

Analyse inforensique avancée et réponse aux incidents – 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 : AIRI3

€ 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

Techniques avancées pour 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'OS Windows, TCP/IP, Linux

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

PROGRAMME

Programme détaillé

Techniques avancées

- VSS (Volume Shadow Copy Service)
- Carving
- Anti-Forensic et timestomping
- Spécificités Active Directory (AD)
- Exemple de travaux pratiques (à titre indicatif)

Recherche d'artefact sur AD Introduction à Volatility

- Données volatiles
- Analyse d'un dump mémoire
- Extraction et analyse des process

Exemple de travaux pratiques (à titre indicatif) Recherche d'un malware à l'aide de Volatility

Exemple de travaux pratiques Détail des exercices, TD et TP dans le programme ci-dessus

Modalité d'évaluation des acquis En cours de formation, par des études de cas ou des travaux pratiques

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, autodiagnosics, 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.