Amer Ashoush

Cairo, Egypt | +20 100 854 8758 | Ashoushamer2004@gmail.com |
linkedin.com/in/amerashoush2468 | amerashoush.netlify.app | github.com/Mororock6

Education

Arab Academy for Science & Technology and Maritime Transport — Heliopolis, Cairo
Bachelor of Science in Computer Science (Cybersecurity) — *Sep. 2022 – Expected Jul. 2026*

- GPA: 3.3/4.0
- Core concepts: Malware Analysis, DFIR, Operating Systems, SSDLC, Data Structures, and Object-Oriented Programming
- Received Best Project Award in Introduction to Cryptography, DFIR, Ethical Hacking, and Blockchain courses

Experience

Incident Management Intern — Apr. 2026 – Expected Jun. 2026
Geidea — *Hybrid, Egypt*

- Selected for a 3-month Incident Management internship supporting the handling and coordination of low- to medium-priority incidents in a hybrid enterprise environment

SOC Trainee — Jul. 2025 – Aug. 2025
WE/Zerosploit — *Hybrid, Egypt*

- Strengthened SOC skills by practicing networking, Linux, Active Directory administration, and troubleshooting in lab environments
- Configured ELK as a SIEM solution 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 Nginx as a WAF to protect web applications

Data Entry Analyst — May 2025 – Jun. 2025
Vultara, Part-Time — *Remote, United States*

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

MS Dynamics CRM Developer Intern — Jul. 2024 – Aug. 2024
Ejada — *Cairo, Egypt*

- Assisted in developing and customizing CRM solutions using Microsoft Dynamics
- Added basic JavaScript features to improve user interactions in CRM forms
- Helped create and test plugins to extend CRM functionality

Projects & Research

Prompt Injection Testing on Open-Source LLMs | *Ollama, FastAPI, NeMo Guardrails, OWASP LLM01* Jan. 2026

- Deployed LLaMA 3 8B locally using Ollama and exposed a vulnerable FastAPI-based API to simulate real-world LLM security weaknesses
- Implemented and validated mitigations using NeMo Guardrails, input sanitization, and output filtering, significantly reducing prompt injection success

Threat Intelligence Analysis Using MITRE ATT&CK Framework | *Threat Intelligence, SOC Analysis* Dec. 2025

- Conducted comparative threat intelligence analysis of Scattered Spider and APT29 using the MITRE ATT&CK framework
- Produced a structured security report simulating real-world defensive analysis and SOC threat modeling

Malware Analysis Project - Zeus Banking Trojan | *Ghidra, IDA, Wireshark, Procmon* May 2025

- Dissected Zeus malware using static, dynamic, and advanced static analysis, uncovering key obfuscation and command-and-control patterns

- Produced a professional threat intelligence report documenting indicators of compromise, persistence mechanisms, and memory artifacts

Mini Security Operations Center (SOC) with ELK Stack | *ELK, Fluent Bit, n8n, VirusTotal* Aug. 2025

- Built a mini SOC for centralized log collection, parsing, and security monitoring using the ELK Stack
- Implemented custom log parsing, ingest pipelines, and detection rules to identify suspicious activity from security logs
- Automated threat enrichment and alerting using n8n workflows integrated with the VirusTotal API

Student Financial Portal Security Implementation | *TLS, Active Directory, Group Policy* Feb. 2024

- Designed secure portal access using HTTPS (TLS) with isolated Active Directory-based authentication
- Deployed a DMZ-style infrastructure with strict firewall rules and Group Policy-enforced access control

Active Directory Implementation & Administration | *Windows Server, Active Directory* Feb. 2024

- Configured domains, organizational units, and Group Policies for secure resource management
- Managed NTFS and shared permissions and administered domain authentication for joined devices

Security Onion on AWS | *AWS, Security Onion, Traffic Mirroring* Jul. 2024

- Designed and deployed Security Onion on AWS using VPCs, subnets, EC2 instances, and Elastic IPs for monitoring
- Configured SSH key-based access and traffic mirroring to enable full packet capture and network analysis

CTF Challenges and Forensic Analysis | *Digital Forensics, Web Exploitation, Network Security* Apr. 2024

- Built a custom steganography-based CTF challenge using Foremost, Binwalk, and ExifTool to strengthen practical forensic analysis skills
- Completed 100+ hands-on cybersecurity challenges across TryHackMe, CTFlearn, and CyberDefenders

Certifications

CompTIA Security+ (SY0-701) Jan. 2026 – Jan. 2029
CompTIA *Certification*

Certified in Cybersecurity (CC) Jun. 2024 – Jun. 2027
(ISC)2 *Certification*

CCNA Course Apr. 2025 – Jul. 2025
Nile University *Training*

AWS Services Fundamentals May 2026
INE *Course Completion Certificate*

Junior Cybersecurity Analyst Jun. 2024
Cisco *Certification*

Health Information System Course Jan. 2023 – Feb. 2023
Hospital 57357 *Training*

Technical Skills

Security Areas: SIEM, Incident Response, Network Security, Risk Management, Threat Detection, Active Directory
Tools: Burp Suite, Splunk, Nmap, ELK, Jira, Wireshark, Snort, Nessus, Microsoft Threat Modeling Tool, Ghidra
Spoken Languages: Arabic (Native), English (IELTS 6.5 - B2), German (B1)
Professional Interests: Security Research, Capture-the-Flag Challenges, Threat Analysis
Interpersonal Skills: Teamwork, Communication