Cedric Miller

cedric7m@yahoo.com | http://www.linkedin.com/in/cedric-miller2020

Objective

Security Engineer with active TS/SCI clearance and extensive experience securing CI/CD pipelines, cloud infrastructure, and mission-critical applications across DoD and federal programs. Skilled in vulnerability assessment, artifact integrity, and policy enforcement using tools like Jenkins, SonarQube, Nexus, and Fortify. Seeking to apply secure SDLC practices, automation, and risk mitigation strategies to protect enterprise systems in high-assurance environments.

Active Security Clearance: **Top Secret SCI**
IAT II Certification

- **Security+**

IAT III Certification

- **CISSP**

Relevant Projects

K3s Resume Platform | Personal DevSecOps / GitOps Homelab Project, (2026 – Present)
Technical Scope: ***Python, FastAPI, Docker, Git, GitHub, GitHub Actions, GitHub Container Registry (GHCR), K3s, Kubernetes, kubectl, Helm, Traefik, Flux CD, Kustomize, Flux ImageRepository, ImagePolicy, and ImageUpdateAutomation, Trivy, Syft, Cosign, Kyverno, Bash, WSL2, Ubuntu, VS Code, SQLite, SSH, GitOps deployment workflows, digest-pinned promotion, SBOM generation, vulnerability gating, and policy-based admission control. This tooling stack aligns with the project's documented architecture around single-node K3s, GitHub Actions CI, GHCR, Flux GitOps, Trivy, Syft, Cosign, and optional Kyverno hardening.***

- Built a single-node K3s GitOps platform to host a resume application and RSS aggregation service, separating application source from cluster desired state across dedicated app and GitOps repositories.
- Implemented GitHub Actions CI to build and publish container images to GHCR, generate SBOMs, run vulnerability scans with critical-severity gating, and sign artifacts to strengthen software supply chain integrity.
- Designed Flux-based deployment automation using image repository, policy, and update resources to monitor registry changes, reconcile desired state from Git, and support controlled dev-to-prod promotion workflows.
- Hardened the platform with production-oriented controls by enforcing digest-pinned images in prod, blocking mutable image usage through Kyverno admission policy, and validating rollout behavior through live reconciliation and deployment testing.
- Troubleshot end-to-end issues across Kubernetes, Flux, GitHub Actions, GHCR, SSH, and admission policy behavior, resolving image update, rollout, and reconciliation failures in a live homelab environment.

Jarvis Consulting Agent Platform | Personal Product / Automation Project, (2026 – Present)
Technical Scope: ***Orgo, GitHub, Git, Claude-assisted development, prompt engineering, agent workflow design, task routing, Markdown-based system and skill definitions, Bash automation, repo integrity checks, environment bootstrapping, secrets hygiene, security boundary enforcement, approval-gated execution, and reusable client-deliverable templates.***

- Built a private AI agent platform in Orgo and GitHub to support consulting workflows for SEO audits, website issue resolution, security reviews, and research synthesis.
- Designed a modular orchestrator-plus-specialist architecture with task-routing rules, reusable skill definitions, and structured prompt assets to improve consistency and maintainability across workflows.
- Implemented explicit human approval checkpoints for destructive edits, external integrations, production-like actions, and security boundary expansion to enforce a security-first operating model.
- Developed reusable task prompts, client-facing summary/proposal/handoff templates, and repo bootstrap/integrity-check scripts to standardize delivery quality and reduce manual setup overhead.
- Established repo-scoped security controls and documented policies for secrets hygiene, `.env` handling, filesystem boundaries, and approved execution behavior during early-stage agent development.

Work Experience

Security Engineer / DevSecOps Xfinion, (Oct 2024 – June 2025)

Technical Scope: ***Jenkins, SonarQube, MSBuild, YAML, PowerShell. Groovy, Nexus repo, Nexus IQ, infra as code, Secure SDLC, Linux, Windows, AWS, Azure, Docker, Git, ServiceNow, FedRamp***

- Enforced secure SDLC practices by integrating SonarQube scans, artifact validation, and Nexus IQ policies into CI/CD pipelines.
- Hardened Jenkins workflows for Windows (MSI) and Docker-based releases, enabling compliant, auditable software deployments.
- Designed security exemption and credential-scoped override workflows to support secure artifact publishing without policy violations.
- Standardized YAML pipeline templates and validation logic to mitigate scan bypasses and misconfigurations.
- Authored security KBs resolving pipeline issues related to certificate chains, scan failures, and repository access.
- Acted as security liaison to development teams, guiding STIG alignment, scanner error resolution, and secure job permissions.

