Abdoulaye Touré

Administrateur Système et réseaux

Portfolio · GitHub · TryHackMe · LinkedIn

+33 644 93 26 27
ablayetoure2014@gmail.com
Local: Île-de-France

Profil

Double compétence lettres/tech. J'automatise la détection et la réponse (ELK, playbooks) et convertis les signaux en insights actionnables. Je cherche un poste d'analyste ou administrateur systèmes junior pour créer de l'impact.

Expériences et réalisations sélectionnées

Développeur Full Stack Freelance | Skeelfully • Paris

Juillet 2025 – Octobre 2025

• Développement d'une marketplace connectant porteurs de projet et talents

• Migration vers Node 16 et correctifs de compatibilité Webpack.

• Optimisation CI/CD et durcissement des dépendances NPM.

Stage – Audit & Pentest | ADVENS • Paris

Mars 2025 – Juin 2025

• Audits techniques et tests d'intrusion web/réseau (Burp Suite, Nmap, SQLMap).

• Threat Hunting et corrélation SIEM via ELK/Kibana.

• Automatisation du reporting (Bash/PowerShell) et restitution technique.

Développeur Web & Web Mobile | Entourage • Paris

Octobre 2022 – Novembre 2023

• Conception d'applications sécurisées (Node.js, React, MySQL).

• Durcissement des API et intégration de la CI/CD.

• Suivi qualité et conformité aux standards AppSec (OWASP).

Formations

Mastère – Expert en cybersécurité
Oteria Cyber School, Genvilliers | Septembre 2025 – en cours
Cybesérité, administration systemes réseaux et sécurité, cloud

Bac+4 – Administrateur d'infrastructures sécurisées (RNCP 37680)
ALT-RH, Paris | 2024 – 2025
Cursus validé par un stage de 5 mois chez ADVENS — voir Expériences.

Bac+3 – Développeur Web & Web Mobile
WebForce3, Paris | 2022 – 2023

Bac+2 – Développeur Intégrateur Web
OpenClassrooms, Paris | 2022

Bac+5 – Littérature & civilisation anglophone (américaine & caribéenne)
UCAD, Dakar | 2011 – 2015

Centres d'intérêt

Veille sécurité, programmation, TryHackMe/RootMe, Taekwondo, course à pied, lecture, Baseball

Langues

• Français (courant) • Anglais (courant) • Espagnol (intermédiaire)

Projets

Purple Team Lab – Infrastructure de simulation

MITRE ATT&CK | Suricata | ELK

• Scénarios mesurables ATT&CK (détection'investigation'réponse) sur lab segmenté (Public/DMZ/Privé).
• Chaîne Suricata + ELK : collecte, corrélation, dashboards par use-cases SOC, playbooks d'investigation.

Dashboard SIEM Personnalisé

Kibana | Alerting | Baselines

• Vues ciblées (phishing, exécutions suspectes, latéralisation) et indicateurs de priorisation SOC.
• Règles d'alerting + baselines pour optimiser le ratio signal/bruit et réduire les faux positifs.

Plateforme de Simulation Phishing

GoPhish | SMTP | Awareness

• Campagnes avec modèles, tracking et tableaux de bord (taux de clic, signalement) ; retours d'expérience.
• Industrialisation du reporting pour libérer du temps d'analyse à plus forte valeur ajoutée.

Liens utiles

Portfolio https://abdou-cyber.dev

GitHub https://github.com/ablayeT?tab=repositories

LinkedIn https://www.linkedin.com/in/abdoulaye-toure-b37b30100/

TryHackMe https://tryhackme.com/p/ablaye.toure0

Compétences

SOC & Blue Team : Threat Hunting via SIEM (ELK), ingénierie de la détection (corrélation, baselines), orchestration de la réponse à incident (playbooks), analyse forensique.

Pentest & Red Team : Audit d'applications web (OWASP), tests d'intrusion internes/externes, cartographie et réduction de la surface d'attaque.

Systèmes / Réseau : Linux (admin/durcissement), segmentation réseau, journalisation, supervision.

Automatisation / Dev : Automatisation & scripting : Bash, PowerShell, Node.js ; CI/CD ; documentation et rapports normalisés.

Outils : Elasticsearch, Logstash, Kibana, Suricata, Wireshark, Nmap, Burp Suite, SQLMap, Git, Docker