MOHAMED HAKAM KOUBAA

Alternance Cybersécurité | Détection & Réponse Incidents (SOC)

HakamKoubaa@gmail.com +33 6 15 92 19 30 Paris, France hakam-koubaa
Akatsuki1995

*Étudiant Mastère Cybersécurité (Bac+5), focus SOC, maîtrise Splunk/Wazuh. Passionné Threat Hunting (MITRE ATT&CK) & IR (NIST). Rigoureux, curieux, communicant (même sous pression). Recherche alternance **3 sem. entreprise / 1 sem. cours**.*

FORMATION

Mastère Cybersécurité & Cloud (Bac+5)

IPSSI

2025–2027 (en cours) Paris

- Projets Blue Team: SIEM (Splunk, Wazuh), Threat Hunting (MITRE), Wireshark, forensique.
- Délégué: coordination ateliers, remontée feedbacks qualitatifs.

Dipl. Ingénieur - Réseaux Informatiques

INSAT

2017–2022 Tunis

- Spécialisation Cybersécurité & Cryptographie.
- Projets: sécurisation TLS, PKI, pentesting réseau.

EXPÉRIENCE PROFESSIONNELLE

Stagiaire Cybersécurité - Simulations

TheForage (Virtuel)

Jan–Mars 2025 À distance

- **Conception** & **création** 10+ règles corrélation Splunk (phishing, brute-force).
- **Déploiement** playbooks IR (NIST) pour 5 scénarios, réduisant TdR simulé de 30%.

Responsable SI & Transformation Digitale

VIKA Group

2022 – 2024 Tunis, Tunisie

- **Architecture** et **déploiement** d'une plateforme SaaS sécurisée (+100 clients) : WAF, validation des entrées, chiffrement AES-256. Résultat :
  Aucune vulnérabilité SQLi/XSS critique détectée sur 12 mois (audits mensuels).
- **Automatisation** de la migration des processus métier vers le cloud, entraînant une réduction des coûts opérationnels de 40% et une amélioration de la traçabilité.
- **Implémentation** d'un monitoring SIEM (ELK Stack) pour la détection proactive d'anomalies sur 10+ types de logs.

COMPÉTENCES TECHNIQUES

SOC / Blue Team

Splunk (avancé) | Wazuh | Elastic SIEM | MITRE ATT&CK | NIST CSF/RMF | Threat Hunting | Playbooks IR | EDR

Réseaux & Investigation

TCP/IP | Wireshark | Forensique (Autopsy)

Cloud & SecOps

AWS/GCP Security | Docker Security | DevSecOps | ISO 27001/RGPD

Scripting & Automatisation

Python (IR, malware) | Bash/PowerShell | Git | CI/CD (bases)

PROJETS PERSONNELS CLÉS

SIEM Perso (Home Lab)
Splunk & Wazuh pour analyse logs (pare-feu, Win, Lin). Simulation attaques (Metasploit), dashboards détection.

CTF & Labs Pratiques
Top 10% HackTheBox. +50 labs Blue Team TryHackMe (IR, forensique, détection).

CERTIFICATIONS

- **CC – Certified in Cybersecurity (ISC2)** – Obtenue 2025
- **CompTIA Security+** – Examen prévu Sept. 2025

LANGUES

Français
Anglais
Arabe

SAVOIR-ÊTRE

Rigueur/Méthode | Curiosité Tech. | Communication | Adaptabilité | Gestion Stress | Esprit d'équipe