RAYEN GAIED

+216 99-454-709 | rayen.gaied@eniso.u-sousse.tn | Tunis, Tunisie (Ouvert à la mobilité)
in/rayen-gaied | github.com/rayenTech | 𝕄 medium.com/@Cyberayen

Profil

Ingénieur en Technologies de l'Information et de la Communication, spécialisé en Cybersécurité, axé sur le développement de solutions de sécurité avancées mettant l'accent sur l'utilisation de l'intelligence artificielle (IA) et d'outils open source afin d'automatiser les processus, renforcer la sécurité des systèmes et garantir la conformité aux normes de gouvernance et de gestion des risques.

Domaines d'Expertise

Surveillance des opérations de cybersécurité - Détection et réponse aux incidents - Évaluation et gestion des vulnérabilités - Surveillance et audit de la sécurité des réseaux - Automatisation des politiques et de la gestion des risques - Automatisation des audits de sécurité et de performance basés sur l'IA - Automatisation des audits de conformité et de risque.

Formation

Ing. TIC, Spéc. Cybersécurité *École Nationale d'Ingénieurs de Sousse* **Sousse, Tunisie** *2022-2025*
Cours principaux : Sécurité des réseaux, Sécurité sans fil et mobile, Big Data, Processus stochastiques, QoS, Machine Learning, Techniques avancées & DevOps.

Classe Préparatoire MPSI *Institut Préparatoire de Monastir* **Monastir, Tunisie** *2020-2022*
Cours principaux : Mathématiques, Physique avancée, Programmation orientée objet, Python, Bases de données.

Expérience Professionnelle

Consultant en Cybersécurité *(Talan)* **Tunis, Tunisie** *02/2025 - 08/2025*
- Développer et tester des LLMs pour automatiser l'analyse d'alertes dans un SOC, incluant la recherche de similarité et l'indexation via vector embeddings, permettant de réduire les faux positifs de 61%.
- Intégrer des flux de Cyber Threat Intelligence dans Security Onion et Elastic pour enrichir les indicateurs de compromission de 100% et améliorer la détection des menaces.

Stagiaire en Sécurité des Applications *(PURA Solutions)* **Sousse, Tunisie** *07/2024 - 09/2024*
- Concevoir et configurer un environnement de test pour sécuriser les données médicales dans le cloud avec Wazuh, Flask RBAC et Redis.
- Analyser les vulnérabilités avec Nessus, OWASP ZAP et Nmap et mettre en place une authentification sécurisée via OAuth 2.0.
- Simuler des attaques, examiner les journaux et produire des rapports de sécurité détaillés.

Pentester et Analyste Vulnérabilités *(Hacktify Cyber Security)* **En ligne, Inde** *01/2024 - 03/2024*
- Auditer les vulnérabilités avec Nessus et prioriser les correctifs.
- Investiguer les incidents de sécurité, incluant accès non autorisé et malwares, à l'aide de Wireshark et ELK Stack.
- Exploiter les failles via Metasploit et Burp Suite pour tester la robustesse des systèmes.

Stagiaire en Télécommunications *(Tunisie Telecom)* **Sousse, Tunisie** *07/2023 - 09/2023*
- Configurer et optimiser les routeurs ADSL/VDSL pour un fonctionnement sécurisé et performant.
- Analyser les réseaux mobiles 3G/4G et identifier les vulnérabilités.
- Collaborer avec l'équipe de recherche pour évaluer la sécurité et les protocoles mobiles.

Certifications

- ISC2 Cyber Security Certified - ISC2
- Certified Cybersecurity Technician (C-CT) - EC-Council
- Red Hat OpenShift Administration I: Operating a Production Cluster 4.14 - RedHat
- Fortinet Certified Associate in Cyber Security - Fortinet
- Google Cyber Security Professional - Google

Compétences

- **Outils de sécurité :** Wireshark, Nmap, OWASP ZAP, RSA Archer, pare-feu, IPS/IDS, ELK Stack, SIEM, Active Directory, Cyber Threat Intelligence (CTI)
- **Référentiels et standards :** ISO 27001, NIST CSF, RGPD
- **Outils réseau et virtualisation :** Protocoles Internet (TCP/IP, IPsec. . .), Cisco Packet Tracer, VMware ESXi, KVM, XEN, Docker
- **Intelligence artificielle et apprentissage automatique :** LLMs, SLMs, RAGs, ingénierie de prompts, modèles d'embedding, bases de données vectorielles
- **Langages de programmation :** Python, C, MATLAB, Bash
- **Systèmes d'exploitation :** Linux/Unix, Windows
- **Cloud computing :** Microsoft Azure, Google Cloud Platform (GCP)

Projets et Publications Sélectionnés (Plus de projets disponibles sur mon GitHub)

- **Interpréteur d'alertes IA pour analystes SOC** (En cours) : Déployer un système IA avec LangChain, FAISS et LLMs pour interpréter automatiquement les alertes IDS/IPS, avec enrichissement des données via OpenCTI, génération d'analyses lisibles et envoi de notifications, ce qui permet de réduire le MTTD et le MTTR de 33%.
- **Simulation SIEM pour la visualisation de données de sécurité** (Sep. 2024) : Développer une simulation SIEM en Python pour transmettre en temps réel des incidents de sécurité à ThingSpeak et assurer la visualisation des données via des graphiques interactifs. GitHub
- **Système de détection et de réponse aux menaces avec VirusTotal, Wazuh et ELK Stack** (Août 2024) : Mettre en place Wazuh pour détecter les anomalies en temps réel et intégrer l'API VirusTotal pour analyser automatiquement les fichiers suspects. Centraliser, traiter et visualiser les logs via l'ELK Stack pour renforcer la détection des menaces et améliorer l'efficacité de la réponse.
- **DevSecOps : Revue de littérature multivocale** (Gaied, R., 2024) : Rédiger une revue de littérature complète sur l'évolution, les défis et les bénéfices de l'intégration de la sécurité dans les pratiques DevOps, en automatisant et en collaborant entre équipes de développement, opérations et sécurité. Medium
- **WEBCHAT** (Déc. 2023) : Développer une application simple utilisant HTML, JavaScript natif et Flask pour le concours "Nuit de l'Info 2023", permettant de communiquer avec l'API OPENAI déployée sur Azure. GitHub

Leadership et Engagement Communautaire

- Classé dans le top 1% mondial sur la plateforme CyberDefenders Blue Teaming, 3^{e} place en Tunisie.
- Membre et activiste du North American Tunisian Engineers Group (NATEG) à l'ENISo, où je contribue activement aux initiatives et événements.
- Formateur en cybersécurité à l'American Corner / AMIDEAST Sousse, où je dispense des formations impactantes et sensibilise à la sécurité numérique.
- Diplômé avec distinction de l'Institut AMEL, reconnu pour mon expertise en sécurité numérique et ma contribution à la défense des droits humains.
- Ancien innovateur et chercheur à l'Association Tunisienne pour le Futur de la Science et de la Technologie (ATAST), où j'ai mené des projets de recherche et d'innovation.
- Ancien Ambassadeur pour le Dialogue en Tunisie, formé par l'initiative de dialogue du Danish Youth Council (DUF), où j'ai promu le dialogue et la médiation.