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 distributed systems, multi-cloud platforms, and enterprise security infrastructure across fintech, payments, publishing, and technology organizations. Deep expertise in Kubernetes, bare-metal clusters, cryptocurrency trading platforms, and real-time data processing at massive scale managing 30,000+ servers globally.

• **Platform Engineering Expert** specializing in multi-cloud architectures spanning AWS, GCP, and bare-metal infrastructure with proven track record delivering 76% cost reductions, 100x performance improvements, and enterprise-grade security solutions. Expertise in Kubernetes operators, GitOps workflows, and infrastructure as code across diverse deployment environments.

• **Security and Compliance Leader** with deep expertise in application security, WAF management, encryption systems, and regulatory compliance (PCI DSS, FedRamp, SOX) having founded security teams, built SIEM systems processing petabytes of data, and managed Web Application Firewalls for entire banking organizations.

• **Distributed Systems Architect** creating scalable data engineering platforms processing millions of real-time events, federated observability systems handling high-cardinality metrics across multiple clusters, and cryptocurrency market data platforms tracking 4.1M+ trading pairs with sub-10ms latency.

• **Technical Leadership and Innovation** across diverse domains including AI-powered automation achieving 85% MTTR reduction, open source contributions listed in awesome-go, comprehensive technical training curriculum development, and founding engineering teams from ground up establishing world-class standards and practices.

Experience

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

• Architected multi-cloud hybrid platform spanning AWS, GCP, and bare-metal achieving 76% cost reduction and 40% latency improvement while eliminating vendor lock-in through cloud-agnostic Kubernetes design using Talos, Flux, and best-in-class open source technologies.

• Built federated observability system solving metrics vs logs cardinality problem across distributed clusters using specialized architecture: Loki for log streaming, Elasticsearch for high-cardinality WAF analytics, Prometheus + Thanos for cross-cluster federation processing 2M+ ModSecurity logs daily with 95% storage savings.

• Created AI-powered diagnostic automation using Claude Code CLI with custom MCP tools achieving 85% MTTR reduction and 60-80% automation of routine operational diagnostics through template-driven Slack bot investigations with professional PDF report generation.

• Designed distributed data curation platform for cryptocurrency markets handling 4.1M+ unique trading pairs with sub-10ms change detection latency, eliminating $120k-$240k annual S3 API costs while filtering 70%+ scam tokens through extensible middleware architecture adopted by 27+ internal services.

• Implemented comprehensive infrastructure as code managing multiple AWS accounts plus Azure resources with GitOps workflows, cross-account IAM, and bare-metal Talos Kubernetes clusters featuring full-disk LUKS encryption and custom Key Management System integration.

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

• Automated FedRamp compliance processes for Amazon Global Accelerator enabling Federal government customers through continuous security validation and 50% faster authorization workflows while maintaining zero compliance violations.

• Developed Kubernetes Operators for AWS WAF providing declarative security policy management with 95% reduction in deployment time and 100% Kubernetes-based management of AWS resources through custom

resource definitions and GitOps integration.

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

• Built self-bootstrapping one-click Kubernetes platform supporting SaaS, cloud-premises, on-premises, and air-gapped installations creating itself ex nihilo with PTT stack, metrics, visibility, and auto-unsealing CA described by customers as 'flawless' and 'easiest, highest quality software installation we have ever seen'.

• Architected voice bot framework enabling automated voice interactions on Orion PTT platform supporting 100+ customer use cases including COVID epidemiological contact tracing system for Massachusetts Bay Transit Authority with real-time location tracking and privacy-preserving design.

• Solved thundering herd scaling problem by migrating from AWS Application Load Balancers to Network Load Balancers with Layer 7 switching moved to Kubernetes ingress controllers, eliminating service disruptions from fleet-wide device restart traffic spikes.

Scribd | *Principal DevSecOps Engineer* | 2018-2020

• Founded and led Scribd's first Security Team establishing security practices, tooling, and culture for rapidly scaling platform serving millions of users globally with zero major security incidents and transformation to security-first organization.

• Built scalable SIEM system from scratch processing petabytes of log data for worldwide CDN footprint with self-service dashboard enabling company-wide visibility, real-time threat detection, and user behavior analysis discovering abuse patterns and bot activity.

• Created YAML interface for Hashicorp Vault simplifying secrets management for 100+ engineers through proper separation of duties where developers define secrets structure but cannot access production values, released as open source with community adoption.

• Designed Kubernetes clusters with Fastly CDN integration for global JavaScript asset management achieving 99% cache hit rates and 50% bandwidth cost reduction through automated cache expiration tracking and multi-region optimization.

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

• Built Identity and Access System for Algorithms & Analytics department providing seamless authentication across all resources, instances, and containers maintaining 100% uptime during company SSO breach when vendor systems failed.

• Implemented AWS IAM Role/STS credentials on developer laptops through AWS metadata service manipulation enabling passwordless authentication with zero code changes to Amazon SDK and eliminating credential leaks across 100+ developers.

Apple | *Lead DevOps Engineer* | 2015-2017

• Led Apple Pay DevOps team achieving historic first in Apple's history by obtaining full hardware ownership breaking through traditional organizational barriers and establishing precedent for modern administration and audit patterns.

• Designed first automated test-driven CI/CD system for Apple Pay with dynamic environment creation per pull request, complete isolation, full testing, and automatic cleanup revolutionizing deployment practices with zero deployment-related outages.

• Architected command and control system managing 30,000 servers worldwide orchestrating flawless Apple Pay China launch with zero downtime during critical 2015-2017 period demonstrating global scale reliability.

• Created private OpenStack cloud from unused hardware achieving 100x acceleration of build and test cycles while implementing security-first architecture so robust that Apple's security teams required standing down protections to complete penetration testing.

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

• Developed and managed Web Application Firewalls for entire U.S. Bank as team of two with organization trusting 'WAF policy for all of US Bank boiled down to: Nik says so' backed by management maintaining zero breaches across diverse applications and PCI DSS compliance.

• Built Encryption Key Management and Distribution System saving over $1M compared to vendor bids, still in production use today, supporting multiple countries with one-button SSL certificate deployment and secure key distribution replacing failed commercial PKI.

• Designed Credit Card PAN Encryption and Tokenization System for merchant acquiring protecting millions of transactions with role-based access controls, scalable highly available architecture, and PCI DSS compliance with zero PAN data breaches.

Skills

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

Cloud Platforms: AWS, GCP, Azure, OpenStack

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

Databases: PostgreSQL, MySQL, Oracle, Redis, ClickHouse, TimescaleDB, DynamoDB, GraphQL

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

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

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

Open Source Projects

Dynamic Binary Toolkit (DBT) - Self-updating signed binary distribution system building, testing, publishing, and updating itself in flight. Listed in awesome-go.

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

Go Mason - Clean-room CI testing tool for local development enabling testing of CI pipelines on laptops before pushing. Listed in awesome-go.

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

Hasura Operator - Kubernetes Operator for declaratively managing Hasura GraphQL instances extending K8s API for GraphQL infrastructure.

Kubectl SSH OIDC - kubectl plugin providing passwordless authentication using SSH keys with OAuth2 Token Exchange flow eliminating browser-based authentication.

Dex SSH Connector - SSH authentication connector for Dex identity provider implementing RFC 8693 with SSH-signed JWTs for enterprise Kubernetes authentication.