Ahmed Raafat

SOC Analyst T1

Cairo, Egypt | +201277441063 | ahmedrahmed2022@gmail.com
Linkedin: https://linkedin.com/in/ahmed-raafat-6366a4231
GitHub: https://github.com/Ahmed98955

PROFILE

BIS graduate with a strong foundation in cybersecurity and IT. Passionate about SOC operations, threat detection, and incident response. Completed courses in CompTIA A+, Network+, Security+, and several Cisco programs. Skilled in Bash scripting and Python, with training in eCIR fundamentals through NetRiders Academy. Team-oriented and eager to contribute to securing digital environments.

EDUCATION

Bachelor of BIS, GPA: 3.19/4 09/2021 – 06/2025
El-Gazera Institute for Computer and Information Systems
Cairo, Egypt

COURSES

eCIR – NetRiders Academy (Prep Course)

- Gained foundational skills in incident handling, threat analysis, and SOC procedures based on eLearnSecurity's eCIR methodology.

CompTIA Security+ (SY0-601) – (Self Study)

- Studied risk management, cryptography, threat detection, incident response, and secure network architecture.

CompTIA Network+ (Self Study)

- Covered network protocols, routing and switching, IP addressing, and troubleshooting network issues.

CompTIA A+ (Self Study)

- Focused on computer hardware, operating systems, software troubleshooting, and basic IT support skills.

ISC2 Certified in Cybersecurity (CC)

- Official ISC2 certification covering security principles, network security, access control, risk management, and incident response.

Cisco Cybersecurity & Networking Courses (Self Study)

- **Introduction to Cybersecurity (Leaders Foundation for Administrative Sciences)**
  – Explored cybersecurity principles, common threats, and the basics of securing networks, systems, and data.
- **Network Defense**
  – Studied core concepts of network security including firewalls, access control, intrusion prevention systems, and risk mitigation techniques.
- **English for IT 1**
  – Focused on developing professional English skills for technical communication, job readiness, and workplace interaction in the IT field.

Bash Scripting – Learn Linux TV (Self Study)

- Learned core shell scripting concepts including variables, loops, conditionals, and automation techniques using Bash.

SOLUTIONS & TOOLS

- **SIEM Tools:** Splunk, Elastic SIEM (Kibana, Logstash)
- **Threat Intelligence:** MITRE ATT&CK, VirusTotal, AlienVault OTX, AbuseIPDB
- **Sandbox Analysis:** ANY.RUN
- **Log Analysis:** Kibana, Splunk Search Processing Language (SPL)
- **Incident Response:** Playbooks, IOC Investigation, CTI Usage
- **Scripting & Automation:** Bash Scripting, Python Basics, C++ Basics
- **Network Analysis:** Wireshark, TCP dump
- **Endpoint Security Tools:** Antivirus, HIDS/NIDS
- **Monitoring Tools:** Netstat, Sysmon, Windows Event Viewer

CERTIFICATIONS

- **eCIR Prep** – NetRiders Academy (Preparation course based on eLearnSecurity's eCIR)
- **Certified in Cybersecurity (CC)** – ISC2 (Official Certification)
- **Network Defense** – Cisco
- **Introduction to Cybersecurity** – Cisco (via Leaders Foundation for Administrative Sciences)
- **English for IT 1** – Cisco
- **Graduation Project Certificate** – EGI (Excellent Grade)

PROJECTS

Graduation Project – Robotic Arm Vehicle

El-Gazera Institute for BIS — Grade: Excellent

- Developed an Arduino Mega and ESP32-CAM controlled robotic vehicle with a 6-DOF arm, Mecanum wheels for omni-movement, Bluetooth control, ultrasonic obstacle detection, and automated arm sequences.
  Code & documentation: https://github.com/Ahmed98955/BT-RoboCar
  More Projects: github.com/Ahmed98955

LANGUAGES

- **Arabic – Native**
- **English –upper of Intermediate (B2) .** Actively improving technical and professional communication skills.