Ashton Ward

El Dorado, Arkansas
Email: ashtonrjward2@gmail.com | Phone: (870) 853 - 7182 | Website: https://ashtonward.tech

---

SUMMARY

Threat-focused security practitioner with hands-on experience designing, tuning, and validating SIEM detections, simulating real-world attacks, and automating security workflows. Strong foundation across networking, hosts, and cloud security concepts, with a defensive mindset built through Cyber Defense homelab work, QA automation, and National Guard network operations. Highly motivated to operate and improve Cyber Defense Center (CDC) detection, response, and threat integration capabilities.

CORE SKILLS

- SIEM Detection Engineering (Wazuh)
- Threat Detection & Alert Tuning
- Incident Response Support & Log Correlation
- Security Automation & Orchestration (Python, n8n)
- REST APIs & JSON Parsing
- Networking (TCP/IP, VLANs, Routing)
- Linux & Windows Internals
- Docker & Virtualization (Proxmox)
- Cloud Security Fundamentals (GCP concepts)
- Git & GitHub Version Control
- Threat Modeling & MITRE ATT&CK Mapping

EXPERIENCE

Quality Assurance Engineer I

Murphy USA – El Dorado, AR
October 2024 – Present

- Developed and executed automated test suites, improving defect detection and validation of system behavior.
- Built a custom TCP server to communicate with a simulator, handling buffers, protocol emulation, data parsing, and card data handling.
- Analyzed network traffic and application behavior to identify defects, edge cases, and abnormal conditions.
- Strengthened troubleshooting, root-cause analysis, and structured debugging skills directly applicable to incident response workflows.

Team Lead – Network Administration

United States Army National Guard – Pine Bluff, AR
January 2019 – Present

- Led and supported network administration teams operating in regulated, security-sensitive environments.
- Configured routers, managed switches, and encryption devices to ensure secure communications.
- Stabilized and maintained virtualized server environments on Dell PowerEdge systems.
- Applied defense-in-depth principles, network segmentation, and operational security controls.
- Held Secret-level Security Clearance.

Information Technology Help Desk

Southern Arkansas University – Magnolia, AR
August 2021 – October 2023

- Supported enterprise Windows environments including Active Directory domain-joined systems.
- Diagnosed network connectivity, DNS, and authentication issues impacting users.
- Assisted with system imaging, asset deployment, and endpoint lifecycle management.

Information Technology Intern

Drew Memorial Health System – Monticello, AR
May 2020 – August 2020

- Assisted with network troubleshooting, static IP management, and endpoint support in a healthcare environment.
- Supported installation and maintenance of security cameras and structured cabling.

PROJECTS

Cyber Defense Home Lab (Private)

- Designed and operated a private cyber defense lab on a Dell PowerEdge R730 using Proxmox virtualization.
- Deployed and tuned Wazuh SIEM for host and network-based detection across Windows and Linux systems.
- Simulated real-world attacks using intentionally vulnerable machines to validate detections and reduce false positives.
- Correlated logs across endpoints, network devices, and cloud-exposed services to identify suspicious activity.
- Automated security workflows using Dockerized services and n8n for enrichment and response logic.
- Implemented network segmentation using VLANs and enterprise networking equipment (Cisco 3900, Catalyst 3650).
- Published services securely using Cloudflare Tunnels and Zero Trust access controls.

EDUCATION

Bachelor of Science – Computer Science
Cybersecurity & Privacy Option
Southern Arkansas University – Magnolia, AR
Spring 2024

ADDITIONAL

- Strong interest in Cyber Defense, Threat Detection, and SOC Operations
- Comfortable operating in high-noise, fast-paced security environments
- Actively expanding Python-based SOAR and cloud security automation capabilities