Naim Hariri

Beirut, Lebanon · +961 71 266 959 · naimhariri8@gmail.com · github.com/chefxx1 · linkedin.com/in/naim-hariri

EDUCATION

Beirut Arab University — B.S. Computer Science, Cyber Security Track — Sep 2023 – Jun 2026

- Relevant coursework: Network Security, Cryptography, Computer Networks, Operating Systems.

PROJECTS

CatalogAI — Senior Project — GitHub

Stack: React · Node.js · Express · MySQL · Gemini · Groq

- Led a four-person team to build an AI-powered SaaS platform for e-commerce product catalogs, developed in collaboration with Integrated Digital Systems (IDS) with weekly technical reviews.
- Developed the core workflow that turns hours of manual product research and copywriting into minutes: scan a barcode or photo, generate AI product listings with Gemini, and export to major e-commerce platforms.
- Implemented JWT authentication, Google OAuth, role-based access control, per-token rate limiting, Helmet security headers, input sanitization, and SHA-256 hashed password-reset tokens.

soc-log-analyzer — GitHub

Stack: Python · Sigma · MITRE ATT&CK · pytest

- Built a Python tool that parses Windows Security Event Logs and runs five ATT&CK-mapped detections (brute force, password spraying, privilege escalation, after-hours logins, external IP logins) using Sigma YAML rules.
- Generated SOC triage reports in text, JSON, and CSV, backed by a 24-test suite.

phishing-analyzer — GitHub

Stack: Python · Threat Intelligence APIs · pytest

- Developed an email triage tool that parses .eml files, runs nine header checks (SPF, DKIM, DMARC, spoofing, dangerous attachments), extracts IOCs, and enriches them through VirusTotal, URLhaus, and AbuseIPDB.
- Returns a MALICIOUS / SUSPICIOUS / CLEAN verdict with recommended analyst actions, validated by 49 tests.

network-traffic-analyzer — GitHub

Stack: Python · Scapy · MITRE ATT&CK · pytest

- Created a Scapy-based PCAP analyzer that detects C2 beaconing, port scanning, data exfiltration, DNS tunneling, and DGA domains using entropy and timing analysis.
- Outputs analyst reports, SIEM-ready JSON, and NIST 800-61 incident response reports, with 36 tests covering all detections.

EXPERIENCE

Community Operations Lead — Online Gaming Community (85,000+ members) — Remote · Jul 2021 – Feb 2026

- Managed operations and a team of staff for a large online gaming community, handling user issues and service delivery.
- Handled client communication end to end, fulfilling thousands of in-game service orders over five years of continuous operations.
- Configured and maintained game server files (spawn systems, loot tables, base configurations) and built a custom Python Discord bot that automated ticket responses and event scheduling, replacing previously manual work.

TECHNICALSKILLS

Languages: Python · Bash · SQL · JavaScript · C · HTML/CSS

Frameworks: React · Node.js · Express · REST APIs · LLM Integration (Gemini, Groq)

Security: MITRE ATT&CK · Sigma Rules · Log Analysis · SIEM Concepts · Incident Response · Threat Detection · Phishing Analysis · IOC Enrichment · Network Forensics · PCAP Analysis · NIST 800-61

Tools: Wireshark · Scapy · Sysmon · Wazuh (learning) · Git · Docker · MySQL

CERTIFICATIONS&AWARDS

- Google Cybersecurity Professional Certificate — Coursera
- Lebanese Collegiate Programming Contest (LCPC) — Participant

LANGUAGES

Arabic — Native · English — Fluent