

# Investigation numérique Linux

## 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 :** INL

## PRÉSENTATION

### Objectifs & compétences

acquérir les compétences et la méthodologie pour une investigation numérique sur les systèmes GNU / Linux. La méthodologie et l'étude des différents artefacts sont développées et mises à jour régulièrement afin que le candidat puisse pratiquer ce qu'il a vu en formation sur les dernières versions des systèmes GNU / Linux.

### Public visé

administrateur, analyste SOC, ingénieur sécurité.

### Pré-requis

connaissance sur les OS Windows, TCP/IP, Linux.

## € Tarifs

**Prix public :** 3349 €

### 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)

## Lieux & Horaires

**Durée :** 28 heures

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

## PROGRAMME

### Jour 1 matin

#### Section 1

- La réponse à incident et l'investigation numérique Normes et méthodologies NIST / SANS PRIS / ISO Cadre légal

#### Section 2

- Linux : Concepts fondamentaux Jour 1 après-midi

#### Section 3

- Live Forensics Sources et commandes associées Outils

#### Section 4

- Prélèvement Concepts et Pré-requis

### Jour 2 matin

#### Section 5

- La mémoire vive Prélèvement Physique Virtualisée Validation du prélèvement Chain of custody /evidence Analyse Fonctionnement de Volatility 2/3 Concepts (profil, vtype, volshell) Liste des modules + méthodologie TP Jour 2 après-midi

#### Section 6

- La mémoire vive (TP/TD) TP/TD

### Jour 3 matin

#### Section 7

## Prochaines sessions

Consultez-nous pour les prochaines sessions.

– La mémoire de masse Prélèvement Physique Virtualisée

### Jour 3 après-midi

#### Section 8

- Analyse Concepts (ext4, VFS, ...) Timeline Génération et analyse Artefacts Services  
Journalisation système logs

### Jour 4 matin

#### Section 9

– Cas d'étude 1 Exploitation d'un frontal web

#### Section 10

– Cas d'étude 2 Exploitation de la CVE-2012-22205 Jour 4 après-midi

#### Section 11

– Cas d'étude 3 Rootkit Userland

## 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.