

Analyse inforensique avancée et réponse aux incidents – niv perfectionnement et expert

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Éligible au CPF : Non

Domaine : Cybersécurité - sécurité informatique

Action collective : Non

Filière : Investigation, réponses à incidents

Rubrique : Investigation numérique - inforensic

Code de formation : AIRI2

€ Tarifs

Prix public : 1400 €

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

PRÉSENTATION

Objectifs & compétences

Réaliser une investigation numérique sur le système d'exploitation Windows

Public visé

Administrateurs, analystes SOC et ingénieurs sécurité.

Pré-requis

Avoir des connaissances sur l'IOS Windows, TCP/IP, Linux - Avoir suivi le cours Ref AIRI1

PROGRAMME

Programme détaillé

Etat de l'art de l'investigation numérique

- Introduction à l'investigation numérique
- Lien entre les différentes disciplines Forensics
- Méthodologie d'investigation légale (chaîne de custody, rapport et méthode OSCAR)
- Vocabulaire et taxonomie
- Les différents OS Windows
- Les fondamentaux Windows
- Fondamentaux Windows
- Système de fichiers / Arborescence
- Séquence de boot Windows
- Base de registre
- Logs (evtx, log pilotes...)
- Variables d'environnements
- Services et les différents accès (services.exe, Powershell)
- Fondamentaux FAT32
- Fondamentaux NTFS (New Technology File System)

Exemple de travaux pratiques (à titre indicatif) Analyse d'un disque

Collecte des données

- Les outils du marché (SleuthKit)
 - Présentation du Framework ATT&CK du MITRE et points d'entrées des cyberattaques
 - Arbres d'attaque
 - Les signes de compromissions (corrélation ATT&CK)
 - Collecte des données physique et virtualisation
 - Présentation du Lab
 - Exemple de travaux pratiques (à titre indicatif)
- Collecte de données

Artefacts

📍 Lieux & Horaires

Durée : 14 heures

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

📅 Prochaines sessions

Consultez-nous pour les prochaines sessions.

Différents artefacts Internet

- Pièces jointes
- Open / Save MRU
- Flux ADS Zone. Identifier
- Téléchargements
- Historique Skype
- Navigateurs internet
- Historique
- Cache
- Sessions restaurées
- Cookies

Différents artefacts exécution

- UserAssist
- Timeline Windows 10
- RecentApps
- Shimcache
- Jumplist
- Amcache.hve
- BAM / DAM
- Last-Visited MRU
- Prefetch

Différents artefacts fichiers / dossiers

- Shellbags
- Fichiers récents
- Raccourcis (LNK)
- Documents Office
- IE / Edge Files

Différents artefacts réseau

- Termes recherchés sur navigateur
- Cookie
- Historique
- SRUM (ressource usage monitor)
- Log Wi-Fi

Différents artefacts comptes utilisateur

- Dernières connexions
- Changement de mot de passe
- Echec / réussite d'authentification
- Evènement de service (démarrage)
- Evènement d'authentification
- Type d'authentification
- Utilisation du RDP (Remote Desktop Protocol)

Différents artefacts USB

- Nomination des volumes
- Evènement PnP (Plug et Play)
- Numéros de série

Différents artefacts fichiers supprimés

- Tools (recurva...)
- Récupération de la corbeille
- Thumbcache
- Thumb.db
- WordWheelQuery

Exemples de travaux pratiques (à titre indicatif) Recherche d'un spear shipping Retracer l'exécution d'un programme Découverte d'un reverse shell Analyse eternal blue Première investigation

MODALITÉS

Modalités

Modalités : en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – 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, autodiagnostic, 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.

Validations des acquis : grille d'évaluation des acquis établie par le formateur en fin de formation.