KHODOR JLAILATI

Beirut, Lebanon • khodorjlaylati@outlook.com • (+961) 81614171 • linkedin.com/in/khodor-jlailati

EXPERIENCE

CYBERARM **Beirut, Lebanon**
SOC Analyst **2021-Present**

- Monitored and inspected alerts within the SIEM console to identify malicious activities.
- Analyzed security events derived from data sources such as NIDS, Firewalls, DNS, and Windows Events, where the total number of events was more than 50 million.
- Implemented filtering rules to drop unnecessary events by 35%, optimizing storage use and improving system efficiency.
- Fine-tuned the alarms dashboard for an accurate alerting system by establishing suppression rules that reduce false positive alerts by 40%.
- Performed static and dynamic malware analyses utilizing FLARE VM for host-based indicators and REMnux for network-based indicators; Collected IOCs from more than 10 malware samples.
- Developed new use cases on the SIEM platform to generate optimized and efficient alerts by 20%.
- Provided vital support to security incident managers and team members during major security incidents.
- Conducted vulnerability assessments on more than 200 servers.
- Analyzed phishing emails to detect potential threats and improved email security measures.
- Generated customized reports through the SIEM console to support investigations and meet client needs.
- Enhanced SIEM platform efficiency by optimizing storage, achieving a remarkable 35% reduction in the projected data consumption.
- Developed over 20 targeted use cases, improving alarm efficiency.
- Wrote and deployed batch files that automated data collection, extracting logs from over 200 servers. The process streamlined data access and analysis.
- Achieved a notable 40% increase in threat detection and incident response efficiency within the initial six months, contributing significantly to the overall security posture of the organization.
- Played a vital role in revamping the security infrastructure and implementing cutting-edge technologies.

EDUCATION

ARTS, SCIENCES AND TECHNOLOGY UNIVERSITY IN LEBANON **Beirut, Lebanon**
Bachelor of Science in Computer Science **2017-2021**

- Presented an ecommerce mobile application using Flutter framework developed by Google.

CERTIFICATIONS

- Technical Associate for Detection & Response by **Trend Micro Campus**
- eLearn Security Junior Penetration Tester by **INE** (eJPTv2)
- Practical Malware Analysis & Triage by **TCM Security**
- Network Security Associate 1, NSE2 and NSE3 by **Fortinet**
- Google IT Support Professional Certificate by **Google**
- INE Certified Cloud Associate by **INE**

SKILLS

- Linux | Windows Server| Wireshark | Procmon | Process Hacker | Autorun | Fiddler | Burp Suite | FlareVM| OleTools| TCPView| USM Anywhere | Security Monitoring | Vulnerability Assessment | SIEM | Root Cause Analysis | Phishing Analysis | Cyber Kill Chain | MITRE ATT&CK | Ethical Hacking

LANGUAGES

- **Arabic:** Native | **English:** Fluent