OMAR EL KADIRI

Rabat, Hay Rachad omarelkadiri2035@gmail.com 0659855701 in/omar-el-kadiri

SUMMARY

Étudiant en Ingénierie Informatique - Cyber Sécurité et Confiance Numérique (II-CCN), passionné par la sécurité des SI, la détection des menaces, les SOC et les solutions SIEM. Intéressé par l' intégration de l'IA en cybersécurité, je recherche un stage ingénieur PFA pour approfondir mes compétences et contribuer à des projets concrets et innovants en cybersécurité.

EXPERIENCE

Stage - Implémentation d'un SIEM avec Elastic Stack

Ministère du Transport et de la Logistique **Août 2024 - Septembre 2024, Agdal, Maroc**

- Mise en place d'un réseau virtuel sécurisé dédié à la collecte centralisée des logs, avec installation et configuration des agents de surveillance (Packetbeat, Filebeat, Syslog). Développement de mécanismes de détection automatique des attaques (DoS/DDoS, brute-force, connexions suspectes) et création d'un système d'alerte automatisé via scripts Bash et intégration avec Slack. Renforcement de la sécurité des communications avec SSL/TLS pour l'ensemble de la stack Elastic.

PROJECT

Conception d'un Système de Détection d'Intrusions basé sur l'IA avec algorithmes supervisés

- Classification des attaques via dataset NSL-KDD, optimisation pour réduire les faux positifs, déployé avec Flask/Streamlit.

Détection d'Attaques et Sécurisation d'Infrastructure (en cours - équipe de 6 personnes)

- Projet visant à concevoir une infrastructure sécurisée avec DMZ, double pare-feu, Active Directory et port mirroring, mise en place d'un système de détection multi-modèles intégré à un SIEM ELK avec Zeek et Suricata, pour analyser les logs (AD, réseau, etc) et détecter les attaques en temps réel.

Conception d'une infrastructure sécurisée à double pare-feu

- Déploiement d'une infrastructure segmentée (DMZ, LAN, Local_Service, ADMIN) avec OPNsense et pfSense en double pare-feu, Intégration de Zeek (IDS) et Suricata (IPS) pour la surveillance et la prévention des intrusions. Mise en place de services essentiels (DNS, Apache, Samba), sécurisés via Webmin, avec routage statique, NAT hybride et filtrage basé sur le moindre privilège.

Détection des Anomalies Réseau avec ML - SIEM Elastic Stack

- Développement d'un système de détection autonome d'anomalies réseau via un algorithme de la ML Isolation Forest, intégré à Elastic Stack. Prétraitement des logs en Python, backend Java pour analyse temps réel, alertes automatisées (Slack, Dashboard) et interface JavaFX.

EDUCATION

Ingénierie Informatique : Cybersécurité et Confiance Numérique | ENSET Mohammedia | 2023 - 2026

DEUST MIP (Mathématiques, Informatique, Physique) | FST Errachidia | 2021 - 2023

SKILLS

Réseaux & Systèmes : Notions essentielles en réseaux, virtualisation, cloud, conteneurisation, IoT. Administration et sécurisation des systèmes Windows (Active directory, GPO) & Linux, configuration de firewalls.

Cybersécurité & SIEM : Analyse des menaces, gestion et corrélation des logs, SIEM avec Elastic Stack (collecte, normalisation, détection des menaces, dashboards), détection des attaques via les IDS/IPS. Gestion des risques (EBIOS, MEHARI), cryptographie, blockchain, sécurité des SI.

Cyber & IA : Intégration de l'intelligence artificielle dans les solutions de sécurité

Développement & Programmation : C, C++, Java, Python, JavaScript, PHP, structures de données, analyse de complexité, scripting Bash.

Langues : Arabe : maternelle, Français : B2, Anglais : A2

Soft Skills : Déterminé, créatif, adaptable, responsable, vital en groupe et doté de compétences en résolution de problèmes.

CERTIFICATIONS

- Huawei : HCIA-Security V4.0
- Cisco : CyberOps Associate (50%), Linux Unhatched, Linux Essentials, Networking Essentials, Introduction to IoT
- Red Hat : Linux Fundamentals 9.1.