OUCHINE NABYL

Junior Cybersecurity Analyst & Engineer – En dernière année d'ingénierie en cybersécurité, à la recherche d'un stage PFE.

+212 720421930 nabylouchine@gmail.com Nabyl OUCHINE

Profil

Étudiant en dernière année d'ingénierie à l'INPT, passionné par l'**ingénierie de la cybersécurité** et l'**analyse SOC**. Motivé par la **détection**, l'**investigation** et l'**automatisation** des incidents, ainsi que par la **conception**, le **déploiement** et l'**amélioration continue** des solutions de sécurité, je souhaite mettre mes compétences au service de la **protection** et de la **résilience des systèmes d'information**.

Parcours Académique

Institut National des Postes et Télécommunications (INPT) **2023 – Présent**
Ingénieur d'État en cybersécurité et confiance numérique *Rabat*

Faculté des Sciences et Techniques (FST) **2021 – 2023**
Diplôme d'Études Universitaires Scientifiques et Techniques (DEUST) *Errachidia*

Expérience Professionnelle

Stage en cybersécurité — GSNA Solutions **Juil. – Août 2025**

Développement d'un prototype de tests d'intrusion automatisés avec l'IA (**Gemini, DeepSeek**) et intégration de la génération de rapports. Utilisation d'outils offensifs (**Kali Linux, Metasploit, Nmap, Nikto, Gobuster**), participation à la **CTI**, contribution aux démarches **ISO 27001** et gestion de projet en **Agile**.

Stage en cybersécurité — SEKERA **Mai. – Juin 2025**

Automatisation de l'analyse forensique des emails par IA . Workflow complet : parsing des en-têtes (SPF, DKIM, DMARC), extraction d'IOC et scoring de risque avec **LLM**. Enrichissement via **VirusTotal, Shodan, AbuseIPDB** et reporting automatisé pour accélérer les investigations SOC.

Stage en cybersécurité – Analyste SOC — EncryptedGelabs **Mars – Mai 2025**

Opérations SOC et analyse de menaces. Collecte et gestion de logs (**Syslog, ELK, Wazuh**) et détection/réponse aux incidents avec SIEM (**Splunk, Wazuh**). Intégration de Threat Intelligence et simulation d'attaques pour renforcer la sécurité.

Projets académiques

Network Traffic Analysis – PCAP Investigation **2025**

- Analyse de fichiers **PCAP** pour détecter des activités suspectes et corréler le trafic réseau à des incidents de sécurité à l'aide de **tcpdump** et **Wireshark**.
- **Compétences et outils** : tcpdump, Wireshark, analyse réseau, protocoles TCP/IP, investigation SOC.

SOC Architecture with CTI-based Detection on AWS **févr – juin 2025**

- Conception et déploiement sur **AWS EC2** d'une architecture SOC intégrant **Elastic Stack**, **TheHive**, **MISP**, **Cortex** et **OTX**, avec **Docker**, pour l'automatisation de la corrélation des **IoC CTI** et la création de **règles de détection personnalisées**.
- **Compétences et outils** : AWS, Docker, Elastic Stack, TheHive, MISP, Cortex, OTX, automatisation SIEM.

Réponse automatisée aux incidents avec SOAR & EDR **févr 2025**

- Création de playbooks SOAR avec **Tines** et intégration de **LimaCharlie** pour l'EDR, permettant alertes automatiques et isolement des endpoints compromis.
- **Compétences et outils** : Tines, LimaCharlie, SOAR, EDR, automatisation des réponses.

Compétences

- **Sécurité SOC & Forensique**: Détection et investigation des incidents | Analyse de logs systèmes, réseaux et sécurité | Investigation d'alertes SIEM | Application des frameworks **MITRE ATT&CK** et **Cyber Kill Chain** | Réponse aux incidents.
- **Réseaux et protocoles**: Routage et commutation (OSPF, RIP, ISIS, BGP) | VLAN, ACL, VPN, IPSEC | TLS/SSL, HTTPS, cryptographie et chiffrement | Sécurité réseau : pare-feu, IDS/IPS.
- **Outils** : **Splunk**, **Wazuh**, **TheHive**, **Cortex**, **VirusTotal**, Kali Linux, Atomic Red Team | Packet Tracer, GNS3.
- **Virtualisation & conteneurisation**: VMware, VirtualBox, Vagrant, Docker.
- **Automatisation & scripting**: Scripts Bash pour automatisation des workflows SOC.
- **Compétences interpersonnelles**: Rigueur, analyse critique, gestion du stress, travail en équipe.

Langues

Anglais : lu , écrit , parlé **Français** : lu , écrit , parlé **Arabe** : lu , écrit , parlé (bilingue)