Ahmed Khaled A. Awwad

SOC Analyst Tier 1

in Ahmed Awwad 🔗 Blog 🛡 Military service: Completed

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 systems' security tools by utilizing advanced threat detection techniques, incident response strategies. In order to achieve that I consider myself as self-learner, self-motivated, and dedicated to pursuing my goals to build a focused career.

EDUCATION

Bachelor of Communication and Electronics Engineering,   2016 – 2022
Faculty of Engineering Helwan University
    Project: **Email Anti-spammer system** ⬈
    Degree: **Excellent**

EXPERIENCE

Armed Forces

SOC Analyst   Jul 2023 | Confidential
    Monitor OSSIM SIEM, maintain and developed **Kaspersky** server and managed devices. Ensuring protection against malware and cyber threats.

Network and Systems Administrator   Jul 2023 | Confidential
    Manage all military **internal network**, systems, also configure and **maintain** their devices.

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 apps.

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

COURSES & INTERNSHIPS

Cyber Security Engineer, *Udacity* ⬈   Jul 2022 – Nov 2022

CCNAv7, *National Telecommunication Institute (NTI)* ⬈   Oct 2022 – Nov 2022

Foundations of Operation MITRE ATT&CK, *ATTACKIQ Academy* ⬈   Sep 2022

Cyber Security Engineer Intern, *VTF* ⬈   May 2022 – Jul 2022

Intro to IT & Cybersecurity, *Cybrary* ⬈   May 2021

CEH & Pentesting Fundamentals, *Trend Micro & CyberTalents* ⬈   Jun 2021 – Aug 2021

Full Stack Web Developer, *Udacity* ⬈   Nov 2017 – Feb 2018

Front-End Web Developer, *Udacity*   Nov 2017 – Feb 2018

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

SOFT SKILLS

Verbal Communication

Adapt with work environments | Team Work

Negotiation skills

Self Learner | Time Management

Problem solving

Critical and Logical Thinking

Business acumen | Customer Service Orientation

LANGUAGES

Arabic   ● ● ● ● ●
   Mother tongue

English   ● ● ● ○ ○
   B2- Upper Intermediate

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 using AI Machine learning to analysis and prediction.

Auxilio Robotic, *IEEE RAS , Certificate* ⬀
   control team leader. Our objective is to structure **Line follower Robot,** automatically or manually.