

ASHFORD ASHIOFU

DevSecOps Engineer | Platform Engineer | Site Reliability Engineer

Houston, TX | (832) 640-4340 | acashiofu@gmail.com | U.S. Citizen

Active DoD Secret | Active IRS MBI Public Trust | Eligible for MRPT

PROFESSIONAL SUMMARY

DevSecOps and Platform Engineer with 10 years of experience building secure CI/CD pipelines, hardened AWS EKS platforms, and NIST 800-53 aligned automation for federal programs. Hands-on across GitHub Actions, Jenkins, Terraform, Terragrunt, Kubernetes, OpenShift, and Istio, and the security tooling that gates them: SonarQube, Snyk, OWASP ZAP, tfsec, Checkov, Trivy, gitleaks, Syft, Cosign, OPA Gatekeeper, and Kyverno. Experienced producing ATO artifacts, POA&M evidence, and continuous-monitoring reports. Works on fully integrated Agile product teams using Jira and Confluence.

CORE SKILLS

DevSecOps Pipelines: GitHub Actions, Jenkins, GitLab CI, Argo CD, Argo Rollouts, release gates, artifact signing (Cosign, Sigstore), SBOM generation (Syft, Gype), blue/green and canary deployments

Security Automation: SAST (SonarQube), SCA (Snyk, Dependabot), DAST (OWASP ZAP), container scanning (Trivy), IaC scanning (tfsec, Checkov, Trivy), secrets detection (gitleaks, trufflehog), policy-as-code (OPA Gatekeeper, Kyverno), runtime monitoring (Falco)

AWS Security Services: EKS, S3, VPC, IAM, IRSA, Security Hub, Inspector, WAF, Secrets Manager, Config, GuardDuty, KMS, CloudTrail, CloudWatch, Route 53

Kubernetes and Containers: AWS EKS, Red Hat OpenShift, Helm, Kustomize, Istio (mTLS, AuthorizationPolicies), NetworkPolicies, RBAC, SCC, image hardening (distroless, Chainguard), admission controls, workload identity (IRSA, EKS Pod Identity), External Secrets

Infrastructure as Code: Terraform, Terragrunt, Ansible, Puppet, Chef, HashiCorp Vault, provider mirrors, module registries

Observability and SRE: Prometheus, Grafana, ELK, EFK, OpenSearch, Splunk, Dynatrace, New Relic, Nagios, Zabbix, SLI/SLO, error budgets, incident response, post-mortems

Compliance and Governance: NIST 800-53, RMF, ATO process, POA&M, continuous monitoring, audit evidence, STIG and CIS baselines, least-privilege access, DoD and IRS secure delivery

Cloud Platforms: AWS (primary), Microsoft Azure, Google Cloud Platform

Languages and Scripting: Python, Bash, Zsh, Groovy, YAML, HCL, SQL

Delivery and Collaboration: Agile and Scrum (standups, sprint planning, demos, retrospectives), Atlassian Jira, Confluence, GitHub Enterprise, GitLab, Slack

KEY CAREER ACHIEVEMENTS

- Delivered NIST 800-53 aligned DevSecOps controls (SAST, SCA, IaC scanning, container scanning, secrets detection, SBOM, artifact signing) in a federal CI/CD pipeline, producing ATO artifacts and continuous-monitoring evidence for delivery reviews.
- Hardened AWS EKS platforms with IRSA workload identity, Kyverno admission controls, NetworkPolicies, External Secrets with AWS Secrets Manager, and Falco runtime monitoring, cutting Security Hub critical findings by 55% quarter over quarter.
- Led migration of on-premises infrastructure to AWS, reducing operational costs by 30% while improving scalability and reliability.
- Migrated CI/CD from Jenkins to GitHub Actions with embedded security gates, cutting deployment time by 40% and increasing deployment frequency by 40%.

- Built reusable Terraform and Terragrunt modules that standardized multi-environment AWS deployments and reduced provisioning time by 60%.
- Automated configuration management with Ansible, reducing manual configuration errors by 80% across the Linux fleet.
- Implemented Prometheus and ELK observability with SLO-based alerting, cutting system downtime by 60% through proactive detection.
- Rolled out Istio service mesh (mTLS, AuthorizationPolicies) across Kubernetes namespaces for secure east-west traffic and improved microservices observability.

