

Formation Investigation Forensic Windows

Réf. SF34464

Conduire une investigation numérique sur un environnement Windows !

5 j Durée	3 750 € HT Inter / participant	10 250 € HT Intra (≤12 pers.)	0 Sessions à venir
--------------	-----------------------------------	----------------------------------	-----------------------

Objectifs pédagogiques

- ✓ Définir le périmètre d'une investigation et préparer une démarche DFIR/forensic (hypothèses, priorités, risques).
- ✓ Corréler des éléments hétérogènes pour reconstruire une timeline et répondre aux questions d'enquête (quoi / quand / comment / avec quels impacts).
- ✓ Mettre en œuvre une collecte / acquisition pertinente (volatile & persistante) en assurant intégrité, traçabilité et documentation.
- ✓ Formaliser les résultats dans une restitution adaptée.
- ✓ Identifier et exploiter les principaux artefacts Windows utiles à la qualification d'un incident (système, exécution, persistance, activité utilisateur).

Public visé & prérequis

Public visé Administrateurs systèmes et réseaux, Auditeurs, Responsables de la sécurité des systèmes d'information (RSSI)

Prérequis Bonnes bases en sécurité et en administration Windows (concepts OS, comptes, journaux, réseau). Une première exposition à la réponse à incident est un plus.

Programme détaillé

Cadrage & méthodologie d'investigation

Objectifs d'une investigation (techniques, conformité, preuve, aide à la décision)
Définition du périmètre : poste/serveur, compte(s), période, hypothèses, priorisation
Rôles & responsabilités : first responder vs analyste, interactions SOC/CSIRT/IT
Principes de traçabilité : journal d'actions, gestion des accès, conservation des éléments
Bonnes pratiques de traitement de la preuve numérique (référentiels de type ISO/IEC 27037)

Collecte / acquisition & préservation de la preuve

Stratégies d'acquisition : triage vs acquisition complète, volatil vs persistant
Acquisition "à chaud" / "à froid" : impacts, risques, arbitrages
Intégrité : hachage, scellés logiques, contrôles de cohérence, chaîne de possession
Gestion des supports spécifiques : postes distants, VM, supports chiffrés (selon contexte)
Organisation des données : nomenclature, stockage, gestion des volumes et de la confidentialité

Fondamentaux Windows utiles à l'investigation

Rappels OS : comptes, sessions, permissions, services, tâches planifiées
Systèmes de fichiers & horodatages : lecture, interprétation, limites
Registre Windows : structure, logique d'extraction, typologies d'artefacts
Journaux & traces système : Event Logs, traces sécurité, applications et sécurité endpoint
Gestion des pièges classiques : horloges, timezone, nettoyage, artefacts manquants

Artefacts d'exécution, de persistance et d'activité sur le poste

Indices d'exécution et d'utilisation (selon version/paramétrage) : programmes lancés, historique d'ouverture, traces d'installation
Persistance : mécanismes courants (services, tâches, clés registre, démarrage, etc.)
Activité fichiers/dossiers : création, modification, accès, suppressions et récupération

Périphériques & mobilité : USB, Wi-Fi, profils, connexions, empreintes d'usage

Indicateurs de compromission : comportements suspects, anomalies de configuration, contournements

Navigation web, messagerie et usages “utilisateur”

Traces navigateur : historique, téléchargements, cookies/cache (selon navigateur)

Artefacts liés aux documents : pièces jointes, fichiers récents, accès partagés

Messagerie : indices côté poste (client), notions de collecte côté serveur (si applicable)

Scénarios d'attaque orientés utilisateur : phishing, drive-by, pièces jointes malveillantes

Signaux d'exfiltration : volumes, destinations, outils, “data staging” (selon contexte)

Construction du scénario : corrélation & timeline

Méthode de corrélation multi-sources (logs, registre, FS, artefacts applicatifs)

Construction d'une timeline : granularité, normalisation, gestion des incertitudes

Qualification de l'incident : TTP, chronologie, périmètre impacté, zones d'ombre

Documentation : éléments probants, hypothèses, limites, répétabilité

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

Note moyenne des participants de la filière Cybersécurité et Protection des Données : 4,9/5 — 13 avis

William B. — Prévoir l'envoi à chaque participant du livre de CISS au moins un mois avant la formation.

Mickael L. — il est top Romain GARCIA

Ils nous font confiance

Cette année notre filière Cybersécurité et Protection des Données a accompagné plus de 69 entreprises dont :

AVEM MÉTROPOLE DE LYON ACTIMAGE CONSULTING SAS ADISTA ADVENTIEL AIGA ALCYOR ALDORIA ALSTOM ALTEN SA +59 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com