Oussama EL Maskaoui *Elève ingénieur en Cyber Security*

oussama.elmaskaoui@gmail.com
+212 614974221
Casablanca, Maroc
oussama-el-maskaoui

Education

2023/09 – 2026/06
RABAT, MAROC

Ecole Mohammadia des ingénieurs
Génie Réseaux et Cybercecurity
- Actuellement en dernière année génie Réseaux et Telecom.

Expérience Professionnelle

2025/04 – 2025/09
Casablanca, Maroc

SOC analyst
Sekera
Projet Vinici Logic - Plateforme d'Automatisation SOC avec IA
- Développement d'une plateforme d'automatisation SOC basée sur des agents IA (LangChain/LangGraph) pour l'investigation autonome des alertes
- Architecture multi-agents pour TheHive, OpenSearch SIEM, Microsoft 365 et analyse de menaces et de phishing (OCR, sandbox, enrichissement)
- Intégration multi-sources : VirusTotal, AbuseIPDB, Microsoft Graph API, avec reporting aligné MITRE ATT&CK
- **Résultats** : -70% MTTR, 85% d'automatisation L1, zéro false positif escaladés

Certificats

- CompTIA Security + (SY0-701)
- Aws Cloud Practitioner essentiels
- SOC analyst Path (LetsDefend)
- CCNA : introduction to network

Projets Personnel

Active Directory
- Configuration d'Active Directory et mise en place d'un Domain Controller, avec simulation d'une attaque via Kali Linux, analysée et visualisée à l'aide de **Splunk**.

Automating Threat Detection and Response with SOAR & EDR
- Mise en place d'un système automatisé de détection et de réponse aux menaces avec **Lima Charlie (EDR) & Tines (SOAR)** .

SOC Lab with n8n (en cours)
- Déploiement d'un environnement SOC intégré combinant **Security Onion** (NSM), **Wazuh** (SIEM/EDR), **TheHive/Cortex** (gestion d'incidents et enrichissement IOC) et **n8n** (orchestration SOAR) pour la détection, l'analyse et la réponse automatisée aux menaces.

Vulnerability Assessment
- Utilisation de Nessus sur Kali Linux pour identifier et analyser les vulnérabilités d'une machine virtuelle Windows, renforçant ainsi la sécurité du système.

Home lab
- Simulation d'une attaque réseau avec Kali Linux, analyse du trafic avec Wireshark, et configuration de pare-feu sur Ubuntu pour renforcer la sécurité.

Compétences

Analyse et sécurité
- Wireshark Tenable Nessus, Active directory , splunk, ElasticSearch, opensearch ,Wazuh ,sysmon, SOAR, EDR, TheHive, Linux , bash scripting ,VirusTotal, AbuseIPDB, Shodan, MITRE ATT&CK, Anyrun .

Public speaking
- Compétence affirmée en prise de parole en public

Langages de programmation
- Python , language C et SQL

Intelligence artificielle et automatisation
- LangChain, APIs IA, Agents LLM, Automatisation SOC

Langues

- Anglais
- Francais
- Arabe