Mostafa Mahmoud Mabrouk

SOC Analyst Intern | SOC Tier 1 | Blue Team

+201149496432 | mostafamahmoud01005376205@gmail.com | Cairo, Egypt | Linkedin.com/in/mostafa-mahmoud

SUMMARY

Third-year Information Technology student specializing in Cybersecurity and Blue Team operations, with hands-on experience in security monitoring, log analysis, and Tier 1 security alert triage. Familiar with SOC workflows, SIEM-based monitoring, and initial incident investigation using digital forensics and OSINT techniques. Seeking a SOC Analyst Internship or SOC Tier 1 Trainee role to support detection, analysis, and escalation within a Security Operations Center environment.

EDUCATION

Bachelor of Information Technology - Faculty of Computers & Information – Luxor University | Jun 2027

TECHNICAL SKILLS

• **SOC & Blue Team Operations:** Security Monitoring, Alert Triage, Log Analysis, Incident Detection, Initial Incident Investigation, SOC Workflows
• **SIEM & Security Monitoring:** Splunk, ELK Stack, SIEM Monitoring
• **Digital Forensics & DFIR:** Autopsy, FTK, Volatility Framework, Eric Zimmerman Forensic Tools, Memory Analysis, Disk Analysis
• **Network Analysis & Monitoring:** Wireshark, tcpdump, Tshark, NetworkMiner, Network Traffic Analysis
• **Threat Intelligence & OSINT:** OSINT Fundamentals, IOC Identification, Threat Analysis

HANDS-ON SECURITY LABS & PRACTICAL EXPERIENCE

- Monitored security events and analyzed alerts using SIEM platforms (Splunk, ELK Stack).
- Conducted initial incident investigation and alert triage aligned with SOC Tier 1 responsibilities.
- Applied digital forensics techniques in DFIR labs, including memory and disk analysis.
- Participated in Blue Team labs and Capture The Flag (CTF) challenges simulating real-world attack scenarios.

CERTIFICATIONS

- **eCTHP – Certified Threat Hunting Professional** - INE Security | 2025
- **Introduction to Cybersecurity – Cisco**

COURSES AND TRAINING

- Blue Team Junior Analyst Pathway
- Introduction to Threat Hunting
- Introduction to Network Analysis
- Introduction to OSINT

COMPETITIONS & ACHIEVEMENTS

1st Place – Azhar University CTF | 1st Place – Upper Egypt CTF (Aswan) | Ranked 4th globally on CyberDefenders | 2nd Place – Blue Arena

LANGUAGES

Arabic: Native **English:** Professional Working Proficiency