Khaled Gamal Abdelhaleem

Dairout Center, Assiut, Egypt

+20 108 015 1904 khaledgamal123h@gmail.com linkedin.com/in/khaledgamal-cyber

Professional Summary

Motivated and detail-oriented **Cybersecurity Analyst** and aspiring **CSA (Certified SOC Analyst)** with hands-on SOC experience. Skilled in real-time monitoring, threat detection, log analysis, incident response, and forensic investigation. Strong technical foundation in networking, scripting, malware analysis, and security automation. Familiar with cyber threat intelligence frameworks such as MITRE ATT&CK and Cyber Kill Chain.

Education

Bachelor's Degree (In Progress) in Information Technology (Cybersecurity Track)
Faculty of Computers and Information, Egyptian E-Learning University (EELU)
Expected Graduation: 06/2026 — Entering 4th Year
Relevant Coursework: Network Security, Incident Response, Digital Forensics, Malware Analysis, Computer Networks, Operating Systems.

Core Competencies

- **SOC Operations:** Security monitoring, alert triage, threat investigation, incident documentation.
- **Security Tools:** SIEM (Splunk, ELK), EDR, IDS/IPS, Firewalls.
- **Forensic Tools:** Autopsy, FTK Imager, Volatility.
- **Threat Intelligence:** MITRE ATT&CK, Cyber Kill Chain, OSINT.
- **Networking:** TCP/IP, DNS, VPN, Cisco routing & switching, firewall rule configuration.
- **Programming:** Python, Bash, PowerShell for automation; Java; basic web technologies (HTML/CSS).
- **Malware Analysis:** Static and dynamic analysis techniques for identifying IOCs.
- **Databases:** SQL, MySQL, MongoDB.
- **Systems Administration:** Linux, Windows Server.
- **Soft Skills:** Communication, analytical thinking, problem-solving, time management.

Certifications

- **CCNA — Routing & Switching (Cisco)**
- **Switching Technologies (Cisco)**
- **Java Programming**
- **Python for Cybersecurity**
- *In Progress:* CompTIA Security+, CSA (Certified SOC Analyst)

Selected Projects

- **SIEM Automation:** Automated log parsing and alert correlation using Python, reducing triage time by 30%.
- **Blue Team Playbook:** Developed IR playbooks for ransomware and phishing attack simulations.
- **Network Infrastructure Setup:** Designed a secure office network with VLAN segmentation and firewall rules.
- **Forensic Case Study:** Analyzed disk images using Autopsy to extract evidence for a simulated breach investigation.

Professional Experience

SOC Analyst Intern — Digital Pioneers Initiative *01/2025 – 03/2025*
Ministry of Communications, Egypt

- Monitored and analyzed over 5,000 daily security events via SIEM to detect and respond to threats.
- Contained and mitigated simulated cyberattacks, achieving a 100% incident resolution rate in drills.
- Produced detailed incident reports, reducing post-incident review time by 20%.

Cybersecurity Trainee / SOC Intern *01/2024 – Present*
Remote Labs / Self-Learning

- Completed hands-on training via TryHackMe and Blue Team Labs Online.
- Created Python scripts for repetitive security tasks, improving analysis efficiency by 25%.
- Conducted penetration testing using Metasploit, Nmap, and Wireshark.

Languages

- **Arabic:** Native proficiency
- **English:** Intermediate proficiency

Available for internships and junior SOC roles. References available upon request.