Anass El Mazdougui

Étudiant Ingénieur en dernière année en Cybersécurité à l'INPT — En recherche de stage PFE

+212 6 49 01 17 58 — anasselmazdougui@gmail.com — LinkedIn
Portfolio — TryHackMe (Top 1%)

Profil

Étudiant ingénieur en **cybersécurité** à l'INPT, avec de solides bases en **SOC**, **SIEM** et **SOAR**.Passionné par la **détection de menaces** et la **sécurité des systèmes d'information**, classé **Top 1% sur TryHackMe**. En recherche d'un **stage PFE en cybersécurité** dès **janvier/février 2026**.

Formation

Institut National des Postes et Télécommunications (INPT), Rabat 2023 – 2026
Cycle d'Ingénieur en Cybersécurité et Confiance Numérique Rabat

FST Al Hoceima 2021 – 2023
DEUST en Mathématiques-Informatique-Physique (MIP) Al Hoceima

Expérience Professionnelle

SEKERA GROUP 07/2025 – 09/2025
Stagiaire en Cybersécurité

- Développement d'un outil Python d'analyse forensique d'emails intégrant un moteur d'analyse multi-couches (**headers, URLs, contenu, images et fichiers joints**)
- Intégration du système dans la chaîne de traitement du **SOC** pour automatiser le triage et l'enrichissement des alertes emails, réduisant le **temps d'analyse des emails**
- Centralisation des résultats dans un **rapport unifié** permettant une prise de décision rapide sur la criticité des incidents

Projets Académiques et Personnels

Déploiement d'un workflow d'automatisation entre LimaCharlie (EDR) et Tines (SOAR)

- Conception et déploiement d'un **système automatisé de détection et réponse** aux cybermenaces
- Développement de **règles de détection** pour les outils de credential dumping (**LaZagne**)
- Implémentation de **workflows d'isolation automatique** des endpoints compromis via **Slack/Email**
- *Outils :* ***LimaCharlie EDR, Tines SOAR, Slack API, règles YARA***

Intégration CTI avec ELK SIEM

- Intégration réussie de la **Cyber Threat Intelligence (CTI)** dans un **SIEM basé sur ELK**
- Enrichissement des logs collectés avec des **indicateurs de menace internes et externes**
- Amélioration de la **corrélation des événements** et génération d'**alertes plus pertinentes**
- *Outils :* ***ELK Stack (Elasticsearch, Logstash, Kibana), MISP, feeds CTI***

Déploiement IDS/SIEM complet avec pare-feu

- Conçu et déployé une **infrastructure de sécurité complète** incluant un pare-feu **pfSense**, un **IDS Suricata** et une intégration avec **Wazuh**
- Architecture permettant une **détection proactive**, une **réponse rapide** et une **visibilité complète** sur la sécurité du réseau
- *Outils :* ***pfSense, Suricata IDS, Wazuh SIEM,monitoring temps réel***

Compétences Techniques et Interpersonnelles

- **Réseaux & Protocoles :** TCP/IP, UDP, FTP, DNS, DHCP, VLAN, VPN, NAT
- **Routage & Commutation :** OSPF, BGP, ACL supervision réseau
- **Sécurité des Réseaux :** IDS/IPS, pare-feu, SIEM, détection et corrélation d'événements
- **Systèmes & Virtualisation :** Linux (Debian/Ubuntu), Windows Server, VMware, VirtualBox
- **Outils d'Intrusion :** Nmap, Hydra, John, WPScan, Burp Suite, Metasploit
- **Programmation et Automatisation :** Python, Bash,C,scripts d'analyse et de réponse
- **Soft Skills :** Communication claire, esprit d'équipe, adaptabilité, sens du conseil

Certifications

- **Junior Cybersecurity Analyst Career Path — Cisco**
- **Cybersecurity Fundamentals — IBM**
- **Practical Ethical Hacking — TCM Academy**

Langues

- **Arabe** — Maternelle
- **Français** — Courant
- **Anglais** — Professionnel