Aaron Johnson | Cybersecurity & AI Practitioner

Las Vegas, NV • 7am–6pm PT • Remote-friendly
aj@aaronjohnson.tech • (424) 312-4117 • aaronjohnson.tech • linkedin.com/in/aaronjohnsontech
Contractor Services: Network & System Administration • Threat Visibility & SIEM Tuning • M365 Security Hygiene

Professional Summary

Security-minded operations leader turned Cybersecurity & AI Practitioner, focused on small-team outcomes. I design and harden networks and systems, tune SIEM and monitoring solutions, and layer in lightweight AI workflows that are actually utilized. In my HSOC home lab and consulting projects, I've shipped SSH hardening and network lock-downs, segmented pfSense environments, Wazuh/Security Onion/Splunk visibility, and M365/Entra security hygiene with clear before/after results. Known for plain-language communication, I transform detections, risk assessments, and AI experiments into practical playbooks and executive briefs that empower stakeholders to act with confidence.

Core Skills

- Threat Visibility & SIEM Tuning: Splunk, Wazuh; log triage, detections, dashboards; noise-cut plans and before/after metrics.
- Network & System Administration: pfSense/VLANs/VPNs, baseline hardening (Windows/macOS/Linux), secure backups, least privilege.
- Microsoft 365 Security Hygiene: Entra ID (Azure AD), Intune, MFA & Conditional Access, email auth (SPF/DKIM/DMARC).
- Scripting & Automation: PowerShell, Bash, Python; Docker Compose (YAML).
- Platforms: Windows • RHEL • Kali • Ubuntu • macOS • CentOS

Certifications & Achievements

- CompTIA Security+ (2024) - Verify
- ThriveDX Cybersecurity Professional Program - Graduated Top of Cohort
- National Cyber League - Top 15% Overall (Fall 2025)

PROFESSIONAL EXPERIENCE

HSOC Cyber - Cybersecurity Analyst, Team Lead | Remote — Aug 2023 - Present

- Lead the HSOC Cyber R&D Lab, a virtualized ecosystem (Windows, Linux, pfSense, Splunk, Wazuh) supporting purple team simulation and analyst training.
- Conduct MITRE ATT&CK–aligned adversary simulations, including persistence and credential-access scenarios, to reduce triage time ~25% with clearer dashboards and playbooks.
- Develop and fine-tune Splunk and Wazuh detections to achieve a ~35% reduction in false positives and improve SNR.
- Manage incident response investigations across Windows, macOS, and Linux systems, trace root causes, and implement endpoint hardening and containment strategies.
- Create risk registers and CISSP-style control frameworks for lab exercises, mapping control selection to impact/likelihood matrices.
- Mentor a distributed team of 10+ analysts in log triage, threat detection, and technical report writing.
- Document all research, playbooks, and detections for the HSOC → ESOC transition initiative, and prepare scalable models for production SOC environments.

Chick-fil-A - Director of Operations | Las Vegas, NV — *Oct 2018 - Oct 2025*

- Directed 20+ staff in high-volume operations, maintaining a minimum of 12% yearly profit.
- Improved throughput by 18% by standardizing process controls.
- Developed a leadership pipeline, promoting five employees into management roles.

Consulting Projects (aaronjohnson.tech)

- SSH hardening & network lock-down - Default-deny baseline, SSH from approved IP only, ED25519 key-only auth; Result: single management path, brute-force attempts denied.
- Local AI SOC notes (private RAG) - Docker Compose (Ollama, OpenWebUI, Qdrant, Retriever) bound to loopback; Result: sub-second lookups, zero data leaves host.
- CISSP Mini-Risk Assessment - 3-slide exec brief mapping assets to likelihood/impact; Result: ~60% risk reduction after firewall/NSG + SIEM tuning.

EDUCATION

- B.S., Cybersecurity & Information Assurance (in progress) - Western Governors University (WGU), Expected June 2026
- Cybersecurity Professional Bootcamp Certificate - ThriveDX, Miami, FL (2022–2023)
  Coursework: Incident Response, Cloud Security, Programming, Database Systems, OS Fundamentals