

# Analyse Inforensique Windows – Niveau 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 :** AIW3

## PRÉSENTATION

### Public visé

Administrateur, analyste SOC, ingénieur sécurité

### Pré-requis

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

**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](mailto:contact@aston-institut.com)

## PROGRAMME

### Programme détaillé

#### Section 1

Techniques avancées VSS Carving Anti-forensic et Timestomping

#### Section 2

Introduction à volatility Données volatiles Analyse d'un dump mémoire Extraction et analyse des process

Exemple de travaux pratiques

TP1 Exercices d'investigations

TP2 Recherche d'un malware à l'aide de Volatility

Modalité d'évaluation des acquis Auto-évaluation des acquis par la stagiaire via un questionnaire Examen pour l'obtention d'un Badge Investigation numérique Windows ESD Academy (Prévoir un supplément de 495 €/examen/stagiaire)

## 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.

## 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.