



L'ANALYSE APRES INCIDENT (ANALYSE FORENSIC)

Objectifs pédagogiques

Comprendre comment constituer un dossier juridique suite à l'intrusion d'un tiers dans le Système d'informations d'une entreprise.

Public	DSI, Maîtrise d'ouvrage, Directeur de projet, chef de projet et toute personne impliquée dans le domaine de la cybersécurité.
Prérequis	Bonne connaissance de cybersécurité.
Compétences visées à l'issue de la formation	<ul style="list-style-type: none">■ Connaître les principes généraux des aspects juridiques■ Maîtrise de la mise en pratique de l'analyse
Déroulement de la formation	Cours théorique en présentiel.
Modalités pédagogiques	<p>Centrées sur l'acquisition de compétences opérationnelles et dans un objectif d'emploi, les modalités pédagogiques s'appuient sur un dispositif de cours en présentiel.</p> <p>Pendant toute leur formation, les apprenants ont accès à des cours en centre et à une plateforme pédagogique en ligne leur permettant d'accéder à des ressources complémentaires.</p> <p>Les modalités pédagogiques précises de chaque formation sont communiquées aux futurs apprenants au cours de leur entretien de recrutement avec le responsable de formation.</p>
Durée	3 jours (21 heures)
Horaires	9h00 - 17h00 Pausas : 11h / 15h Déjeuner : 12h30 - 13h30
Dates et lieu	Dates : voir le planning de formation Cyber Sécurité Lieu : Toulouse
Délai d'accès	<p>Le délai d'accès à une formation monétique GLS2i Software est compris entre 2 et 3 semaines, selon le calendrier de la formation et le dispositif de financement mobilisé.</p> <p>Anticipez dès maintenant votre projet de formation.</p>
Tarifs	<p>En inter : 1500 € HT (déjeuners inclus)</p> <p>En intra : demandeur un devis</p>
Méthodes et matériels mobilisés	Un ordinateur portable sera exigé.
Méthodes d'évaluation	Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mise en situation, travaux pratiques...



L'ANALYSE APRES INCIDENT (ANALYSE FORENSIC)

Accessibilité	La formation est accessible aux personnes à mobilité réduite.
Formateurs	Les formateurs disposent de compétences pédagogiques, fonctionnelles et techniques dans le domaine de la nouvelle technologie et la cybersécurité .
Support	le support de cours « Analyse après incident » au format PDF sera remis à chaque participant en début de la formation.



L'ANALYSE APRES INCIDENT (ANALYSE FORENSIC)

Programme de la formation

- **Présentation générale**
- **Les aspects juridiques**
 - Les bases légales de la sécurité de l'information,
 - La classification des crimes informatiques,
 - Le rôle de l'enquêteur et de l'infoperspective (Forensic data analysis),
 - Les acteurs technico-juridiques (**CERT-FR** (centre gouvernement de veille d'alerte, et de réponse aux attaques informatiques), agences nationales, gendarmerie...)
- **La détection de l'incident**
 - Repérer les anomalies,
 - Passage en revue des outils de détection d'incident,
 - Mise en œuvre d'un IDS / IPS
- **Mise en pratique au travers de l'analyse d'un système informatique**
 - Analyse des anomalies,
 - Établissement de l'incident de sécurité,
 - Diagnostic technique et neutralisation de la menace,
 - Recherche de l'origine de l'attaque,
 - Mise en place de contre-mesures
- **Débriefing et conclusion**



O.F. Déclaration d'activité N° 76311168831
la préfecture de la région Occitanie
Mise à jour le 03/03/2024

L'ANALYSE APRES INCIDENT (ANALYSE FORENSIC)

Notes