

Investigation numérique des réseaux (Computer Forensics)

3 jours (21 heures)

Expertise

Présentiel ou classe à distance

à partir de

2 355 € HT par personne (TVA en vigueur) Repas inclus en présentiel

Contenu mis à jour le 25/09/2026. Document téléchargé le 06/10/2026.

Objectifs

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.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

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

Prérequis

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

Programme

1 Pendant votre formation

Investigation numérique des réseaux (Computer Forensics)

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 Wirehark, 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

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

Modalités 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

Accessibilité aux personnes en situation de handicap

Détails de la session

Du 14 décembre 2027 au 16 décembre 2027 (3 jours / 21 heures)

Paris La Défense

Du 14 décembre 2027 au 16 décembre 2027 Paris La Défense

- 14 décembre 2027 9h00 - 16h00
- 15 décembre 2027 9h00 - 16h00
- 16 décembre 2027 9h00 - 16h00