Mahmoud Rashad Mahmoud

SOC Analyst

Cairo, Egypt · +20 1129266308 · www1aborashad@gmail.com
LinkedIn: mahmoud-rashad · GitHub: MedoRashadfci medium: aborashad

Professional Summary

SOC Analyst with a strong network security background (CCNA certified). Completed the SOC Tier 1 path and actively solve IR and blue-team challenges on CyberDefenders and TryHackMe. Skilled in SIEM monitoring, log analysis, threat detection, and incident handling.

Education

Bachelor of Computer Science and Information 2022–Present
Faculty of Computers and Information, Assiut University

Certifications & Courses

Pre Security - Cyber Security 101 - SOC 1 (TryHackMe) - Cisco Certified Network Associate - Cyber Security Training (ITI & CyberTalents) - Network Security (NTI) - Red Hat System Administration I - eCIR (Netriders) - eJPT v1 (Netriders) - Red Teaming, Ethical Hacking, Bug Hunting & Penetration Testing (Udemy)

Technical Skills

Programming: Python, PHP, C++, Java, JavaScript
Networking: NAT, VLANs, ACLs, Security Protocols, Troubleshooting
Cybersecurity: SOC Monitoring, Penetration Testing, Vulnerability Assessment, CTFs
Tools: Wazuh, pfSense, Burp Suite, Nmap, Metasploit, Wireshark, OWASP ZAP, Packet Tracer

Experience

SOC Analyst Intern — ITSolera Jul-Sep 2025
Gained hands-on experience in security monitoring, SIEM operations, and network protection. Learned how to deploy and configure Wazuh, enable FIM, analyze security alerts, and integrate logs from pfSense firewall. Developed strong skills in log analysis, incident detection, firewall configuration, and building a mini SOC environment.

Projects

Network Security Simulation
Simulated enterprise infrastructure with VLANs, ACLs, VPN, AAA, Syslog, and NTP.
GreenSecurity Platform
Developed a Flask/PostgreSQL backend for cybersecurity services (scanning, reporting, encryption).
Wazuh & pfSense Lab – ITSolera Training
Worked on deploying and configuring Wazuh SIEM and pfSense firewall as part of ITSolera's hands-on training. Set up Wazuh Manager, added agents, enabled File Integrity Monitoring (FIM), analyzed alerts, and integrated pfSense logs for centralized monitoring. Gained practical experience in log analysis, alert triage, and building a mini SOC environment.