

Nik Ogura

San Diego County, USA

[GitHub](#) — [LinkedIn](#) — [Website](#)

Aut viam inveniam, aut faciam (I will find a way, or I will make one)

Professional Summary

- **Principal Engineer / CIO** with proven track record architecting enterprise-grade platforms spanning multi-cloud, bare-metal, and air-gapped environments for fintech, crypto trading, and global scale systems
- **Platform Engineering Leader** who has built self-bootstrapping Kubernetes systems, AI-powered security automation, and infrastructure serving millions of users with 100x cost optimizations and zero-downtime deployments
- **Security-First Architect** with deep expertise in PKI, encryption, compliance (FedRamp, PCI DSS), and creating security systems that have withstood penetration testing by Apple's internal security teams
- **Open Source Contributor** with multiple projects listed in awesome-go, including self-updating binary distribution systems, Kubernetes operators, and novel authentication patterns
- **Innovation Driver** who has achieved multiple "firsts" including first automated CI/CD at Apple, first hardware ownership for Apple Pay, and revolutionary approaches to secrets management and voice-driven automation

Experience

Terrace | CIO & Director of Infrastructure and Security | 2023-Present

- **Multi-Cloud Platform Architecture:** Architected enterprise-grade crypto trading platform spanning AWS, GCP, and bare-metal with GitOps deployment model, achieving 76% cost reduction and 40% latency improvement while eliminating vendor lock-in
- **Crisis Management Leadership:** Restored critical systems and protected intellectual property during personnel turnover within hours, achieving zero business disruption and 100% IP retention through emergency access controls and audit trails
- **Observability Cost Optimization:** Designed scalable monitoring systems from scratch using Prometheus + Thanos federation, replacing commercial SaaS solutions with 100x cost reduction while improving Mean Time To Detect
- **AI-Powered Security Automation:** Built Slack-integrated AI bots for automated security and deployment incident response, providing 24/7 automated coverage with 80% reduction in manual triage and 50% faster Mean Time To Resolution
- **Product Relaunch Engineering:** Re-architected entire platform from database to frontend in under 3 months, reducing latency from 600ms to microseconds and increasing data capacity by 100x to enable flagship product launch
- **Bare-Metal Encryption & Key Management:** Designed custom KMS for LUKS full-disk encryption on Talos Kubernetes clusters, eliminating \$10k-\$20k monthly AWS data egress costs while maintaining operator-controlled security

Amazon Web Services | Systems Development Engineer, Senior DevOps Consultant | 2022-2023

- **FedRamp Compliance Automation:** Automated compliance processes for Federal government cloud systems, achieving 100% automation of compliance checks with 50% faster authorization and zero compliance violations for Amazon Global Accelerator
- **AWS WAF Kubernetes Operator:** Developed Kubernetes Operators for Amazon WAF with declarative policy management and GitOps-friendly infrastructure as code, achieving 95% reduction in WAF policy deployment time

Orion Labs | Head of Infrastructure, Principal Engineer | 2020-2022

- **SaaS and On-Premises Platform:** Built stand-alone, self-bootstrapping, one-click Kubernetes system working across cloud, on-prem, and air-gapped environments, achieving 100% customer satisfaction in evaluations with customers describing installation as “flawless” and “highest quality software installation we have ever seen”
- **COVID Contact Tracing for MBTA:** Developed privacy-preserving epidemiological contact tracing system for Massachusetts Bay Transit Authority serving greater Boston area, enabling real-time location tracking and voice/text replay capabilities for transit workers and riders during pandemic
- **Thundering Herd Solution:** Solved massive traffic spike problem by migrating from AWS Application Load Balancers to Network Load Balancers and moving Layer 7 switching to Kubernetes ingress controllers, eliminating service disruptions from fleet-wide device restarts
- **Voice Bot Framework:** Built framework for voice-driven automation on Orion PTT platform, enabling 100+ customer voice automation use cases and creating differentiated offering in voice communications market

Scribd | Principal DevSecOps Engineer | 2018-2020

- **Founded Security Team:** Established Scribd's first dedicated Security Team, building team from 0 to 5 members and transforming security posture for rapidly scaling company serving millions of users globally with zero major security incidents
- **SIEM System for Global CDN:** Built scalable SIEM system from scratch handling petabytes of log data with real-time threat detection, discovering user behavior patterns and bot activity while providing company-wide self-service analytics
- **Managed Secrets System:** Created YAML interface on Hashicorp Vault enabling 100+ engineers to define secrets and access control without seeing production values, achieving zero secrets leaks and later released as open source project
- **Kubernetes + CDN Integration:** Designed K8s clusters with native tooling connecting application workloads to Fastly CDN caches, achieving 99% cache hit rate and 50% bandwidth cost reduction through automated cache management

