Analyse Inforensique Windows – Niveau Perfectionnement

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Éligible au CPF : Non

Domaine : Développement

Action collective : Non

Filière : Développement - Microsoft

Rubrique : Power Platform

PRÉSENTATION

Objectifs & compétences

Gérer 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 Trier les informations pertinentes et les analyser Utiliser les logiciels d'investigation numérique Maîtriser le processus de réponse à un incident

Public visé

Administrateur, analyste SOC, ingénieur sécurité

Pré-requis

Connaissances su l'OS Windows, TCP/IP, Linux Avoir Suivi le cours Réf: AIW1

PROGRAMME

Programme détaillé

Section 1

Artefacts
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 wifi

Différents artefacts comptes utilisateur Dernières connexions – Changement de mot de passe – Echec /Réussite d'authentification – Evènement de service (démarrage) – Evènement d'authentification – Typed'authentification – Utilisation du RDP

Différents artefacts USB Nomination des volumes - Evènements PnP (Plug& Play) – Numéros de série

Différents artefacts fichiers supprimés Tools – Récupérations de la corbeille – Thumbcache – Thumb.db – WordWheelQuery Spécificités Active Directory

Exemple de travaux pratiques TP1 Première investigation
Modalité d'évaluation des acquis Auto-évaluation des acquis par la stagiaire via un questionnaire

Code de formation : AIW2

€ 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.
- **Pôle Emploi** sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
- **CPF** -MonCompteFormation

Contactez nous pour plus d'information

Lieux & Horaires

Durée : 14 heures

Délai d'accès :
Jusqu'à 8 jours avant le début de la formation

Prochaines sessions

Consultez-nous pour les prochaines sessions.

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)