Hamdy M Helmy, SOC Analyst Tier 1

Alexandria, Egypt, +201027220596, general@hamdyh.com

LINKS

Linkedin

PROFILE

SOC Analyst Tier 1 with hands-on experience in **incident response**, **threat detection**, and **security monitoring**. Proficient in **Splunk**, **QRadar**, and **SIEM tools**, with expertise in **firewall management**, **ethical hacking**, and **network security**. Strong communicator and team player in 24/7 SOC environments.

EMPLOYMENT HISTORY

Jul 2022 — Oct 2022

Info Sec Trainee, PharmaOverSeas

Alexandria

- Managed **network and firewall authorizations** to ensure system safety.
- Conducted hands-on training in **cloud security** and **networking**.
- Gained experience in **incident response** and **security monitoring**.

Jun 2020 — Oct 2021

Full Stack Developer, Upwork

- Worked to assess competing websites in regards to content, look, and feel.
- Worked as a productive and positive team member to design, code, test, report, and debug operations.
- Managed front-end and back-end development in the company's Portfolio Analyst, Employee Track, and Account Management systems

EDUCATION

Oct 2019 — Jun 2023

Bachelor's degree, Information Technology, Damanhour University

Damanhour

IT is a field that manages, processes, and shares information through tech. It includes programming, networking, database management, and web development. An IT degree can lead to a successful career in a high-demand field.

Jul 2023 — Aug 2023

Summer Course, Network Security, Information Technology Institute (ITI)

Alexandaria

Completed the **ITI Summer Course in Network Security** (85%, 108 hours), covering computer networks, cybersecurity fundamentals, firewall technologies, Windows Server, and Red Hat Administration. Supplementary courses included Python programming, ethical hacking, and VMware Cloud Foundation, building a solid IT security foundation.

LICENSES & CERTIFICATIONS

Jul 2023

CT Blue Team Scholarship 2023 Certification

CyberTalents

Completed the **CyberTalents Blue Team Scholarship 2023** in collaboration with Trend Micro, focusing on advanced courses in SOC analysis and threat hunting. Gained hands-on experience in threat mitigation and career guidance through one-on-one mentorship with cybersecurity experts.

Jul 2023

CyberOps Associate

Cisco

- Understanding of cybersecurity operations principles and concepts.
- Knowledge of security monitoring, intrusion detection, and incident response techniques.
- Familiarity with network intrusion analysis, endpoint threat analysis, and data and event analysis.
- Understanding of security operations center (SOC) functions and responsibilities.

Jul 2023

Network Security

Cisco

- Competence in implementing Cisco network security solutions to mitigate threats and vulnerabilities.
- Understanding of core security technologies, concepts, and best practices.
- Knowledge of securing network devices, such as routers and switches.
- Ability to configure and manage Cisco security appliances, like firewalls and Intrusion Detection Systems (IDS)

Jan 2023

Security Analyst Bootcamp

Virtually Testing Foundation

- I possess accomplishment descriptions for various skills related to data analysis using machines.
- I am proficient in creating dashboards and have experience with Splunk Enterprise Security and SIEM.
- I am skilled in using Splunk Enterprise for advanced searching and analysis.
- My expertise has been utilized to reduce downtime, improve system reliability, optimize search performance, and achieve a more proactive security posture.

Nov 2022

CC: Certified in Cybersecurity (CC)

(ISC)2

- Proficient in network security, access control, and business continuity.
- Prioritizes security principles to safeguard systems and data.
- Knowledgeable in disaster recovery and incident response.
- Able to quickly address security issues.

Oct 2022

Cybersecurity (SOC Track)

AMIT Learning

- Covered cybersecurity fundamentals, threat and vulnerability management, incident response and forensics, malware analysis and reverse engineering, and QRadar and SOAR.
- Equipped with skills to detect and respond to security threats, making proficient in cybersecurity.
- The certificate demonstrates expertise in the field and can be used to showcase qualifications to potential employers.

Jul 2022

Pre Security

TryHackMe

Completed the **Pre-Security** course on **TryHackMe**, covering essential cybersecurity concepts, including network fundamentals, web security, Linux and Windows basics, and introductory threat analysis. Gained hands-on experience with SIEM tools, incident response, and ethical hacking techniques to enhance security skills.

TECHNICAL SKILLS

SOC Tools: Splunk, QRadar, SIEM

Incident Response: Threat detection, mitigation, recovery

Networking: Firewall management, IDS/IPS

Programming: Python, Bash scripting

Operating Systems: Windows Server, Linux (RedHat)

SOFT SKILLS

Communication

Problem Solving

Team Collaboration

VOLUNTEERING

Feb 2022 — Present

Community Founder of Egypt Stady Camp

- Founded a community to guide individuals on **self-study skills** in cybersecurity.
- Led initiatives to support aspiring cybersecurity professionals.

LANGUAGES

English	Highly proficient
Arabic	Native speaker
German	A1