Ziad Mohamed Amer

SOC Analyst Tier 1

ziad.amer200@gmail.com | 01092561554 | Cairo | https://www.linkedin.com/in/ziadamer111/

| Military Status: Completed

Profile

Aspiring SOC Analyst with a strong passion for cybersecurity and a commitment to protecting organizations from digital threats. Possesses excellent analytical skills with a deep focus on investigation. Eager to contribute to a Security Operations Center (SOC) team by leveraging a proactive mindset and a dedication to continuous learning.

Education

Bachelor in Computer Science (GPA : 2.9) **09/2019 – 07/2023**
El-Shorouk Academy

Graduation Project (Excellent)
Uni-Bus, Developed a comprehensive Flutter-based transportation system tailored for university students.

Experience

We Innovate | SOC Track (3 months) **01/2025 – 04/2025**

- **SOC Engineering**
  Developed and implemented a home lab environment to simulate a SIEM. Configured and deployed Winlogbeat and Filebeat on multiple VMs to collect and forward logs to ELK.
- **Splunk labs** (boss of the soc)
- **Threat Detection**
  Developed and implemented detection rules to identify and mitigate security threats, including brute force attacks, unauthorized Windows Registry modifications.
- **Phishing**
  identifying phishing threats, including email and social engineering.
- **Incident Response**
  Responded to security incidents by identifying, containing, and resolving threats. Investigated issues, documented findings, and helped prevent future attacks.
- **SOAR**
  using Tines integrated with VirusTotal API to build a (SOAR) platform, automating the handling of security alerts.
- **Threat Intelligence**
  Conducted in-depth research on SYS01 (MetaStealer), identifying IOCs and mapping TTPs to the MITRE ATT&CK framework, Additionally, investigated the Black Basta Ransomware Campaign, focusing on its exploitation of Microsoft Teams phishing tactics.

Skills

- **Network Concepts:** Understanding OSI model, Firewalls, VLans and Monitor network traffic
- **SIEM Tools:** Experience with Splunk, ELK Stack (Elasticsearch, Kibana).
- **Threat Detection:** Knowledge of detecting malware, phishing, brute force attacks, and privilege escalation.
- **Log Analysis:** Proficient in analyzing logs from Windows Event Viewer, Syslog, and Firewalls.
- **Network Analysis:** Skilled in using Wireshark for packet capture and traffic analysis.
- **Endpoint Security:** Basic understanding of EDR tools (CrowdStrike).
- **Network Security:** Understanding of firewalls, IDS/IPS, and network protocols (TCP/IP, DNS, HTTP/HTTPS).
- **Threat Intelligence:** Ability to research IOCs and map TTPs to MITRE ATT&CK framework.
- **Automation Tools:** Familiarity with SOAR platforms (e.g., Tines).
- **Operating Systems:** Proficient in Windows and Linux environments.
- **Vulnerability Management:** Basic knowledge of vulnerability scanning tools (Nessus, OpenVAS).

Tools

- Elasticsearch & Kibana
- MITRE ATT&CK
- The Hive
- Urlscan
- VirusTotal
- Splunk
- ANY.RUN
- MISP
- MxToolbox
- Wireshark

Courses

- SANS SEC 450 Blue Team Fundamentals | Self-Study (in progress)
- TCM SOC 101 (in progress)
- CompTIA Security+ | Netriders Academy
- eJPT | Netriders Academy
- MCSA (Active Directory) | Self-Study
- CCNA | Self-Study

Certificates

Computer Network Fundamentals | MaharaTech ITI Learning Platform

Introduction to Network Security | MaharaTech ITI Learning Platform

Activities

CyberDefenders | Hands-on

TryHackMe | Hands-on

acm International Collegiate Programming Contest