Nima Khalil

SOC Analyst | Cybersecurity & Security Monitoring Specialist

+971 56 328 8867

Nimaterawi@gmail.com

Dubai, United Arab Emirates

https://nima-12-7.github.io/portfolio/#/home

About Me

Cybersecurity professional with a Master's degree in Cybersecurity and over five years of experience in IT operations and secure software development. Hands-on training in SOC operations including SIEM (Splunk), log analysis, alert triage, and incident response simulations. Experienced in system monitoring, access control, and data protection within government environments. Seeking a SOC Analyst (L1) position in the UAE.

Core Competencies

Security Operations

- Security Monitoring & Alert Triage 24/7
- Log Analysis & Event Correlation
- SIEM (Splunk – hands-on labs)
- Incident Response Fundamentals

Threat Detection (Phishing, Brute-force, Flood Attacks)

Security & Forensics Tools

- FTK Imager
- Autopsy
- Maltego
- Wireshark
- FortiGate Firewall (basic configuration)

Systems & Networking

- Windows & Linux Administration
- VMware
- TCP/IP Fundamentals
- Backup & Restore Procedures

Programming & Automation

- Python (Automation, Pandas, Security Scripts)
- Odoo (Python Backend)
- Django
- SQL Queries
- VBA

Data & Reporting

- Power BI

Professional Experience:

Ministry of Finance – Security-Focused Web Developer

Aug 2023 – Oct 2025

- Implemented data protection practices to safeguard sensitive financial information.
- Monitored application and system logs to detect suspicious activities and potential security incidents.
- Assisted in strengthening internal security controls and access management.

PACI organization - Web Developer

(Nov 2021 _ Aug 2023)

- Assisted in maintaining system integrity and data protection standards.
- Designed and implemented a Loan Management System using Odoo (Python backend).
- Performed system monitoring and troubleshooting.
- Conducted data recovery and managed content security practices.

Kima Company _ Network Support

(Sep 2019 _ Sep 2020)

- Installing and configuring systems (Windows/Linux)
- Performing backups and restores
- Preparing VMWare machines
- Developing System (VBA/SQL server)

UNV _ IT Technician

(Jan 2012 _ Jan2017)

- Provided first-level IT support for hardware, software, and network issues.
- Managed ticketing systems and incident tracking.
- Implemented endpoint protection and antivirus updates.
- Promoted secure computing practices across the organization.

Projects (Security-Focused)

- Conducted simulated SOC investigations using Splunk logs.
- Performed network traffic analysis using Wireshark.
- Investigated phishing and brute-force attack scenarios in lab environment.
- Developed Python scripts for log parsing and anomaly detection.

Certifications and Trainings

- Cisco Certified Network Associate (CCNA)
- Network +
- Security +
- Maintenance A+
- Threat Intelligence (Training Completed)
- EC-Council SOC Training (In Progress – Hands-on Splunk Labs)

Education

- Master's Degree in Cybersecurity – Arab American University (2024).
- Bachelor's Degree in Information & Communication Technology – Al-Quds Open University (2011)

Languages

- Arabic – Native
- English – Professional Working Proficiency