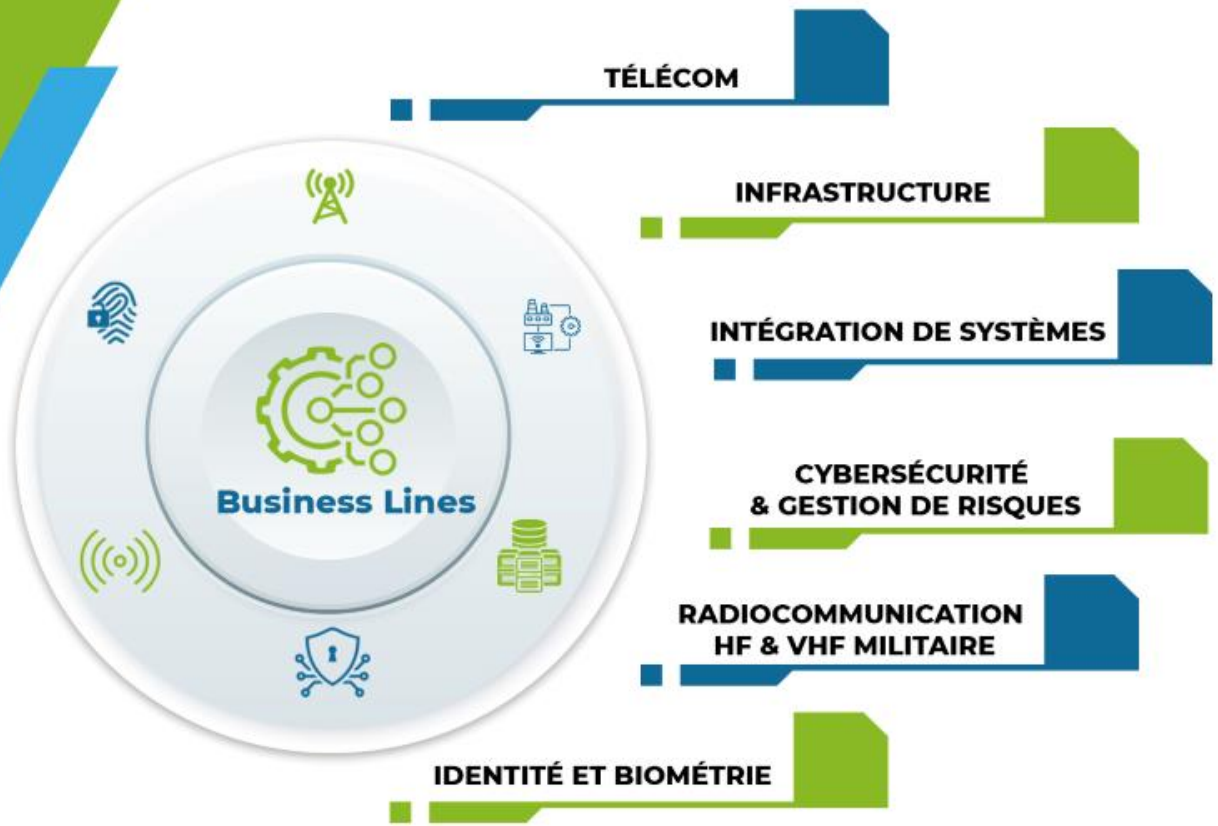
SANCFIS

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

Modules de Formation Cyber sécurité



3. Déploiement et fonctionnement IDS/IPS (3 jours)

Introduction

L'objectif du cours est de fournir des connaissances techniques, une sensibilisation et des systèmes pratiques de détection et de prévention des intrusions (IDS / IPS). Le cours fournira une compréhension claire de la façon d'instrumenter votre réseau et permettra aux participants d'effectuer une analyse et une reconstruction détaillées des incidents..

Le contenu des cours

- **Introduction à IDS/IPS**
  - Qu'est-ce qu'un IDS/IPS
  - Types d'IDS/IPS
  - Classement des alertes
- **Déploiement IDS/IPS**
  - Stratégie de déploiement
  - Présentation de la suricate
  - Présentation de Wazuh
- **Paramétrage et administration**
  - Stratégie de détection et rédaction de règles
  - JSN (Suricata)
  - HIDS (Wazuh)
- **Limitations et techniques de contournement**
  - Gestion des capteurs et des règles
  - Techniques adverses

Résultats d'apprentissage

- Comprendre et analyser le trafic IDS/IPS pour atténuer les menaces
- Identifiez les activités potentiellement malveillantes
- Pratique sur la détection et l'analyse
- Configurer et exécuter le capteur IDS/IPS et écrire des signatures
- Déployer, implémenter et administrer IDS/IPS

prérequis

- 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
- Connaissance de base des systèmes de gestion des informations et des événements de sécurité (SIEM)
- Connaissance de base des concepts de criminalistique numérique

Durée

- 3 Jours

SANCFIS

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