Hiring Brief

Security Operations | Detection Engineering | Incident Response | AI Security

Remote preferred | Las Vegas hybrid acceptable

SNAPSHOT

Aaron Johnson Tech / AJT

Cybersecurity professional focused on cleaner triage, tuned detections, incident-response support, and AI-assisted SOC workflows. I document the evidence trail behind the work so teams can review it quickly.

TARGET ROLES

- SOC Analyst / MDR Analyst
- Detection Analyst / Detection Engineering Support
- Incident Response Analyst / Security Analyst
- AI-assisted security operations workflow builder

CREDENTIALS

- B.S. Cybersecurity & Information Assurance
- CompTIA SecAI+
- Security+ | CySA+ | PenTest+ | Data+
- HSOC cyber apprenticeship and lab leadership

IMMEDIATE STRENGTHS

Alert triage, evidence handling, detection validation, MITRE ATT&CK; mapping, phishing workflow documentation, Linux access hardening, SIEM review, private RAG security workflows, and operator-friendly playbooks.

PORTFOLIO PROOF

Wazuh SSH brute-force detection	Custom rule logic, telemetry review, dashboard validation, MITRE mapping.
Linux secure access baseline	SSH key-only access, UFW default-deny, trusted-source control, rollback.
Private RAG stack for SOC notes	Ollama, OpenWebUI, Qdrant, Docker, FastAPI, privacy-aware retrieval.
Phishing defense workflow	Triage, indicators, evidence handling, escalation, and user communication.
Controlled offensive lab series	Offensive concepts reframed for defensive telemetry and detection thinking.

TEAM VALUE

I bring an operations mindset to security work: structured notes, clear handoffs, rollback thinking, tool discipline, and the habit of turning one investigation into a reusable process.

CONTACT

Website: aaronjohnson.tech

Email: aj@aaronjohnson.tech

LinkedIn: linkedin.com/in/aaronjohnsontech

GitHub: github.com/aaronjohnsontech

Resume: aaronjohnson.tech/resume