SAMI ALI

samiali38183@gmail.com | (571) 290-8908 | samiali38183.github.io | linkedin.com/in/sami-ali-1a4b89345 | github.com/samiali38183

PROFESSIONAL SUMMARY

Cybersecurity student (B.S. Information Technology, GPA 4.0) with hands-on experience as a Vulnerability Assessment Team intern at DHS (CBP). CompTIA Security+ and AWS Certified Cloud Practitioner. Builds Python security engineering tools for detection testing, static analysis and vulnerability prioritization, shipped with tests and CI, and documents measured results and limits.

CORE COMPETENCIES

Python • Sigma • MITRE ATT&CK • Atomic Red Team • taint analysis / SAST • OWASP Top 10 • vulnerability management (Nessus/Tenable) • CISA KEV / EPSS / CVSS • NIST CSF • AWS fundamentals • Docker • Kubernetes / Helm (deployed on kind in CI) • Terraform (validated, LocalStack) • GitHub Actions • Prometheus • Git • pytest • Power BI • Wireshark • Linux

CERTIFICATIONS

Certifications: CompTIA Security+ | AWS Certified Cloud Practitioner
In progress: AWS Certified Security – Specialty | OSCP
Work authorization: U.S. Citizen

PROFESSIONAL EXPERIENCE

Vulnerability Assessment Team Analyst Intern | Dept. of Homeland Security (CBP) | Ashburn, VA | May 2026 – Aug 2026

- Matched Nessus/Tenable scan results against the CISA Known Exploited Vulnerabilities (KEV) catalog to identify high-risk systems and aged findings.
- Designed a risk-based prioritization method weighing KEV status, asset criticality, exposure, EPSS and CVSS, and benchmarked remediation against CISA BOD 26-04 timelines.
- Built a multi-page Power BI dashboard and an executive briefing on actively exploited vulnerabilities and mitigations for technical and leadership audiences.
- Wrote compliance reports and remediation recommendations aligned with the NIST Cybersecurity Framework and FedRAMP.

PROJECTS

tripline — Detection-as-code quality gate (Python)

- Gate that compiles Sigma rules to Python predicates, replays recorded telemetry (Atomic Red Team on Linux and Windows runners; public AWS CloudTrail replays) for 14 MITRE ATT&CK techniques, and fails pull requests when an expected rule stops firing; 212 tests.
- The stock SigmaHQ setuid/setgid rule flagged neither of the 2 attack events among 36 recorded events; a replacement rule flags both and 106 of 108 generated evasion variants (stock rule: 0). 13 of 14 scenarios pass: 8 on unmodified SigmaHQ rules, 5 needing rules written for the project.

sinkline — Static analyzer for Python web apps

- Interprocedural taint analysis that traces request input to dangerous sinks across functions and files; 43 rules and 151 sink signatures mapped to OWASP Top 10 and CWE; SARIF output, GitHub Action, zero dependencies, 184 tests.
- On the independent OWASP BenchmarkPython (10 taint categories, own scoring script): true-positive minus false-positive rate +0.52 vs. Bandit +0.07 and Semgrep OSS +0.04; no coverage of weak hashing, weak PRNG, cookie flags or trust boundaries. Fixed a shell-injection flaw in its own GitHub Action.

kevgate — Vulnerability-intake service with a DevSecOps pipeline

- FastAPI service that ranks scanner findings by CISA KEV, EPSS, CVSS and asset criticality, with hashed scoped API keys, rate limiting, JSON logs and Prometheus metrics; 277 tests. Ships a hardened container, a Helm chart (restricted pod security, NetworkPolicy) and Terraform validated against LocalStack.
- GitHub Actions pipeline: Semgrep, Bandit, pip-audit, gitleaks, checkov, Trivy; kind deploy with a NetworkPolicy enforcement test; ZAP baseline (67 rules pass, 0 failures). Release image signed with cosign (keyless) with SBOM and build-provenance attestations.

EDUCATION

Bachelor of Science, Information Technology | Minor: Cybersecurity
George Mason University | Expected May 2028 | GPA: 4.0

Associate of Science, Information Technology
Northern Virginia Community College | May 2026 | GPA: 3.7