Rayen Gader

Cyber Security Engineer

Location: Ariana, Tunisia **Phone:** (+216) 27 80 58 84 **Email:** rayengader9@gmail.com **LinkedIn:** in/rayengader • rayengader.github.io

PROFILE

Cyber Security Engineer with **2+ years** in a managed SOC at Global IT Vision. Deploys and tunes client detection platforms (**Darktrace NDR**, **LogRhythm SIEM**, **CrowdStrike XDR**); **L2 SOC analyst** on the alerts they raise. Designed a full **NIST SP 800-61 aligned SOC** (**10 components**, 8 open source, **MTTD < 1 min**). **18 certifications**, **top 1% globally** on TryHackMe.

PROFESSIONAL EXPERIENCE

Cyber Security Engineer — **November 2023 – Present**
Global IT Vision — *Tunis, Tunisia*

- Commissioning, tuning and optimisation of the detection tooling across the client estate: use case design, correlation rule authoring, false-positive reduction.
- Qualification and in-depth investigation of escalated alerts: attack scenario reconstruction, root cause, containment, prioritised remediation and reporting to decision-makers.
- Proactive threat hunting, security posture advisory and upskilling of client teams.

Cybersecurity Intern — **May – June 2024**
Pwn & Patch Tunisia — *Tunis, Tunisia*

- **Phishing simulation project** taken from target to report: **OSINT** reconnaissance, custom phishing scenarios and templates, campaigns triggered and tracked through an **API**; fully functional and **completely documented** (reproducible procedure, awareness debrief).

Final-Year Intern (Bachelor's) — **February – July 2023**
DEFENSYLAB — *Tunis, Tunisia*

- **Cybersecurity training platform** (**Odoo**-based LMS) dedicated to **internal curricula**: module catalogue, learner paths, progress tracking and **hands-on labs** attached to each module; driven from requirements to **production release**.

PROJECTS & ACHIEVEMENTS

- **Full SOC aligned with NIST SP 800-61** (final-year project, Global IT Vision, 2026) — Detection and response chain built, deployed and validated end to end: **10 components**, **8 of them open source**, segmented by a **Palo Alto** NGFW — **Wazuh** (SIEM, 4 correlated sources, 8 agents), **Suricata** (NIDS), **CrowdStrike Falcon** XDR + *Identity Protection* on **Active Directory**, **TheHive/Cortex/MISP** (SOAR, VirusTotal/AbuseIPDB enrichment), **Zabbix/Prometheus/Grafana** (NOC) and **n8n** (notification). Validated by **2 MITRE ATT&CK scenarios** (FTP brute force, SQL injection, *webshell*): **MTTD < 1 min**, contextualised alert without human action.
- **APT34 (OilRig) threat analysis** — Profiling of the Iranian group (**MITRE ATT&CK G0049**): TTPs mapped across the *kill chain*, dissection of **3 malware families** (POWRUNER, BONDUPDATER, RDAT) and of the C2 infrastructure. Deliverables: actionable detection rules and **MITRE D3FEND** countermeasures.
- **Other** — Automated DNS/IP blocking from threat intelligence feeds (Python + PostgreSQL); AES, RSA and ECC implemented from the specifications; secure web applications (MERN, PHP/MySQL, *bcrypt*).

TECHNICAL SKILLS

Blue Team / SOC:	L2 SOC analysis • SIEM monitoring • threat hunting • incident response (NIST SP 800-61) • forensics
Platforms:	Darktrace NDR • LogRhythm SIEM • CrowdStrike Falcon XDR • Wazuh • Suricata • Palo Alto NGFW • TheHive • Cortex • MISP • Zabbix • Prometheus • Grafana • n8n
CTI & detection:	MITRE ATT&CK • D3FEND • OpenCTI • APT profiling • IoC analysis • VirusTotal • AbuseIPDB
Offensive:	Penetration testing • OSINT • phishing simulation • Burp Suite • Metasploit • Nmap • BloodHound • Hashcat
Standards:	NIST SP 800-61 • ISO/IEC 27001 • NIST CSF • CIS Controls • OWASP • PCI-DSS
Dev & systems:	Python • Bash • JavaScript • Node.js • SQL • Linux (RHEL, Kali, Parrot) • Windows Server • Active Directory

CERTIFICATIONS

- **eCDFP**, Digital Forensics Professional, INE — 2026
- **eCTHP**, Threat Hunting Professional, INE — 2026
- **eCIR**, Incident Responder, INE — 2026
- **eEDA**, Enterprise Defense Administrator, INE — 2026
- **eJPTv2**, Junior Penetration Tester, INE — 2025
- **CEH**, Certified Ethical Hacker, EC-Council — 2025
- **CSA**, Certified SOC Analyst, EC-Council — 2025
- **RHCSA**, Red Hat Certified System Administrator — 2024
- **LRSA**, LogRhythm Security Analyst — 2025
- **CCFA**, Certified Falcon Administrator, CrowdStrike — 2026
- **LRPA**, LogRhythm Platform Administrator — 2025
- **Darktrace**, Cyber Engineer — 2025
- **Darktrace**, Threat Visualizer Essentials — 2025
- **CNSP**, Certified Network Security Practitioner — 2025
- **BTJA**, Blue Team Junior Analyst — 2024
- **CPP**, ManageEngine PAM360 — 2024
- **CPP**, ManageEngine Key Manager Plus — 2024
- **THM**, Pentesting, Pentest+, Web Fundamentals — 2023

EDUCATION

Engineering Degree, Network & Information Systems Security — TEK-UP University, Tunis — 2023–2026
SOC Analyst certification track (CEH, CSA, CyberOps, ISO 27001) — Clevory Training, Tunis — 2024
Bachelor's Degree, Telecommunications & Network Security — ISET'COM, Tunis — 2020–2023

Languages: Arabic (native) • French (fluent) • English (fluent) • CTF: TryHackMe, HackTheBox