Nathaniel Gibbs

(503) 555-0186 | nathaniel.gibbs@example.com | linkedin.com/example/nathanielgibbs | Portland, OR 97205

SUMMARY

Senior Security Engineer with 11 years protecting technology and digital health environments through practical blue-team engineering. Builds **security tooling**, automates investigations, assesses third-party suppliers, maps **data flows**, and turns findings into clear remediation plans. Leads **incident response** for credential misuse, endpoint threats, phishing, malware, anomalous access, and exposed AWS resources. Strengthens macOS fleets with CrowdStrike Falcon, EDR, **application control**, and threat detection. Partners with DevOps on IAM, storage permissions, network paths, CI/CD secrets, and cloud vulnerabilities. Explains technical risk clearly to product, operations, procurement, legal, privacy, and executive audiences. Ready to help Cedarwell Behavioral Health protect sensitive information, support dependable therapy services, and grow practical security capabilities across its remote organization.

EXPERIENCE

Senior Security Engineer, Blue Team

September 2019 - Present

Harborline Wellness Technologies

Portland, OR

Owns blue-team engineering for a remote digital health platform, directing endpoint, cloud, identity, supplier risk, **security tooling**, and incident response programs across **AWS** workloads and approximately 1,200 employee devices.

- Built **Python** and Rust utilities that enriched Falcon alerts with identity context, shortening repetitive investigation work.
- Directed vendor reviews for regulated health data, mapping flows and presenting control gaps for procurement decisions.
- Led credential misuse response by containing accounts, preserving evidence, validating eradication, and recording lessons learned.
- Expanded **macOS** protection through Falcon policies, **application control**, device standards, and threat-detection tuning.
- Partnered with **DevOps** on AWS IAM, storage, network paths, and CI/CD secrets, producing verified remediation plans.
- Presented security risk clearly to product, operations, procurement, and executive stakeholders during high-impact reviews.

Security Engineer

January 2018 - August 2019

Northstar Care Systems

Denver, CO

Delivered security engineering for healthcare software, connecting AWS reviews, endpoint telemetry, identity events, supplier assessments, incident investigations, and SQL analysis with customer trust and audit readiness.

- Created Python and **PHP scripts** that enriched alerts and tracked supplier evidence across security reviews.
- Performed third-party assessments with questionnaires, architecture reviews, data-flow diagrams, and evidence validation for onboarding.
- Investigated phishing and malware cases with infrastructure, application, legal, and privacy partners.
- Improved **Okta** lifecycle controls by reviewing privileged groups, sign-on policies, multifactor coverage, and dormant accounts.
- Presented technical findings to product and operations groups, connecting remediation with customer trust and service availability.
- Queried authentication, application, and audit datasets with **SQL** during investigations involving suspicious access and exposure.

Security Analyst / Security Engineer

June 2016 - December 2017

Blue Mesa Software Group

Phoenix, AZ

Supported a growing security operations program through endpoint and cloud monitoring, Falcon tuning, AWS reviews, supplier data-flow analysis, incident triage, and investigation scripting.

- Tuned Falcon detection policies after reviewing false positives, malware samples, and recurring workstation attack patterns.
- Mapped vendor integrations and application **data flows**, identifying unsupported access before production approval.
- Correlated authentication, application, and endpoint records with SQL and Python during security investigations.
- Reviewed AWS **IAM**, security groups, logging, and S3 access patterns with development teams.
- Prepared concise incident summaries that helped engineering managers choose practical remediation actions.
- Triaged endpoint and cloud alerts, escalating confirmed incidents through documented response procedures.

Information Security Analyst

June 2015 - May 2016

Canyon Ridge Digital

Tempe, AZ

Monitored endpoint, identity, and network events for a SaaS environment while supporting supplier assessments, AWS reviews, macOS standards, access investigations, and response documentation.

- Maintained supplier assessment records with policies, testing summaries, access diagrams, and response evidence.
- Reconciled user, device, and application records with SQL during access reviews and account investigations.
- Assisted senior engineers with AWS IAM, logging, storage permissions, and network segmentation reviews.
- Validated macOS encryption, screen locks, administrative access, and approved-application settings for endpoint standards.
- Produced response playbooks and investigation checklists that improved consistency for service desk teams.
- Documented investigation timelines and escalated suspicious activity requiring containment or senior review.

PROJECTS

AWS Blue-Team Control Review 2024

Mapped AWS identities, storage permissions, network paths, and CI/CD secrets into a practical review program. Findings became prioritized fixes with verification steps for DevOps partners.

Endpoint Detection Tuning Program 2022

Refined CrowdStrike Falcon policies across macOS devices by studying false positives, malware patterns, and user impact. Clearer detections helped analysts focus on meaningful signals.

Supplier Data-Flow Assessment Framework 2020

Created a repeatable assessment approach for vendors handling sensitive health information. Questionnaires, diagrams, evidence checks, and risk decisions gave stakeholders a shared view.

LEADERSHIP & AWARDS

- Received an internal Security Impact Award for building reusable investigation automation and improving analyst response consistency.
- Recognized by engineering leadership for translating AWS and endpoint risk into clear remediation decisions for non-technical partners.
- Led cross-functional incident response sessions that connected security, infrastructure, product, legal, and privacy teams around shared outcomes.

EDUCATION

B.S. in Information Systems 2015

Arizona State University GPA: 3.7 *Tempe, AZ*

Coursework: *Database Systems, Network Security, Information Assurance, Systems Analysis*

CERTIFICATIONS

- AWS Certified Security - Specialty 2023
- Okta Certified Professional 2022
- GIAC Certified Incident Handler (GCIH) 2021

TECHNICAL SKILLS

- **Cloud Security:** AWS, IAM, S3
- **Endpoint Security:** CrowdStrike Falcon, EDR, macOS
- **Security Coding:** Python, Rust, PHP
- **Database Investigation:** SQL, query crafting, database structures
- **Identity Management:** Okta, multifactor authentication, sign-on policies
- **Incident Response:** Evidence preservation, containment, eradication
- **Third-Party Risk:** Supplier assessments, security questionnaires, control validation
- **Security Automation:** Alert enrichment, internal scripts, workflow automation
- **Application Security:** Application control, vulnerability review, threat detection
- **Cloud Operations:** AWS logs, CI/CD secrets, network paths
- **Data Governance:** Data-flow mapping, regulated health data, access reviews

SKILLS

- Security Assessments
- Incident Response
- Threat Detection
- Endpoint Security
- AWS Security
- IAM
- Okta
- CrowdStrike Falcon
- macOS Security
- Python
- Rust
- PHP
- SQL
- Security Automation
- Data-Flow Mapping

PROFESSIONAL AFFILIATIONS

- Member, Information Systems Security Association, with regular exchange on blue-team engineering and incident response.
- Member, Cloud Security Alliance, following practical guidance on AWS security, identity, and cloud risk management.

LANGUAGES

- English (Native)
- Spanish (Intermediate)

ADDITIONAL INFORMATION

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

REFERENCES

AVAILABLE ON REQUEST