Ali Ajam

SOC Analyst

ali.ajam7117@gmail.com +961 81 817 846 Lebanon linkedin.com/in/ali-ajam7

PROFILE

SOC Analyst with hands-on experience in Tier 1 security operations within an MSSP environment. Experienced in SIEM monitoring, alert triage, phishing analysis, and incident escalation across multiple client environments. Strong foundation in networking, Active Directory, and cloud fundamentals, with a focus on building deep blue team expertise and security operations mindset.

EXPERIENCE

SOC Analyst Intern 10/2025 – PRESENT
Potech Remote, Lebanon

- Monitored security events using a centralized SIEM platform to detect suspicious activity across multiple client environments.
- Performed Tier 1 alert triage, validating severity and distinguishing false positives from potential security incidents.
- Investigated alerts by analyzing logs, indicators of compromise (IOCs), and event context, escalating confirmed threats according to SOC procedures.
- Conducted phishing email investigations, including header analysis, URL and attachment inspection, and reputation checks using VirusTotal.
- Operated effectively in a fast-paced, high-pressure SOC environment, managing multiple alerts while maintaining investigation accuracy.
- Maintained clear incident documentation, investigation notes, and SOP updates to support SOC workflows.
- Assisted in training and mentoring interns, explaining SOC workflows, alert triage methodology, and investigation steps.

EDUCATION

Bachelor of Computer Science 10/2024 – 06/2027
Lebanese International University

SKILLS

- SIEM Monitoring & Alert Triage
- Incident Detection, Validation & Escalation
- Phishing & Email Security Analysis
- Active Directory & Identity Fundamentals
- Networking Fundamentals
- Windows & Linux Fundamentals
- SOC Documentation, SOPs & Playbooks

PROJECTS

Active Directory Security Lab

- Deployed and configured a Windows Server Active Directory environment with Windows client machines.
- Created and managed Organizational Units (OUs), users, and security groups following enterprise-style structure.
- Implemented Group Policy Objects (GPOs) to enforce system and user security policies.
- Demonstrated understanding of identity and access management concepts relevant to SOC monitoring and investigations.

CERTIFICATIONS

- AWS Certified Cloud Practitioner
- Cisco CCNA: Introduction to Networks
- TCM Security - Practical Help Desk Associate