ISSE / DevSecOps VTG, (May 2023 – Oct 2024)

Technical Scope: ***Infra as code, Python, Tekton, Secure SDLC, Linux, Windows, RedHat Openshift, Coverity, CodeDx, Git, AWS, Azure, FedRamp***

- Conducted static code analysis and vulnerability remediation using Coverity and CodeDX, ensuring compliance with STIG and DoD cybersecurity controls for classified systems.
- Hardened CI/CD pipelines in Red Hat OpenShift with Tekton by embedding security gates and IaC validation for mission-critical deployments.
- Led resolution of infrastructure security issues impacting access control, permissions, and encryption standards in secure desktop environments.
- Advised development teams on secure coding practices, vulnerability prioritization, and security gate integration across internal pipelines.
- Acted as security liaison between engineering and government stakeholders, facilitating risk mitigation and secure software release approvals.

Cloud Security Engineer at AWS, (Sept 2021 – March 2023)

Technical scope: ***AWS (CloudWatch, CloudTrail, GuardDuty, Direct Connect, Lambda, EC2, S3, IAM, KMS, VPC Networking), CloudFormation, Serverless ADC, Python (Boto3), Bash, Splunk, SIEM Integration, Jenkins, CI/CD Automation, Zero Trust Architecture, Monitoring Dashboards, Incident Response, FedRAMP, STIG***

AWS Serverless-ADC Team

- Developed automation to detect certificate expiration across 1,000+ endpoints, integrating alerts with CloudWatch dashboards.
- Built secure backend APIs using IAM and KMS, aligned to Cloud SRG requirements for classified workloads.
- Hardened serverless deployment processes through embedded access validation and input security controls.

AWS Network DX Team

- Supported deployment and security of backend services for AWS Direct Connect and VPN platforms.
- Built internal monitoring tools for port metering, object state visibility, and usage billing integrity.
- Strengthened network control plane reliability by embedding alerting and access control enforcement logic.

AWS Security Isengard Service Team

- Resolved high-priority cloud security incidents including IAM policy violations, API misconfigurations, and baseline drift in classified environments.
- Authored formal runbooks to streamline response to recurring access control and escalation scenarios, reducing resolution time across teams.

- Proposed architecture changes to improve least privilege enforcement, auditability, and service integrity at scale.

Cyber Analyst (Systems/Software) at Northrop Grumman, (May 2020 -Sept 2021)
Technical Scope: ***C++, Java, Python, JavaScript, Redux, React, typescript, HTML, CSS, SCAP, HBSS, ACAS, Fortify SAST***

- Conducted enterprise vulnerability assessments using ACAS, HBSS, and SCAP tools, ensuring compliance with DoD security standards across mission-critical systems.
- Analyzed source code with Fortify SAST, validated findings, and cleared false positives to support focused remediation efforts by development teams.
- Evaluated new software development tools for security risk using CVE reviews, EOL status, and SAM.gov registration, contributing to procurement and ATO decisions.
- Developed Python-based code generation tools to accelerate secure C++ module development for Battlefield Airborne Communications Node (BACN) systems.
- Documented and tested IRAD code integrations to support hardened embedded system deployments for airborne platforms.
- Acted as a liaison between security and engineering teams to align development workflows with secure coding guidelines and assessment readiness.

Addtional Experience

Software Engineer Intern at Qualcomm, (May 2019 - August 2019)
Software Engineer Intern at Mozilla, (May 2018 - August 2018)

Education

Master's Degree in Cybersecurity & Information Assurance, GPA: 3.9
Grand Canyon University, Phoenix, AZ

Bachelor of Science in Computer Engineering, GPA: 3.5
San Diego State University, San Diego, CA

CS Projects

- Single cycle Processor, multicycle processor, Pipeline Processor (Fall 2019; Verilog)
- 16-bit half address architecture virtual machine translator (Fall 2016; Java)
- 16-bit half address architecture assembler translator (Fall 2016; Java)
- Numerous projects of implementing data structures on algorithms (Spring 2018; Java)

Hardware Projects

- Universal Asynchronous Transmitter/Receiver on Spartan 6 FPGA (Spring 2019; Verilog)
- Interactive Simon Says Game on Spartan 6 FPGA (Spring 2019; Verilog)