# OUCHINE NABYL

**Étudiant ingénieur en dernière année spécialisé en cybersécurité, à la recherche d'un stage PFE**

+212 720421930 nabylouchine@gmail.com Nabyl OUCHINE

## Profil

Étudiant en cybersécurité à l'INPT, passionné par les environnements **SOC**, la détection et la réponse aux incidents. Motivé par l'investigation d'alertes et l'amélioration des défenses, je souhaite mettre en pratique mes compétences en **analyse de logs, détection d'incidents et automatisation des workflows SOC** tout en contribuant à la sécurité opérationnelle des organisations.

## 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 d'automatisation de tests d'intrusion avec IA (**Gemini, DeepSeek**) et pipelines **Python** pour la découverte de vulnérabilités et la génération de rapports (HTML/PDF). Expérience pratique sur **Kali Linux, Metasploit, Nmap, Nikto, Gobuster**. Participation aux activités de **Cyber Threat Intelligence (CTI)** et contribution aux initiatives **ISO 27001**. Coordination d'équipe et suivi 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

**Intégration de la Cyber Threat Intelligence dans un SIEM Open Source** **avr – juin 2025**

- Déploiement sur **AWS EC2** d'un SIEM basé sur **ELK Stack**, enrichi par **MISP** et **OTX** pour l'automatisation et la corrélation des IoC.
- **Compétences et outils** : AWS, ELK, MISP, OTX, Filebeat, automatisation SIEM.

**End-to-End SOC Architecture with Threat Intelligence on AWS** **févr – avr 2025**

- Mise en place d'une architecture SOC scalable intégrant **Elastic Stack**, **TheHive**, **MISP** et **Cortex**, orchestrée avec **Docker**.
- **Compétences et outils** : AWS, Docker, Elastic Stack, TheHive, MISP, Cortex, VirusTotal API.

**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)