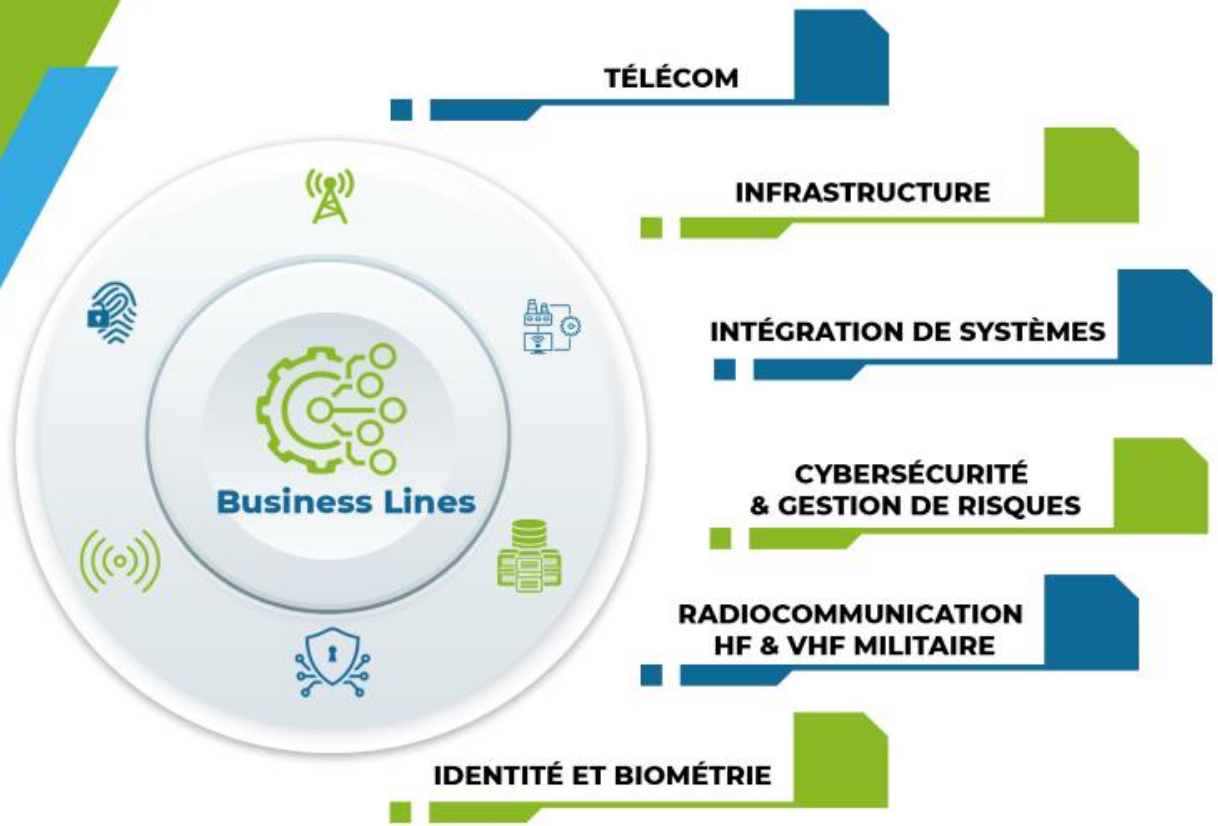
SANCFIS

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

Modules de Formation Cyber sécurité



4. Enquête et criminalistique numérique (4 jours)

Introduction

Ce cours fournit aux participants les compétences et les connaissances nécessaires pour comprendre la criminalistique numérique et les méthodologies de réponse aux incidents et d'enquête connexes. Ce cours permet aux participants de réaliser des actions essentielles pour récupérer des informations exploitables, collecter des indices, compléter des analyses pratiques et répondre efficacement aux incidents.

Le contenu des cours

- **Introduction à la criminalistique numérique**
  - La criminalistique numérique dans le monde d'aujourd'hui
  - Processus d'enquête numérique
  - Les meilleures pratiques
- **Sensibilisation aux logiciels malveillants**
  - Logiciels malveillants et infections
  - L'investigation numérique dans un environnement compromis
- **Structuration et acquisition de données**
  - Vue d'ensemble des supports de stockage
  - L'acquisition des données
  - Acquisition de données statiques
  - Acquisition de données volatiles
  - Acquisition dans des environnements virtuels
- **Structuration et acquisition de données**
  - Récupération de données à partir de partitions supprimées
  - Analyse des preuves volatiles
  - Analyse du journal
  - Capture de réseau et criminalistique
- **Méthodes anti-légales**
  - Techniques, attaques et contre-mesures
- **Meilleures pratiques mondiales en criminalistique numérique**
  - Vue d'ensemble de la structuration et des acquisitions de données des supports de stockage

Résultats d'apprentissage

- Décrire les aspects juridiques et les règles d'enquête médico-légale, les méthodes d'enquête médico-légale standard et les techniques d'analyse de l'information
- Découvrir les techniques de récupération d'informations
- Démontrer une compréhension des techniques d'enquête, des outils de récupération et d'analyse, des processus et des procédures de réponse aux incidents
- Découvrez les meilleures pratiques pour interagir avec des organisations qualifiées, les principes et les processus d'investigation numérique

4. Enquête et criminalistique numérique (suite)

Conditions préalables

- 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 de l'analyse des logiciels malveillants et de l'ingénierie inverse
- Connaissance de base de la réponse aux incidents et des concepts d'investigation numérique
- En plus des connaissances ci-dessus, un prérequis recommandé est d'assister au cours de renseignement sur les cybermenaces avant ce cours.

Durée

- 4 Jours

SANCFIS

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