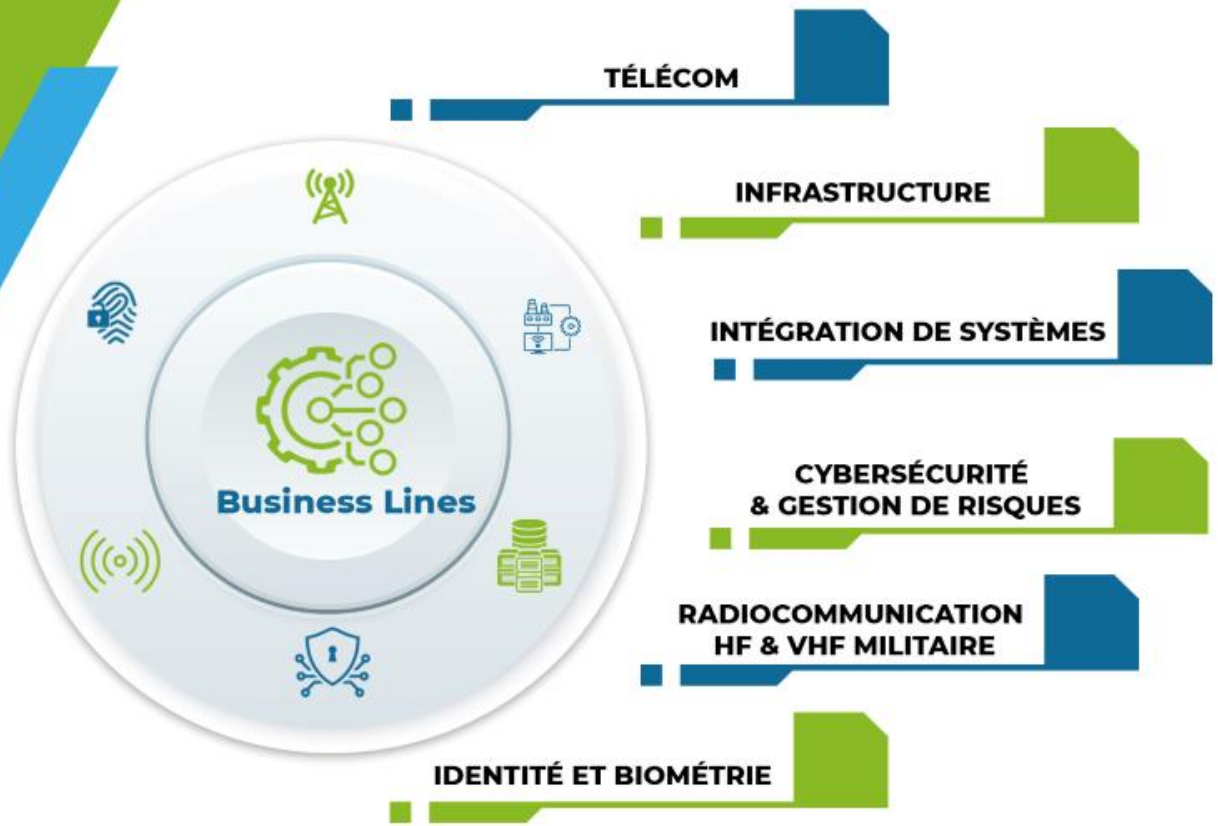
SANCFIS

Côte d'Ivoire Sénégal Ghana Mali Bénin Niger Cameroun Burkina faso Guinée

Modules de Formation Cyber sécurité



1. Fondamentaux de la cybersécurité pour l'informatique (4 jours)

Introduction

L'objectif du cours est de permettre aux participants de se concentrer sur les concepts fondamentaux de la cybersécurité etsensibiliser les professionnels de l'informatique. Le cours est particulièrement adapté aux personnes faisant partie d'une équipe informatique.Les praticiens de la sécurité générale, les administrateurs système, les professionnels de l'informatique et les architectes de la sécurité bénéficieront de la compréhension de la conception, de la construction et de l'exploitation de leurs systèmes pour atténuer les cyberattaques.

Le contenu des cours

- **Introduction à la cybersécurité**
  - Historique des événements marquants de la cybersécurité
  - Définitions et références de la cybersécurité
  - Les étapes d'une cyberattaque
- **Gestion des risques et menaces**
  - S'assure du respect de l'évolution des lois et des réglementations applicables
  - Mises à jour constantes sur la stratégie de cybersécurité pour tirer parti des nouvelles technologies et des informations sur les menaces
  - Concepts critiques de la sécurité d'entreprise
  - Fournit la politique de sécurité à l'autorité compétente pour assurer son application
  - CIA Triad, confidentialité, fiabilité, répudiation et contrôle d'accès
- **Sécurité des réseaux, sécurité des systèmes et sécurité des applications**
  - Meilleures pratiques de renforcement
  - Echanges et sécurité des données
  - Outils d'analyse de vulnérabilité
  - Produit et technologies (AV, IDS, IPS, SIEM)

1. Fondamentaux de la cybersécurité pour l'informatique (suite)

- **Gestion de crise**
  - Méthodologie de planification de la gestion de crise
  - Évaluation des menaces et des risques
  - Hiérarchiser les décisions et les activités

Résultats d'apprentissage

- Définir ce qu'est la cybersécurité
- Se sensibiliser à la sécurité du réseau
- Différencier les différents types de logiciels malveillants
- Avoir un aperçu des problèmes juridiques et de la gestion des incidents
- Établissez des mesures de sécurité efficaces que le service informatique peut mettre en œuvre, que les auditeurs peuvent valider et que les dirigeants peuvent comprendre
- Décrire les sujets, les termes, les technologies et les concepts de sécurité de l'information
- Assimiler et appliquer la Confidentialité, l'Intégrité et la Disponibilité (CIA) pour la priorisation des ressources de sécurité critiques
- Décrire le renforcement du système
- Définir les correctifs du système
- Déterminer l'approche utilisée par de nombreux attaquants informatiques

Conditions préalables

- Connaissances de base en cybersécurité
- Familier avec les fonctions informatiques et les organisations informatiques

Durée 4 jours -

SANCFIS

TÉLÉCOM | INFRASTRUCTURE | INTÉGRATION DE SYSTÈMES | CYBERSÉCURITÉ | RADIOCOMMUNICATION | IDENTITÉ ET BIOMÉTRIE