MOHAMED HAKAM KOUBAA

Cybersecurity Apprenticeship | Incident Detection & Response (SOC)

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

Master's student in Cybersecurity (Master's level), SOC focus, proficient in Splunk/Wazuh. Passionate about Threat Hunting (MITRE ATT&CK) & Incident Response (NIST). Rigorous, curious, effective communicator (even under pressure). Seeking an apprenticeship: ***3 weeks at company / 1 week of courses****.*

EDUCATION

Master's Degree in Cybersecurity & Cloud Computing (Master's level)

IPSSI

2025–2027 (Ongoing)   Paris

- Blue Team Projects: SIEM (Splunk, Wazuh), Threat Hunting (MITRE), Wireshark, forensics.
- Class Representative: coordinated workshops, gathered qualitative feedback.

Engineering Degree - Computer Networks

INSAT

2017–2022   Tunis

- Specialization in Cybersecurity & Cryptography.
- Projects: TLS security, PKI infrastructure, network penetration testing.

PROFESSIONAL EXPERIENCE

Cybersecurity Intern - Simulations

TheForage (Virtual Program)

Jan–Mar 2025 (3 months)   Remote

- **Designed** & **created** 10+ Splunk correlation rules (phishing, brute-force).
- **Deployed** IR playbooks (NIST-based) for 5 scenarios, reducing simulated response time by 30%.

IT Manager & Digital Transformation Lead

VIKA Group

2022 – 2024   Tunis, Tunisia

- **Architected** and **deployed** a secure SaaS platform (+100 clients): WAF, input validation, AES-256 encryption. Result:
  No critical SQLi/XSS vulnerabilities detected over 12 months (monthly audits).
- **Automated** business process migration to the cloud, reducing operational costs by 40% and improving traceability.
- **Implemented** SIEM monitoring (ELK Stack) for proactive anomaly detection across 10+ log types.

TECHNICAL SKILLS

SOC / Blue Team

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

Networking & Forensics

TCP/IP · Wireshark · Forensics (Autopsy)

Cloud & SecOps

AWS/GCP Security · Docker Security · DevSecOps · ISO 27001/GDPR

Scripting & Automation

Python (IR, malware analysis) · Bash/PowerShell · Git · CI/CD (basics)

KEY PERSONAL PROJECTS

Personal SIEM (Home Lab)
Deployed Splunk & Wazuh for log analysis (firewall, Windows, Linux). Simulated attacks (e.g., Metasploit) and created custom detection dashboards.

CTF Challenges & Practical Labs
Top 10% on HackTheBox. Completed 50+ Blue Team labs on TryHackMe (IR, forensics, intrusion detection).

CERTIFICATIONS

- **CC – Certified in Cybersecurity (ISC2)** – Obtained 2025
- **CompTIA Security+** – Exam scheduled Sept. 2025

LANGUAGES

French	●●●●◐
English	●●●●●
Arabic	●●●●●

SOFT SKILLS

Rigor/Methodology · Tech. Curiosity · Communication · Adaptability · Stress Management · Teamwork