Sécurité défensive

Investigation numérique (Computer Forensics)

5 jours (35h00) | ★★★★½ 4,6/5 | SEC-INVFOR | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Document mis à jour le 30/05/2023

Objectifs pédagogiques

- Mettre en pratique les compétences générales sur l'investigation numérique.

Modalités et moyens pédagogiques

Formation délivrée en présentiel ou distanciel* (e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour les cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatique...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

** nous consulter pour la faisabilité en distanciel*

*** ratio variable selon le cours suivi*

Niveau requis

Avoir des connaissances généralistes en programmation, réseau et système.

Public concerné

Développeurs, pentesters et consultants en informatique.

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

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 (Adress 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 plug-in)
- Analyse des principaux artefacts
- Retracer la création d'un profil
- Monter une partition MBR (Master Boot Record) et GUID (Globally Unique Identifier)
- EXT / SWAP

Exemple de travaux pratiques (à titre indicatif)

- *Analyser un simple Malwares*

Jour 4

- Création de la timeline et exploitation des metadatas (STK et Python)
- Analyse des logs systèmes et applications : historique, logins et droits

Investigation Web

- Analyse de logs (déclinaison top 10 OWASP)
- Analyse de base de données
- Scripting Python (RegEx)
- Désobfuscation

– Cas d'usage (analyse d'une backdoor PHP)

Exemple de travaux pratiques (à titre indicatif)

– *Détecter une attaque SQLI (SQL Injection)*

Jour 5

Android

– Présentation d'Android (historique et architecture)
– Installation d'un lab (ADB, genymotion...)
– Dump mémoire
– Analyse des logs, base de données et navigateurs
– Description des valises UFED (Universal Forensic Extraction Device)
– Principe de fonctionnement
– Différentes sauvegardes réalisables
– Analyses via UFED Physical Analyzer
– Scripting avec Python

iPhone

– Présentation iOS et architecture
– Acquisition logique
– Acquisition physique
– Jailbreak
– Analyse des différents artefacts iOS

Examen M2i (en option)

– Prévoir l'achat de l'examen en supplément
– L'examen (en français) sera passé le dernier jour, à l'issue de la formation et s'effectuera en ligne
– Il s'agit d'un QCM dont la durée moyenne est d'1h30 et dont le score obtenu attestera d'un niveau de compétence
– L'examen n'est pas éligible au CPF, mais permettra néanmoins de valider vos acquis

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

Modalités d'évaluation des acquis

– En cours de formation, par des études de cas ou des travaux pratiques
– Et, en fin de formation, par un questionnaire d'auto-évaluation et/ou un examen M2i

Les + de la formation

Un examen M2i permettant de valider vos acquis à l'issue de la formation est disponible sur demande (coût : 120€).