Stitch Fix | Sr. DevOps/SRE | 2017

- **IAM System for Data Science:** Built Identity and Access System for Algorithms & Analytics department providing seamless authentication across environments, achieving 100% uptime during company's 3rd-party SSO breach when vendor systems went down
- **IAM Authentication Innovation:** Enabled AWS IAM Role/STS credentials on developer laptops by bending AWS metadata service, providing seamless local/cloud development experience for 100+ developers with zero credential leaks

Apple | Lead DevOps Engineer | 2015-2017

- **Historic Apple Pay DevOps Leadership:** Led first Apple Pay DevOps team to achieve full hardware ownership - a historic first in Apple's history - breaking through traditional barriers and setting precedent for future teams
- **First Automated CI/CD at Apple:** Designed and implemented first automated test-driven CI/CD system for Apple Pay with dynamic environment creation per pull request, achieving zero deployment-related outages during critical 2015-2017 period
- **Global Apple Pay China Launch:** Architected command and control architecture managing 30,000 servers worldwide for Apple Pay China launch, achieving zero downtime during global deployment
- **Private OpenStack Innovation:** Created private OpenStack cloud from unused hardware, achieving 100x acceleration of build and test cycle and proving private cloud viability when datacenter was still under construction

- **Security-First Infrastructure:** Designed OpenStack deployment so secure that Apple's own security teams couldn't penetrate until protections stood down, setting new security standard and proving security and usability can coexist

U.S. Bank | Security Architect, Application Architect | 2007-2014

- **Enterprise WAF Management:** Solely developed and managed Web Application Firewalls for entire U.S. Bank over 5 years with team of 2, achieving zero breaches while maintaining PCI DSS and OWASP Top Ten compliance
- **Encryption Key Management System:** Developed PKI and key management service saving over \$1M compared to vendor bids, supporting multiple countries with one-button delivery across network tiers, still in production 15+ years later
- **Credit Card PAN Security:** Designed Credit Card PAN Encryption and Tokenization System for Merchant Acquiring payment processing, securing millions of transactions with zero PAN data breaches while maintaining PCI DSS compliance

Skills

Languages: Golang, Bash, Perl, Python, Ruby, Java, Groovy, JavaScript, TypeScript

Cloud Platforms: AWS, GCP, Azure, OpenStack

Kubernetes: EKS, AKS, Rancher, Kubeadm, Replicated, Talos, Operator Framework, Minikube, Helm, Kustomize

CI/CD: Jenkins, GitHub Actions, TeamCity, Travis, CircleCI, FluxCD, ArgoCD, Tekton

Databases: Postgresql, MySQL, Oracle, Redis, Clickhouse, TimescaleDB, DynamoDB, GraphQL

Security: OpenSSL, OpenSSH, Luna HSMs, OpenVPN, SIEM, Kerberos, PKCS, IPsec, PKI, OIDC, SAML, JWT

Networks: TCP/IP, DNS, Load Balancers, Proxies, Istio, Consul, Nginx, HAProxy, Envoy

Open Source Projects

Dynamic Binary Toolkit (DBT) - Self-updating signed binary distribution system listed in awesome-go, builds, tests, publishes, and updates itself in flight for distributing tools in cloud, containers, and laptops

Go Mason - Tool for clean-room CI testing locally, listed in awesome-go, enables testing CI pipelines on laptop before pushing

Managed Secrets - YAML interface on Hashicorp Vault created at Scribd, allows teams to manage secrets without accessing production values, used in production at multiple companies

NamedReturns Linter - golangci-lint plugin enforcing named return values for self-documenting code, established organization-wide engineering standards

K8S Cluster Manager - Command line tool for managing bare-metal and VM Kubernetes nodes on Talos Linux, used in production for managing multi-cluster environments

Hasura Operator - Kubernetes Operator for declaratively managing Hasura GraphQL instances, extends K8s API for GraphQL infrastructure

Kubectl-SSH-OIDC - kubectl plugin providing passwordless authentication using SSH keys and Dex IDP with novel OIDC Token Exchange flow for CLI tools