Nour Gehad Elmaghalawy

Cairo, Egypt, nourimaghalawy@gmail.com, 0 1023072796 | 01021225178
LinkedIn: linkedin.com/in/nourmaghalawy, Medium: medium.com/@nourimaghalawy
LetsDefend: app.letsdefend.io/user/nourelmaghalawy, Military Service: Completed

Professional Summary

SOC Analyst Trainee with hands-on experience in SIEM monitoring, alert triage, and incident response using Splunk, ELK Stack, and FortiSIEM. Experienced in phishing analysis, malware triage, IDS/IPS monitoring with Snort, and security automation using SOAR and n8n. Motivated to grow within a SOC or cybersecurity operations team.

Education

B.Sc. in Information Technology, Damietta University (Sep 2019 to Jul 2023)

Experience

SOC Analyst Trainee

WE Innovate Cybersecurity Academy (Round 1 - 2025) Powered by ZeroSploit MEA and Information Technology Institute (ITI), Nov 2025 to Present

- Developing advanced skills in threat detection, incident response, and security monitoring within simulated SOC environments.
- Working collaboratively with cybersecurity professionals and peers on real-world defensive operations and analysis.
- Strengthening practical expertise in using industry-standard tools and frameworks to identify and mitigate cyber threats.

Networking, Cybersecurity Fundamentals Trainee

BARQ Systems, Round 12, Cairo, Egypt, Oct 2025 to Nov 2025

- Completed intensive training covering networking and security fundamentals.
- Gained hands-on experience with Juniper Routers & Switches (interface setup, routing policies, OSPF, and traffic filtering).
- Practiced FortiGate Firewall configurations, including NAT, firewall policies, IPsec VPNs, and High Availability (HA).
- Strengthened troubleshooting, teamwork, and technical skills through practical lab exercises.

Cybersecurity Intern

BEDO Company, Damietta, Egypt, July 2022

- Conducted hands-on labs using Linux and Kali Linux, focusing on vulnerability discovery and enumeration techniques.
- Analyzed attack vectors for network and web applications, documenting findings along with suggested mitigations.
- Assisted with SOC tasks, including log reviews, alert triage, and incident documentation.

Graduation Project, Facial Recognition System, November 2022 to July 2023

- Developed a prototype facial recognition system aimed at enhancing security monitoring.
- Managed dataset collection, model evaluation, and testing processes.
- Documented the project architecture and created a demo for the evaluation.

Technical SKILLS

- SOC & Incident Response: Alert triage, incident handling, SOC playbooks
- SIEM & Detection Engineering: Splunk, IBM QRadar, FortiSIEM, ELK Stack, detection rules (Windows Event IDs)
- SOAR & Automation: SOAR workflows design and execution, Security automation using n8n, Alert enrichment and response automation
- Threat Analysis: Phishing analysis, malware triage, info-stealer behavior analysis
- Network Security: TCP/IP, Wireshark, Snort IDS/IPS rule creation and tuning, firewalls, WAF
- Endpoint & OS Security: Windows Security Events, Linux (Kali, Ubuntu), EDR/AV concepts
- Web Security: OWASP Top 10, Web attack detection, vulnerability assessment (basic)
- Forensics & Malware: Evidence collection, Dynamic malware analysis concepts, sandboxing concepts
- Automation & Scripting: Python (security automation), Bash (log parsing), GitHub

Courses & certificates

- SOC Analyst Path Certification (LetsDefend, 2024)
- eCIR, Netriders Academy (2025)
- Digital Forensics Essentials, EC-Council (2024)
- Wireless Networks Penetration Testing (2024)
- Malware Analysis Skill Path Certification, LetsDefend (2024)
- Fortinet Certified Fundamentals in Cybersecurity, Fortinet (2024)
- NDG Linux Unhatched, Cisco Networking Academy (2024)
- FortiSIEM 5.2 Self-Paced Training, Fortinet (2024)
- Splunk Beginner Learning Path, Splunk (2024)
- CCNA, Cisco (2023, self-study)
- MCSA, Microsoft (2023, self-study)
- Cisco CyberOps Associate, Cisco (2024, self-study)

(Certificates and proofs available upon request)

Achievements

- Ranked 17th on LetsDefend local leaderboard (practical skills demonstrated)
- Graduation project graded Excellent (A)

Languages

- Arabic, Native
- English, Intermediate (continuously improving)