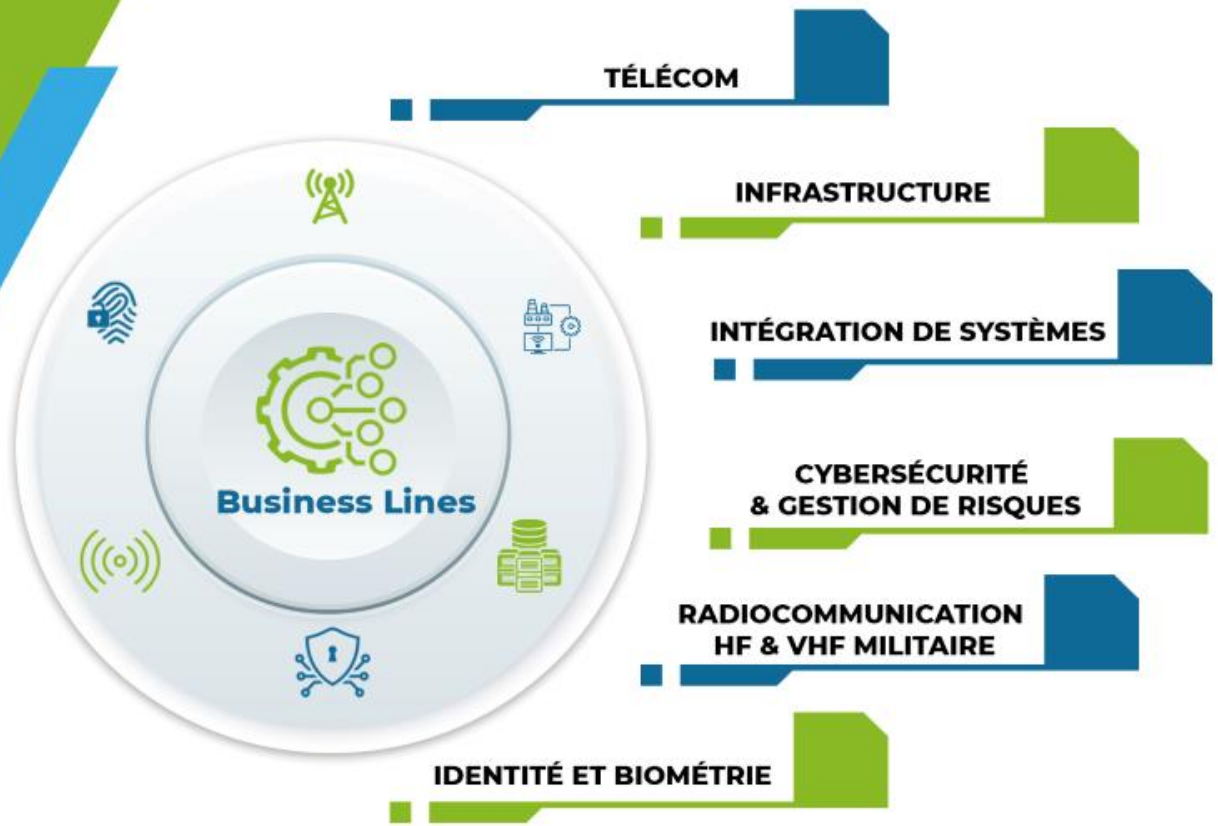
SANCFIS

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

Modules de Formation Cyber sécurité



2. Menaces et vulnérabilités en matière de cybersécurité (5 jours)

Introduction

L'objectif du cours est de permettre aux participants d'acquérir une compréhension des cybermenaces, d'apprendre et d'utiliser des techniques courantes de piratage éthique afin d'évaluer les impacts du piratage et de leur permettre de s'assurer que leurs systèmes sont suffisamment protégés, pour atténuer l'impact d'une cyberattaque.

Le contenu des cours

- **Risques et menaces**
  - Histoire
  - Besoins en cybersécurité
  - Législation
  - Méthodologies d'audit
- **Reconnaissance**
  - Reconnaissance sur Internet
  - Reconnaissance sur dossiers
  - Reconnaissance sur LAN
  - Contre-mesures
- **Scanning**
  - Balayage des ports avec Nmap
  - Forger des paquets avec Scapy
  - Analyse des vulnérabilités à l'aide d'OpenVAS
  - Énumération des utilisateurs
  - Contre-mesures
- **Techniques d'exploitation**
  - Fondamentaux de l'exploitation
  - Un focus sur Metasploit Framework
  - Contre-mesures
- **Intrusion sur les réseaux Wi-Fi**
  - Introduction aux réseaux sans fil
  - Découverte et reniflage de réseau
  - Attaques cryptographiques
  - Autres méthodes d'intrusion
  - Contre-mesures
- **Attaques de mots de passe**
  - Mots de passe et authentification
  - Principes et techniques
  - Mettre ces techniques en pratique
  - Contre-mesures
- **Vulnérabilités des applications Web**
  - Détection de vulnérabilité
  - Vulnérabilités courantes
  - Injection de commande
  - Contre-mesures

2. Menaces et vulnérabilités en matière de cybersécurité (suite)

Résultats d'apprentissage

- Décrire les aspects juridiques des cyberattaques
- Appliquer la méthodologie de test de pénétration des réseaux
- Expliquer les techniques d'analyse de réseau
- Décrire les techniques d'évaluation de la vulnérabilité
- Définir les méthodes d'intrusion et d'attaque
- Appliquer les techniques d'exploitation du réseau
- Démontrer une compréhension des techniques d'attaque par mot de passe
- Décrire les techniques d'attaque Web et Wi-Fi
- Appliquer des règles de renforcement communes pour renforcer la sécurité

Conditions préalables

- Connaissance de base du modèle d'interconnexion de systèmes ouverts (OSI)
- Connaissance de base de TCP/IP et des protocoles réseau
- Connaissance de base des systèmes d'exploitation Windows
- Connaissance de base des systèmes d'exploitation UNIX / Linux
- Connaissance de base des menaces de cybersécurité et des méthodes d'attaque
- En plus des connaissances ci-dessus, un prérequis recommandé est d'assister au cours sur les fondamentaux de la cybersécurité pour l'informatique avant ce cours.

Durée

- 5 Jours

SANCFIS

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