ELIA EL KHOURY

Security Automation & DevOps Engineer

eliaelkhoury.eng@gmail.com | linkedin/elia-elkhoury | github/lell0 | eliaelkhoury.vercel.app | +961 71 931 464

SUMMARY

Automation and DevOps focused security engineer with 5+ years designing, containerizing, and operating production automation infrastructure. Built a distributed, Docker-packaged attack surface management platform from scratch, automated security analysis pipelines alongside DevSecOps teams, and shipped 50+ orchestration playbooks and Python tools that run unattended across 30+ client environments. Track record of infrastructure-level impact: deployment time cut from hours to minutes via containerization, 40% MTTR reduction, 30% less manual toil, 60% faster automated reporting. Open to relocation; currently working remotely for a Dubai-based firm.

SKILLS

Automation & Orchestration: Python automation at scale, Palo Alto Cortex XSOAR (50+ playbooks, custom integrations, API-driven workflows), Bash scripting, scheduled/unattended job orchestration, event-driven pipelines

DevOps & Infrastructure: Docker (containerized multi-service sensor stack), GitHub Actions (CI/CD), Linux administration, Git, distributed controller/sensor architecture, MongoDB, deployment automation, DevSecOps pipeline integration

APIs & Integration: REST API design and consumption, third-party tool integration (SIEM, EDR, WAF), log ingestion pipelines, webhook/enrichment workflows

AI & Automation: Agentic AI workflows, LLM integration for triage/enrichment, Stable Video Diffusion, Computer Vision

Security Operations: Incident Response, Attack Surface Management, OSINT, Offensive Simulation, Phishing Analysis

Programming: Python, Java, Bash, C++, Flutter, Arduino

Encryption: Hybrid RSA/AES (EncChat)

EXPERIENCE

Cybersecurity & Automation Engineer

Sep 2022 – Present

Coordinates · Dubai, UAE (Remote)

- Architected and built an enterprise ASM platform from scratch in Python: distributed sensor-controller architecture, centralized server, MongoDB backend. Tracks 500+ external assets across 30+ client environments with automated vulnerability identification and remediation workflows.
- Containerized the full sensor stack with Docker, standardizing builds and cutting deployment time from hours to minutes across client environments.
- Partnered with the DevSecOps team to automate security analysis pipelines, embedding checks into delivery workflows; reduced false positives and improved detection coverage.
- Built and maintained REST integrations with third-party security tools to unify log ingestion, detection enrichment, and remediation automation across multiple client environments.
- Developed 50+ XSOAR playbooks and the Python automation behind them, orchestrating SIEM, EDR, and WAF workflows; 40% MTTR reduction, 35% less manual workload, triage cut from hours to minutes.
- Automated scheduling and execution of 20+ offensive simulations (scanning, exploitation) across deployed sensors, giving clients continuous, hands-off visibility into external exposure.
- Integrated agentic AI models into SOC operations for detection, triage, and response; LLM-based correlation and intel enrichment cut analyst intervention by ~30%.
- Engineered an end-to-end automated phishing check flow: malicious attachments, phishing indicators, redirect chains, malicious QR codes (quishing), homoglyphs, impersonation, spoofing, consolidated into structured triage output, significantly cutting email investigation time.
- Built a passive asset discovery workflow comparing expected vs. observed coverage per environment (missing assets, identity/role gaps, absent log sources) using SIEM queries and EDR telemetry; continuous blind-spot visibility with zero active-scan noise.

IoT Engineer

Jan 2022 – Sep 2022

SAWA Group · Baalbek, Lebanon

- Built an IoT flowmeter system tracking water volumes from trucks to tanks (Arduino Mega + NodeMCU) with a Flutter app for real-time telemetry and remote monitoring.
- Added a NodeMCU-hosted fallback web interface for manual control; maintained the platform through multiple feature and bug-fix cycles.

