Kossi Richard Allado

Étudiant ingénieur en Cybersécurité et IA

Stage PFA : Cybersécurité | SOC | Offensive Security

LinkedIn | GitHub | Portfolio | TryHackMe

Casablanca, Maroc
+212 621 074 305
alladokossirichard2025@gmail.com

Profil

Étudiant en 2ème année du cycle ingénieur en Cybersécurité et Intelligence Artificielle à l'ENSA Beni Mellal. Profil orienté cybersécurité opérationnelle, avec pratique documentée en SOC, investigation, hardening Linux, sécurité web/réseau, IAM et Offensive Security dans des labs contrôlés.

Recherche un stage PFA de 2 mois, disponible dès le 1er juillet 2026, pour contribuer à des missions de surveillance sécurité, analyse d'alertes, sécurisation des systèmes et tests techniques encadrés. Capacité à documenter clairement les preuves, les impacts et les recommandations.

Compétences techniques

SOC / investigation : analyser et corréler des événements, extraire des IOC, reconstruire une timeline et qualifier une alerte – Splunk, Sysmon, auditd, logs Linux/Windows, MITRE ATT&CK.
Sécurisation systèmes / accès : durcir SSH et les comptes, filtrer les accès, suivre les fichiers critiques et valider la remédiation – Linux, UFW, Fail2ban, Lynis, auditd, Keycloak, MFA/TOTP, RBAC.
Offensive Security : réaliser reconnaissance, énumération, exploitation contrôlée et validation de vulnérabilités web/réseau – Kali Linux, Nmap, Hydra, Burp Suite, DVWA, Netcat.
Réseau / forensic / reporting : capturer le trafic, analyser les services exposés, préserver des preuves et formaliser les constats – Wireshark, tcpdump, FTK Imager, WinPMEM, Autopsy, Volatility 3.
Automatisation / data : préparer des données, automatiser des tâches simples et documenter des résultats reproductibles – Python, Bash, SQL, Pandas, Scikit-learn, Git/GitHub.

Projets

Linux Server Compromise & Forensic Investigation Lab — Red Team + Blue Team / DFIR
Dépôt GitHub

- Environnement multi-VM : Kali Linux attaquant et Ubuntu Server cible avec SSH, UFW, auditd et Fail2ban.
- Exécution contrôlée de la chaîne d'attaque : reconnaissance Nmap, brute-force SSH via Hydra, accès initial, élévation de privilèges, persistance et reverse shell Netcat.
- Analyse post-compromission des connexions SSH, commandes, activité sudo, comptes créés, flux réseau et artefacts auditd.
- Remédiation : blocage UFW, suppression du compte malveillant, reset du mot de passe, revue sudo/SSH et Fail2ban.

Volt Typhoon Intrusion Investigation — SOC / Threat Hunting / Reporting
Étude technique

- Environnement TryHackMe avec Splunk et journaux Windows/applicatifs simulant une intrusion de type Volt Typhoon.
- Analyse d'un compte compromis, de PowerShell/WMIC, d'un web shell, de Mimikatz, du C2 et de l'effacement de journaux.
- Reconstruction des phases de l'intrusion, extraction des IOC, construction d'une timeline et mapping MITRE ATT&CK.
- Documentation de requêtes de détection et de recommandations de confinement et de remédiation.

Web & Network Security Labs — Offensive Security Web / Réseau
Dépôt GitHub

- Lab web Docker/DVWA : tests SQL injection et XSS, analyse de l'absence de validation des entrées et contre-mesures.
- Lab réseau depuis un terminal Linux : capture tcpdump/Wireshark, scan Nmap et identification des services exposés.
- Lab MITM multi-VM Kali Linux, Fedora et Windows : ARP poisoning, observation du trafic et propositions de mitigation.

Cross-platform Intrusion Investigation Lab SOC / Corrélation de logs
Dépôt GitHub

- Environnement multi-VM : Kali Linux comme source d'attaque, Ubuntu Server comme cible SSH et Windows Server pour compléter l'analyse des traces.
- Génération contrôlée d'un brute-force SSH avec Nmap/Hydra, puis corrélation des journaux Linux, d'Event Viewer et de Sysmon.

Linux Hardening & Audit Labs Audit / Hardening / Remédiation
Dépôt GitHub

- Lab Ubuntu/Apache2 : diagnostic d'un blocage SELinux/AppArmor via auditd/audit2why et correction des contextes sans désactiver les contrôles.
- Lab audit Linux : baseline Lynis, surveillance de fichiers critiques avec auditd et vérification chkrootkit/rkhunter.

Identity & Access Security Labs IAM / MFA / PKI
Dépôt GitHub

- Labs Keycloak sur Linux/Docker : utilisateurs, rôles, RBAC, MFA/TOTP et vérification de scénarios d'autorisation.
- Lab SSH MFA sur Linux avec PAM/Google Authenticator ; lab OpenSSL/PKI consacré aux clés, certificats, signatures et chiffrement.

Windows Server Forensic Investigation Lab DFIR / Forensic
Dépôt GitHub

- Environnement : Windows Server compromis et poste forensic Linux/CAINE pour préserver et examiner les éléments collectés.
- Acquisition disque/mémoire avec FTK Imager et WinPMEM, puis analyses Autopsy/Volatility 3 et reconstruction de la timeline.

Expérience

Stagiaire IA / Maintenance prédictive Août 2025
ONEE - Branche Eau, Kasba Tadla

- Préparation et analyse de données capteurs de pompe haute pression afin d'identifier des signaux de défaillance.
- Entraînement d'un modèle Random Forest avec Python, Pandas et Scikit-learn pour classifier un risque de défaut.
- Construction d'une interface de test et documentation du prototype dans une logique de diagnostic technique.

Formation

Cycle ingénieur – Cybersécurité et Intelligence Artificielle, ENSA Beni Mellal 2024 – Présent
DEUST – Mathématiques, Informatique, Physique, FST Fès 2022 – 2024 – Mention Bien
Baccalauréat scientifique – Série D, Lycée de Djagblé, Togo 2022 – Mention Très Bien

Certifications et réalisations

Cybersécurité : TryHackMe Top 1% | Junior Penetration Tester Learning Path | Cisco Ethical Hacker.
Fondations : IBM Introduction to Data Engineering | Google Cybersecurity Foundations | Google Play It Safe : Manage Security Risks | Udemy Linux Command Line.
Compétitions : CSIA CTF 2026 : 1ère place, équipe GHOSTSHELL | CiteFlag 2026 : finaliste, 6ème place avec Team CHILA.

Langues

Français : courant | Anglais : professionnel technique | Éwé : langue maternelle