OMAR K. MESLMANY

Beirut, Lebanon | +961 71568979 | Omar12z@outlook.com

PROFESSIONAL SUMMARY

SOC Analyst with hands-on experience in enterprise Security Operations Center (SOC) environments, specialized in real-time threat monitoring, security event correlation, and incident triage using IBM QRadar and Splunk. Skilled in analyzing high-volume log data across network, endpoint, and Active Directory environments to identify Indicators of Compromise (IOCs) and suspicious patterns. Experienced in Tier 1 alert triage, structured escalation, and incident documentation aligned with industry best practices.

TECHNICAL SKILLS

- SIEM Monitoring & Event Correlation
- IBM QRadar & Splunk Log Analysis
- Alert Triage & Incident Escalation
- MITRE ATT&CK; (Basic Knowledge)
- TCP/IP, DNS, DHCP
- Windows Administration & Active Directory Log Review
- Wireshark (Basic Packet Inspection)

EDUCATION

Bachelor of Science (BS) in Information & Communication Technology – Lebanon

PROFESSIONAL EXPERIENCE

SOC Analyst Trainee – PO Tech (SOC Team) | Jan 2025 – Dec 2025 •

Monitored security events using IBM QRadar and Splunk

• Investigated SIEM offenses and correlated logs from multiple sources

• Performed Tier 1 alert triage and validated security events

• Escalated confirmed incidents according to SOC procedures

• Prepared detailed technical incident reports

IT Support Intern – AzkaTech (Beirut) | Oct 2018 – Jun 2019

• Provided first-level technical support

• Diagnosed hardware and software issues

IT Support Intern – Al Khair Fund (Dar Al Fatwa) | Oct 2019 – Apr 2020

• Installed and configured workstations and software
• Provided end-user technical assistance

IT Support Intern – Iso Green | Mar 2021
• Delivered on-site IT support
• Resolved technical issues and system malfunctions

Community Facilitator – ACTED | Aug 2020 – Jan 2021
• Coordinated outreach activities and supervised volunteers
• Prepared structured operational reports

LANGUAGES

- Arabic – Native
- English – Very Good
- French – Very Good