PROFESSIONAL EXPERIENCE

DevSecOps Engineer / Site Reliability Engineer (Contractor)

Aug 2025 – Present

Booz Allen Hamilton | Houston, TX

- Deliver secure CI/CD automation, Terraform workflow controls, and NIST 800-53 aligned platform engineering for a federal data platform, contributing to ATO artifacts and continuous monitoring across development, performance, pre-production, and production environments.
- Design and maintain GitHub Actions workflows for Terraform CI with SonarQube SAST, tfsec and Checkov IaC scanning, Trivy container and configuration scanning, gitleaks secrets detection, and pull-request scoped validation on air-gapped, self-hosted runners.
- Build reusable DevSecOps pipeline patterns for linting, scanning, approval gates, and environment-aware deployments mapped to NIST 800-53 CM, AC, and SI control families to streamline ATO evidence collection.
- Standardize Terragrunt configurations across four environments to enforce state, provider, and IAM guardrails, eliminating configuration drift and enabling rollbacks in under 10 minutes.
- Implement least-privilege GitHub Enterprise authentication using OIDC, SSO, and fine-grained tokens for CI access to Nexus and internal registries, closing long-lived credential findings during compliance review.
- Configure a Terraform provider mirror for restricted environments using Nexus, .terraformrc, and local plugin caches for AWS, Vault, and related providers, keeping provider retrieval inside the enterprise boundary.
- Triage CI/CD security and reliability findings into Jira remediation tickets, drive remediation SLAs with engineering teams, and validate closure through re-scans and post-fix pipeline runs.
- Produce continuous-monitoring artifacts and POA&M evidence, including control mappings, vulnerability reports, and scan outputs, for federal delivery reviews.
- Collaborate with engineering on a fully integrated Agile product team through sprint planning, demos, and retrospectives, and maintain Confluence runbooks for platform patterns and incident response.

DevOps Engineer / Site Reliability Engineer (Remote)

Sep 2023 – May 2025

Booz Allen Hamilton | Houston, TX

- Migrated CI/CD from Jenkins to GitHub Actions with embedded SAST, SCA, Trivy container scanning, secrets detection, and approval gates in multi-stage workflows, cutting deployment time by 40% and establishing a DevSecOps baseline across services.
- Deployed hardened workloads on AWS EKS using Helm and GitHub Actions GitOps, including IRSA workload identity, Kyverno admission controls, NetworkPolicies, and in-cluster Trivy image scanning, reducing image CVE backlog by 70%.
- Built secure-by-default Terraform modules for VPC, EKS, IAM, S3, and Security Groups with tfsec and Checkov policy-as-code gates that blocked misconfigurations before apply and cut Security Hub critical findings by 50%.
- Delivered OIDC-based, keyless AWS access for GitHub Actions runners via Terraform, eliminating static AWS credentials from CI and closing a persistent audit finding.
- Ran incident response and post-mortems on production infrastructure, converting root causes into Jira remediation tickets and validating closure, cutting recurring incident classes by 40%.

- Automated build orchestration, manifest generation, Syft-based SBOM export, and signed artifact publishing to JFrog Artifactory in Python and Bash to harden the internal software supply chain.
- Rolled out Istio with mTLS and AuthorizationPolicies for service-to-service communication and distributed tracing across Kubernetes namespaces.
- Authored Prometheus-based Argo Rollouts AnalysisTemplates and Bruno API health checks that block bad canary deployments, sustaining deploy success above 98%.

