RONY TADROS

Bsalim, Lebanon | (+961) 81-886-392 | tadrosrony@hotmail.com | www.linkedin.com/in/rony-tadros-233127235

WORK EXPERIENCE

ABSEGA **Jun–Jul 2026**
SIEM Engineering Intern *Lebanon*

- Contributed to the design and deployment of the ThePhish, TheHive, and Cortex triage stack for end-to-end phishing email analysis
- Configured and tuned Cortex threat intelligence analyzers to improve phishing-detection accuracy within the SOC workflow
- Integrated an AI-based agentic system into Wazuh to enhance automated alert triage and response

Hiperlinx **Aug 2025–Feb 2026**
Cybersecurity Analyst (Detection & SOC Engineering) *Lebanon*

- Conducted security assessments to help identify threats and vulnerabilities across client environments
- Worked as a Level 1 SOC analyst, monitoring and triaging security alerts
- Served as SOC engineer, supporting SIEM configuration and rule maintenance
- Created detection rules mapped to the OWASP Top 10

Arab Finance Corporation (AFC) **Jun–Sep 2024**
Junior IT Systems & Network Administrator *Lebanon*

- Administered Oracle systems: access, reporting, patching, backup and recovery, scripted in PL/SQL and Bash
- Ran daily system and security monitoring across servers, network devices, and Windows endpoints
- Maintained access control, IT asset inventory tracked in GLPI, technical documentation, and system upgrades

Saint Joseph University (USJ) **Jun–Aug 2023**
IT Support Intern *Lebanon*

- Imaged and deployed workstations, installed antivirus, joined machines to the domain, and repaired hardware faults

PROJECTS

Automated Phishing Analysis Lab
Self-directed home lab: ThePhish, TheHive, Cortex, Docker

- Deployed an automated phishing email triage integrating ThePhish, TheHive, and Cortex in a Dockerized Ubuntu environment
- Configured Gmail IMAP ingestion, enabled and tuned Cortex threat intelligence analyzers
- Developed a custom Cortex analyzer using oledump.py to detect malicious VBA macros in Office attachments, and extended ThePhish to automatically extract and analyze files inside ZIP/7z archives
- Validated the email achieving Safe/Suspicious/Malicious verdict classification with automated email notifications

Cloud Security Checklist Automation
Master's Project, USJ

- Automated an AWS and Azure security-checklist framework on Nessus, Prowler, and ScoutSuite
- Scripted compliance auditing, log monitoring, patch management, access auditing

EDUCATION

MSc, Cybersecurity, Saint Joseph University of Beirut (USJ) **Sep 2023–Jun 2025**

BSc, Computer Science, Saint Joseph University of Beirut (USJ) **Sep 2020–Jun 2023**

SKILLS

- **Detection & Response:** detection engineering (OWASP Top 10), SIEM (Wazuh), phishing and malware analysis, IR
- **Automation & Tools:** TheHive, Cortex, ThePhish, oledump.py, Nessus, Prowler, ScoutSuite, Docker
- **Cloud & Systems:** AWS, Azure security auditing, Linux (Ubuntu, Kali), Windows Server, networking
- **Code & Data:** Python, C#, C++, SQL, PostgreSQL, Oracle Database, MySQL
- **Languages:** Arabic (native), French and English (professional)

CERTIFICATIONS AND ACTIVITIES

Cisco CCNAv7: Introduction to Networks. Lebanese Scouts: member and leader, 2009–2023.