Mazen Abu Ghazaleh

NOC Technician & Cybersecurity Student

Laurel, MD · mazen@abughazaleh.work · github.com/MazenJ200 · linkedin · (301) 323-5184

NOC technician and cybersecurity student with hands-on production infrastructure experience: KVM virtualization across 13+ hypervisors, Cisco networking (BGP/OSPF), monitoring at scale, and TLS/security hardening. Run a two-node Proxmox home lab powering a custom AI-assisted vulnerability-triage pipeline, self-host live production sites behind Cloudflare Tunnel, and hunt on public bug-bounty programs. Pursuing Security+, CySA+, and Cloud+ alongside a B.S. in Cybersecurity. Targeting a SOC, security-engineering, or systems role.

EXPERIENCE

Network Operations Center Technician (Tier 1)
Apr 2025 – Present

AiNet · Laurel, MD

- Operate production infrastructure across a fleet of 13+ KVM hypervisors and 40+ Cisco/Juniper switches.
- Built a 6-GPU inference rig from decommissioned datacenter hardware into a 48 GB VRAM pool serving a 35B model at ~33 tok/s, the compute base for an internal AI ops agent.
- Diagnosed a fleet-wide Nagios blind spot where a local disk check masked real full disks across 84 hosts; remediated so genuine alerts fire again.
- Authored the VM fleet backup strategy: changed-block incremental capture into OpenStack Swift with dedup, encryption, retention, and Nagios-monitored jobs; piloted on a production host.
- Executed live RAID 0 to RAID 5 migrations with zero guest downtime, including a 3-drive rebuild on the largest host.
- Live-migrated 9+ production VMs across hypervisors over shared NFS, resolving cache-mode and snapshot edge cases without service interruption.
- Migrated a production BGP peering session from an aging 3750 to a 6500-class switch; documented neighbor, prefix-list, and route-map config before a clean cutover.
- Discovered a certificate-distribution host publishing every domain's TLS private key over unauthenticated public HTTPS; verified seven wildcard keys downloadable off-network, established a 19-month exposure window, and produced the remediation plan (keys had to be regenerated, not merely reissued).
- Deployed an OpenVAS scanner in a dedicated VM with custom profiles aligned to the asset inventory; ran the recurring monthly scan and documented findings.
- Remediated a customer site with a broken TLS chain: installed intermediates, enforced HTTPS, and added HSTS, CSP, and hardening headers, verified end-to-end.

Store Manager
Oct 2023 – Apr 2025

Talk N' Fix · MD

Promoted from Repair Technician after the first year

- Ran daily store operations end to end: staffing, scheduling, and opening/closing procedures.
- Owned inventory and parts ordering, tracking stock levels and margins to keep common repairs in stock.
- Handled customer escalations and warranty disputes; reconciled daily sales and cash handling.
- Hired, trained, and supervised junior technicians; set repair workflow and quality standards.

Repair Technician
Oct 2022 – Oct 2023

Talk N' Fix · MD

- Diagnosed and repaired hardware faults across phones, laptops, and desktops.
- Performed data recovery and malware removal while preserving customer privacy and chain of custody.
- Quoted repairs, explained options clearly, and kept detailed tickets for every device.

Mazen Abu Ghazaleh

NOC Technician & Cybersecurity Student

SELECTED PROJECTS

AI-Powered Vulnerability Triage Pipeline (home lab)
Python · bash · Kali · Ollama · Hermes · reconFTW

- Automated recon (reconFTW, nuclei, ffuf, sqlmap, httpx, naabu) against authorized scopes, normalized into a prompt-ready dataset.
- Two local Ollama models on a GPU-passthrough VM organize findings, score severity, and write a report delivered over Telegram via a Hermes agent.

AEROS UAV Risk Platform; deployment & hosting
FastAPI · Docker · nginx · Cloudflare Tunnel · RAG/FAISS

- Took a partner's Dockerized FastAPI + local-RAG backend from repo to a live public site, self-hosted on the Proxmox lab.
- Exposed it via Cloudflare Tunnel (no open ports) behind an nginx same-origin reverse proxy; segmented and firewalled off from the rest of the lab.

Agent Tesla RAT Analysis
Static & dynamic malware analysis · Procmon · Wireshark · sandbox

- Unpacked the sample, mapped its configuration, traced persistence and process behavior, and captured the exfiltration channel.
- Documented indicators of compromise in a full written report.

Network Security Analyzer
Python · Scapy · Flask · WebSockets · Docker

• Live packet capture with anomaly detection and a real-time WebSocket dashboard; Dockerized for one-command deployment.

Dealership Management Platform (hackathon, team of 3)
Next.js · React · Supabase · text-to-SQL

- Built the core DMS (inventory, CRM, desking/F&I, BHPH loans, accounting, P&L, service) plus natural-language Q&A over dealership data via read-only, guardrailed text-to-SQL.

TECHNICAL SKILLS

Security:	Kali, OpenVAS, reconFTW, nmap, nuclei, ffuf, sqlmap, hashcat, Wireshark, TLS/PKI, OWASP
Infrastructure:	Proxmox, KVM/QEMU, libvirt, VFIO passthrough, LVM-Thin, ZFS, Docker, NFS
Networking:	Cisco IOS, BGP, OSPF, VLANs, route-maps, UFW, Tailscale, Cloudflare Tunnel/Access
Monitoring:	Nagios, Munin, Beszel, Uptime Kuma, NUT, RANCID, SNMP, smartctl
Languages:	bash, Python, Java, TypeScript (Next.js/React); systemd, Git, cloud-init

EDUCATION & CERTIFICATIONS

B.S. Cybersecurity — **University of Maryland Global Campus** (Expected Jul 2027)
A.S. Cybersecurity — **Howard Community College** (Graduated 2026)
A.S. Computer Science — **Howard Community College** (Graduated 2026)

Google IT Automation with Python (completed) · Anthropic AI Fluency & Claude 101 (completed) · CompTIA Security+ SY0-701 (in progress) · CompTIA CySA+ CS0-003 (in progress) · CompTIA Cloud+ CV0-003 (in progress)

DoD CDSE training: OPSEC Awareness · Insider Threat Awareness · Safeguarding PII · Cybersecurity Awareness