Kenneth Benitez

(703) 555-8614 kenneth.benitez@example.com linkedin.com/example/kennethbenitez Arlington, VA 22203

SUMMARY

Principal Cyber Security Engineer with 15 years securing **Linux**, cloud, container, and **production infrastructure** across regulated federal environments. Builds security tooling, automated controls, **Infrastructure as Code**, and CI/CD integrations for public and private clouds. Hands on work includes AWS, GCP, Kubernetes, Python, REST APIs, HTTP, encryption, authorization, threat modeling, security policy, and NIST 800 53 controls. Partners with service teams to turn **functional security requirements** into practical engineering decisions, reusable frameworks, and systematic remediation. Maintains active TS/SCI with CI polygraph, DoD 8570/8140 IAT Level II compliance, current Computing Environment credentials, and AWS Security Specialty certification. Brings principal level technical leadership, clear documentation, and production judgment that supports secure federal delivery.

EXPERIENCE

Principal Cyber Security Engineer, Federal Cloud Engineering

February 2021 - Present

Aegis Federal Cloud Engineering

Arlington, VA

Leads security engineering for regulated federal workloads across Linux, AWS, Kubernetes, containers, Infrastructure as Code, and production cloud operations. Guides service teams, owns technical decisions, and converts policy into durable automated controls.

- Built Python controls for Linux and cloud workloads, giving federal teams repeatable production safeguards.
- Embedded **Infrastructure as Code** checks within **CI/CD** pipelines, creating auditable security changes.
- Mapped threat models and **NIST 800 53** controls, clarifying evidence paths for reviewers.
- Integrated **security tooling** through **REST APIs** and HTTP, applying encryption and authorization patterns.
- Advised service teams on **Kubernetes** and container risks, resolving recurring infrastructure issues systematically.
- Maintained clearance documentation and security engineering records supporting federal delivery reviews.

Senior Cyber Security Engineer, Cloud Infrastructure

May 2017 - January 2021

Sentinel Ridge Technologies

Herndon, VA

Engineered cloud and **container security** for federal infrastructure, combining automation, policy interpretation, API integration, and technical consultation. Supported delivery teams through risk reviews, control implementation, and production issue resolution.

- Automated Linux baseline validation with **Python**, reducing manual review effort across infrastructure releases.
- Created Terraform controls for cloud resources, improving consistency across repeatable deployment environments.
- Applied **threat modeling** during architecture reviews, exposing misuse paths before production approval.
- Connected security services through REST APIs, HTTP, **encryption**, and **authorization schemas**.
- Reviewed Kubernetes workloads and container images, guiding teams through practical remediation decisions.
- Translated **NIST 800 53** requirements into functional security documentation for federal stakeholders.

Cyber Security Engineer, Defense Systems

June 2013 - April 2017

BluePeak Defense Systems

Alexandria, VA

Delivered security engineering for defense platforms, supporting **Linux** systems, cloud adoption, container controls, automation, and compliance evidence. Worked with architects and delivery teams on risk decisions that protected production services.

- Implemented Python security **automation** for production systems, replacing repetitive control checks with reliable workflows.
- Provisioned secure infrastructure through Terraform, preserving change history for compliance reviews.
- Documented functional requirements from **security policy**, helping engineers connect controls with system behavior.
- Built **HTTP** integrations for **security tooling**, using encryption and authorization patterns for protected exchanges.
- Assessed cloud and container risks during design reviews, directing teams toward actionable fixes.
- Prepared **NIST 800 53** evidence packages, supporting technical reviews and federal authorization activities.

Systems Security Engineer, Infrastructure Protection

July 2011 - May 2013

Capital Secure Computing

Fairfax, VA

Supported systems security engineering for federal infrastructure, with focus on Linux protection, automation, technical documentation, and control implementation. Collaborated with senior engineers on production safeguards and compliance focused delivery.

- Hardened **Linux** systems against documented risks, improving baseline consistency across supported environments.
- Scripted recurring security checks with Python, giving engineers faster visibility into control gaps.
- Assisted **Infrastructure as Code** reviews, identifying configuration risks before deployment approval.
- Supported **REST API** testing with HTTP and authorization controls for infrastructure integrations.
- Contributed **threat modeling** sessions, recording security assumptions and practical mitigation actions.
- Organized **NIST 800 53** evidence, helping senior engineers answer federal assessment questions.

PROJECTS

Federal Cloud Control Automation 2025

A recurring control gap prompted a reusable automation effort. Built Python and Terraform patterns that connected cloud security checks with CI/CD evidence, supporting consistent safeguards across public and private cloud infrastructure.

Kubernetes Security Integration 2023

Container teams needed clearer risk signals before release. Integrated Kubernetes and container security checks with REST services, encryption, authorization, and delivery workflows for more predictable production decisions.

LEADERSHIP & AWARDS

- Principal technical leadership recognition for reusable federal cloud security controls and production automation.
- Engineering recognition for clear NIST 800 53 evidence mapping and practical service team consultation.
- Federal delivery recognition for maintaining active clearance, certification readiness, and disciplined security documentation.

EDUCATION

Bachelor's Degree in Computer Science 2011

George Mason University GPA: 0 *Fairfax, VA*

Coursework: *Operating Systems, Computer Networks, Software Engineering, Information Security*

CERTIFICATIONS

- Active TS/SCI with CI Polygraph 2026
- CompTIA CySA+ 2025
- DoD 8570/8140 IAT Level II 2026
- AWS Certified Security Specialty 2024

TECHNICAL SKILLS

- **Operating Systems:** Linux, Unix, Bash
- **Cloud Platforms:** AWS, GCP, Private cloud
- **Container Platforms:** Kubernetes, Docker, Container images
- **Infrastructure as Code:** Terraform, CloudFormation, Configuration management
- **Programming and Scripting:** Python, Bash, Automation scripting
- **Delivery Pipelines:** CI/CD, Git, Pipeline controls
- **Security Standards:** NIST 800 53, DoD 8570, DoD 8140
- **Security Analysis:** Threat modeling, Risk assessment, Security policy
- **API Integration:** REST API, HTTP, JSON
- **Cryptography and Access:** Encryption, Authorization, Authentication
- **Cloud Security:** AWS security, GCP security, Private cloud security
- **Compliance Credentials:** CompTIA CySA+, AWS Security Specialty, Computing Environment credential

SKILLS

- Linux
- AWS
- GCP
- Kubernetes
- Containers
- Python
- CI/CD
- Threat modeling
- NIST 800 53
- REST API
- HTTP
- Encryption
- Authorization schemas
- Infrastructure as Code
- Cloud security

PROFESSIONAL AFFILIATIONS

- Member, Cloud Security Alliance, with focus on cloud controls and secure infrastructure.
- Member, Information Systems Security Association, sharing federal security engineering practices with peers.

LANGUAGES

- English (Native)
- Spanish (Proficient)

ADDITIONAL INFORMATION

Work Status : Authorized to work in United States. No sponsorship required.

REFERENCES

AVAILABLE ON REQUEST