AHMED MOHAMED ELNAHAS

SOC Analyst (L1) — Cybersecurity Student

Damanhour, Egypt | +20 155 568 9884 | ae320455@gmail.com | linkedin.com/in/ahmed-elnahas | github.com/ae320455-art

PROFESSIONAL SUMMARY

Cybersecurity student specializing in SOC operations, log analysis, and threat hunting. Hands-on practical experience across Splunk, Elastic/Kibana, and Volatility gained through structured blue-team labs (CyberDefenders, TryHackMe, LetsDefend, Blue Team Labs Online). Comfortable investigating phishing, malware, network intrusions, and memory forensics cases end to end, and mapping findings to MITRE ATT&CK. Seeking an entry-level SOC Analyst L1 role or freelance security analysis engagement.

TECHNICAL SKILLS

- SIEM & Log Analysis: Splunk (SPL), Elastic Stack / Kibana (KQL)
- Forensics: Volatility 2 & 3 (memory forensics), Wireshark, tcpdump (network forensics)
- Detection & Monitoring: Suricata, Sigma rules, Snort rules, IOC extraction, alert triage
- Frameworks: MITRE ATT&CK mapping, incident response lifecycle
- Other: TCP/IP & network fundamentals, phishing email analysis, vulnerability assessment basics, OSINT

PRACTICAL EXPERIENCE

Blue Team Lab Practitioner — *Self-directed / Home SOC Lab* Ongoing

- Built and maintain a home SOC lab (Ubuntu Server on VMware) running Splunk with the BOTSv3 dataset for realistic investigation practice.
- Completed hands-on investigations on CyberDefenders: ElasticCase, Ramnit, Reveal, DumpMe, HoneyBOT, XLMRat, and Web Investigation challenges.
- Practiced SPL query writing and log correlation via TryHackMe (Splunk Basics, Exploring SPL) and additional exercises on LetsDefend, Blue Team Labs Online, and CyberHaze.
- Worked structured malware and phishing analysis cases through TCM Security's SOC 101 course, including PCAP-based investigations and phishing email breakdowns.
- Analyzed SQL injection attempts, Log4Shell exploitation artifacts, and network intrusion patterns using Elastic/Kibana and Splunk in parallel.

EDUCATION

B.Sc. in Accounting and Information Systems — Cybersecurity Track — *Damanhour National University*

- Coursework: Discrete Mathematics, Computer Networks (OSI/TCP-IP), Information Security Fundamentals

CONTINUOUS LEARNING

- TryHackMe — Splunk Basics, Exploring SPL
- TCM Security — SOC 101
- CyberDefenders, Blue Team Labs Online, LetsDefend, CyberHaze — ongoing blue-team lab practice

FREELANCE / INDEPENDENT SERVICES

- Log analysis and SIEM query support (Splunk)
- Threat hunting and IOC identification
- Incident investigation and security reporting
- Security consultation for small teams and individuals

LANGUAGES

Arabic (Native) • English (Professional working proficiency)