Mohamed Ashraf Abdallah

SOC Analyst Tier 1

mohamed.ashraf.abdallah65@gmail.com | +201121154504 | Minya Al Qamh, Al Sharqia, Egypt

LinkedIn Profile: https://www.linkedin.com/in/mohamed-mooka/

Portfolio Website: https://mohamedmooka7.github.io/

PROFILE

- Dedicated cybersecurity professional with experience in monitoring and responding to security incidents in a Tier 1 SOC environment. Skilled in using SIEM tools, IDS/IPS, and threat analysis to detect and mitigate potential threats effectively.

EXPERIENCE

Ethical Hacking Internship – National Telecommunication Institute (NTI) *11/2025 - 1/2026*

- Gained hands-on experience in vulnerability assessment, network monitoring, malware analysis, and web security testing.
- Familiar with attack detection techniques, SIEM related concepts, and threat analysis using Kali Linux, Nmap, Wireshark, Metasploit, and Burp Suite.

SOC Analyst (Tier 1) Security Operations Center **Bincom Global – London, UK (Remote)** *1/2026 - Present*

- Monitor and analyze security alerts and events using SIEM solutions (Splunk).
- Investigate and triage 500+ security alerts to identify potential threats and incidents.
- Perform log analysis across multiple security devices and network sources.
- Detect, analyze, and respond to network-based attacks and suspicious activities.
- Escalate confirmed incidents according to SOC incident response procedures.

EDUCATION

Faculty of Computers and Informatics, Bachelor's Degree in Computer Science *2023-2027*
Zagazig University

CERTIFICATIONS & TRAINING

- Certified Network Security Practitioner (CNSP)
- CompTIA Security+ SY0-601 Prep
- SEC450 – GSOC Prep
- SEC504 Incident Responder and Handler (netriders.academy)
- eCIR Prep Incident Responder (netriders.academy)
- eJPT v1 (netriders.academy)
- CCNA
- Certified Windows Server 2019

TECHNICAL SKILLS

- Threat Intelligence: VirusTotal, AbuseIPDB, OSINT, IOC Analysis
- Frameworks: MITRE ATT&CK, Incident Response Lifecycle
- Security Monitoring: SIEM (Splunk, ELK), Alert Triage, Log Correlation
- Mapped security incidents to MITRE ATT&CK techniques to improve threat classification and response accuracy.
- Security Solutions: Firewall, IDS/IPS, Proxy, WAF, Antivirus, Suricata, Snort, EDR, Palo Alto, F5, Trellix Security
- NDR, XDR, Google Cloud
- Operating Systems: Linux, Windows, Mac
- Network Traffic Analysis (TCP/IP, DNS, HTTP, SSL)
- Log Analysis
- Packet analysis
- Ethical Hacking Tools: Nmap, Metasploit, Burp Suite, Wireshark, Tcpdump
- Web Technologies: HTML, CSS, JS

SOFT SKILLS

- Teamwork
- Ability to Work Under Pressure
- Analytical thinking
- Communication
- Willingness to Learn and Develop

PROJECTS

DFIR Investigation: Confirming Kerberoasting Activity, This investigation demonstrates how identity-based attacks can be confidently confirmed by correlating authentication logs with endpoint execution evidence, rather than relying on single alerts.

Portfolio Link: https://mohamedmooka7.github.io/project-dfir

LANGUAGES

- **Arabic : Native**
- **English: Professional Working Proficiency (CEFR B2)**