Mohammed Ziyad

Burbank, IL 60459 · moefire610@gmail.com · (708) 265-9864 · linkedin.com/in/mohammed-ziyad-b41a2224a

SOC Analyst · CompTIA Security+ Certified

SUMMARY

Entry-level SOC analyst, CompTIA Security+ certified (SY0-701), with hands-on practice working simulated SOC alert queues end to end: alert triage, investigation in Splunk (SIEM), Wireshark, and Windows and Linux logs, phishing analysis, true vs. false positive decisions, and incident response documentation through closure or escalation. Brings nine years as a General Manager handling escalations under pressure, keeping regulatory compliance records, and holding a team to written procedures.

CERTIFICATIONS & TRAINING

- CompTIA Security+ (SY0-701) — CompTIA, October 2026 (valid through October 2029)
- Mastercard Cybersecurity Job Simulation — Forage, November 2026
- Splunk Education — Intro to Splunk and Using Fields (eLearning), October 2026
- ITIL 4 Foundation — 2025 · Google Foundations of Cybersecurity — Coursera, 2025
- Google IT Support Professional Certificate — Coursera, 2023

SKILLS

Security operations: alert triage, security monitoring, incident response (NIST SP 800-61 lifecycle), true vs. false positive analysis, log analysis, phishing and email header analysis, threat detection, indicators of compromise (IOCs), MITRE ATT&CK, escalation
Tools: Splunk (SIEM: SPL searches, fields, reports), Wireshark, Windows Event Logs, Linux command line, LetsDefend SOC simulator (EDR, log management, email security, case management)
Security controls: firewalls, IDS/IPS, EDR, proxies, identity and access management (IAM), MFA, SSO, encryption, PKI, vulnerability management
Networking and systems: TCP/IP, DNS, DHCP, common ports and protocols, Windows, Linux, Active Directory basics, troubleshooting
Governance, risk and compliance (GRC): NIST Cybersecurity Framework (CSF), risk assessment, HIPAA, PCI DSS, ISO 27001, ITIL 4 incident and change management

SECURITY PROJECTS & HANDS-ON LABS

SOC alert triage and case management — *LetsDefend SOC Analyst Simulator (Hack The Box)*

- Worked a simulated Tier 1 alert queue end to end: prioritized alerts by severity, investigated each with EDR, log management, and email security tools, and closed or escalated every case with a written note
- Separated true positives from false positives and recorded the evidence behind each verdict

SIEM and phishing investigations — *TryHackMe SOC Level 1 path*

- Investigated simulated incidents through Splunk searches, Wireshark packet captures, and Windows and Linux event logs
- Took phishing emails apart — headers, sender domain, links, and attachments — and documented each verdict
- Mapped attacker activity to MITRE ATT&CK and used the Pyramid of Pain to decide which IOCs to prioritize

Phishing awareness simulation — *Mastercard Cybersecurity Job Simulation (Forage)*

- Designed a simulated phishing email for a security awareness campaign, built on the pretexts and warning signs real attackers use
- Interpreted the simulation results to find where staff were most at risk and where awareness training was needed

Incident reconstruction from evidence — *CyberDefenders blue team challenges*

- Rebuilt the timeline of simulated attacks from packet captures and log evidence to establish what happened and when

EXPERIENCE

General Manager · John's Live Poultry · Chicago, IL *2017–Present*

- Handle the day's problems as they come — customer issues and escalations, staffing gaps, inventory discrepancies — deciding what gets fixed now and what gets escalated, and documenting each one through to resolution
- Keep the business compliant with health, safety, and regulatory requirements: maintain the required records, follow up on every gap, and correct the underlying process so it doesn't recur
- Reconcile inventory and ordering against records, investigate the cause of discrepancies, and correct them early
- Enforce documented standard operating procedures; supervise, schedule, and train staff and manage time and attendance

Freelance PC Builder & Technician · Self-employed · Chicago, IL *2024–Present*

- Built and delivered 50+ custom desktop PCs for paying customers, from choosing parts that fit each customer's budget and needs through assembly and testing
- Install and set up Windows, drivers, and updates on every build; troubleshoot hardware and startup problems so every system runs reliably at delivery

EDUCATION

Reavis High School — High School Diploma