

# 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 and CIO** with 25+ years of experience architecting enterprise-grade distributed systems, multi-cloud platforms, and security-first infrastructure spanning cryptocurrency trading, financial services, and high-scale consumer applications
- **Platform Engineering Expert** specializing in Kubernetes, bare-metal clusters, and hybrid multi-cloud architectures with proven track record managing global infrastructure of 30,000+ servers and delivering 76% cost reductions through architectural optimization
- **Security and Compliance Leader** with deep expertise in WAF deployment, PKI systems, encryption, and regulatory compliance (PCI DSS, FedRamp) having founded security teams and protected millions of financial transactions with zero major security incidents
- **Open Source Contributor** and technical innovator creating production-grade tools for secrets management, binary distribution, code quality enforcement, and AI-powered operational automation adopted across multiple organizations
- **Technical Leadership** across diverse domains including distributed data systems processing millions of cryptocurrency trading pairs, real-time observability at petabyte scale, and automated compliance validation for infrastructure-as-code

## 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 cloud-agnostic design preventing vendor lock-in, achieving 76% cost reduction and 40% latency improvement through strategic infrastructure optimization
- **Federated Multi-Cluster Observability:** Solved impossible observability trade-off by designing specialized federated system spanning distributed clusters - Loki for log streaming, Elasticsearch for high-cardinality WAF analytics, Prometheus+Thanos for metrics federation, processing 2M+ ModSecurity logs daily with 85% MTTR reduction
- **AI-Powered Security & Incident Response:** Automated security and deployment incident response with AI bots achieving 24/7 automated coverage, 80% reduction in manual triage, and 50% faster MTTR through Slack-integrated diagnostics handling WAF blocks, vulnerability reports, and deployment issues autonomously
- **Distributed Data Curation Platform:** Architected extensible middleware pipeline for cryptocurrency market data with cache-agnostic ETL architecture, serving 27+ dependent services with sub-10ms change detection across 4.1M+ trading pairs while eliminating \$120k-\$240k annual storage costs
- **Infrastructure as Code:** Established comprehensive Terraform infrastructure managing multiple AWS accounts plus multi-cloud resources with custom GitOps workflow, cross-account IAM with OIDC, and declarative infrastructure ensuring audit trails and regulatory compliance

[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, 50% faster authorization, and zero compliance violations enabling Federal customers to use Global Accelerator
- **Kubernetes Operators for AWS Services:** Developed Kubernetes Operators for Amazon WAF enabling declarative policy management, GitOps-friendly infrastructure as code, and 95% reduction in WAF policy deployment time with 100% Kubernetes-based management of AWS resources
- **Global Scale Infrastructure:** Secured and maintained Amazon Global Accelerator systems for FedRamp com-

pliance with continuous compliance monitoring and automated security tooling for Federal government cloud requirements

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

- **SaaS and On-Premises Platform:** Built stand-alone, self-bootstrapping Kubernetes system supporting SaaS, cloud-prem, on-prem, and air-gapped installations with one-click deployment achieving 100% customer satisfaction in evaluations and described as 'flawless' by enterprise customers
- **Solved Thundering Herd at Scale:** Migrated from AWS ALB to NLB with Layer 7 switching in Kubernetes ingress controllers to handle massive traffic spikes from fleet-wide device restarts that exceeded ALB's autoscaling capabilities, eliminating service disruptions
- **COVID Contact Tracing for MBTA:** Built privacy-preserving epidemiological contact tracing system for Massachusetts Bay Transit Authority using voice bot-enabled platform with real-time location tracking and conversation replay, supporting public health response for greater Boston area
- **Voice Bot Framework:** Developed API-driven framework for Voice Bots on Orion Platform enabling automated voice interactions and workflow automation for customers in mission-critical voice communications

