Ilias Belharda

Ingénieur Cybersécurité | SOC & Blue Team (Junior)
Morocco | +212 600102919 | belharda.ilias@gmail.com | ilias belharda | Portfolio

Profil

Ingénieur cybersécurité junior avec une expérience pratique en opérations SOC, simulation d'attaques APT et sécurisation d'Active Directory.
Solide expertise en détection des menaces, réponse aux incidents et supervision SIEM via Wazuh, combinée à la sécurité réseau et IDS/IPS avec Suricata.
À l'aise en sécurité défensive tout en maîtrisant les fondamentaux du pentest, avec de bonnes compétences en documentation et en travail collaboratif.

Compétences Techniques

- **Sécurité offensive** : Pentest, tests d'intrusion, injection SQL, phishing, reconnaissance
- **Sécurité défensive** : Wazuh, Suricata, durcissement Active Directory, IDS/IPS
- **Forensique & analyse** : reverse engineering, sandboxing, analyses forensiques
- **Outils & compétences en développement** : SQLMap, Meterpreter, Nessus, Wireshark, Sage, Burp Suite, développement logiciel
- **Systèmes** : Windows Server, Linux, VMware / VirtualBox
- **Réseaux** : Nmap, OSINT, SMB, sécurisation des connexions

Education

Université Internationale de Rabat (UIR) **2023 - 2025**
Master en Cybersécurité *Rabat*

Université Internationale de Rabat (UIR) **2020 - 2023**
Classes Préparatoires intégrées - Informatique *Rabat*

Certifications

- **Fortinet: FCSS – OT Security 7.2 Self-Paced**
- **Cisco Networking Academy: Introduction to IoT and Digital Transformation**
- **Cisco Networking Academy: Introduction to IoT (Course Completion)**
- **Huawei: HCIA-IoT V3.0 – 2024-05-23**
- Red Hat System Administration I 9.0

Expérience Professionnelle

AXA GBS **Feb 2025 - Aug 2025**
Stage de fin d'études (SOC/BLUE Team) *Rabat*
Projet : Simulation d'une attaque APT sur une infrastructure Active Directory et mise en place de mesures de défense – Mention Très Honorable

- Conception et déploiement d'une infrastructure Active Directory virtualisée
- Simulation complète d'une attaque APT (reconnaissance, phishing, injection SQL, exploitation, persistance, mouvement latéral, SMB)
- Mise en œuvre de contre-mesures défensives : SIEM Wazuh, Suricata IPS, durcissement AD, contrôles anti-phishing
- Supervision et analyse de plus de 20 alertes de sécurité via une plateforme SIEM
- Tri, classification, escalade et documentation des incidents
- Collaboration avec les équipes réseau et sécurité dans le cadre des processus de
- réponse aux incidents

TBEM **Jul 2024 - Aug 2024**
Stagiaire assistant ingénieur *Rabat*

- Analyse de vulnérabilités et contribution au renforcement de la sécurité des systèmes d'information

Milroad **Aug 2024 - Sep 2024**
Stagiaire technicien *Safi*

- Configuration de routeurs et switches, dépannage réseau et documentation sécurité

NTSI Tanger **Jul 2022 - Aug 2022**

Stagiaire ouvrier *Tanger*

- Utilisation de Sage pour la gestion commerciale et tâches techniques liées aux réseaux

Langues

•Francais (TCF B2)
•Anglais (EFSET C1)
•Arabe (Native)

Projets Académiques

Analyse du Dark Web & Reverse Engineering d'exploits
Création d'un environment sandbox, reverse engineering de contenus d'exploit, évaluation des risques

Simulation d'attaque de phishing
Développement d'un clone Spotify pour sensibilisation à la cybersécurité

Forensique Navigateur

Analyse des activités utilisateur avec Browser History Examiner

Injection NoSQL
Présentation technique et démonstration d'exploitation