Sécurité défensive

Investigation numérique des réseaux

3 jours (21h00) | ⭐⭐⭐⭐½ 4,6/5 | SEC-INFRES | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Contenu mis à jour le 18/10/2024. Document téléchargé le 08/12/2024.

Objectifs de formation

A l'issue de cette formation, vous serez capable de :

- Décrire les concepts fondamentaux de l'investigation numérique des réseaux
- Identifier les techniques d'acquisition, d'analyse et d'interprétation des données réseau
- Utiliser les outils Windows ou Linux pour la collecte et l'analyse des données réseau
- Appliquer les meilleures pratiques pour sécuriser et documenter les investigations numériques
- Rédiger un rapport et présenter des résultats.

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, 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 certains 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 informatiques...) 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*

Prérequis

Avoir de bonnes connaissances sur le hacking, la sécurité, le modèle OSI et les protocoles TCP/IP.

Public concerné

Administrateurs systèmes et réseau, analystes SOC, RSSI, pentesteurs ou auditeurs.

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 et principes fondamentaux

- Définition et importance de l'informatique légale
- Principes et méthodologies de base
- Les différents types de criminalistique informatique
- Légalité et conformité de la démarche
- Considérations éthiques dans les investigations
- Les méthodes de collecte de preuves numériques
- L'identification et la préservation des preuves
- L'importance de la Timeline
- Le laboratoire d'investigation
- Minimiser les interférences avec le sujet
- Automatiser les processus

Déterminer s'il s'agit d'un incident

- Méthodologie et points d'importance
- Présentation du framework ATT&CK du MITRE et points d'entrée des cyberattaques
- Les signes de compromission (Corrélation ATT&CK)

Les équipements réseaux

- Les enjeux du réseau dans le domaine de l'informatique légale
- Les éléments de base d'un environnement réseau dans le contexte du Computer Forensics
- Les équipements et leurs rôles
  - Switches, Routeurs, Firewalls, Firewalls NG, IPS, IDS, Syslogs, SIEM...
- Les distributions et les outils populaires
  - Kali, Parrot Security OS, BlackArch Linux, CAINE, NST, Tails...
  - Wireshark, Nmap, TCPdump, WINdump, netcat, snort, ettercap, Zeek...

Exemples de travaux pratiques (à titre indicatif)

- *Installation et configuration d'un environnement d'investigation*
- *Déploiement d'outils, dont Nmap et Wirehsark, sur un environnement en mode pont transparent*

La collecte de données

- Les types de données réseau
- Le positionnement de la sonde de capture
- Les méthodes d'acquisition (passives et actives)
- Les outils d'acquisition

- La capture de trafic sur les Appliances
- La capture de trafic en environnement virtuel avec NFV
- L'obfuscation réseau
- L'anti-Forensic et le Timestomping
- La gestion et le stockage sécurisé des données
  - Stratégies de stockage sécurisé
  - Le rôle du hash de l'image
- La documentation des processus de collecte

Exemples de travaux pratiques (à titre indicatif)

- *Capture d'un trafic réseau avec Windows ou Linux*
- *Analyse d'un trafic obfusqué*
- *Documenter les actions réalisées*

Jour 2

L'analyse des paquets

- Structure des paquets réseau
- Identification des protocoles et services
- Types de menaces (DoS, DDoS, Man-in-the-Middle...)
- Filtrage des paquets
- Analyse des sessions TCP
- Les protocoles nécessitant l'attention de l'investigateur
- Techniques de détection et d'analyse des malwares
- Suivre un attaquant exploitant des techniques de rebond

Exemples de travaux pratiques (à titre indicatif)

- *Utilisation d'un analyseur de paquets pour afficher, filtrer, isoler et analyser un trafic spécifique*
- *Détermination de l'usage réel d'un flux réseau*
- *Identification de trafics illégitimes*
- *Documentation des actions réalisées*

Exploitation de sondes IPS et IDS

- Le rôle des IPS et des IDS
- Le positionnement des sondes
- La gestion des paramètres principaux
- La gestion des règles

Jour 3

Exploitation de sondes IPS et IDS - Suite

Exemples de travaux pratiques (à titre indicatif)

- *Installation d'un IPS ou d'un IDS sous Windows ou Linux*
- *Paramétrage de la sonde et de la remontée d'alerte*
- *Création de règles personnalisées correspondant à l'environnement de formation*
- *Détection d'un trafic illégitime en temps réel*

La corrélation

- Création de la Timeline
- Corrélation des éléments entre les différentes analyses

Exemples de travaux pratiques (à titre indicatif)

- *Création d'une Timeline sur la base des éléments collectés dans les travaux pratiques précédents*
- *Détermination du scénario d'attaque de l'ensemble des éléments évoqués*

La rédaction du rapport d'analyse

- Les éléments du rapport
- Le formalisme du rapport
- La diffusion et le stockage du rapport

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

Accessibilité de la formation

Le groupe M2i s'engage pour faciliter l'accessibilité de ses formations. Toutes nos formations sont accessibles aux personnes en situation de handicap : les détails de l'accueil des personnes sont consultables sur la page Accueil PSH.

Modalités et délais d’accès à la formation

Les formations M2i sont disponibles selon les modalités proposées sur la page programme.
Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation.
Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.