Mahdi Ghaznawy

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

U.S. Citizen | Clearance-Ready

PROFESSIONAL SUMMARY:

Cybersecurity Analyst with a strong foundation in SOC operations, threat detection, and incident response, reinforced by hands-on experience running IronGrid Security, a lab-based cybersecurity environment since 2022. Skilled in SIEM tuning, vulnerability management, and forensic investigation using tools such as Splunk, Wazuh, Nessus, pfSense, and FTK Imager. Adept at producing executive-ready reports, triage notes, and playbooks aligned to NIST 800-53 and industry best practices. Holds multiple industry certifications including Security+, CySA+, Pentest+, SSCP, and Linux Essentials, with a Bachelor's degree in Cybersecurity & Information Assurance. Clearance-ready and recognized for combining technical expertise with clear, stakeholder-focused communication to deliver actionable security insights.

EDUCATION

Western Governors University – Salt Lake City, UT
Bachelor of Science in Cyber Security and Information Assurance | May 2025

CERTIFICATIONS

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

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

PROFESSIONAL EXPERIENCE

IronGrid Security – Cybersecurity Analyst & Founder

December 2022 – Present | Remote (Lab Environment & Simulated Client Engagements)

Key Projects & Achievements

- SIEM Operations: Designed and tuned 24+ Splunk dashboards and 60+ custom correlation rules for Windows Event, firewall, and endpoint telemetry, reducing false positives and improving incident triage efficiency.
- Incident Response: Authored IR playbooks and executed mock containment/eradication procedures for credential dumping, ransomware, and phishing incidents; produced executive summaries for stakeholders.
- Vulnerability Management: Conducted regular Nessus and OpenVAS scans, identified critical exposures (e.g., SMBv1, FTP anonymous access), and documented CVSS-based remediation plans.
- Network Security Engineering: Configured pfSense firewalls, VLAN segmentation, IDS integrations, and automated alert pipelines to SIEM.
- Forensics & Threat Hunting: Used FTK Imager and Autopsy for file recovery and evidence preservation; executed hypothesis-driven hunts for lateral movement, persistence mechanisms, and data exfiltration indicators.
- Security Awareness: Developed phishing simulations with GoPhish, reducing simulated click-through rates from 25% to under 10% in lab-based campaigns.

- Documentation: Produced client-style SOC deliverables, including triage notes, incident reports, vulnerability assessments, and mitigation roadmaps aligned to NIST 800-53 and industry best practices.

TECHNICAL SKILLS

- **Threat Detection:** Splunk, IOC analysis, Windows Event Viewer, malware indicators
- **Security Tools:** Nmap, Wireshark, Autopsy, FTK Imager, Microsoft Defender, pfSense
- **Incident Response:** Phishing triage, SIEM alert triage, evidence handling, timeline creation
- **Networking & Infra Security:** TCP/IP, DNS, DHCP, VPN, VLANs, WPA3, firewall rules, DMARC/SPF/DKIM
- **Scripting & Automation:** Python (log parsing), Bash, CLI tools for triage

PROJECTS

Digital Forensics & Insider Threat Investigation

- Conducted forensic investigation on suspected insider threat
- Recovered and analyzed deleted files tied to IP theft and attempted sale via crypto
- Documented evidence of unauthorized access, flagged GDPR and company violations
- Created formal report for disciplinary and legal action

Attack Response & Risk Assessment – "Azumer Water"

- Analyzed a social engineering attack, identified failure points in training and MFA
- Assessed CIA triad breakdowns, policy gaps, and compliance issues
- Delivered technical and managerial remediation plan, including IR plan and MFA rollout

Network Security Audit – Nmap & Wireshark Assessment

- Detected open ports, vulnerable services (e.g., FTP, SMBv1, HTTP), and potential EternalBlue exposure
- Identified abnormal packet behavior, DNS anomalies, and TCP resets suggesting scan attempts
- Proposed mitigations: disable SMBv1, switch to HTTPS, implement IDS/IPS monitoring

Cybersecurity Infrastructure Upgrade – Kabul Law Firm

- Deployed pfSense firewall and segmented guest/staff networks via VLANs
- Centralized endpoint protection with Defender and automated daily cloud backups
- Led phishing simulations and achieved employee awareness boost (25% → <10%)
- Created full documentation, policy recommendations, and backup recovery plans

WLAN & Mobile Security Assessment – Alliah Corp

- Identified WLAN threats (rogue APs, Evil Twin) and BYOD risks
- Recommended WPA3, MDM, encryption, device wipe, and DNS tunnel detection strategies
- Mapped threat scenarios and applied FISMA, GLBA, and NIST 1800-22 standards