs Navigateurs Messageries Skype / Onedrive / Dropbox Exemple de travaux pratiques (à titre indicatif) Trouver une intrusion via une attaque par Spear Phishing Jour 3 Analyse simple de Malwares Les menaces et leurs mécanismes Etat des lieux démarche et outils (file, nm, readelf...) Mettre en place un environnement de test Sandbox Analyse simple avec Strace, Ltrace et GDB (GNU Debugger) Mécanismes de persistance Techniques d'évasion Analyse mémoire sous Windows Principe Volatility Forensic Linux Analyse de la mémoire vive Volatility avancé (ajout de plugin)

...

Parcours de formation personnalisable ?

Oui

Type de parcours

Individualisé

Validation(s) Visée(s)

> Attestation de fin de formation

Et après ?

Suite de parcours

Non renseigné

Calendrier des sessions

Numéro Carif	Dates de formation	Ville	Organisme de formation	Type d'entrée	CPF	Modalités
00222346	du 01/02/2021 au 31/12/2024	Mérignac (33)	M2I FORMATION MERIGNAC		Non éligible	FPC