Rayen Gader

Ingénieur Cybersécurité

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

PROFIL

Ingénieur Cybersécurité, **+2 ans** en SOC managé chez Global IT Vision. Déploiement et réglage des plateformes de détection clients (**Darktrace NDR**, **LogRhythm SIEM**, **CrowdStrike XDR**) ; **analyste SOC L2** sur les alertes qu'elles produisent. Concepteur d'un **SOC aligné NIST SP 800-61** (**10 composants**, 8 open source, **MTTD < 1 min**). **18 certifications**, **Top 1 % mondial** sur TryHackMe.

EXPÉRIENCE PROFESSIONNELLE

Ingénieur Cybersécurité — **Novembre 2023 – Présent**
Global IT Vision — *Tunis, Tunisie*

- Mise en service, réglage et optimisation des outils de détection du parc client : conception des cas d'usage, écriture des règles de corrélation, réduction des faux positifs.
- Qualification et investigation approfondie des alertes escaladées : scénario d'attaque, cause racine, confinement, remédiation priorisée et restitution aux décideurs.
- Chasse aux menaces proactive, conseil en posture de sécurité et montée en compétence des équipes clientes.

Stagiaire Cybersécurité — **Mai – Juin 2024**
Pwn & Patch Tunisia — *Tunis, Tunisie*

- **Projet de simulation de phishing** mené de la cible au rapport : reconnaissance **OSINT**, scénarios et modèles d'hameçonnage personnalisés, campagnes déclenchées et suivies par **API** ; chaîne pleinement fonctionnelle et **intégralement documentée** (mode opératoire reproductible, sensibilisation).

Stagiaire de fin d'études (Licence) — **Février – Juillet 2023**
DEFENSYLAB — *Tunis, Tunisie*

- **Plateforme de formation cybersécurité** (LMS sous **Odoo**) dédiée aux **cursus internes** : catalogue de modules, parcours apprenants, suivi de progression et **labs pratiques** rattachés à chaque module ; conduite du besoin à la **mise en production**.

PROJETS & RÉALISATIONS

- **SOC complet aligné NIST SP 800-61** (PFE, Global IT Vision, 2026) — Chaîne de détection et de réponse montée, déployée et validée de bout en bout : **10 composants** dont **8 briques open source**, segmentés par un pare-feu **Palo Alto** — **Wazuh** (SIEM, 4 sources corrélées, 8 agents), **Suricata** (NIDS), **CrowdStrike Falcon** XDR + *Identity Protection* sur l'**Active Directory**, **TheHive/Cortex/MISP** (SOAR, enrichissement VirusTotal, AbuseIPDB), **Zabbix/Prometheus/Grafana** (NOC) et **n8n** (notification). Validée par **2 scénarios MITRE ATT&CK** (force brute FTP, injection SQL, *webshell*) : **MTTD < 1 min**, alerte contextualisée sans intervention humaine.
- **Analyse du groupe APT34 (OilRig)** — Profilage du groupe iranien (**MITRE ATT&CK G0049**) : TTP cartographiées sur la *kill chain*, dissection de **3 familles de maliciels** (POWRUNER, BONDUPDATER, RDAT) et de l'infrastructure C2. Livrables : règles de détection et contre-mesures **MITRE D3FEND**.
- **Autres** — Blocage DNS/IP automatisé à partir de flux de renseignement (Python + PostgreSQL) ; AES, RSA et ECC implémentés depuis les spécifications ; applications web sécurisées (MERN, PHP/MySQL, *bcrypt*).

COMPÉTENCES TECHNIQUES

Blue Team / SOC :	Analyse SOC L2 • supervision SIEM • chasse aux menaces • réponse à incident (NIST SP 800-61) • forensic
Plateformes :	Darktrace NDR • LogRhythm SIEM • CrowdStrike Falcon XDR • Wazuh • Suricata • Palo Alto NGFW • TheHive • Cortex • MISP • Zabbix • Prometheus • Grafana • n8n
CTI & détection :	MITRE ATT&CK • D3FEND • OpenCTI • profilage d'APT • analyse d'IoC • VirusTotal • AbuseIPDB
Offensif :	Tests d'intrusion • OSINT • simulation de phishing • Burp Suite • Metasploit • Nmap • BloodHound • Hashcat
Normes :	NIST SP 800-61 • ISO/IEC 27001 • NIST CSF • CIS Controls • OWASP • PCI-DSS
Dév. & systèmes :	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

FORMATION

Diplôme d'Ingénieur, Sécurité des Réseaux et Systèmes d'Information — Université TEK-UP, Tunis — 2023–2026
Formation certifiante Analyste SOC (CEH, CSA, CyberOps, ISO 27001) — Clevory Training, Tunis — 2024
Licence, Télécommunications & Sécurité des Réseaux — ISET'COM, Tunis — 2020–2023

Langues : Arabe (maternelle) • Français (courant) • Anglais (courant) • CTF : TryHackMe, HackTheBox