COMPETENCES

Cybersécurité / Cyberdéfense

- **Firewalling & filtrage : firewalls, ACL, politiques de filtrage**
- **IDS/IPS : détection d'intrusions, règles signatures, gestion des faux positifs**
- **Analyse réseau : Wireshark, inspection profonde, analyse de flux et anomalies**
- **Sécurisation des communications : VPN/IPSec, TLS**
- **bonnes pratiques Linux & Windows**
- **Gestion d'incidents & SOC : niveau 1/2**
- **Veille & analyse de menaces : exploitation rapports CERT/ANSSI**

IAM / Contrôle d'accès

- AAA : Diameter, TACACS+, LDAP, Kerberos
- Modèles de droits & RBAC
- Gestion du cycle de vie des identités
- Certificats & authentification forte
- Comptes à privilèges (PAM)
- Concepts SSO, MFA, fédération
- Gouvernance des accès
- SELinux (principes, politiques de sécurité, troubleshooting)

Sécurité des SI

- ISO 27001, EBIOS RM, ANSSI
- Analyse de vulnérabilités : Nessus, Nmap
- IPSec, VPN, firewalls, proxies
- SELinux : contexts, policies, MAC, analyse des AVC
- Rédaction de rapports sécurité & conformité

Systèmes & Réseaux

- Linux (Ubuntu), Windows Server
- VLAN, DHCP, DNS, routage, Wireshark
- Virtualisation : VMware, VirtualBox
- Docker, Kubernetes (notions)
- Ansible : inventaires, rôles, playbooks

Analyse de données et développement

- Analyse d'habilitations, détection d'anomalies
- Normalisation & qualité des données
- Tableaux de bord : Power BI, Tableau, Excel
- Python, Java, MySQL
- Scripts d'automatisation

Soft Skills

- Vulgarisation technique, esprit d'analyse
- Présentation aux équipes techniques et métiers
- Gestiondustress &autonomie
- Coordinationinterservices,travailen équipe

FORMATIONS

2023-2025

Master 2 Télécommunications, Réseaux et Cybersécurité

Brest, France

2016 - 2019

Licence Professionnelle en Télécommunications et Réseaux

Bangui, Centrafrique

LANGUES

Francophone

English (CLES B2)

Espagnol

Juste Fourier ACKO

Disponible à partir de Janvier 2026

Mail: ackojuste75@gmail.com
Tel: 07 45 30 04 13
Brest, France

Étudiant en cybersécurité doté d'un profil polyvalent et complet, couvrant la gouvernance, la gestion des risques (ISO 27001, EBIOS RM), la sécurité opérationnelle, l'administration systèmes et réseaux, la détection d'incidents et la sécurisation des architectures. Fort d'expériences significatives administration systèmes & réseaux, analyse data et gestion de projets IT, j'apporte une vision complète mêlant technique, conformité et pilotage de la sécurité.
Rigoureux, curieux et orienté amélioration continue, je souhaite contribuer à la protection, la conformité et la résilience des systèmes d'information au sein d'une équipe cyber exigeante.

EXPÉRIENCES PROFESSIONNELLES

2021 -2022

Data Analyst, Médecins Sans Frontières, Centrafrique

Gestion et analyse des données
Assurer la qualité des données collectées
Normaliser les formats de données
Visualisation des données
Créer des tableaux de bord avec Power BI, Tableau, Excel,
Présenter les résultats aux équipes métiers de façon claire et synthétique
Mettre en place des KPI (indicateurs de performance)
Gestion et coordination de projets

2020 - 2021

Chargé IT, Autorité Nationale des Élections, Centrafrique

Gestion des technologies de l'information et des systèmes informatiques.
Contrôle et évaluation des opérations informatiques et data.
Installation , configuration et administration du réseau.
Assurer le bon fonctionnement de l'ERP de l'entreprise.
Gestion et sécurité des réseaux
Administration systèmes et bases de données
Gérer les outils collaboratifs (M365, Google Workspace...)
Gérer les sauvegardes, la reprise après incident (PRA/PCA)
Coordination de projets IT
Veille technologique

2019- 2020

Administrateur réseaux et systèmes, Orange, Centrafrique

Aider à la configuration et à la supervision de l'infrastructure réseau (LAN/WAN/VLAN).
Gérer des machines virtuelles ou conteneurs (VMware, VirtualBox, Docker).
Participer à la gestion des incidents : analyse de logs, résolution de pannes.
Mettre à jour et documenter des procédures de configuration ou de dépannage.
Assister à la mise en place ou la migrationd'un serveur(DNS, DHCP, mail, etc.)

PROJETS ACADEMIQUES

1. **Cybersécurité - Déploiement d'un IDS et simulation d'attaques**

Mise en place d'un IDS Suricata dans un environnement Docker
Mise en place d'un environnement d'attaque contrôlé (Kali Linux → DVWA)
Exécution de scans réseau automatisés (Nmap) pour tester les capacités de détection de l'IDS
Simulation d'attaques par brute-force (Hydra) et analyse du comportement du système ciblé
Exploitation de vulnérabilités via Metasploit afin d'évaluer la réactivité et la précision des alertes générées.
Analyse approfondie des logs Suricata pour identifier des patterns d'intrusion et calibrer les règles de détection.
Documentation complète des procédures de déploiement, d'attaque et d'analyse pour faciliter la reproductibilité pédagogique.

2. Cybersécurité - Déploiement SIEM–Wazuh

Installation et configuration du manager + agents (Windows, Linux)
Intégration avec OpenSearch/Kibana pour la centralisation et la visualisation des logs
Normalisation et enrichissement des événements (décodages & règles personnalisées)
Mise en place d'alertes sur indicateurs de compromission (IOC)
Tests d'attaques simulées pour valider l'efficacité des détections

3. **Sécurisation d'un réseau d'entreprise multi site: Architecture IAM / AAA**

Mise en place d'une architecture AAA complète (FreeDiameter + LDAP)
Implémentation du RBAC
Authentification forte via certificats (OpenSSL - PKI interne)
Segmentation dynamique via VLAN
Sécurisation des communications (IPsec/TLS)
Documentation & analyse des modèles d'habilitation

4. **Cybersécurité – HIDS & environnements conteneurisés**

Configuration réseau et déploiement d'hôtes vulnérables avec Podman (SQL Injection, Log4Shell).
Intégration de Wazuh Manager + Agents pour la détection d'intrusion hôte (FIM, auditd, syscheck, log monitoring).
Identification et analyse de vulnérabilités via Wazuh et bases de données CVE intégrées.
Corrélation d'événements, classification des alertes, et recommandation de remédiations.

5. **Cybersécurité – Infrastructure as Code (Ansible & FortiGate)**

Mise en place d'une solution d'automatisation pour pare-feu FortiGate (FortiOS API + modules officiels Ansible).
Déploiement de playbooks pour : gestion des interfaces (WAN, LAN, DMZ), création de VIP / objets réseau, configuration de règles et politiques de sécurité, mises à jour et audit de conformité.