Ilias Belharda

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

Summary

Junior Cybersecurity Engineer with hands-on experience in SOC operations, APT attack simulation, and Active Directory security. Strong background in threat detection, incident response, and SIEM monitoring using Wazuh, combined with network security and IDS/IPS using Suricata.

Experienced in both defensive security and penetration testing foundations, with solid documentation and collaboration skills.

Technical Skills

- **Offensive Security**: Pentesting, Penetration Testing, SQL Injection, phishing, reconnaissance
- **Defensive Security**: Wazuh, Suricata, AD Hardening, IDS/IPS
- **Forensics & Analysis**: Reverse engineering, sandboxing, forensics
- **Tools & Development Skills**: SQLMap, Meterpreter, Nessus, Wireshark, Sage, Burp Suite, Software Development
- **Networking**: Nmap, OSINT, SMB, Secure connections
- **Systems**: Windows Server, Linux, VMware/VirtualBox

Education

Université Internationale de Rabat (UIR) **2023 - 2025**
Master's Degree, Cybersecurity *Rabat*

Université Internationale de Rabat (UIR) **2020 - 2023**
Integrated Preparatory Classes, Computer Science Track *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

Professional Experience

AXA GBS **Feb 2025 - Aug 2025**
Final Year Internship (SOC/BLUE Team) *Rabat*
Project: Simulation of an APT attack on an Active Directory infrastructure and implementation of defense measures – Graduated with High Honors

- Designed and deployed a virtualized test infrastructure
- Conducted full APT simulation (reconnaissance, phishing, SQLi, exploitation, persistence, lateral movement, SMB) as part of penetration testing exercises
- Implemented countermeasures: Wazuh, Suricata IPS, hardening, anti-phishing, AD strengthening
- Tools used: SQLMap, Meterpreter, Nessus, Suricata, Wazuh
- Managed security incidents using a SIEM platform: received alerts, performed classification, and escalated critical events
- Alert reception, classification, and escalation
- Incident response procedures (analysis, prioritization, documentation)
- Collaborated closely with network and security teams, providing clear communication and guidance on defense measures

TBEM **Jul 2024 - Aug 2024**
Assistant engineer intern *Rabat*

- Performed vulnerability analysis and exploratory security testing, contributing to information system security hardening within a software development environment

Milroad **Aug 2024 - Sep 2024**
Technician intern *Safi*

- Router/switch configuration, network troubleshooting, security documentation

NTSI Tanger **Jul 2022 - Aug 2022**
Worker intern *Tanger*

- Used Sage for commercial management
- Performed technical tasks related to networking

Languages

- •French (TCF B2)
- •English (EFSET C1)
- •Arabic (Native)

Academic Projects

Dark Web Analysis & Exploit Reverse Engineering

- •Analyzed exploit forums on the Selfless Web
- •Created a secure sandbox environment
- •Reverse engineered downloaded content
- •Assessed security risks and provided recommendations

Phishing Attack

- •Developed a Spotify clone to simulate a phishing attack and raise awareness

Browser Forensics

- •Analyzed browsing history with Browser History Examiner
- •Extracted and correlated user activities

NoSQL Injection

- •Delivered technical presentation and live demonstration
- •Exploited vulnerabilities in NoSQL databases