AARON JOHNSON

Las Vegas, NV | Remote Preferred | 424-312-4117 | aj@aaronjohnson.tech | aaronjohnson.tech | linkedin.com/in/aaronjohnsontech

Security Operations Analyst | Incident Response | Detection Engineering

Cybersecurity analyst and team lead with hands-on experience in SIEM monitoring, alert triage, incident investigation, detection tuning, phishing defense, endpoint security, Linux hardening, and AI-assisted security workflows across Windows, Linux, and macOS environments. Built experience through an HSOC Cyber apprenticeship, structured security operations projects, and documented labs while bringing 10+ years of operations leadership. Skilled in correlating Splunk, Wazuh, firewall, endpoint, and system telemetry to validate suspicious activity, reduce false positives, and support containment and remediation decisions. Holds a B.S. in Cybersecurity and Information Assurance with certifications including SecAI+, CySA+, PenTest+, Security+, Network+, A+, Data+, and Project+.

CORE COMPETENCIES

Security Operations: SIEM monitoring, alert triage, incident investigation, log correlation, detection tuning, case management, escalation, containment support, remediation support
Incident Response: suspicious activity analysis, phishing investigation, evidence handling, incident documentation, MITRE ATT&CK mapping, playbook development
Tools and Platforms: Splunk Enterprise, Wazuh, ServiceNow, Microsoft Defender for Endpoint, SentinelOne, CrowdStrike, Wireshark, pfSense, Linux Auditd, Spiceworks
Systems and Networking: Windows 10/11, Windows Server, Linux, macOS, TCP/IP, DNS, DHCP, VPN, firewall rule analysis, network segmentation
Scripting, AI and Labs: Splunk SPL, Python, PowerShell, Bash, VirtualBox, Docker Compose, Parallels, SSH keys, secure baseline configurations, AI security concepts, AI-assisted security workflows

CERTIFICATIONS

CompTIA SecAI+ | CompTIA CySA+ | CompTIA PenTest+ | CompTIA Security+ | CompTIA Network+ | CompTIA A+ | CompTIA Data+ | CompTIA Project+
ITIL 4 Foundation | LPI Linux Essentials | CompTIA Security Analytics Professional

EDUCATION

Bachelor of Science in Cybersecurity and Information Assurance | Western Governors University | 2026

PROFESSIONAL EXPERIENCE

Cybersecurity Analyst & Team Lead | HSOC Cyber | Remote | Aug 2021 to Present | Apprenticeship

- Investigate security events by correlating SIEM, firewall, endpoint, and system telemetry across Windows, Linux, and macOS environments to identify suspicious activity, scope incidents, and support containment and remediation decisions.
- Monitor and triage alerts in Splunk and Wazuh, using investigation outcomes to tune detection logic and reduce false positives by 35 percent.
- Build and refine SPL searches, Wazuh rules, and detection workflows, using controlled offensive-security scenarios to validate visibility into authentication activity, endpoint behavior, suspicious network traffic, and policy violations.
- Authored multiple security operations playbooks covering triage, investigation, escalation, evidence handling, documentation, and response procedures.
- Mentor analysts on alert triage, case documentation, escalation discipline, and investigation consistency while improving onboarding workflows and reporting quality.
- Support phishing defense through campaign development, suspicious email review, user awareness reinforcement, and repeatable response procedures.
- Map detections and investigation findings to MITRE ATT&CK, NIST CSF, and CIS Controls to identify monitoring gaps and prioritize remediation.

Director of Operations | Chick-fil-A | Las Vegas, NV | Oct 2017 to Oct 2025

- Led daily operations for 20+ employees in a high-volume environment, using SOPs, KPIs, escalation processes, and accountability systems to maintain service continuity under pressure.
- Developed frontline and supervisory talent, promoting five employees into management roles and strengthening documentation discipline, training consistency, and operational resilience.
- Coordinated vendor, facility, and technology-related support needs for store operations, including issue escalation, process documentation, and service-impact communication.
- Managed operational risk and service disruptions by coordinating people, processes, and communication across multiple priorities in fast-paced conditions.

SELECTED SECURITY PROJECTS

SIEM Detection Tuning and Threat Coverage Mapping | Splunk, Wazuh, MITRE ATT&CK, NIST CSF, CIS Controls

- Reviewed alert outcomes, investigation notes, and lab-generated security events to assess detection effectiveness, identify false-positive patterns, and prioritize SIEM tuning opportunities.
- Mapped detections to MITRE ATT&CK and aligned monitoring coverage to NIST CSF and CIS Controls to identify visibility gaps, strengthen threat coverage, and support more consistent analyst triage.

- Delivered a prioritized tuning and remediation summary that reduced identified risk exposure by about 60 percent through improved monitoring logic, alert refinement, and coverage mapping.

Private RAG Stack for SOC Notes | Ollama, OpenWebUI, Qdrant, FastAPI, Docker Compose

- Built a private local RAG workflow for SOC notes and security playbooks using Ollama, OpenWebUI, Qdrant, Docker Compose, and a FastAPI retriever to support AI-assisted knowledge retrieval without sending sensitive security documentation to public AI services.
- Developed an ingestion pipeline that chunks local security notes, generates embeddings with nomic-embed-text, and stores source-backed vectors in a Qdrant collection for retrieval during analyst-style triage workflows.
- Integrated a private OpenWebUI tool connection to query the local retriever API, return top matching evidence chunks, and support more consistent security operations documentation, alert review, and playbook lookup.

Linux Hardening and Secure Access Control | Ubuntu, UFW, OpenSSH, SSH Keys, Change Control

- Implemented a secure Linux access baseline using UFW default-deny firewall rules, SSH key-based authentication, disabled root login, and restricted SSH access from a trusted administrative host.
- Validated secure remote access behavior by testing allowed and denied connection paths, reviewing firewall status, confirming SSH service behavior, and documenting configuration outcomes.
- Documented back-out and recovery procedures to restore SSH or firewall access safely if hardening changes created access or availability issues.