Mahdi Ghaznawy

mahdighaznawy2004@gmail.com • (720) 490-3191 • LinkedIn • GitHub • Website

U.S. Citizen | Clearance-Ready

EDUCATION

Bachelor of Science in **Cyber Security and Information Assurance** | May, 2025 | Western Governors University

PROFESSIONAL EXPERIENCE

NTAC Technician I (**Network Technical Assistance Center**) - **Mercury Fiber** | September 2025 – Present

- Monitor and respond to service-impacting incidents in live production environments
- Analyze logs, network behavior, and system symptoms to identify root causes
- Triage issues and escalate incidents using structured documentation and operational procedures
- Communicate incident details clearly to escalation teams under time-sensitive conditions
- Operate within SLAs while maintaining service availability and accuracy

PROJECT HIGHLIGHTS

Enterprise Network Security Implementation & Hardening:

- Secured small business network using pfSense firewall rules, VLAN segmentation, and endpoint protection
- Reduced attack surface and improved network isolation through layered security controls
- Implemented cloud backups and user awareness training to improve phishing resilience

Digital Forensics Investigation – Insider Threat Analysis:

- Recovered deleted files and analyzed unauthorized access using Autopsy
- Correlated metadata, timestamps, and user activity to identify potential data exfiltration
- Reconstructed user behavior using structured forensic methodology

Network Traffic Analysis & Threat Detection:

- Analyzed network traffic using Nmap and Wireshark to identify vulnerabilities and insecure protocols
- Identified risks including plaintext FTP and legacy SMB exposure
- Recommended secure alternatives and improved monitoring practices

CERTIFICATIONS

1: **CompTIA Security+**
2: **CompTIA CySA+**
3: **CompTIA Network+**
4: **ISC2 Systems Security Certified Practitioner** (**SSCP**)
5: **CompTIA Pentest+**
6: **LPI Linux Essentials**
7: CompTIA A+
8: **ITIL 4 Foundation Certificate in IT Service Management**

TECHNICAL SKILLS

Security Operations & Monitoring: Splunk, Wazuh, Elastic Stack, Azure Sentinel, MISP, VirusTotal
Incident Response & Forensics: Autopsy, FTK Imager, REMnux, NIST 800-61
Vulnerability Management: Nessus, OpenVAS, Qualys, Metasploit, Burp Suite
Networking & Infra Security: Nmap, Wireshark, Zeek, pfSense, Suricata, Snort, VLANs, VPNs
Scripting & Automation: Python, Bash, PowerShell