Amer Ashoush

Cairo, Egypt | Ashoushamer2004@gmail.com | +201008548758 | LinkedIn | GitHub | Portfolio

EDUCATION

Arab Academy for Science and Technology **Heliopolis, Cairo**
Bachelor's of Computer Science | Sep 2022 - Present | GPA: 3.2

- Major: Cybersecurity.
- Core Concepts: Malware Analysis, DFIR, OS, SSDLC, Data Structures, OOP.
- Best Project Award in Entrepreneurship, Introduction to Cryptography courses.

EXPERIENCE

WEInnovate SOC Track Bootcamp (Hybrid, Egypt) July 2025 - August 2025

- Strengthened SOC skills by mastering Networking, Linux, Active Directory administration, and practicing troubleshooting techniques.
- Configured SIEM (ELK) and wrote Snort rules to monitor logs and detect anomalies in simulated environments.
- Built SOAR workflows with n8n, analyzed traffic with Wireshark, and set up a WAF using Nginx to protect web applications.

Data Entry Analyst Part-Time- Vultara, United States (Remote) May 2025 - June 2025

- Researched 20+ automotive cybersecurity threats, incidents, and trends to enrich Vultara's intelligence database.
- Performed online investigations, curated structured datasets, and increased threat intelligence tool accuracy.
- Collaborated with the team to refine data collection and automation pipelines to reduce manual research.

MS Dynamics CRM Developer Intern - Ejada, Cairo July 2024 - August 2024

- Assisted in developing and customizing CRM solutions with Microsoft Dynamics.
- Added basic JavaScript features to improve user interactions in CRM forms.
- Helped in creating and testing plugins to extend CRM functionality.

CERTIFICATIONS

CCNA Course – Nile University April 2025 - July 2025

- Gained hands-on knowledge in network fundamentals, routing & switching concepts, and IP addressing.
- Practiced configuring and troubleshooting routers, switches, and VLANs in simulated environments.
- Built foundational skills in network security, access control, and Cisco IOS command-line interface.

Certified in Cybersecurity CC - ISC2 Jun 2024 - Jun 2027

- Covered key domains including: Access Control, Business Continuity & Disaster Recovery, Network Security, Security Principles, and Incident Response.

Junior Cybersecurity Analyst - Cisco Jun 2024

- Introduction to Cybersecurity: Threat Detection, Data Confidentiality, NMAP.
- Networking basics: Network Concepts, Network Types, Network Media, IP, Protocol Standards, Troubleshooting.

Health Information System Course - Hospital 57357 Jan 2023 - Feb 2023

- Attended a specialized course on health information systems, focusing on medical data management and technology applications.

PROJECTS

Malware Analysis Project – Zeus Banking Trojan May, 2025

- Dissected Zeus malware using static, dynamic and advanced static analysis with Ghidra, IDA, Wireshark, and Procmon, uncovering key obfuscation and C2 patterns.
- Produced a professional threat intel report documenting IOCs, persistence mechanisms, and memory artifacts, simulating a real-world SOC deliverable.

Student Financial Portal Security Implementation Feb, 2024

- Designed a secure student portal with HTTPS and isolated Active Directory authentication.
- Encrypted all internal data flows across clients, proxies, servers, and databases to meet enterprise-grade security standards.
- Simulated infrastructure in a DMZ with strict firewall rules and Group Policy-based access control.

Active Directory Implementation & Administration Feb, 2024

- Configured domains, Organizational Units (OUs), and Group Policies for secure resource management.
- Managed NTFS and shared permissions, reducing unauthorized access risks.
- Joined devices to domains and administered authentication, streamlining identity management.

Security Analyst - AWS July, 2024

Set up Security Onion on AWS

- Designed and deployed Security Onion on AWS, creating VPCs, subnets, EC2 instances, and Elastic IPs for monitoring.
- Configured SSH keypair access and traffic mirroring, enabling full packet capture and network analysis capabilities.

CTF Challenges and Forensic Analysis April, 2024

TryHackMe, PicoCTF, CTFlearn, Personal Project

- Built a custom Steganography-based CTF challenge using Foremost, Binwalk, and Exiftool, enhancing hands-on forensic skills.
- Completed 70+ challenges on TryHackMe, PicoCTF, and CTFlearn, focusing on web exploitation, OS attacks, and network vulnerabilities.

Red - Digital Store May, 2024

- Created a real digital store, specializing in phones, headsets and phone accessories , made using HTML, CSS, PHP, Bootstrap, and JavaScript.

StepUp - Shoes Website May, 2024

- Developed a Java-based e-commerce system with Servlets, JSP, and JavaBeans, enabling product, order, and user account management.
- Designed administrator dashboards for inventory and order handling, increasing usability for non-technical staff.

SKILLS & INTERESTS

- **Technical Skills:** Programming | SIEM | Penetration Testing | Reverse Engineering | Research | Threat Modeling.
- **Tools:** Burpsuite | Splunk | NMAP | ELK| Jira | Wireshark | Snort | Nessus | Microsoft TMT | Ghidra.
- **Languages:** Arabic (Native) | English (IELTS 6.5 – B2 Level, Professional) | German(Basics).
- **Hobbies:** TryHackMe Challenges | Working out | Music | Swimming.
- **Interpersonal Skills:** Teamwork | Communication.