Taha Sakhi

Morocco
+212707853063
sakhitaha@gmail.com
LinkedIn: Taha Sakhi

Work Experience

Cybersecurity Engineer

ITS, Al Akhawayn University (*Ifrane, Morocco*) **Jan 2024 – Present**

- Engineered a custom AI-powered FastAPI SOAR middleware integrating Groq LLMs (Llama 3.1/3.3), AlienVault OTX, and VirusTotal for sub-second alert triage, multi-tiered threat enrichment (Micro/Milli/Second layers), and autonomous Cortex XDR endpoint containment (Auto-L2 Isolation).
- Implemented a PII Sanitization pipeline and SHA-256 behavioral caching to ensure data privacy and ultra-low latency triage of identical future attacks.
- Deployed a distributed Security Onion SOC architecture (Manager/Search nodes) integrated with Palo Alto Cortex XDR, Entra ID, and M365 telemetry via Elastic Agent and Fleet Server.
- Implemented a centralized NOC using SolarWinds Observability (Hybrid Cloud Observability) for 250+ nodes (SNMP v2/v3, WMI, VMware APIs), utilizing AppStack and PerfStack for cross-layer performance correlation.
- Reduced Mean Time to Resolution (MTTR) by 60% by engineering tiered alert engines with suppression to route notifications via Slack, Teams, and Email, preventing ”alert storms” and monitoring dual-ISP failover (Peplink).
- Authored 64 custom KQL detection rules and developed automated backend workflows (enricher.py) to generate MITRE ATT&CK mappings and Markdown investigation guides via LLM.
- Addressed data saturation by developing a surgical Index Lifecycle Management (ILM) advisor (so_ilm_advisor.py) to manage 10.89 GB/day ingestion and free 96.2 GB of Elasticsearch buffer.

Cybersecurity Consultant Intern

Innovatech Consulting (*Casablanca, Morocco*) **May 2025 – Sep 2025**

- Designed scalable, risk-based SOC architectures mapping business categories (A, B1-B3) to tool-agnostic security controls across 5 defense-in-depth layers.
- Deployed an open-source baseline utilizing Wazuh (EDR/SIEM), Security Onion, MISP, and Shuffle, aligning with NIST CSF, ISO 27001, and MITRE ATT&CK frameworks.
- Enforced strict web and mail security policies including SSL/TLS inspection in Squid, and DKIM/SPF/DMARC and URL reputation in Rspamd.
- Validated architectures through multi-stage attack simulations (Phishing, Malware Execution, Credential Dumping), achieving an 85% success rate in detecting memory-resident threats (T1003) via custom Sigma rules and Sysmon tuning.

SOC Analyst Intern

TECHSO GROUP (*Casablanca, Morocco*) **Jun 2024 – Sep 2024**

- Conceived and deployed an automated, 24/7 proactive CVE alerting system transitioning the SOC from manual vulnerability management to real-time operations via OpenCVE APIs and PostgreSQL.
- Developed Python backend scripts (check_vulnerabilities.py) integrating NLP models to monitor NVD feeds and translate technical summaries into French.
- Engineered a dynamic correlation engine (mailer.py) utilizing SMTP and Jinja2 templating to deliver customized HTML security alerts matched strictly to clients’ technological assets (Product/Vendor/General).

Technical Trainer / Expert (Allot ACG2000)

Neurones Technologies & BCRG (*Conakry, Guinea*) **Project**

- Delivered technical masterclasses to the Central Bank of the Republic of Guinea (BCRG) on the Allot ACG2000 communication gateway (DPI-based network intelligence).
- Trained engineering teams on Allot See (Granular traffic analysis/Analytics), Allot Control (QoS bandwidth management/prioritization), and Allot Secure (DDoS protection and URL filtering).
- Guided the configuration of Allot Secure modules to safeguard critical financial infrastructure, ensuring high availability and performance of banking applications.

EDUCATION

Bachelor of Science in Computer Engineering

Al Akhawayn University (*Ifrane, Morocco*) **Sep 2022 - Jun 2026**

- Major: Advanced Computer Science and Computer Systems
- Minor: Business Administration

Baccalaureate in Physics

Lycée La Résidence (*Khouribga, Morocco*) **2022**

- Honors: High Distinction (Very Good)

PROJECTS

CybeAegix – Intelligent Vulnerability Management Platform 2024

- Developed a containerized microservices application using FastAPI and React with automated ETL pipelines (updater.py) to autonomously aggregate vulnerability data from OpenCVE (PostgreSQL).
- Built an enrichment engine using Google Pegasus-XSUM AI (HuggingFace Transformers) to generate readable summaries from technical CWE/CVE documentations.
- Engineered a many-to-many subscription model (User_Product, User_Vendor, User_CWE) and RBAC system for customized, targeted alerting based on infrastructure components.

