

Analyse inforensique avancée et réponse aux incidents – niveau initiation

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 : AIR11

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

[Contactez nous](#) pour plus d'information

PRÉSENTATION

Objectifs & compétences

Les bases de la réponse à incident et de l'analyse inforensique Approche de l'analyse inforensique sur les principaux domaines techniques Analyses ciblées et exercices avancés

Public visé

Professionnels IT en charge de la sécurité des systèmes d'information, l'investigation légale et la gestion d'incidents

Pré-requis

Avoir des connaissances sur l'IOS Windows, TCP/IP, Linux

📍 Lieux & Horaires

Durée : 7 heures

Délai d'accès :

Jusqu'à 8 jours avant le début de la formation

PROGRAMME

Programme détaillé

Mise en place de la réponse à incident

Préparation à la réponse à incident

Détection et analyse

Classification et classement par ordre de priorité Notification Confinement Investigation inforensique Eradication et reprise d'activité Procédure post-incident Que dis la norme ISO 27035 Les systèmes de fichiers Systèmes de fichiers Windows Systèmes de fichiers Linux/BSD L'analyse inforensique et la législation Française Exemple de travaux pratiques

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

📅 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, 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 (validation des acquis)