Arsen Vaneev

(704)-299-8438 | arsen@arsenvaneev.com | github.com/Arsen-V | arsenvaneev.com | linkedin.com/in/arsen-v

EDUCATION and CERTIFICATION

B.S. in Computer Science, Cybersecurity Concentration Expected May 2027

North Carolina State University, Raleigh, NC Dean's List recipient (6x), GPA: 3.8

- **CompTIA Security+ (SY0-701**) - completed Feb 2026
- **SANS SEC495: Building & Securing RAG and Agentic RAG** - completed Jul 2026

EXPERIENCE

Security Intern | CCC Intelligent Solutions | Chicago, IL (Remote) 08/2026 - present

- Rotational cybersecurity internship covering DevSecOps, GRC, and security operations.

Information Security Engineer Intern | ElevateBio | Durham, NC 06/2026 - 08/2026

- Designed and shipped an automated vulnerability risk-acceptance pipeline integrating CrowdStrike Falcon Spotlight and Vanta, replacing a manual vulnerability assessment and risk-acceptance process; determined 1,611 vulnerabilities ahead of an ISO 27001 audit and exposed 370 CVEs requiring immediate remediation.
- Extended the pipeline into an agentic assistant on Amazon Quick, letting engineers query live vulnerability posture and CVEs details in natural language (severity, exploitability, SLA status) instead of manual API calls.
- Contributed to security investigations across CrowdStrike Falcon, Palo Alto/Panorama, NG-SIEM, Meraki, and Axonius; performed device attribution via ARP, MAC OUI, and asset-intelligence correlation to identify a WeChat false positive misclassified as Adobe Flash malware.
- Analyzed 690+ Obsidian Security posture-management findings, distinguishing true MFA gaps from service-account and Okta-federated false positives to reduce manual review effort.

Cybersecurity Analyst | OIT at NC State University | Raleigh, NC 06/2025 - 06/2026

- Mapped campus security controls to NIST CSF categories and NIST SP 800-53 control families to reduce manual review effort.
- Performed vulnerability and risk assessments of third-party vendors; validated NIST requirements, identified control gaps, and recommended fixes.
- Tracked status and metrics in shared workbooks/tickets; produced weekly leadership updates on compliance posture, risks, and timelines.

PROJECTS

- **AI Red-Team Harness**: Adversarial testing suite for LLMs and RAG pipelines, run against self-hosted and hosted LLMs with Garak, Promptfoo, and PyRIT, mapped to the OWASP LLM Top 10, documenting prompt-injection and jailbreak bypasses. Demonstrated an indirect prompt-injection attack against a RAG vector store and implemented a mitigation that reduced attack success, published as a technical writeup. *(in progress – expected Sep 2026)*
- **Vulnerability Risk-Acceptance Engine**: Python tool that ingests findings from multiple vulnerability scanners over OAuth APIs (token refresh, rate-limit backoff, pagination), deduplicates by CVE, and scores each finding against a configurable CVSS-vector rubric. Generates auditable records with compensating-control mapping and flags actively exploited criticals for immediate patching; runs on a weekly GitHub Actions schedule with secrets management.
- **CI/CD & Kubernetes Lab:** Secure CI/CD pipeline with GitHub Actions, Docker, Terraform (Terraform Cloud), and Kubernetes (kind); added Trivy scans, drift detection, and Prometheus/Grafana monitoring.

SKILLS AND LANGUAGES

- **Cybersecurity:** Vulnerability management, SIEM/EDR (CrowdStrike Falcon, NG-SIEM), cloud posture management (Obsidian), CASB/DLP (Netskope), network security (firewalls, Palo Alto/Panorama, routing, subnetting/CIDR), phishing analysis (Abnormal, KnowBe4), asset intelligence (Axonius), GRC (Vanta, NIST CSF, NIST 800-53, ISO 27001), secure network design, risk assessment, security control mapping, common web attack vectors (XSS, SQLi, CSRF), automation, pentesting
- **Tools & Platforms:** Docker, Kubernetes, Terraform, GitHub Actions, Trivy, Prometheus, Grafana, Active Directory, Linux, GitHub, Amazon Quick, Okta, Meraki, Ghidra, Snappass, Snyk, ZAP, TruffleHog, MySQL
- **AI/ML Security:** Retrieval Augmented Generation (RAG), Contextual RAG, Agentic RAG, AI agent design, vector databases, self-hosted LLMs (Ollama), prompt injection defense, LLM information disclosure controls, tokenization and embeddings, hallucination reduction
- **Programming & Scripting:** Python, SQL, C, Java, Bash, ARM Assembly
- **Languages**: Russian (Native), English (Proficient), Ossetic (Intermediate)