Cybersecurity Intern *Oct 2021 – Jan 2022*
Po.Tech Consulting · Mansourieh, Lebanon

- Ran 15+ OSINT investigations; wrote Python scripts automating passive recon, cutting manual research time by 50%.
- Extended the internal OSINT framework "Darkivor" with new techniques and performance improvements.

PROJECTS

EncChat: End-to-End Encrypted Messaging (Android) · *Personal Project*

- Android messaging app with hybrid RSA + AES encryption and zero plaintext exposure at rest or in transit; supports 50+ concurrent users. Evolved from a university prototype into an independently built and maintained product, released through an automated CI/CD pipeline.

Noblo: Restaurant Menu Platform · *Built with a collaborator*

- Multi-tenant B2B SaaS platform where restaurant businesses publish menus and diners browse them. Spring Boot (Java 25), PostgreSQL, and S3 behind a Next.js frontend on Cloudflare: per-tenant storefronts, drag-and-drop menu tree, JWT auth, admin approval flow, and a full audit log. CI/CD tests, builds, and deploys backend and frontend on merge. Live at noblo.xyz.

Calcendar: Scheduling & Billing · *Personal Project*

- Multi-tenant scheduling and billing for independent practitioners: Node.js, Express, and MongoDB with an EJS admin dashboard and a Flutter app. Recurring bookings with live conflict detection, per-client ledger in integer cents, TOTP two-factor, and CI/CD.

Attack Surface Management Platform · *Coordinates*

- Enterprise-grade ASM platform: remote controller, centralized server, distributed Dockerized sensor network spanning 500+ monitored assets across 30+ client environments. MongoDB-backed orchestration and automated security reporting cut report generation time by 60%.

AI Script-to-Animation Platform · *Zaka.ai*

- Collaborative platform automating multi-scene animation generation from single text prompts. Engineered a script-parsing pipeline segmenting prompts into logical scenes, producing high-fidelity images and 5-second clips per scene via Stable Video Diffusion; optimized SVD inference for consistent output across concurrent scene generations.

Phishing Check Flow · *Coordinates*

- End-to-end automated pipeline inspecting inbound email for malicious attachments, phishing indicators, unsafe redirect chains, malicious QR codes (quishing), homoglyphs, impersonation, and spoofing. Consolidates analysis into automated, structured results for faster triage and response.

Asset Discovery · *Coordinates*

- Passive discovery workflow comparing expected vs. observed coverage per client environment to surface missing assets, identity/role gaps, and absent log sources; SIEM queries and EDR telemetry only, no active-scan noise.

Water Truck Flow Meter (IoT) · *SAWA Group*

- IoT metering for water delivery: embedded sensing on Arduino Mega, NodeMCU connectivity, Flutter app for live field readings, plus a NodeMCU-hosted web UI fallback.

Face Mask Detector · *Michel Daher Social Foundation*

- Raspberry Pi computer-vision system with 90%+ mask detection accuracy, integrated with automated access control processing 100+ daily entries in real time.

CERTIFICATIONS

Zaka AI, Artificial Intelligence Program ..... *Dec 2025*
Google Cybersecurity Specialization ..... *Feb 2024*
Flutter Development Bootcamp with Dart ..... *Oct 2023*
JavaScript Algorithms & Data Structures, freeCodeCamp ..... *Mar 2023*
Supervised ML: Regression and Classification (Coursera / Stanford) ..... *May 2022*
Scientific Computing with Python, freeCodeCamp ..... *May 2022*
Practical Ethical Hacking, TCM Security ..... *Sep 2021*
CCNA: Enterprise Networking, Security & Automation ..... *Feb 2021*
CCNA: Switching, Routing & Wireless Essentials ..... *Jul 2020*
CCNA: Introduction to Networks ..... *Jun 2020*
Linux Essentials ..... *Jul 2020*

EDUCATION

B.Eng. in Computer & Telecommunications Engineering *Sep 2019 – Jun 2024*
Antonine University, Baabda, Lebanon