DevOps Engineer (Remote)

Oct 2022 – Jul 2023

Dow Chemical | Houston, TX

- Built end-to-end Jenkins CI/CD with SonarQube SAST, Nexus artifact management, and Docker and Kubernetes deployments to support weekly and out-of-cycle releases with security gates on every merge.
- Tuned application and platform performance under a hardened, patched baseline, cutting p95 latency by 30% across production workloads.
- Operated centralized logging on the EFK stack (Elasticsearch, Filebeat, Kibana) with automated S3 lifecycle archival, meeting retention requirements for compliance and audit review.
- Integrated Red Hat OpenShift with Jenkins and GitHub Actions to run container builds, image scans, and gated promotion across lower and production-like environments.
- Operated OpenShift Routes, Services, Secrets, ConfigMaps, and ImageStreams with SCC and RBAC hardening as the containerization pattern for teams migrating in.
- Automated rolling deployments, rollout validation, and rapid rollback on OpenShift using the oc CLI, Helm charts, and declarative pipelines, keeping release-window rollback under five minutes.
- Stood up Prometheus and ELK monitoring with alerts tied to authentication failures, drift, and TLS expiry to shorten mean time to detect and mean time to recover.

System Engineer (Hybrid)

Aug 2021 – Aug 2022

U.S. Department of the Navy (NAVSEA) | Philadelphia, PA

- Led a team of 12 software and system engineers applying DevSecOps practices to DDG 51 Machinery Control Systems operational testing, introducing secure CI/CD and RMF-aligned control checkpoints.
- Implemented NIST-aligned technical controls including firewalls, intrusion detection and prevention systems, and access controls to support ATO evidence for defense delivery environments.
- Codified Linux security baselines in Ansible, Puppet, and Chef aligned to STIG and CIS, cutting configuration drift by 80% and producing evidence for compliance reviews.
- Instrumented Nagios, Zabbix, and Prometheus monitoring with alerting tied to authentication failures, drift, and availability, shortening incident detection time.
- Wrote Kubernetes and OpenShift deployment standards, RBAC and SCC patterns, and operational runbooks that anchored container-platform modernization for engineering teams.
- Managed compute, storage, and networking infrastructure with hardening baselines and least-privilege access as the foundation for later container and cloud migration.

Cloud Engineer (Hybrid)

Jul 2019 – May 2021

Flowserve Corporation | Virginia Beach, VA

- Administered GitHub Enterprise with SSO, branch protection, CODEOWNERS, and secret scanning enabled by default to harden the source-control layer across the organization.
- Deployed multi-cloud VM workloads (AWS EC2, Azure VMs, Google Compute Engine) with IAM least-privilege, security groups, and automated patching.
- Configured monitoring across CloudWatch, Azure Monitor, and Prometheus with alerts tied to failed logins, IAM changes, and drift alongside performance metrics.
- Centralized logging in ELK and Splunk with retention policies suited to audit and compliance review.

- Automated encrypted, cross-region backups using AWS Backup, Azure Backup, and Google Cloud Storage with tested restore drills, meeting RPO and RTO targets.
- Operated managed cloud databases (Amazon RDS, Azure SQL, Cloud SQL) with encryption at rest and in transit, backup automation, and IAM-based access.
- Ran Red Hat OpenShift container workloads with SCC hardening, RBAC, and image-stream promotion.

Linux Systems Administrator

Aug 2016 – May 2019

Geodetic Positioning Services Limited | Houston, TX

- Provisioned AWS infrastructure in Terraform (EC2, VPC, S3, IAM, RDS, CloudWatch, Route 53) with encryption, VPC segmentation, and least-privilege IAM baked into modules.
- Managed AWS core services with MFA-enforced access, hardened IAM policies, and CloudWatch security alerts across development, staging, and production accounts.
- Ran a hardened Red Hat, Ubuntu, and Amazon Linux fleet with STIG and CIS aligned baselines and automated patching aligned to CVE severity SLAs.
- Automated operating system and package patching so no critical-severity findings remained open beyond a seven-day SLA.
- Configured, tuned, and maintained Linux servers and workstations for performance and security across the fleet.

CERTIFICATIONS AND CLEARANCES

- Project Management Professional (PMP)
- Certified Kubernetes Administrator (CKA)
- AWS Certified Solutions Architect
- CompTIA Security+
- Active DoD Secret Clearance
- Active IRS MBI Public Trust Clearance
- Eligible for Moderate Risk Public Trust (MRPT)

EDUCATION

Bachelor of Science, Engineering

The University of Texas at San Antonio (UTSA) — San Antonio, TX