Analyse Inforensique Windows – Niveau Initiation

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Domaine : Cybersécurité - sécurité informatique

Filière : Investigation, réponses à incidents

Rubrique : Investigation numérique - inforensic

Éligible au CPF : Non

Action collective : Non

PRÉSENTATION

Objectifs & compétences

Découvrir une investigation numérique sur un ordinateur Windows Avoir les bases de l'analyse du numérique sur un serveur web Acquérir les médias contenant l'information Connaître les informations pertinentes et les analyser Découvrir les logiciels d'investigation numérique Connaître le processus de réponse à un incident

Public visé

Administrateur, analyste SOC, ingénieur sécurité

Pré-requis

Connaissances sur l'OS Windows, TCP/IP, Linux

PROGRAMME

Programme détaillé

Section 1

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, Chaîne des évidences)
Présentation du framework ATT & CK du MITRE et points d'entrées des cyberattaques Arbres d'attaque Les signes de compromissions (Corrélation ATT&CK) Vocabulaire, taxonomie Les différents OS Windows

Section 2

Les fondamentaux Windows Système de fichier /arborescence Séquence de boot Windows Base de registre Logs (evtx, log pilotes, etc)
Variables d'environnements Services et les différents accès (services.exe, Powershell) Fondamentaux FAT32 Fondamentaux NTFS

Section 3

Collecte des données Les outils du marché (KAPE, Arsenal, FTKimager, Plaso, Hindsight…)
Collecte des données physique et virtualisation
Présentation du Lab Exemple de travaux pratiques
TD1 Analyse d'un disque
TP1 Analyse d'un disque
TP2 Questionnaire de connaissance
TD2 Collecte de données (en continue)

Modalité d'évaluation des acquis Auto-évaluation des acquis par la stagiaire via un questionnair

Code de formation : AIW1

€ Tarifs

Prix public : 700 €

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 : 7 heures

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

Prochaines sessions

Consultez-nous pour les prochaines sessions.

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