Mohamed Salaheldin Ibrahim

Soc Analyst

Mosalah.desouki@gmail.com +201016808959 Egypt mohamedsalah-blue-team

SUMMARY

Junior SOC Analyst with experience in alert triage, log analysis, and incident response across enterprise attack scenarios. Strong understanding of attack chains, MITRE ATT&CK mapping, and containment decision-making. Experienced with Splunk and QRadar for Windows and Linux telemetry in regulated environments

SKILLS

•SIEM & Detection Splunk (searching, alert investigation, dashboards) IBM QRadar (offense analysis, log correlation), •TCP/IP, DNS, HTTP fundamentals SOC workflows and case handling, •Alert triage and escalation IOC identification and enrichment MITRE ATT&CK mapping Containment and eradication planning, •Operating Systems & Logs Windows Event Logs, basic Windows forensics Linux logs and process analysis

PROJECTS

Threat Intelligence & Incident Response: Full Domain Compromise Analysis, AMIT 03/2025 – 09/2025

•Investigated a simulated Active Directory compromise from initial access via malicious macro to persistence and data exfiltration. •Analyzed Windows event logs and endpoint telemetry to reconstruct the attack timeline. •Mapped attacker techniques to MITRE ATT&CK, including SMB lateral movement (T1021.002) and account manipulation (T1098.002). •Identified IOCs such as malicious executables, C2 infrastructure, and unauthorized accounts. •Produced an incident response report with containment, eradication, and hardening recommendations.

Hands-on Labs & Training (TryHackMe), SOC Level 1

Completed 150+ labs focused on alert triage, phishing analysis, log investigation, and threat intelligence. • Practical exposure to SOC workflows, attacker TTPs, and incident response processes.

PROFESSIONAL EXPERIENCE

Banque Misr, 02/2016 – Present | New Cairo

Administrative Assistant (Corporate Banking & Syndicated Loans) ,

•Supported users in a regulated banking environment, handling email, access, and connectivity issues. •Performed password resets, account troubleshooting, and escalation following internal procedures. •Worked within compliance and audit-driven workflows requiring accurate documentation. •Coordinated with IT teams to resolve incidents and maintain operational continuity.

EDUCATION

Cairo University, Bachelor of Law

CERTIFICATES

(ISC)² CC - Cyber Security Certified

Blue Team Cybersecurity Diploma – AMIT

Grade - 100

TryHackMe SOC Level 1