**Scribd** | *Principal DevSecOps Engineer* | 2018-2020

- **Founded Security Team:** Established Scribd's first dedicated Security Team from ground up, creating security practices, tooling, and culture for rapidly scaling company serving millions of users globally with zero major security incidents
- **SIEM System for Global CDN:** Built scalable SIEM system handling petabytes of log data with code processing, correlating, and consuming information streams, discovering user behavior patterns and bot activity with real-time threat detection and company-wide self-service analytics
- **Managed Secrets System:** Created YAML interface on Hashicorp Vault simplifying secrets management organization-wide with proper separation of duties, multi-auth support (LDAP, TLS, Kubernetes, IAM), used by engineering teams daily and released as open source with community adoption
- **Kubernetes + Fastly CDN Integration:** Designed Kubernetes clusters and native tooling connecting application workloads to global CDN for automated cache management, achieving 99% cache hit rate and 50% bandwidth cost reduction

**Stitch Fix** | *Sr. DevOps/SRE* | 2017

- **IAM System for Algorithms & Analytics:** Built independent Identity and Access System providing seamless authentication across all resources in data science infrastructure, maintaining 100% uptime during company-wide SSO breach when vendor systems failed
- **IAM Authentication on Laptops:** Innovated AWS metadata service implementation enabling IAM Role/STS credentials on developer laptops with zero code alteration of Amazon SDK, providing passwordless authentication used daily by engineering teams with zero credential leaks

**Apple** | *Lead DevOps Engineer* | 2015-2017

- **Led Apple Pay DevOps Team:** Achieved historic first in Apple's history by implementing modern administration and audit pattern, fostering collaboration between Security, Audit, and Engineering, and securing first-ever hardware ownership grant for Apple Pay
- **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, complete isolation, full testing, and automatic cleanup, enabling zero deployment-related outages
- **Command & Control for Global Launch:** Architected command and control system managing 30,000 servers worldwide for Apple Pay China launch with zero downtime during critical launch period
- **Private OpenStack Cloud:** Created private OpenStack cloud from unused hardware achieving 100x acceleration of build and test cycle, so secure that Apple's security teams required standing down protections for penetration testing

**U.S. Bank** | *Security Architect* | 2007-2014

- **Web Application Firewall:** Solely developed and managed WAFs for entire bank with team of two, establishing organization-wide trust with management backing for security decisions, maintaining zero breaches while handling diverse applications with credit card PAN data
- **Encryption Key Management System:** Developed comprehensive key management and distribution service saving over \$1M compared to vendor bids, providing one-button delivery across multiple OS and network tiers with friendly UI for international users, remaining in production 15+ years
- **Credit Card PAN Encryption & Tokenization:** Designed scalable and highly available system protecting millions of credit card transactions in merchant acquiring systems with role-based access controls and PCI DSS compliance, achieving zero PAN data breaches

## Technical Skills

**Cloud Platforms:** AWS, GCP, Azure, OpenStack

**Kubernetes:** EKS, Rancher, Kubeadm, Talos, Operator Framework, Helm, Kustomize

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

**Databases:** PostgreSQL, Redis, MySQL, Clickhouse, TimescaleDB, DynamoDB, Oracle

**Security:** OIDC, SAML, JWT, PKI, OpenSSL, OpenSSH, Kerberos, PKCS, IPSec

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

**Networking:** TCP/IP, DNS, Load Balancers, Istio, Consul, Nginx, HAProxy, Envoy

## Open Source Projects

**Dynamic Binary Toolkit (DBT)** - Self-updating signed binary distribution system for cloud, containers, and laptops. Listed in awesome-go.

**Diagnostic Slackbot** - AI-powered operational diagnostics using Claude Code CLI with custom MCP tools for automated investigation workflows.

**Go Mason** - Clean-room CI testing locally. Test CI pipelines on laptop before pushing. Listed in awesome-go.

**Managed Secrets** - YAML interface on Hashicorp Vault enabling teams to manage secrets without production access. Used in production at multiple companies.

**NamedReturns Linter** - golanci-lint plugin enforcing self-documenting code through named return values.

**Dex SSH Connector** - SSH authentication connector for Dex identity provider implementing OAuth2 Token Exchange with SSH-signed JWTs.

**Kubecti-SSH-OIDC** - kubectl plugin providing passwordless authentication using SSH keys and OIDC Token Exchange flow.