

# Stephen Monclova

hire@clov.dev | LinkedIn | GitHub | Website | Reston, VA

---

DevSecOps Engineer with 10+ years designing and automating secure multi-cloud infrastructure. Proven track record delivering 99.99% uptime across production environments, cutting deployment times by 50% through CI/CD automation, and hardening systems to DISA STIG and SOC 2 compliance. Known for building self-service platform solutions that enable faster, safer software delivery.

## CORE COMPETENCIES

---

- Linux Administration (CentOS, Ubuntu, RHEL, Red Hat Satellite)
- AWS (EC2, S3, VPC, CloudWatch)
- Azure (VMs, Blob Storage, VNet, Monitor)
- OCI (Compute, Block Volumes, Networking)
- GCP (Compute Engine, Cloud Storage, VPC)
- Ansible Core/Tower/AAP
- Terraform, Terragrunt & OpenTofu (IaC)
- CI/CD (GitLab CI, GitHub Actions)
- Application Security (SAST, SCA, Veracode, Prisma Cloud)
- Container Security (Docker, Kubernetes, Twistlock)
- Bash & Python
- Monitoring & Observability (Prometheus & Grafana)
- Security & Compliance (DISA STIG, NIST 800-53, SOC 2, ISO 27001)
- Backup & Disaster Recovery (AWS Backup, rsync, snapshots, DR drills)
- Technical Documentation & Knowledge Sharing
- Analytical Troubleshooting & Root Cause Analysis
- Cross-functional Collaboration
- Tier-2/3 support & 24x7 on-call

## CERTIFICATIONS

---

- CompTIA Security+
- CompTIA Linux+
- CompTIA Network+
- AWS Certified Cloud Practitioner
- Microsoft Certified: Azure Fundamentals
- GitHub Foundations

## PROFESSIONAL EXPERIENCE

---

### DevSecOps Engineer | Southwest Airlines

Remote, US | Jul. 2025 - Present

- Integrated Veracode SAST/SCA scanning into CI/CD pipelines across 15+ application teams, reducing mean time to remediate critical vulnerabilities from 30 days to 7 days.
- Deployed Prisma Cloud policies for infrastructure compliance, achieving 95% policy pass rate across AWS and Azure environments.
- Implemented Twistlock container scanning in build pipelines, blocking 200+ vulnerable images from reaching production monthly.
- Automated security exception workflows reducing approval time from 5 days to 24 hours while maintaining audit compliance.
- Delivered secure IaC training to 8 development teams, improving Terraform security scan pass rates by 40%.
- Led cross-functional security reviews for 3 major releases, identifying and remediating 45 high-severity findings pre-production.

### DevOps Engineer | L3Harris Technologies

Washington, DC | Nov. 2024 - Jul. 2025

- Administered over 250 CentOS/RHEL servers in AWS, Azure, OCI, and GCP; performed weekly patching and DISA STIG hardening to sustain 99.98% uptime.
- Built a Terraform and Ansible Tower pipeline that deploys a full Linux stack with Docker containers in 15 minutes, resulting in 40% faster onboarding.
- Centralized metrics using Prometheus, Grafana, CloudWatch, and Azure Monitor, reducing MTTR by 30%.
- Rolled out Red Hat Satellite content views, eliminating package drift and ensuring 100% patch compliance.
- Tuned systemctl and tuned-profiles to reduce application latency by 22% without additional cost.
- Provided Tier-3/on-call support, resolving P1 incidents in under 20 minutes on average with 98% SLA adherence.
- Migrated over 200 Terraform state files to OpenTofu and automated drift checks using Puppet jobs, reducing configuration drift by 30% across production nodes.

### DevOps Engineer | Amazon Web Services

Arlington, VA | Sep. 2021 - Nov. 2024

- Managed over 300 Ubuntu and RHEL EC2 instances; developed Bash/Python AMI and patch scripts, reducing patch windows by 60%.
- Designed SOC 2-compliant VPCs with transit gateways and private subnets.
- Created CloudWatch alarms and Grafana dashboards, reducing alert noise by 35%.
- Orchestrated Kubernetes blue/green releases with Docker containers, enabling zero-downtime deployments.
- Devised cross-region disaster recovery with AWS Backup and S3 replication, achieving RTO of less than 1 hour and RPO of less than 15 minutes.
- Implemented a GitLab CI/CD pipeline that built, scanned, and released hardened AMIs and Terraform plans, reducing deployment hand-offs and lead time by 25%.

## **Cyber Security Engineer | Defense Intelligence Agency**

Fort Dix, NJ | May 2019 - Sep. 2021

- Led DISA STIG remediation, reducing critical findings by 90% in 6 months.
- Migrated legacy Solaris to hardened RHEL 7 on VMware, boosting performance by 35% and meeting DoD RMF.
- Hardened networks using IDS/IPS, next-generation firewalls, and fine-tuned SELinux policies.
- Integrated AWS Inspector and Azure Security Center scans into the pipeline, surfacing critical CVEs within hours and reducing time-to-remediate by 90%.

## **Systems Administrator | United States Navy**

San Diego, CA | Feb. 2015 - May 2019

- Supported NIPR/SIPR networks with 4000 endpoints; developed Bash automation scripts, saving 400 labor hours per year.
- Maintained 99.8% availability of mission-critical communications through proactive patching.
- Built centralized syslog and Grafana dashboards for real-time operational visibility.

## **EDUCATION**

---

### **Bachelor of Science in Cyber Security | University of Maryland**

Cum Laude | May 2024