Surfood Save – Full-Stack Mobile Marketplace 2025

- Engineered a highly concurrent, cloud-native food waste reduction platform deployed on GCP Cloud Run and managed Cloud SQL (PostgreSQL).
- Developed an asynchronous FastAPI backend and a dual-interface React Native (Expo) mobile application with JWT/OTP authentication (TOTP via pyotp).
- Optimized geolocation queries using SQLAlchemy 2.0 with PostgreSQL GIN indexes and implemented strict inventory locking (with_for_update) to prevent overselling during high traffic.

Shadow Watcher – IoT Smart Room Monitoring 2026

- Designed an embedded C++ physical security system on the Particle Photon platform fusing data from three LDRs and a PIR sensor using a weighted fusion score (Optical/PIR/Directional).
- Implemented an adaptive rolling baseline (1200-sample circular buffer @ 20Hz) to dynamically compute sensor thresholds (4σ), minimizing false positives.
- Categorized anomalies (FLASH, SWEEP, SUSTAINED, PIR_ENTRY) and integrated Microsoft Teams and Power Automate webhooks for real-time alerting and automated forensic JSON logging to Excel.

SECDNS – Secure Custom DNS Protocol 2025

- Developed a custom secure DNS protocol shifting from UDP to TCP to prevent fragmentation, source-port guessing, and cache poisoning attacks.
- Implemented an asymmetric RSA handshake for authenticated session key exchange, coupled with AES-GCM (Galois/Counter Mode) for encrypted data payload integrity and bit-flipping protection.
- Designed custom protocol headers (SECDNS_HELLO, SECDNS_QUERY, SECDNS_RESP) to encapsulate DNS logic within a secure application-layer tunnel.

Remote Rootkit Attack (CVE-2017-5123) Validation 2025

- Executed a full remote kill chain utilizing a CWE-78 web command injection to deliver and compile a custom Linux Kernel Module (LKM) rootkit.
- Exploited the waitid() system call ”write-what-where” primitive (CVE-2017-5123) for privilege escalation and established an ICMP covert communication channel using Netfilter hooks and ”Magic String” triggers.
- Implemented kernel-to-user execution via call_usermodehelper to execute shell commands asynchronously from kernel space.

Security Simulation & Product Enablement Platform (Cloudflare Inspiration) 2025

- Engineered a modular Demo Platform utilizing React 19 and Vite to simulate complex technical security scenarios (WAF, Bot Mitigation, mTLS), facilitating client understanding of enterprise-grade security controls.
- Developed a Dynamic Simulation Engine that autonomously injects specialized demo modules based on configuration schemas, allowing for rapid deployment of new technical attack/defense use cases.
- Programmed a high-performance procedural 3D network topology globe using Three.js and @react-three/fiber to visualize global traffic patterns and attack vectors in real-time.

Secure Elastic Stack Deployment on Azure 2024

- Architected a centralized Observability pipeline deploying Elastic Stack (ELK 8.19.8) on Azure VMs (Ubuntu 24.04 LTS, D2s v3).
- Enforced strict network security (NSG rules), node-to-node SSL/TLS encryption, and Role-Based Access Control (RBAC) via enrollment tokens.
- Deployed the Elastic Agent via Fleet integration for unified policy management and real-time observability of system authentication and resource usage.

TECHNICAL SKILLS

Security & SOC: SOC/NOC Operations, Cloud Security, CSPM, Active Directory, Entra ID, SOAR, SolarWinds HCO (AppStack/PerfStack), Security Onion, Cortex XDR, Wazuh, Zeek, Yara, Sigma Rules, KQL, MISP, TheHive, Shuffle, n8n, Power Automate, Elastalert2, Elastic Agent, Deep Packet Inspection (DPI), Allot ACG2000.

Frameworks & Risk: NIST CSF, ISO 27001, MITRE ATT&CK, CIS Controls 18, FAIR (Quantitative Risk Forecasting).

Programming: Python (FastAPI, SQLAlchemy 2.0), C, C++, Java, Bash, SQL, TypeScript (React 19/React Native/Expo), HTML/CSS, Three.js, Scapy, Jinja2.

DevOps & Cloud: Docker, GCP (Cloud Run, Cloud SQL), Azure, CI/CD, Git/GitHub, PostgreSQL (GIN Indexes), Elasticsearch.

Systems & Network: Linux (LKM, Netfilter), Windows Server, macOS, Aruba Switches, Firewall, FortiGate, Palo Alto NGFW Peplink (ISP Failover), VMware, Particle Photon, SNMP, WMI, TCP/IP, SECDNS.

ADDITIONAL INFORMATION & INTERESTS

Languages: Arabic (Native), French (Advanced), English (Advanced).

Certifications & Training: SANS GIAC Certificate: Cybersecurity Leadership Masterclass (GITEX Africa 2026)
Networking for Cyber Professionals (Zscaler)
Cybersecurity Fundamentals (IBM).

Interests: Swimming, Judo, Hiking.