George Chandler

(510) 555-1842 george.chandler@example.com linkedin.com/example/georgechandler Oakland, CA 94612

SUMMARY

Staff level **product security** engineer with 10 years of experience securing **multi tenant SaaS** platforms that process sensitive and **regulated information**. Combines product security depth with production software engineering in Python and Go, translating threat models and architecture risks into durable controls, automation, and secure code. Leads high risk design reviews and drives findings from **penetration tests**, bug bounty programs, audits, cloud tooling, and hands on testing through verified remediation or documented risk decisions. Builds practical security guidance for engineering teams across AWS IAM, network segmentation, workload isolation, secrets, logging, Kubernetes, CNAPP operations, identity, APIs, and authorization. Partners across product, platform, and infrastructure groups, supports incident response, and applies AI assisted analysis with disciplined source level validation. Brings grounded judgment to complex clinical and regulated data environments.

EXPERIENCE

Staff Product Security Engineer

July 2023 - Present

Harborline Health Technologies

Oakland, CA

Leads product security for multi tenant clinical workflow services handling regulated health information. Owns architecture reviews, **threat modeling**, authorization design, vulnerability validation, cloud security collaboration, and AI assisted security workflows.

- Led security design for clinical workflow services, clarifying trust boundaries around regulated health information.
- Built **Python** threat model automation linking design risks with tickets, evidence, and remediation status.
- Designed OAuth, OIDC, JWT, RBAC, and ReBAC guardrails, then tested tenant isolation across services.
- Reproduced penetration test and **bug bounty** findings through targeted testing and **proof of concept exploits**.
- Partnered on **AWS IAM**, segmentation, Kubernetes isolation, **secrets**, logging, and CNAPP tuning for production.
- Created AI assisted review workflows requiring source validation before recommendations entered engineering work.

Senior Security Engineer

January 2021 - June 2023

Cedar Peak Software

Sacramento, CA

Embedded product security into SaaS design and delivery workflows. Combined Go and Python automation with application testing, security tooling ownership, incident learning, and practical developer guidance.

- Embedded threat modeling and **secure code review** into SaaS design and release workflows.
- Wrote **Go** and Python automation for authorization testing, regression checks, and security evidence collection.
- Used **dynamic testing** and proof of concept development to confirm exploitable application paths.
- Managed security tooling through integration, tuning, triage, upgrades, maintenance, and effectiveness reviews.
- Converted incident root causes into stronger **logging**, test coverage, secure defaults, and developer guidance.
- Mentored engineers on **OAuth**, **SAML**, JWT validation, API design, secrets handling, and remediation.

Security Software Engineer

June 2018 - December 2020

Granite Bay Cloud Systems

Roseville, CA

Built production security software and cloud validation workflows for critical services. Focused on AWS configuration, access policy analysis, application testing, event quality, and safer defaults.

- Built Python automation validating cloud configurations, inspecting access policies, and surfacing actionable security issues.
- Reviewed authentication, authorization, sessions, and APIs for vulnerability classes and verified fixes.
- Implemented **AWS** checks for **IAM**, logging, secrets exposure, and network configuration risks.
- Conducted focused application testing, documenting reproducible attack paths and practical mitigation options.
- Standardized security event fields and alert context across critical services for clearer investigations.
- Contributed **production security** libraries, validation routines, and safer configuration defaults.

Software Engineer, Security

September 2016 - May 2018

Sierra Vista Digital

San Jose, CA

Developed backend services and security controls for a multi tenant platform. Supported APIs, identity flows, automated testing, operations, cloud permissions, and secure coding education.

- Developed Python and **Java** backend services supporting APIs, identity flows, testing, and operations.
- Added secure input validation, authorization checks, and structured security logging across platform services.
- Created automated authentication and access control tests covering token validation and role boundaries.
- Traced vulnerability findings into affected code paths, then validated fixes with focused tests.
- Improved AWS **secrets** handling and service permissions through close infrastructure engineering partnership.
- Documented secure coding patterns and recurring failure modes with practical engineering examples.

PROJECTS

Clinical Tenant Isolation Validation 2024

Created a focused validation program for multi tenant clinical workflows, combining threat modeling, authorization tests, targeted dynamic testing, and evidence based remediation tracking.

Cloud Security Control Automation 2022

Built reusable Go and Python checks for AWS IAM, secrets, logging, network configuration, and workload isolation, giving engineers clearer findings and repeatable verification.

LEADERSHIP & AWARDS

- Recognized by engineering peers for translating complex authorization risks into practical controls and clear remediation guidance.
- Trusted to lead sensitive product security reviews spanning architecture, implementation, testing, and documented risk decisions.
- Selected to develop AI assisted review workflows with source level validation for engineering use.

EDUCATION

Bachelor's Degree in Computer Science 2016

San Jose State University GPA: 3.5 *San Jose, CA*

Coursework: *Software engineering, computer security, algorithms, database systems*

CERTIFICATIONS

- AWS Certified Security, Specialty 2025
- GIAC Web Application Penetration Tester, GWAPT 2023

TECHNICAL SKILLS

- **Programming Languages:** Python, Go, Java
- **Identity Standards:** OAuth, OIDC, SAML
- **Token Security:** JWT, token validation, sessions
- **Authorization Models:** RBAC, ReBAC, tenant isolation
- **Application Security:** API security, secure code review, input validation
- **Cloud Security:** AWS, IAM, CNAPP
- **Cloud Infrastructure:** Kubernetes, network segmentation, workload isolation
- **Security Testing:** Dynamic testing, penetration testing, vulnerability testing
- **Security Operations:** Incident response, logging, alert context
- **Security Automation:** Threat model automation, regression checks, evidence collection
- **Risk Management:** Bug bounty triage, audit findings, risk acceptance
- **AI Security:** AI assisted analysis, source validation, enterprise AI security

SKILLS

- Product Security
- Threat Modeling
- OAuth
- OIDC
- SAML
- JWT
- RBAC
- ReBAC
- API Security
- Secure Code Review
- Python
- Go
- AWS
- IAM
- Kubernetes

PROFESSIONAL AFFILIATIONS

- Professional focus includes product security, regulated data protection, secure software delivery, and cloud security engineering.
- Ongoing practice connects application security with platform engineering, incident learning, and developer enablement.

LANGUAGES

- English (Native)
- Spanish (Intermediate)

ADDITIONAL INFORMATION

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

REFERENCES

AVAILABLE ON REQUEST