OMAR BABBA

Final-year engineering student | Graduation internship, Feb. 2027: GRC • Technical cybersecurity background

Tangier, Morocco | omarbabba27@gmail.com | linkedin.com/in/omarbabba |
github.com/omarbabba779xx | omarbabba.co

PROFILE

Cybersecurity engineering student (computer science and networks), focused on **governance, risk and compliance** (ISO 27001, ISO 27005, EBIOS RM, GDPR, Moroccan Laws 05-20 and 09-08, applied on two GRC platforms built end to end) and backed by a **technical background**: detection, incident response, vulnerability assessment. Used to documenting work precisely (playbooks, management system file, reports) and to working in a team. Fluent in French and English.

EXPERIENCE

SOC Analyst Intern – AI-Augmented Security Pipeline **Jul. 2026 – Aug. 2026**

Amendis (Veolia group), Tangier – Cybersecurity Department

- **Designed and deployed** an end-to-end SOC pipeline: Wazuh alert, Shuffle orchestration, local LLM triage, TheHive case creation, Cortex and MISP enrichment.
- **Raised** MITRE ATT&CK mapping completeness from **40% to 100%** on a set of 25 alerts, using a prompt that enforces a strict JSON format.
- **Validated** 6 controlled attack scenarios (SSH brute force, encoded PowerShell, lateral movement, C2 beaconing…) and **routed** alerts deterministically by severity, with the AI kept advisory.
- **Ensured** traceability (RUN_ID, SHA-256) and quality: **75 automated tests** with CI.

Cybersecurity Awareness Intern **Jul. 2025 – Aug. 2025**

Amendis (Veolia group), Tangier – Cybersecurity Department

- **Analysed** the exposure of SCADA systems in the water and electricity networks; **observed** a real phishing simulation campaign (**click rate down from 25% to 5%** after awareness training).
- **Mapped** the main attacks (phishing, malware, DoS/DDoS, SQL injection) and studied information security fundamentals (confidentiality, integrity, availability, ISO 27001).
- **Explored** the Riot awareness platform used by Amendis and Veolia (training, phishing simulations, email reporting, data leak analysis).

GRC PROJECTS *more projects: omarbabba.co*

Kontrol – Governance Platform Proven on a Complete ISO 27001 Case | *ISO 27001, ISO 27005, NIS2, DORA* 2026

- **Designed** a governance tool (TypeScript) linking obligation, control, evidence, risk and signed decision; tested it on a **complete fictional ISMS**: scope, policy, internal audit, management review (**20 of 21 clauses** met).
- **Assessed** risks per **ISO 27005**: 8 valued assets, 15 scenarios, 11 above risk appetite with a treatment plan; **segregation of duties** enforced by the tool (a risk owner cannot accept their own risk).
- **Wrote** catalogues of **Laws 05-20 and 09-08** article by article; **mapped** 13 frameworks (ISO 27001, NIS2, DORA, AI Act, GDPR…) through 56 controls; wrote a **threat model** (27 threats). Limitations documented. Public code: github.com/omarbabba779xx/kontrol.

Amane GRC – Compliance Platform for Moroccan SMEs | *ISO 27001, Law 09-08, DNSSI, EBIOS RM* 2026

- **Designed** a web application (Node.js, SQLite) linking **ISO 27001:2022, Law 09-08 (CNDP), DNSSI / Law 05-20**, NIST CSF 2.0 and COBIT 2019 through **66 unified controls** (100% of requirements covered); 12 policy templates, versioned and accepted by each employee.
- **Automated 23 compliance tests**: Windows agent (encryption, antivirus, firewall, updates…), Microsoft 365 MFA read through Microsoft Graph, **access reviews** whose closure files the evidence on the related control.
- **Built EBIOS RM** risk analysis (5 workshops), an incident register with a **DGSSI reporting deadline**, the Law 09-08 register and a public Trust Center; tamper-evident log (HMAC-SHA256), 81 end-to-end tests, CI. Code: github.com/omarbabba779xx/amane-grc.

TECHNICAL PROJECTS

Incident Response Playbooks – Incidents, Risk and Compliance | *NIST, ISO 27001, GDPR* 2026

- **5 playbooks** (phishing, malware, compromised account, data breach, DDoS) with severity matrix, decision trees, notification templates and tracking metrics (MTTD, MTTA, MTTC, MTTR); **5 tabletop exercise scenarios** written.
- **Risk:** NIST SP 800-30 and ISO 27005 method (5 × 5 matrix, risk appetite, register, 5 scored scenarios); **compliance:** GDPR procedure (Art. 33 and 34, 72 h, breach register) and mapping to ISO 27001, NIST CSF, CIS, NIS2 and DORA.

SocForge – End-to-End SOC | *Wazuh, OPNsense, Shuffle, TheHive* 2026

- Built a SOC of **12 virtual machines**, wrote **29 detection rules**, documented 16 scenarios and automated the response: in the lab, **attacker blocked 24 s** after the alert.

Vulnerability Assessment Lab | *Nmap, Nikto, Nessus* 2026

- Assessed a deliberately vulnerable machine (Metasploitable2): **29 open ports**, Nessus **69 findings unauthenticated vs. 91 authenticated** (10 → 28 critical), proof of concept and prioritised remediation plan.

EDUCATION

École Marocaine des Sciences de l'Ingénieur (EMSI), Tangier **2022 – 2027**

Engineering degree (5-year programme) – Computer Science and Networks Engineering (IIR), final year

Final-year courses: cybersecurity audit, cybersecurity risk management (in progress); ethical hacking, digital forensics, cloud security.

Certifications: Security Monitoring and SIEM Fundamentals – LinkedIn / Hack The Box (2026); Fundamentals of Blockchain Architecture – LearnQuest (2026); Object-Oriented Programming in C++ – EPFL (2025).

Competition: Holmes CTF 2026 (Hack The Box, Blue Team), as a team: 66th of 5,637 teams, 111/111 challenges, top 1.2% worldwide.

SKILLS

Risk and compliance: assess risks (ISO 27005, EBIOS RM) and map requirements to controls (ISO/IEC 27001, GDPR, NIST, DNSSI, Laws 09-08 and 05-20) in Kontrol and Amane; basics of NIS2, DORA, AI Act.

Deliverables written: statement of applicability, risk register and treatment plan, incident response playbooks, threat model, audit report.

Detection and SOC: automate a detection and response chain (Wazuh, Shuffle, TheHive, Cortex, MISP); write rules mapped to MITRE ATT&CK (Sigma, Splunk); monitor network and endpoints (Suricata, Zeek, Sysmon, Velociraptor).

Forensics: acquire and analyse Windows evidence (FTK Imager, KAPE, Registry Explorer); analyse malware and network traffic (REMnux, NetworkMiner, Wireshark).

Technical audit: assess a system and prioritise remediation (Nmap, Nessus, Nikto); test a web application against the OWASP Top 10 (Burp Suite, OWASP ZAP, Kali Linux).

Development: build tested tools with continuous integration (TypeScript, Node.js, SQLite, Python, Docker, Git, GitHub Actions); administer Linux and Windows (Bash, PowerShell).

Languages: Arabic (native), French (fluent), English (fluent)

INTERESTS

Blue Team CTFs (Hack The Box); monthly threat intelligence reports (LockBit, APT29, Emotet); chess.