COMPETENCES

Cybersécurité & Pentest

- Réalisation de tests d'intrusion web et réseau (OWASP, Nmap, Burp Suite, scans et énumération de services).
- Premiers travaux sur Active Directory et escalade de privilèges Linux/Windows.
- Analyse de vulnérabilités, gestion des permissions, rédaction de rapports et preuves de concept (PoC).
- Scripting Python/Bash pour automatisation de tests et exploitation de vulnérabilités.
- Travail en laboratoires virtuels (VM, Hack The Box, TryHackMe), bonnes pratiques et sensibilisation sécurité.

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

Soft Skills

- Vulgarisation technique, esprit d'analyse
- Présentation aux équipes techniques et métiers
- Gestion du stress & autonomie
- Coordination interservices, travail en équipe

FORMATIONS

2024-2026

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

LinkedIn : linkedin.com/in/juste-acko
Portfolio : ackovski.github.io/ackojuste.github.io

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

Stage en cybersécurité
Disponible à partir de Janvier 2026

Étudiant en Master 2 cybersécurité, orienté sécurité opérationnelle, audit de configuration et détection d'attaques. Expérience pratique en SIEM, IDS, durcissement Linux/Windows et automatisation de contrôles de sécurité (Python, Ansible). Intérêt marqué pour les approches Blue Team, Purple Team et Réponse sur incident (DFIR), avec une sensibilité aux environnements cloud et aux problématiques d'outillage et de reproductibilité.

PROJETS TECHNIQUES

Cybersécurité – Réalisation de tests d'intrusion contrôlés dans un environnement isolé

- Déploiement et configuration d'un IDS Suricata dans un environnement conteneurisé (Docker).
- Conception d'un scénario d'attaque contrôlé (Kali Linux → DVWA) afin d'évaluer les capacités de détection.
- Simulation d'attaques (scan, brute-force, exploitation) et analyse de la couverture de détection associée.
- Analyse des logs Suricata pour identifier des patterns d'intrusion, réduire les faux positifs et ajuster les règles de détection.
- Documentation des scénarios, résultats et recommandations pour assurer la reproductibilité et l'amélioration continue de la détection.

Cybersécurité – Validation de détection via SIEM (Wazuh)

- Déploiement et configuration d'un SIEM Wazuh (manager et agents Windows/Linux) pour la collecte centralisée des événements de sécurité.
- Normalisation et enrichissement des logs (décodages, règles personnalisées) afin d'améliorer la qualité et la pertinence des alertes.
- Définition d'indicateurs de compromission (IOC) et mise en place d'alertes associées.
- Réalisation de scénarios d'attaque simulés (scan, brute-force, exploitation) pour tester la couverture de détection.
- Analyse des alertes générées, identification des angles morts et ajustement des règles dans une logique Purple Team.
- Documentation des tests, résultats et recommandations pour améliorer la détection et la réponse aux incidents.

Cybersécurité – Audit et validation de la sécurité des accès (IAM / AAA)

- Conception et déploiement d'une architecture AAA (FreeDiameter, LDAP) pour la gestion centralisée des accès et des identités.
- Définition et implémentation d'un modèle RBAC afin de limiter les privilèges et réduire la surface d'attaque.
- Mise en place d'une authentification forte basée sur certificats (PKI interne, OpenSSL) et analyse des risques associés.
- Segmentation dynamique du réseau via VLAN et évaluation de l'isolement entre zones fonctionnelles.
- Sécurisation des communications (IPsec, TLS) et validation de la robustesse des canaux d'authentification.
- Analyse des modèles d'habilitation, identification des faiblesses potentielles (sur-privilèges, défauts d'isolation) et formulation de recommandations de durcissement.
- Documentation des contrôles et résultats dans une logique d'audit et d'amélioration continue.

Cybersécurité – Audit de configuration et durcissement Linux / Windows

- Réalisation d'audits de configuration sur des systèmes Linux et Windows afin d'évaluer leur conformité aux bonnes pratiques de sécurité.
- Analyse des mécanismes d'authentification, des permissions et des services exposés pour identifier les surfaces d'attaque.
- Mise en œuvre et analyse de politiques SELinux (MAC) pour renforcer le contrôle d'accès et limiter l'impact d'une compromission.
- Identification des écarts de configuration, évaluation des risques associés et priorisation des actions correctives.
- Rédaction de recommandations de durcissement claires et exploitables dans une logique d'audit et d'amélioration continue.

Cybersécurité – Automatisation des audits et configurations de sécurité

- Développement de playbooks Ansible pour automatiser les configurations sécurisées et les audits de conformité sur des infrastructures réseau.
- Conception de scripts Python pour vérifier l'application des contrôles de sécurité et détecter des écarts de configuration.
- Automatisation de la gestion de pare-feu FortiGate via API (politiques, objets réseau, règles de filtrage) dans une logique de durcissement.
- Validation des configurations appliquées et analyse des écarts afin d'améliorer la cohérence et la sécurité globale.
- Documentation des procédures et des contrôles automatisés pour assurer la reproductibilité et la fiabilité des audits.

EXPÉRIENCES PROFESSIONNELLES

2021 – 2022 - Data Analyst – Médecins Sans Frontières

- Analyse et traitement de données avec Python dans une logique de qualité, de cohérence et de fiabilité de l'information.
- Développement de scripts d'automatisation pour faciliter l'analyse et la détection d'anomalies.
- Conception de tableaux de bord décisionnels permettant un meilleur pilotage des activités et une prise de décision éclairée.
- Sensibilisation aux enjeux de confidentialité et de protection des données dans un contexte humanitaire.

2020 – 2021 - Chargé IT – Autorité Nationale des Élections (RCA)

- Administration de systèmes et réseaux avec prise en compte des exigences de sécurité, de disponibilité et de continuité de service.
- Supervision des infrastructures, analyse des journaux systèmes et participation à la gestion d'incidents techniques et de sécurité.
- Contribution à la mise en œuvre de mesures de sécurisation (contrôles d'accès, durcissement de configurations).
- Rédaction et mise à jour de procédures techniques et de sécurité afin d'améliorer la fiabilité et la traçabilité des opérations.

2019 – 2020 - Administrateur systèmes & réseaux – Orange (RCA)

- Exploitation et sécurisation d'infrastructures systèmes et réseaux dans un environnement opérateur télécom.
- Application de politiques de sécurité réseau et participation à la gestion d'incidents techniques.
- Support aux équipes techniques et contribution à la résolution d'anomalies impactant la disponibilité et la sécurité des services.