

# Mohammed Sbihi

Maroc - Fès

+212 6 36 20 88 30 | mohammedsbihi11@gmail.com | med10s.github.io | Med10S | mohammed-sbihi

## Résumé

Élève ingénieur en 5<sup>e</sup> année en Réseaux et Télécommunications, spécialisé en cybersécurité, passionné par la protection des systèmes d'information et le développement de solutions de sécurité innovantes.

**Objectif :** Réaliser un stage de Projet de Fin d'Études (PFE) en cybersécurité pour développer des systèmes de sécurité avancés et contribuer à l'innovation en matière de détection intelligente des menaces.

## Éducation

### École Nationale des Sciences Appliquées de Fès (ENSAF)

ÉTUDIANT EN INGÉNIERIE DES RÉSEAUX ET TÉLÉCOMMUNICATIONS

Fès, Maroc

Sept. 2021 – Présent

- Poursuite d'un diplôme en Ingénierie des Réseaux et Télécommunications avec une spécialisation en Cybersécurité.
- Développement d'une expertise en sécurité des réseaux et en systèmes de détection d'intrusion.

## Expérience Professionnelle

### Centre Hospitalier Universitaire (CHU) de Fès

STAGIAIRE EN INGÉNIERIE CYBERSÉCURITÉ (PROJET SOC)

Fès, Maroc

Juin 2025 - Août 2025

- Conception et déploiement de A à Z d'un Security Operations Center (SOC)** pour la surveillance d'une infrastructure hospitalière critique.
- Intégration d'une stack SIEM/SOAR complète** incluant Wazuh pour la détection, TheHive pour la gestion des cas, Cortex pour l'analyse et MISP pour le renseignement sur les menaces.
- Automatisation avancée des workflows de réponse aux incidents** via n8n (Node.js) et des scripts Bash, réduisant les temps de réaction manuels.
- Développement de preuves de concept (PoC) d'attaques** (ex: EternalBlue) en Ruby et C pour valider et renforcer l'efficacité des règles de détection de l'IDS (Suricata).

### SNRT

STAGE EN ARCHITECTURE RÉSEAU

Rabat, Maroc

Juillet 2024 - Août 2024

- Réalisation d'un projet de topologie réseau avec GNS3, permettant la modélisation et l'analyse de divers scénarios de sécurité.
- Simulation d'une attaque par Déni de Service (DoS) pour évaluer la résilience du réseau.
- Optimisation des dispositifs pare-feu et des politiques de sécurité afin de renforcer la protection contre les cybermenaces.

## Projets

### Conception et mise en œuvre d'une solution de sécurité complète

Projet de Stage - CHU de Fès

DÉPLOIEMENT D'UN SOC AVEC STACK SIEM/SOAR

Juin 2025 - Août 2025

- Objectif :** Créer un Security Operations Center (SOC) fonctionnel pour détecter, analyser et répondre aux cybermenaces dans un environnement hospitalier.
- Démarche :** Déploiement automatisé de la stack complète (Wazuh, TheHive, Cortex, MISP, Suricata) avec des scripts Bash. Développement de workflows d'orchestration avec n8n pour lier les alertes à la création de cas et à l'analyse automatisée. Validation des défenses par la simulation d'attaques réelles.
- Impact :** Mise en place d'une solution de sécurité proactive, réduisant les délais de réponse et augmentant la visibilité sur les menaces potentielles.

Technologies : Wazuh, TheHive, Cortex, MISP, Suricata, n8n, Sense, OSQuery, Bash, Python, Node.js, Ruby, C, Docker.

### Système de Détection d'Intrusion Distribué (IDS)

ENSAF - Projet de Fin d'Année

IA - CYBERSÉCURITÉ - ARCHITECTURE DISTRIBUÉE

Janvier 2025 - En cours

- Intelligence Artificielle :** Développement d'un ensemble de modèles ML (KNN, MLP, XGBoost) avec 98.1% de précision pour la détection d'intrusions réseau.
- Architecture Microservices :** Conception d'un système distribué temps réel avec capture de paquets, extraction de features UNSW-NB15 et API FastAPI.
- Technologies Avancées :** Stack complète Python, Docker, Redis, Prometheus avec analyse de 9 types d'attaques (DoS, Reconnaissance, Exploitation, etc.).

### Détection d'Anomalies de Connexion avec Java et Isolation Forest

ENSAF

MACHINE LEARNING - CYBERSÉCURITÉ

Nov. 2024 - Déc. 2024

- Développement Backend :** Génération et simulation de logs en Java.
- Machine Learning :** Détection des connexions anormales à l'aide d'Isolation Forest.
- Cybersécurité :** Identification des accès suspects en dehors des horaires habituels.
- Big Data & Analyse :** Traitement et analyse des logs pour la détection d'anomalies.

### Simulation d'un SOC

ENSAF

DEVOPS - CYBERSÉCURITÉ

Février 2025 - Mars 2025

- Cybersécurité :** Détection d'attaques (DDoS, scans, intrusions) avec Suricata.
- DevOps & Conteneurisation :** Déploiement automatisé sur GNS3 avec Docker.
- Virtualisation & Réseaux :** Simulation d'un réseau sécurisé.
- Big Data & SIEM :** Analyse et visualisation des logs avec l'ELK Stack.

## Compétences

|                                      |  |
|--------------------------------------|--|
| <b>Cybersécurité (SIEM/SOAR)</b>     | Wazuh, TheHive, Cortex, MISP, Suricata (IDS/IPS), pfSense, OSQuery     |
| <b>Programmation &amp; Scripting</b> | Bash (automatisation), Python (API), Node.js/JavaScript (n8n), Ruby, C |
| <b>Outils &amp; Environnements</b>   | Docker, Git, GNS3, API REST, Linux, Virtualisation                     |
| <b>Langues</b>                       | Français (Natif), Anglais (Courant), Arabe (Natif)                     |

## Récompenses

---

|      |  |       |
|------|--|-------|
| 2024 | <b>Gagnant</b> , CTF CYBERTHECHDAY 1.0 | ENSAF |
|------|--|-------|

## Activités Parascolaires

---

|               |                       |
|---------------|-----------------------|
| <b>SECOPS</b> | ENSAF                 |
| PRÉSIDENT     | Juin 2024 - Juin 2025 |

- Dirigé et coordonné les activités du club SECOPS, en mettant l'accent sur la cybersécurité et la sensibilisation aux menaces numériques.
- Organisé des sessions de formation, des ateliers et des défis CTF pour améliorer les compétences des membres en cybersécurité.
- Développé des projets simulant des cyberattaques et des stratégies de défense en utilisant des technologies telles que GNS3, Suricata et le Machine Learning.