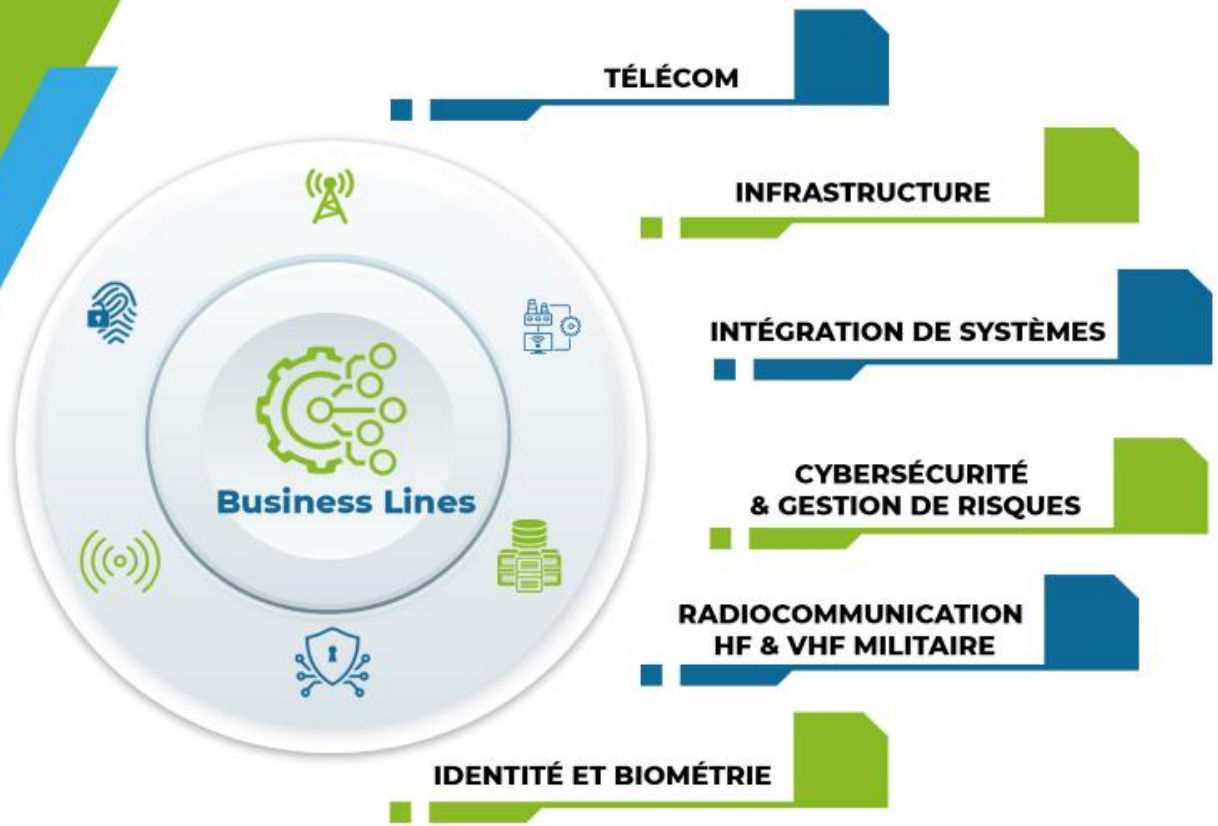
SANCFIS

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

Modules de Formation Cyber sécurité



5. Implémentation SIEM (4 jours)

Introduction

L'objectif du cours est de mettre en évidence les avantages du déploiement d'une gestion des incidents et des événements de sécurité (SIEM) au sein d'un environnement informatique. Le cours fournira aux participants les connaissances, la méthodologie et les processus nécessaires pour résoudre les problèmes de journalisation et surveiller les cybermenaces et les attaques via l'infrastructure SIEM.

Le contenu des cours

- **Présentation du SIEM**
  - Définition et notions
  - Design
  - Composants et architecture
- **Architecture SIEM**
  - Définition et concepts du journal
  - Types de journaux et d'agents
  - Agrégation de journaux
  - Courtier en journaux
  - Stockage des journaux
  - Visualisation des logs, recherche et alerte
- **Analyse tactique**
  - Profilage des services
  - Analyse des terminaux
  - Ligne de base et comportement des utilisateurs

Résultats d'apprentissage

- Acquérir une compréhension concernant le déploiement de SIEM dans un environnement de production
- Décrire les meilleures pratiques, pour la collecte des journaux et la surveillance
- Analysez et combinez plusieurs sources de données pour obtenir une meilleure compréhension des journaux SIEM
- Analyse des alertes standards et priorisation
- Déterminer les données de journal nécessaires pour établir l'efficacité du contrôle de 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
- Connaissance de base des concepts de criminalistique numérique

Durée

- 4 Jours

SANCFIS

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