Mahdi Ghaznawy

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

U.S. Citizen | Clearance-Ready

PROFESSIONAL SUMMARY:

Cybersecurity Analyst with SOC experience in monitoring, investigation, and incident response. Skilled in SIEM tools (Splunk, Wazuh), vulnerability management (Nessus), and digital forensics (Autopsy, FTK Imager). Certified in Security+, CySA+, Pentest+, SSCP, and more, with a B.S. in Cybersecurity & Information Assurance. Clearance-ready and proven under high-pressure conditions.

EDUCATION

Bachelor of Science in Cyber Security and Information Assurance | Graduated May 2025 | WGU

CERTIFICATIONS

CompTIA: **Security+, CySA+, Pentest+, Network+, A+**

ISC2: **SSCP**, Other: **ITIL 4 Foundation**, LPI **Linux Essentials**

PROFESSIONAL EXPERIENCE

Information Systems and Cybersecurity Analyst - IronGrid Security | December 2022 – Present

- **Security Monitoring & Incident Response** – Operated a SOC-modeled environment with SIEM tools (Splunk, Wazuh) to detect, investigate, and resolve security events; reduced false positives by 40% through custom correlation rules and dashboards.
- **Vulnerability Management** – Performed vulnerability scans using Nessus and OpenVAS, prioritized remediation tasks, and validated fixes in accordance with CIS and NIST security standards.
- **Forensic Analysis & Evidence Handling** – Utilized Autopsy and FTK Imager to investigate security incidents, maintain chain-of-custody documentation, and deliver detailed incident reports.
- **Security Awareness & Policy Development** – Designed and implemented user training, policy documentation, and compliance guides for small business environments, boosting phishing detection rates.
- **Network Configuration & Troubleshooting** – Configured and maintained switches, firewalls, and VPNs; resolved connectivity issues and implemented network segmentation for improved performance and security posture.

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

PROJECT HIGHLIGHTS

- **Digital Forensics & Insider Threat:** Recovered deleted files tied to IP theft, documented violations, and produced formal legal reporting.
- **Risk Assessment – Azumer Water:** Identified MFA gaps in a social engineering incident, delivered technical and policy remediation plans.
- **Network Security Audit:** Discovered open ports and EternalBlue exposure; implemented IDS/IPS and secure protocols.
- **Cybersecurity Infrastructure Upgrade – Kabul Law Firm:** Deployed firewalls, segmented networks, centralized endpoint protection, and improved phishing resilience by 60%+.
- **WLAN & Mobile Security Assessment – Alliah Corp:** Identified rogue APs and BYOD risks, recommended WPA3, MDM, and DNS tunnel detection strategies.