



## LE HACKING ET LA SECURITE

### Objectifs pédagogiques

Comprendre les techniques de collecte d'information et de mesure de la vulnérabilité d'un système cible et apprendre à mettre en œuvre les contre-mesures appropriées.

<b>Public</b>	DSI, Maîtrise d'ouvrage, Directeur de projet, chef de projet et toute personne impliquée dans le domaine de la cybersécurité.
<b>Prérequis</b>	Bonne connaissance de la cybersécurité.
<b>Compétences visées à l'issue de la formation</b>	<ul style="list-style-type: none"><li>■ Les fondamentaux de hacking et de la sécurité</li><li>■ Hacking et sécurité avancée</li></ul>
<b>Déroulement de la formation</b>	Cours théorique en présentiel.
<b>Modalités pédagogiques</b>	<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>
<b>Durée</b>	3 jours (21 heures)
<b>Horaires</b>	9h00 - 17h00 Pause : 11h / 15h Déjeuner : 12h30 - 13h30
<b>Dates et lieu</b>	<b>Dates :</b> voir le planning de formation Cyber Sécurité <b>Lieu :</b> Toulouse
<b>Délai d'accès</b>	<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>
<b>Tarifs</b>	<p>En inter : 1500 € HT (déjeuners inclus)</p> <p>En intra : <b>demandeur un devis</b></p>
<b>Méthodes et matériels mobilisés</b>	Un ordinateur portable sera exigé.



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

## LE HACKING ET LA SECURITE

<b>Méthodes d'évaluation</b>	Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mise en situation, travaux pratiques...
<b>Accessibilité</b>	La formation est accessible aux personnes à mobilité réduite.
<b>Formateurs</b>	Les formateurs disposent de compétences pédagogiques, fonctionnelles et techniques dans le domaine de la nouvelle technologie et la cybersécurité .
<b>Support</b>	le support de cours « <b>Le hacking et la sécurité</b> » au format PDF sera remis à chaque participant en début de la formation.



## **Programme de la formation**

- **Les fondamentaux de la sécurité des réseaux**
- **Les attaques à distance**
- **Les attaques système**
- **La sécurité du système :**
  - les outils de base permettant d'assurer le minimum de sécurité à un S.I.,
  - la cryptographie,
  - le chiffrement des données,
  - la détection d'activité anormale,
  - le rôle de la base de registre,
  - le firewalling, l'anonymat
- **Protocole TCP/IP**
- **Veille technologique (vocabulaire spécifique ...)**
- **Collecte d'informations**
- **Mesure de la vulnérabilité par scan et prise d'empreinte**
- **Recherche de failles : vulnérabilités réseau, applicative, web etc.**
- **Etude des cas : Mise en oeuvre d'une stratégie d'attaque**
- **Conclusion et débriefing**



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

---

## LE HACKING ET LA SECURITE

---

### Notes