Raylee Hawkins

SOC Analyst (T1/T2) candidate focused on detection engineering + security automation

North Alabama (Huntsville-adjacent) | raylee@hawkinsops.com | GitHub | hawkinsops.com | LinkedIn

Summary

- Build and validate deployable detections across Sigma, Wazuh, and Splunk with reproducible verification workflows and proof artifacts.
- Maintain evidence-first quality controls using verified counts, CI-aligned checks, ATT&CK mapping, and lab validation.

Skills

- **Detection:** Sigma, Wazuh rule authoring, Splunk SPL
- **Tooling:** PowerShell, Python, Git, GitHub Actions
- **Frameworks:** MITRE ATT&CK, SOC triage workflow, incident response fundamentals
- **Lab/Validation:** Proxmox, Windows/Linux telemetry generation, reproducible test runs

Projects

HawkinsOperations (Primary Portfolio Repo)

- Built and maintain a detection and response library with verified inventory: 105 Sigma rules, 29 Wazuh rule blocks (25 XML files), 8 Splunk detections, and 10 IR playbooks.
- Implemented proof-first validation workflow (scripts, documentation, CI alignment) so reviewers can reproduce claims directly from repo artifacts.

SOC Triage Simulator

- Built an interactive triage workflow artifact to practice investigation steps, evidence review, and analyst decision flow.
- Added repeatable drill structure and checklists to demonstrate process discipline, not one-off screenshots.

Home Lab Validation Environment

- Built a Proxmox-based validation lab with Wazuh and Splunk components to test detection behavior before publishing artifacts.
- Use lab runs to validate telemetry assumptions and improve signal quality in portfolio content.

Additional

- "Eligible to obtain clearance; willing to pursue sponsorship."

PDF download path: **/assets/Raylee_Hawkins_Resume.pdf**