Investigation numérique Windows

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Éligible au CPF : Non

Domaine : Cybersécurité - sécurité informatique

Action collective : Non

Filière : Investigation, réponse à incident

Rubrique : Investigation numérique - inforensic

PRÉSENTATION

Objectifs & compétences

À l'issue de cette formation, les participants seront capables de :
• Comprendre l'objectif et l'utilité d'une investigation numérique
• Collecter les sources d'indices post-compromission sans altérer la preuve
• Exploiter les différents artefacts d'un système Windows
• Retracer un chemin d'attaque
• Restituer l'incident et dresser un plan d'action stratégique de reprise d'activité

Public visé

Administrateurs, RSSI, équipes CERT / CSIRT, Auditeurs

Pré-requis

Bases intermédiaires en systèmes Windows (Fonctionnement, composants)
• Utilisation du terminal et outils open sources (Linux / Windows)
• Connaissances théoriques en techniques offensives (scanning, latéralisation, escalade de privilèges)

PROGRAMME

1. État de l'art de l'investigation numérique

• **Terminologie essentielle**

Cette section aborde les notions fondamentales de l'investigation numérique :

- **Forensic :** Définition et enjeux de la discipline.
- **Chain of custody / chain of evidence :** Description des processus de traçabilité et de préservation des preuves.
- **Artefacts / Evidence :** Identification des éléments numériques exploitables dans une enquête.
- **Timeline :** Utilisation des frises chronologiques pour reconstituer les événements.

• **Réponse à incident : cadre et mise en pratique**

- **Définition**
- **Exemple de cas maîtrisé :** Étude d'un scénario concret pour illustrer les bonnes pratiques
- **CSIRT (Computer Security Incident Response Team) :** Rôle et fonctionnement des équipes dédiées.
- **IOC/IOA (Indicators of Compromise / Indicators of Attack) :** Comment identifier et interpréter les signes d'une intrusion ?

• **Différents types de forensics**

L'investigation numérique se décline en plusieurs spécialités, chacune adaptée à un environnement spécifique :

Code de formation : FORENSICWIN

#CYBERSÉCURITÉ #WINDOWS #FORENSIC

€ Tarifs

Tarif & financement :
Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :
Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.
Le dispositif FNE-Formation.
L'OPCO (opérateurs de compétences) de votre entreprise.
France Travail: sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
CPF -MonCompteFormation
Contactez nous pour plus d'information : contact@aston-institut.com

Lieux & Horaires

Durée : 35 heures

Rythme : 5 jours. 28 Septembre au 2 Octobre 20267 au 11 Décembre 2026

Délai d'accès : Jusqu'a 8 jours avant le début de la formation, sous condition d'un dossier d'inscription complet

Prochaines sessions

Consultez-nous pour les prochaines sessions.

- Forensic réseau
- Forensic système
- Forensic mobile
- Forensic cloud

• **Méthodologie : approches structurées et bonnes pratiques**

• **Méthodologie NIST :** Présentation du cadre proposé par le National Institute of Standards and Technology.
• **Bonnes pratiques :** Recommandations pour garantir l'intégrité des preuves et l'efficacité des investigations.
• **Considérations légales :** Respect des réglementations et des procédures judiciaires.

2. Investigation mémoire de masse

Généralité : les bases de l'investigation sur supports de stockage

Présentation des fondamentaux de l'investigation avec :

- Les différents types de supports (disque dur, SSD, clé USB, etc.)
- Les notions essentielles liées aux structures de démarrage (MBR / BIOS / UEFI)
- Le concept de carving (pour la récupération de fichiers supprimés)

• **Imaging : création et gestion des copies forensiques**

- Définition et objectifs de la création d'une copie forensique
- Les méthodes de réalisation : outils et protocoles pour garantir l'intégrité des données
- Les différents formats d'image utilisées : comparaison des formats utilisés (RAW, EWF, AFF, etc.)

• **Collecte d'artefacts : identification et extraction des preuves**

- Liste les artefacts à collecter selon les objectifs d'investigation
- Présentation des méthodes de collecte via Windows ou via Linux

TP 1 / Acquisition

3. Analyse des artefacts : exploitation des traces numériques

• **Outils d'analyse**

Présentation des principaux outils pour extraire et analyser les artefacts Windows (Autopsy / The Sleuth Kit, Zimmerman Tools, Nirsoft, Plaso)

• **Artefacts liés au système de fichiers (NTFS / HDD)**

- Fonctionnement du système de fichiers NTFS
- L'importance du $MFT pour retracer les fichiers et leurs métadonnées
- Les techniques de timestomping pour falsifier les horodatages

• **Artefacts internet**

- Les traces laissées par la navigation web : historique, cookies, cache, téléchargements, signets et mots de passe
- La zone Identifier qui renseigne sur l'origine des fichiers

• **Artefacts d'exécution**

Présentation de différents outils liés à l'exécution des programmes (Prefetch, ShimCache, AmCache, UserAssist, Jump Lists, SRUM)

• **Artefacts liés des fichiers/dossiers**

Artefacts permettant de reconstituer l'activité de l'utilisateur (LNK Files, Recent Files, Shellbags, Recycle Bin, Thumbcache)

• **Artefacts USB**

Même approche avec Registre USB, Log PnP, PID / VID, setupapi

TP 2 / Analyse des artefacts

• **Artefacts réseau**

Comprennent la configuration IP, l'historique réseau et les logs WLAN pour retracer les connexions, les réseaux fréquentés et les échanges réalisés

• **Artefacts d'authentifications**

Présentation des journaux d'authentification, local

• **Artefacts Active Directory**

Reconstitution de l'état et l'évolution du domaine en abordant les éléments persistants, les attributs de réplication et l'utilisation d'outils comme ADTimeline

• **Persistances Windows**

- Détail des mécanismes utilisés pour se lancer au démarrage : clés RUN, services, tâches planifiées, WinLogon
- Méthodes pour automatiser la recherche de ces artefacts

TP 3 / Compromission du SI

4. Analyse de mémoire volatile

• **Acquisition**

- Avantages et inconvénients de l'acquisition mémoire : Types de dump et d'espace
- Méthodologie d'acquisition pour garantir l'intégrité des preuves

• **Volatility**

- Présentation de ce framework d'analyse mémoire
- Notion de profiles
- Différence entre Volatility 2 et Volatility 3
- Modules d'analyses

TP 4 / Analyse de la mémoire

5. Live Forensic

• **Principe**

Avantages / inconvénients

• **Collecte d'informations**

Présentation des outils pour collecter des artefacts : sysinternals, Bento

• **Automatisation**

Automatisation de la collecte et de l'analyse avec :

- OSQuery
- Velociraptor
- GRR Rapid Response
- Playbook & procédures pour standardiser les actions
- Plateforme SOAR pour orchestrer les enquêtes et déclencher les réponses automatisées

MODALITÉS

Modalités

Modalités : en présentiel, distanciel ou mixte – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise

Pédagogie : essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.

Ressources techniques et pédagogiques : Support de formation au format PDF ou PPT, Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom

Pendant la formation : mises en situation, autodiagnostics, travail individuel ou en sous-groupe sur des cas réels

Méthode

Fin de formation : entretien individuel

Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation

Assiduité : certificat de réalisation (validation des acquis)