# 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 platforms spanning multi-cloud, bare-metal, and hybrid Kubernetes environments. Proven track record delivering cryptocurrency trading platforms, fintech infrastructure, and global-scale systems for Apple Pay (30,000+ servers), with expertise in distributed systems, data engineering, platform engineering, and security architecture.

• **Platform Engineering Expert** specializing in Kubernetes, multi-cloud architecture (AWS, GCP, Azure), and bare-metal infrastructure with demonstrated capability building self-bootstrapping, air-gapped deployment systems and achieving 76% cost reductions through strategic architectural decisions and open-source adoption.

• **Security and Compliance Leader** with deep expertise in Web Application Firewalls, PKI, encryption systems, and regulatory compliance (PCI DSS, FedRamp) having founded security teams from ground up, built SIEM systems processing petabytes of data, and designed zero-trust architectures surviving real-world insider attacks.

• **AI and Automation Pioneer** creating production-grade AI-powered operational tooling achieving 85% MTTR reduction and 60-80% automation of routine diagnostics through custom Claude-based Slack bots, federated observability platforms processing 2M+ security events daily, and comprehensive incident response automation.

• **Engineering Leadership and Team Building** across diverse domains including global distributed teams spanning multiple continents, contract-to-hire systems with production validation requirements, comprehensive technical training and curriculum development, and extreme capital efficiency strategies eliminating hundreds of thousands in annual recurring costs through strategic open-source adoption.

## Experience

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

• Architected multi-cloud hybrid Kubernetes platform spanning AWS, GCP, and bare-metal achieving 76% cost reduction and 40% latency improvement while eliminating vendor lock-in through strategic use of Talos, Flux, Prometheus, Thanos, Grafana, Istio, and Kafka with zero licensing costs beyond compute.

• Executed complete forensic response and asset recovery from critical insider threat incident where former executive seized GitHub organization and production database, demonstrating zero-trust architecture effectiveness under real adversarial conditions with full operational recovery within hours and zero customer data loss.

• Designed federated multi-cluster observability platform processing 2M+ ModSecurity security events daily across distributed infrastructure, implementing specialized architecture using Loki for log streaming, Elasticsearch for security analytics, and Prometheus+Thanos for metrics federation, enabling 85% MTTR reduction through AI-powered diagnostic automation.

• Built distributed data curation platform for cryptocurrency markets handling 4.1M+ unique trading pairs with 1 microsecond retrieval latency of popular tokens, implementing extensible middleware pipeline with fraud detection, caching patterns, and adaptive TTL strategies while eliminating $120k-$240k annual S3 API costs through strategic storage optimization.

• Established globally distributed engineering organization spanning North America, South America, Europe, Africa, and India using contract-to-hire model with 30-day production validation periods, comprehensive documentation-first culture, and asynchronous communication patterns enabling 24/7 development cycle with maintained quality standards.

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

• Automated FedRamp compliance processes for Amazon Global Accelerator enabling Federal government cloud deployments with 100% automation of compliance checks, 50% faster authorization timelines, and zero compliance violations through comprehensive security tooling and continuous compliance validation.

• Developed Kubernetes Operators for AWS WAF providing declarative policy management and GitOps-friendly infrastructure as code, achieving 95% reduction in WAF policy deployment time and 100% Kubernetes-based management of AWS security resources through custom resource definitions and automated reconciliation.

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

• Built stand-alone, self-bootstrapping, one-click Kubernetes platform supporting SaaS, cloud-premises, on-premises, and air-gapped installations with integrated PTT stack, metrics visibility, and auto-unsealing CA using Vault, achieving 100% customer satisfaction in evaluations described as "flawless" and "easiest, highest quality software installation we have ever seen".

• Engineered COVID epidemiological contact tracing system for Massachusetts Bay Transit Authority (MBTA) using voice bot-enabled platform with real-time location tracking, conversation replay capabilities, and privacy-preserving design enabling contact notification without exposing personal information across greater Boston metropolitan area.

• Solved thundering herd scaling problem affecting fleet-wide device restarts by migrating from AWS Application Load Balancers to Network Load Balancers with Layer 7 switching moved to Kubernetes ingress controllers, eliminating service disruptions from synchronized device reconnections and massive traffic spikes exceeding ALB autoscaling capabilities.

