Raylee Hawkins

Huntsville-adjacent (North Alabama) • raylee@hawkinsops.com • github.com/raylee-ops

Summary

SOC analyst candidate focused on detection engineering and security automation. Builds deployable detections w ith verification artifacts, maps content to MITRE ATT&CK, and validates in a home lab (Proxmox + Wazuh + Splun k).

Core Skills

- Detection engineering: Sigma, Wazuh rules, Splunk SPL
- Threat modeling: MITRE ATT&CK mapping, hypothesis-driven hunting
- Automation: PowerShell, Python, GitHub Actions (verification + reports)
- Operations: Git, documentation-first workflows, reproducible evidence

Selected Projects

HawkinsOperations (github.com/raylee-ops/HawkinsOperations)

- Multi-platform detections + IR playbooks with proof pack and CI-validated counts.

Triage Simulator (hawkinsops.com/triage.html)

- Interactive SOC workflow drills with investigation pivots and evidence checklists.

Home Lab Validation (Proxmox + Wazuh + Splunk)

- Telemetry generation and detection testing using repeatable, snapshot-driven runs.

RH_MIGRATION_2026_V2

- Migration proof trail and runbooks packaged for recruiter-readable evidence.

Portfolio is evidence-first: counts and structure are verifiable in the repo.