Mohamed Aziz Sghaier

3 rue Soutrane, 06560 Valbonne
☎ +33 6 02 54 82 81 ✉ Mohamed-Aziz.Sghaier@eurecom.fr

Objective

Eager to start my first role as a Cybersecurity Engineer or Security Advisor starting from the 1st of February. Strong focus on cloud-native and DevSecOps security, with hands-on experience designing and enforcing Kubernetes security policies, and integrating SAST, SBOM analysis, secret detection, malware scanning into CI/CD pipelines and cloud natice security. Background in system security, reverse engineering, and data-driven security analysis, with practical projects demonstrating adaptability, automation skills, and strong problem-solving capabilities in real-world security environments.

Education (BAC +6)

EURECOM Sophia Antipolis **2023-2026**
Post Master's in Security *Sophia Antipolis, France*

SUP'COM **2021-2023**
ICT Engineering *Tunis, Tunisia (ranked 19/140)*

IPEIN, Nabeul **2019-2021**
Pre-Engineering in Math/Physics *Nabeul, Tunisia (Ranked 74/1789)*

Skills

- **Cybersecurity & DevSecOps:** SAST, SBOM, Secret Detection, Malware Analysis, CI/CD Security, Supply Chain Security, SOC , Siem , Splunk , Fuzzing
- **Cloud & Container Security:** Docker, Azure, Kubernetes Security, Policy Enforcement, Runtime Security (Tetragon), Container Image Scanning
- **Static & Binary Analysis:** Reverse Engineering, Vulnerability Analysis, Binary Exploitation, Ghidra, Capstone, Sanitizers (ASan, TSan)
- **Programming:** C, C++, Python, Bash, MATLAB
- **Security Tooling:** Syft, Grype, Clang-Tidy, Cppcheck, Bear, ClamAV, Git
- **Operating Systems:** Linux (Ubuntu), Kernel Internals, System Security
- **Networking/Telecom:** CCNA1, TCP/IP, 5G Architecture (RAN, Core), Openairinterface, GSM/LTE/UMTS
- **AI & Data Science:** Machine Learning (Stanford-authorized certification), Malware Detection, Feature Engineering, Computer vision
- **Languages:** English (TOEIC 920/980), French (Fluent)

Experience

BubbleRAN (6 Months, ongoing) — Sophia Antipolis **2025**
End-to-End Security for Cloud-Native 5G & CI Hardening ***(SAST | SBOM | CI Security | Fuzzing| Kubernetes | SecOps)*** *France*

- Designed and implemented a **project-agnostic static analysis and security orchestration framework** covering bug detection, secret scanning, malware analysis, and SBOM generation for heterogeneous 5G components.
- Integrated **automated security gates in CI/CD pipelines (secure by design)**, including SAST, dependency and container scanning, continuous CVE monitoring, and security score computation to prevent vulnerable releases.
- Extended testing beyond static analysis using **dynamic analysis techniques**: applied **AddressSanitizer (ASAN)**, **ThreadSanitizer (TSAN)**, and **coverage-guided fuzzing** to uncover memory safety violations, race conditions, and crash-inducing inputs in 5G workloads.
- Developed a **runtime security rApp** for Kubernetes-based 5G network functions, leveraging **Tetragon/eBPF** to monitor execution, enforce least-privilege policies, and terminate unauthorized or malicious processes at kernel level.
- Validated end-to-end security under **realistic attack scenarios**: blocked malware execution, prevented lateral movement across pods, and enforced binary integrity and process allowlisting.
- Produced **consolidated security reports and quantitative scores** combining code quality, supply-chain risk, and runtime exposure to support informed remediation and hardening decisions.

MOABI Solutions (2 Months) — Sophia Antipolis **2025**
Kernel Symbol Table Leakage : ***Meltdown | KASLR | Kernel Reverse Engineering*** *France*

- Exploited Meltdown vulnerability to read protected kernel memory and reveal critical data.
- Combined KASLR prefetch side-channel techniques with Meltdown to locate and leak the kernel symbol table (___ksymtab).
- Analyzed leaked data to understand the runtime kernel functions and structure.
- Successfully demonstrated a complete attack chain bypassing KASLR and accessing kernel secrets.

EURECOM (3 Months) — Sophia Antipolis **2024**
Secure Python Libraries Detection & Malware Analysis *France*

- Designed a hybrid source-based method to detect Python malware.
- Built and labeled datasets; applied ML models to classify malicious PyInstaller binaries.
- Developed a prototype for detecting suspicious Python packages and libraries.
- Reverse engineered PyInstaller binaries to reveal malicious behavior and obfuscation patterns.