Esmail Nouralden

Cybersecurity Analyst

Cairo, Egypt | +201003546479 | esmailnouralden@gmail.com | linkedin.com/in/esmailnouralden

Summary

Cybersecurity Analyst with hands-on SOC operations, log analysis, threat detection, and Linux administration experience. Skilled in Splunk, QRadar, ELK, Suricata, Wireshark, and Python for security monitoring, triage, and incident response. Knowledgeable in phishing, malware, brute-force, ransomware, and network traffic analysis.

Skills

Technical Skills:

- **SIEM Tools:** Splunk, IBM QRadar, Elastic (ELK) Stack
- **Security Tools & Technologies:** Wireshark, Burp Suite, Suricata (IDS/IPS), Metasploit, Trellix (EDR/XDR/NDR), F5, Palo Alto, Google Cloud Security
- **Core Competencies:** Incident Response, Log Analysis, MITRE ATT&CK, Vulnerability Assessment
- **Networking:** TCP/IP, HTTP/HTTPS, DNS, FTP, SSH, VPN, Firewall
- **Programming:** Python, C
- **Systems:** Linux Administration, Windows Server

Soft Skills:

- Communication Skills
- Analytical Problem-Solving
- Team and Cross-Functional Collaboration
- Technical Documentation and Reporting
- Presentation Skills

Experience

ISTQSERVER — **Maadi, Egypt**

Linux System Administrator — **Oct 2024 - Present**

- Maintain and harden Linux servers, ensuring 99.9% uptime, stable production performance, and secure operations.
- Conduct system audits, patching, and health checks to reduce vulnerabilities and strengthen system resilience.
- Monitor and analyze logs, troubleshoot servers via platforms, and coordinate remediation with datacenter teams.

National Telecommunication Institute (NTI) — **Internship**

Cybersecurity Trainee — **Sep 2025 - Nov 2025**

- Performed SOC, network, and cloud security labs using F5 and Trellix, gaining practical incident response skills.

Certifications

eLearnSecurity Certified Incident Responder (eCIR)

Education

Modern Sciences and Arts University — **Giza, Egypt**

Bachelor of Engineering in Electrical, Communication and Electronic Systems — **Sep 2019 - Jul 2024**

GPA: 3.28

IT Gate Academy — **Nasr City, Egypt**

Diploma in Cybersecurity Engineering — **Sep 2022 - Sep 2023**

Grade: Very Good

Projects

Security Triage Project — L1 Analyst (Hands-on project)

Ingested and correlated Windows, Linux, and Suricata logs in Splunk; validated alerts, analyzed PCAP traffic in Wireshark, identified IOCs, and prepared escalation-ready findings mapped to MITRE ATT&CK.

Smart Road Security System for Stolen Car Detection (Graduation project)

- Built an AI-based stolen car detection system in Python/C paired with real-time alerting.

Achievements

SOC Analyst – Job Role Path – Hack The Box (HTB)

- Hands-on SIEM monitoring, log analysis and network traffic analysis, plus basic DFIR for security incidents.

Courses

- CCNA
- MCSA
- Linux Administration I
- Python Programming for Security Applications
- Fortinet NSE 4
- CEH
- IBM Security QRadar SIEM Foundations
- eCIR Preparation

Languages

Arabic: Fluent — **English: Intermediate (B2)**