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

• Founded and led Scribd's first Security Team from ground up, establishing security practices, processes, tooling, and culture for rapidly scaling company serving millions of users globally, transforming security posture and enabling confident growth with zero major security incidents.

• Built scalable SIEM system processing petabytes of log data from worldwide CDN footprint with code handling massive information streams exceeding traditional storage capabilities, implementing real-time threat detection, user behavior analysis, bot activity discovery, and self-service analytics dashboard enabling company-wide visibility.

• Created managed secrets system with YAML interface on Hashicorp Vault supporting multi-auth (LDAP, TLS Certificate, Kubernetes, IAM), enabling developers to define secrets structure and access control without accessing production values, achieving zero secrets leaks across 100+ engineers and releasing as open-source project with community adoption.

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

• Built Identity and Access Management system for Algorithms & Analytics department providing seamless authentication across all resources, instances, and containers with independent architecture that maintained 100% uptime during company-wide third-party SSO breach, protecting data science infrastructure through autonomous operation.

• Implemented AWS IAM Role/STS credentials on developer laptops through innovative AWS metadata service integration requiring zero code alteration of Amazon SDK, enabling passwordless authentication and seamless local/cloud development experience across 100+ developers with zero credential leaks.

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

• Led Apple Pay DevOps team implementing modern administration and audit pattern, achieving first-in-Apple's-history hardware ownership grant for Apple Pay through collaboration between Security, Audit, and Engineering, breaking traditional barriers and setting precedent for future teams.

• 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 rapid safe deployments and serving as model for other teams with zero deployment-related outages.

• Architected command and control system managing 30,000 servers worldwide for global Apple Pay launch including China deployment, maintaining zero downtime during critical 2015-2017 period with flawless operational record across global financial services infrastructure.

• Created private OpenStack cloud from unused hardware achieving 100x acceleration of build and test cycle while overcoming datacenter space limitations, enabling dynamic virtual environments on demand and proving

private cloud viability for development velocity.

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

• Developed and managed Web Application Firewalls for entire U.S. Bank with team of two over 5+ years, tuning rulesets for diverse applications, educating developers on secure coding practices, and maintaining OWASP Top Ten and PCI DSS compliance with zero breaches across organization's complete application portfolio.

• Built Encryption Key Management and Distribution Service saving over $1M compared to vendor solutions, creating one-button delivery across multiple operating systems and network tiers with friendly UI for non-technical users in multiple countries, teaching self Java development to complete first Java application still in production 15+ years later.

• Designed Credit Card PAN Encryption and Tokenization System for Merchant Acquiring payment processing with scalable, highly available architecture implementing role-based access controls, protecting millions of credit card transactions with zero PAN data breaches and full PCI DSS compliance.

**Wells Fargo** | *Sr. Software Engineer* | 2014

• Built static code analysis tools for Puppet DSL using Antlr lexer and parser to validate Governance, Risk Management, and Compliance (GRC) requirements, enabling automated pre-deployment compliance validation against regulatory baselines and establishing continuous compliance validation with complete audit trails.

**Data Recognition Corporation** | *Principal DevOps Engineer* | 2014-2015

• Designed auto-scaling Continuous Delivery environment for educational testing platform, migrating multiple applications from proprietary systems to open source platforms while eliminating vendor lock-in, reducing deployment time from weeks to hours, and establishing comprehensive DevOps curriculum covering technology, disciplines, and cultural transformation.

**Skills**

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

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

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

**Databases:** Postgresql, Mysql, Oracle, Redis, Clickhouse, TimescaleDB, DynamoDB, GraphQL

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

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

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

**Open Source Projects**

**Diagnostic Slackbot** - AI-powered Slack bot for automated operational diagnostics using Claude Code CLI with custom MCP tools, achieving 85% MTTR reduction and 60-80% automation of routine diagnostics

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

**Dex SSH Connector** - SSH authentication connector for Dex identity provider implementing OAuth2 Token Exchange (RFC 8693) with SSH-signed JWTs

**Kubectl-SSH-OIDC** - kubectl plugin providing passwordless Kubernetes authentication using SSH keys and Dex IDP

**RAG Code Indexer** - Production-grade code indexing system parsing Go codebases into Elasticsearch for AI-assisted development with AST-based semantic analysis

**NamedReturns Linter** - Custom Golang linter enforcing named return values for self-documenting code