

Rony Tanios Tadros

[Address:](#) Bsalim, Lebanon

[Mobile:](#) +961 81 886 392 | [Email:](#) tadrosrony@hotmail.com | [LinkedIn:](#) www.linkedin.com/in/rony-tadros-233127235

About Me: Graduate with a Master’s degree in Cybersecurity and hands-on experience in SOC operations, SIEM administration, and IT systems and network administration. Experienced in threat detection, security monitoring, phishing analysis, and security automation. Passionate about cybersecurity, incident response, and developing practical security solutions that strengthen organizational security and improve SOC operations.

Education

2023-2025	Master’s Degree in Cybersecurity, University Saint Joseph (USJ)-Lebanon
2020 – 2023	Bachelor’s Degree in Computer Science, University Saint-Joseph (USJ) – Lebanon

Projects and co-curricular

I. Automated Phishing Email Analysis Lab — ThePhish SOC Integration

Cybersecurity Home Lab | Docker · TheHive · Cortex · Ubuntu

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.

II. International Open Bidding Competition 2022:

(From 25 march 2022 to 1 April 2022)

Took part in an international project that required working with teams of experts with various skills who were stationed abroad.

Create a web-based information system prototype as if you were submitting a proposal to be the contractor for a project with a deadline.

The prototype was written in HTML and CSS for the front end and PHP for the back end.

I worked on the database, we used MYSQL to create the tables

III. Automation of cloud security checklist:

Master project

Implemented an automated cloud security checklist to enhance cloud infrastructure security across AWS and Azure platforms.

Utilized tools such as Nessus, Prowler, and ScoutSuite for security scanning, compliance auditing, and threat detection. Automated processes including log monitoring, patch management, access auditing, incident remediation, and secure backup operations.

Contributed to continuous improvement by testing, reviewing, and documenting the security automation framework.

Experience

Internship at ABSEGA in the SIEM Department

(June 2026-July 2026)

- Contributed to the design and deployment of the ThePhish automated phishing analysis, integrating TheHive and Cortex for end-to-end email triage
- 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

Cybersecurity analyst at Hiperlinx

(from August 2025-February 2026)

- Conduct security assessments
- SOC analyst level 1
- SOC engineer
- Help identify threats and vulnerabilities
- Create detection rules based on the OWASP top 10

Junior IT system and network administrator at Arab Finance Cooperation (AFC)

(from June 2024-September 2024)

- Perform daily system and security monitoring
- Provide technical support and troubleshooting for employees
- Develop and maintain technical documentation and manuals
- Maintain access control, phone systems, and IT asset inventory
- Implement system upgrades and new technology solutions
- Manage Oracle systems (user access, reports, patching, and maintenance)
- Monitor and maintain database backup and recovery processes
- Ensure network security, server health, and software updates
- Install, configure, and maintain Windows-based systems
- Create utilities and scripts to optimize system performance

Internship at Saint Joseph university (USJ) in the support department

(from June 2023-August 2023)

- Tackle hardware-related challenges, including setting up new computers and ensuring proper image installation
- Implement necessary antivirus software on systems
- Diagnose and resolve hardware malfunctions (e.g., replacing faulty disks, identifying problematic RAM modules, addressing battery issues)
- Verify computer names for seamless university network domain registration
- Identify and resolve software anomalies and errors to ensure smooth operations

Leadership and Volunteering Activities

2009-2023	Lebanese Scout
-----------	----------------

Skills

LANGUAGES	Arabic (Native), French (Professional), English (Professional)
TECHNICAL	SIEM(Wazuh), SOC, Malware Analysis, Python, Security Automation, Linux(Ubuntu, Kali), Windows, Docker, Networking, PostregesSQL, Oracle Database, C#, C++
SOFT	Problem-solving, Teamwork, Leadership, Analatycal Skills, Adaptability, Communication.

Certification

CCNAV7: Cisco Introduction to Network