CAMERON WOODWARD

Senior Security Engineer

Centreville, VA | (540) 550-5418 | cameronwoodward0@gmail.com | github.com/cnw2bx | linkedin.com/in/woodwardcn

SUMMARY

Security engineer with 5+ years hardening AWS cloud infrastructure and enforcing security controls across the software delivery lifecycle. Deep hands-on experience with AWS IAM, S3, and container/Kubernetes security, including designing SDLC scan-gate controls that block non-compliant releases before deployment. Background includes applied cryptography and cross-organizational security program leadership. AWS Certified Solutions Architect; pursuing an M.S. in Computer Science (AI Specialization) at Georgia Tech.

CORE COMPETENCIES

AWS Cloud Security • Container & Kubernetes Security • Vulnerability Management • SDLC Security Controls • Secure Code Scanning (SAST/DAST) • Applied Cryptography • Python, Go, Bash

PROFESSIONAL EXPERIENCE

Security Engineer II — Capital One *McLean, VA | Aug 2022 – Present*

- Operate the SDLC security gate governing container release decisions enterprise-wide — scanning thousands of container images across the artifact registry and millions of containers across production workloads daily, blocking non-compliant builds before deployment.
- Directed the strategic integration of container and image vulnerability scanning platforms across two Fortune 200 organizations onto a unified system, achieving full compliance ahead of a federal deadline.
- Re-engineered the enterprise registry scanning pipeline architecture, cutting average container scan time 62% (4 min → 1.5 min) across all company-wide scans.
- Architected a scheduler and redrive Lambda system with dead-letter-queue reprocessing, achieving 100% scan coverage while raising automated test coverage from 71% to 100%.
- Built Java and Go APIs powering B2B virtual card payment creation, and led a company-wide Java 8 to 17 migration across production services.
- Contributed to VulnHunter, Capital One's open-source vulnerability scanner combining SAST-style code analysis with chained-attack (DAST-like) detection — now public at github.com/capitalone/vulnhunter.
- Deployed Wiz runtime security sensors across containerized Fargate workloads, engineering the integration and delivering full unit and acceptance test coverage.
- Led resolution of high-severity production incidents, including a full scanning-platform outage, coordinating cross-team response and executive communication to restore service same-day.

Software Developer — CGI Federal *Fairfax, VA | Aug 2021 – Aug 2022*

- Architected a financial planning and tracking application for a federal agency, integrating custom C# plug-ins with Microsoft Power Platform to streamline budgetary reporting.
- Automated infrastructure provisioning with Puppet Bolt and resolved production issues through root-cause incident analysis, improving deployment reliability.

Software Developer Intern — Bluestone Analytics *Charlottesville, VA | Jan 2021 – May 2021*

- Built Python web scrapers and AWS S3/Kibana data pipelines supporting federal cybercrime investigations into dark web threat activity.
- Applied cryptography: parsed and mapped PGP keys to threat actor identities using the PGPy library, supporting attribution in active investigations.

EDUCATION & CERTIFICATIONS

M.S. in Computer Science, AI Specialization — Georgia Institute of Technology (Expected 2029) — In Progress

B.S. in Computer Science, Cybersecurity Focus, Minor in Business — University of Virginia, GPA 3.7

AWS Certified Solutions Architect – Associate | SAFe 6 Scrum Master

TECHNICAL SKILLS

Languages: Python, Go, Java, Bash, C++, C#, SQL

Cloud & Security: AWS, Qualys, Wiz, AquaSec, Docker, Kubernetes, Fargate, JFrog Artifactory, Jenkins, Splunk, New Relic

Practices: CI/CD Pipeline Security, IAM & Secrets Management, Incident Response, Agile/SAFe