





Ahmed Khaled A. Awwad

SOC Analyst Tier 1

 Ahmed Awwad  +201117753991  a.k.awad97@gmail.com  Military service: Performed


Electronics and Communication Engineer, Jr SOC Analyst with 1 year of experience in analysis and cooperation in incident investigations. seeking to leverage my skills in a challenging SOC Analyst Tier 1 role. Committed to enhancing security operations by utilizing advanced threat detection techniques, incident response strategies. Self-learner, self-motivated, and dedicated to pursuing my goals to build a focused career.

ACHIEVEMENTS

CTFs writeups, *Awwad's Blog* 

Cybertalents,
Top 200 in Egypt rank. 

Foundations of Operation MITRE ATT&CK, *ATTACKIQ Academy* 

Cisco CCNAv7 
Introduction to Networks
Switching, Routing, and Wireless Essentials
Enterprise Networking, Security, and Automation

SKILLS

SIEM Solutions | EDR | SOAR

Incidents Investigation

Infrastructure & System Security

Application & Network Security

Linux | Cryptography | R&D

Network & Systems administration

Programming
Python, Bash, C++..


Technical Reporting/Writing

LANGUAGES

Arabic
Mother tongue

English
B2- Upper Intermediate

EDUCATION

Bachelor of Communication and Electronics Engineering,
Faculty of Engineering Helwan University
Project: **Email Anti-spammer system** 
Degree: **Excellent**

EXPERIENCE

Armed Forces

Kaspersky Administrator
Jul 2023 | Confidential
Served as Kaspersky Administrator. Monitored, maintained, and developed Kaspersky servers and managed devices. Ensuring robust protection against malware and cyber threats.


Network and Systems Administrator
Jul 2023 | Confidential
Serving as a Network and computer systems administrator. Manage all military internal networks, systems, install, configure, and maintain organizations' computers.

Optima Professional Services (OPS)

SOC Analyst
Jul 2023 – 2024 | Part time

SOC Analyst | Tier 1
Oct 2022 – May 2023 | Full time
Monitor and analyze incidents. Analyzing Business environment and traffic **baseline** to enhance SOAR playbooks to reduce **False-Positive** repeated incident rate. Also help reduced incident **response time** through efficient monitoring and analysis. **Follow-up** with the IT Teams and other business units to develop action plans to mitigate identified vulnerabilities.

Excel Codes, *Back-end Developer intern*

Sep 2017 – Dec 2017
"ICenna  " Website and Mobile Application
Back-End Developer for Python (Django) for websites and applications.

Freelancer, *Curriculum writer*

Aug 2017 – Jan 2019
Physics & Mathematics content **writer**, booklets content **designing** and **translating** Arabic content to English

PROJECTS

Spamurai, *Graduation project* [↗](#)

Spamurai is Email Anti-spammer system in cyber security field. It is Research and development (R&D) project aim to find and implement a solution to detect and prevent or lessen the interaction of users with any adware, harmful/spam emails based on content analysis as URL, TEXT and Files.

Auxilio Robotic, *IEEE RAS, Certificate* [↗](#)

IEEE Helwan Student Chapter

I was assigned to lead control team & code via Arduino.

Our objective is to structure Line follower Robot help disabled people by carrying different objects with controllable arm and following the line path to a certain destination automatically or manually through an application to control direction and movement.

COURSES & INTERNSHIPS

CCNAv7, *National Telecommunication Institute (NTI)*

Oct 2022 – Dec 2022

Network fundamentals, network access, IP connectivity & services, Network security fundamentals, and laying the foundation for network automation and programmability.

Certificates [↗](#)

Cyber Security Engineer, *Udacity* [↗](#)

Jul 2022 – Nov 2022

Nanodegree Expert level program by egFWD ITIDA [↗](#) .

- Security Engineering Fundamentals
- System Security
- Infrastructure Security
- Application Security

Nanodegree Certificate [↗](#)

Cyber Security Engineer Intern, *VTF* [↗](#)

May 2022 – Jul 2022 | Online

Cyber Security Teams and their roles. Gained knowledge in Splunk, Mitre Att&ck, OSINT, Pfsense, Cloud and Presenting skills.

Certificate [↗](#)

Pentester trainee, *Trend Micro & CyberTalents*

Jun 2021 – Aug 2021

Penetration Testing cycle and phases. Dived deep into OWASP top 10 vulnerabilities.

Achieved top 10 in the evaluation CTF.

Certificate [↗](#)

Full Stack Web Developer, *Udacity*

Feb 2018 – May 2018 | Online

“One Million Arab Coder” in Full-Stack Web Developer.

- Python Language
- Version control : Git - GitHub

Certificate [↗](#)

Front-End Web Developer, *Udacity*

Nov 2017 – Feb 2018 | Online

“Google Developer Challenge” in Front-End Web.