

OMAR AHMAD

SOC Analyst T1 — Cybersecurity Specialist

+20 10 99838993 • Alexandria, Egypt • omarabdelmawla9477@gmail.com

[LinkedIn](#)

PROFESSIONAL SUMMARY

Cybersecurity professional with comprehensive training in SOC operations, incident response, and threat intelligence. Hands-on experience in digital forensics, network security, and security tools. Certified in CTIA and trained in DFIR methodologies. Seeking SOC Analyst position to leverage technical skills in threat detection and incident handling.

EDUCATION

Bachelors of Computer Science and Information Technology (Networks and Cybersecurity) Egypt-Japan University of Science and Technology (EJUST) 2021 - 2025

TECHNICAL SKILLS

- **SOC Operations:** Incident Handling, Threat Detection, Security Monitoring, SIEM (Splunk, ELK), EDR
- **Threat Intelligence:** CTI Lifecycle, Kill Chain Methodology, IOC Analysis, Threat Hunting
- **Digital Forensics:** Forensic Imaging, Memory Analysis, Network Forensics, Timeline Analysis
- **Network Security:** CCNA, Firewall Management (PaloAlto, FortiGate), Wireshark, Nmap
- **Security Tools:** Burp Suite, Metasploit, Volatility, Autopsy, FTK Imager, Splunk, ELK Stack
- **Programming:** Python (Security Automation), PHP, JavaScript, SQL, HTML/CSS
- **Platforms:** Linux, Windows Server, Active Directory, Oracle Database

CERTIFICATIONS

- **eCIR** - INE Cyber Incident Responder (2025)
- **CTIA** - EC-Council Certified Threat Intelligence Analyst (2024)
- **eJPTv1** - Junior Penetration Tester from Netriders Academy(2023)
- **Security+** - From Netriders Academy (2024)
- **Google Cybersecurity Professional Certificate** (2023)

PROFESSIONAL EXPERIENCE

DFIR Bootcamp – ITI in collaboration with Cyber Talents Oct 2024 – Nov 2024

- Conducted digital forensics investigations including disk imaging and memory analysis
- Performed intrusion detection using Splunk and ELK stack for log analysis
- Gained hands-on experience with Wireshark, Volatility, Autopsy, and FTK Imager
- Developed incident response procedures for various attack scenarios

EC-COUNCIL & ITI Cyber Threat Intelligence Scholarship

Mar 2024 – Jun 2024

- Certified Threat Intelligence Analyst (CTIA) with focus on kill chain methodology
- Performed threat intelligence requirements planning and data collection
- Conducted threat analysis and produced intelligence reports
- Implemented IOC management and threat hunting techniques

Network Security Trainee – ITI

Aug 2023 – Sep 2023

- Completed comprehensive network security training including CCNA 200-301
- Gained expertise in firewall configuration (PaloAlto, FortiGate NSE4)
- Practiced ethical hacking techniques and vulnerability assessment
- Implemented network security controls and monitoring solutions

Digital Egypt Pioneers Program - MCIT Apr 2024 – Oct 2024 *Cyber Security Incident Response Analyst - Job Profile*

- Completed intensive 6-month program sponsored by Ministry of Communications and Information Technology
- Specialized in Cyber Security Incident Response Analyst job profile
- Gained expertise in incident detection, analysis, containment, eradication, and recovery
- Developed practical skills in security incident handling and response procedures
- Recognized for achieving excellence in the program

Freelance Coding Instructor – YAT Learning Solutions

Dec 2024 – Present

- Teach programming fundamentals and cybersecurity concepts

PROJECTS

Security Automation Tools

Python

- Developed Python scripts for security automation and threat intelligence gathering
- Created tools for log analysis, IOC extraction, and security monitoring

Library Management System

PHP, MySQL, JavaScript

- Full-stack web application with security-focused implementation
- Implemented secure authentication and data protection measures

Network Security Assessment

CCNA, Security Tools

- Designed and implemented secure network architecture
- Conducted vulnerability assessments and penetration testing

COMPETITIONS & ACHIEVEMENTS

- **3rd Place** - ITI CTF Round 3 2024 (Awarded CTIA certification voucher)
- **DFIR Competition Winner** - Cyber Talents CTF (Awarded eCIR certification voucher)
- Participant in multiple cybersecurity competitions focusing on SOC operations

TRAINING & WORKSHOPS

- Digital Forensics and Incident Response Bootcamp (ITI/Cyber Talents)
- Cyber Threat Intelligence Analyst Program (EC-Council/ITI)
- Network Security Intensive Training (ITI)
- Oracle SQL Database Programming Certification
- Python Intermediate & OOP Programming (DataCamp)