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

LA CRYPTOGRAPHIE

Objectifs pédagogiques

- Comprendre les bases de la cryptographie ainsi que les algorithmes
- Comprendre les différents niveaux d'attaques
- Comprendre la sécurité liée à la cryptographie ainsi que l'architecture d'utilisation des clés

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 la cybersécurité.
Compétences visées à l'issue de la formation	▪ Maîtriser les techniques de la cryptographie
Déroulement de la formation	Cours théorique en présentiel.
Modalités pédagogiques	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. 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. Les modalités pédagogiques précises de chaque formation sont communiquées aux futurs apprenants au cours de leur entretien de recrutement avec le responsable de formation.
Durée	5 jours (35 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	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. Anticipez dès maintenant votre projet de formation.
Tarifs	En inter : 2000 € HT (déjeuners inclus) En intra : **demander un devis**
Méthodes et matériels mobilisés	Un ordinateur portable sera exigé.

LA CRYPTOGRAPHIE

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…
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 « **La cryptographie** » au format PDF sera remis à chaque participant en début de la formation.

Programme de la formation

- **Présentation générale**
- **Comprendre les concepts de base de la cryptographie**
  - La terminologie
  - Les acteurs
  - Les concepts du chiffrement
  - Les secrets
  - Les clés
  - Les fonctions
- **Comprendre les algorithmes**
  - Les classes d'algorithmes
  - Les algorithmes classiques
  - Les algorithmes modernes : DES, 3DES,… AES
  - Du RSA vers les courbes elliptiques
- **Comprendre les bases de la cryptanalyse**
  - Les niveaux d'attaques
  - Les attaques "Force Brute"
  - Les attaques par dictionnaire
  - Les compromis espace-temps
- **Comprendre la sécurité liée à la cryptographie**
  - Les besoins (les biens concernés)
  - Les analyses de risques
  - Un exemple d'application sur le système "Carte bancaire"
  - Les architectures et principes de sécurité
  - Les fonctions
  - Un exemple de transaction monétique sécurisée
- **Comprendre l'architecture d'utilisation des clés**
  - La génération des clés – Les cérémonies de clés
  - La distribution de clés
  - Les certificats et la chaîne de Certificats
  - Les enceintes sécuritaires : HSM, modules cryptographiques, etc.
- **Conclusion et débriefing**

Notes