

Viam inveniam, aut faciam.

(I will find a way, or I will make one)

Professional History

Terrace: 2023 - Director of Cloud Infrastructure and Security

- Architected a multi-cloud, hybrid Kubernetes platform spanning various cloud providers and on-premises bare-metal systems. Migrated from GCP to AWS and On Premesis.
- Protected company intellectual property during a critical turnover period, swiftly restoring systems within hours.
- Drove Observability initiatives in Engineering Management by designing scalable monitoring systems, resulting in a 100x reduction in monitoring costs.
- Elevated to CIO and Head of Engineering, overseeing the global team in re-architecting Terrace's core product for DeFi, CeFi, and Cryptocurrency trading, integrating Fintech, Blockchain, Observability, and Security on Kubernetes.
- Automated Security and Deployment incident response with AI bots that work through Slack to diagnose and resolve WAF blockages, Vulnerability Reports, and Deployment issues in Kubernetes, Nginx, and ModSecurity.
- Launched Terrace's flagship product in less than 3 months from assumption of new duties by re-architecting the entire platform from the database to the front-end to meet business requirements around scale and latency. Brought latencies of > 600ms down to in some cases *microseconds* and scaled the data handling capabilities of the product by over 100x.

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

- Automated processes to secure and maintain Amazon Global Accelerator systems for FedRamp compliance.
- Provided internal Security Consulting for Amazon Global Accelerator, holding certifications as AWS Solutions Architect and Hashicorp Vault Professional.
- Developed Kubernetes Operators for Amazon Web Application Firewall implementation.

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

- Led a team managing Infrastructure/DevOps/SRE responsibilities on AWS, Azure, and On-Prem systems.
- Designed and implemented a Kubernetes platform enabling secure voice communications in cloud, on-prem, and air-gapped installations.
- Developed contract tracing systems for public transportation during Covid outbreak.
- Built a Framework for Voice Bots using Orion Platform on Kubernetes.
- Established engineering standards and conducted technology training for all employees.

Scribd: 2018 - 2020 Principal DevSecOps Engineer, Sr. DevOps/SRE

- Founded and led Scribd's Security Team
- Developed a scalable SIEM system to monitor and secure Scribd's global CDN for customer data protection
- Implemented a Web Application Firewall to safeguard Scribd's services and network
- Created an easy-to-use YAML interface on Hashicorp Vault 'Managed Secrets' for efficient management of sensitive information, now an Open Source project
- Designed Kubernetes clusters and native tooling that connected application workloads to Fastly CDN caches for tracking cache expiration of precompiled javascript code at a global scale
- Established an Identity and Access System with PKI to defend internal networks and Kubernetes clusters from unauthorized access

Stitch Fix: 2017 - 2017 Sr. DevOps/SRE

- Developed an Identity and Access System for the Algorithms & Analytics department to access all resources in the stack securely and reliably.

- Created an AWS IAM Role based development allowing seamless code execution between local machines and EC2 nodes.
- Built a cloud-based system for interactive containers, enabling Data Scientists to run code near their data seamlessly as if it were local.

Apple: 2015 - 2017 Lead DevOps Engineer

- Led Apple Pay DevOps team in implementing a modern administration and audit pattern, fostering collaboration between Security, Audit, and Engineering which led to full hardware ownership by Apple Pay. This was a first in Apple's history.
- Designed and implemented the first automated test-driven CI/CD system for Apple Pay at Apple.
- Architected the command and control architecture for global Apple Pay launch in China, managing 30k servers worldwide.
- Created a private OpenStack cloud to accelerate Apple Pay's build and test cycle by 100x, overcoming infrastructure limitations and cloud usage restrictions.
- Developed a container-based system enabling end-to-end integration testing of Apple Pay platform on any laptop, a pioneering achievement within Apple.

U.S. Bank: 2007 - 2014 Security Architect, Application Architect, Sr. Systems Engineer / SRE

- Worked as a Security Architect for Corporate Payment Systems, providing consultation on Threat Modeling, Penetration Testing, and Security Remediation.
- Solely developed and managed Web Application Firewalls (WAF) for the entire U.S. Bank over 5 years while concurrently serving as Security Architect.
- Provided consultancy and training on Automated Testing, including developing training materials and teaching classes through the organization's internal development platform.
- Managed Payment Systems' reliability engineering (SRE), ensuring PCI DSS compliance, and implemented Observability, Monitoring, and Alerting systems. Established Encryption and Tokenization mechanisms for PAN data in Merchant Acquiring systems.
- Developed an Encryption Key management and distribution service utilized by numerous users across various countries. It's still in use today, and saved over \$1m based on competing products available at the time.
- Engineered systems for Code Signing, Continuous Integration, and Artifact Storage.

Skills

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

Frameworks: Spring, Antlr, Gherkin, Cucumber, PyTest, Test::More, Go Test, Godogs, Selenium

Disciplines: Agile, Test Driven Development, Behavior Driven Development, Rugged, SOLID

Compute / Virtualization: Bare Metal, VmWare/ESX/ESXi, Qemu, KVM, OpenStack, EC2, GCP, Azure, Virtual-Box, XHyve, Vagrant, Libvirt, Proxmox

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

Operating Systems: Linux, Windows, MacOS, Unix, Talos

Web Servers/ Load Balancers: Nginx, Apache, Envoy, HAProxy

Containerization: Kubernetes, ECS, Docker, Containerd

Security: OpenSSL, OpenSSH, Luna HSMs, OpenVPN, SIEM, Kerberos, PKCS, IPSec

Firewalls: IPTables, PF, AWS WAF, Fastly WAF, ModSecurity

Databases: Postgresql, Mysql, Oracle, Redis, Clickhouse, TimescaleDB, DynamoDB, Hasura, GraphQL, Atlas, S3, MinIO

Configuration Management: Puppet, Chef, Ansible, Terraform, Pulumi, CloudFormation

Continuous Integration/ Testing: Jenkins, GitHub Actions, TeamCity, Travis, CircleCI, FluxCD, ArgoCD, Tekton

Version Control: Git, Subversion, Mercurial, GitHub, GitLab

Hyperscalers/Compute Cloud: AWS, Azure, GCP, OpenStack

Access and Identity: LDAP, OIDC, SAML, FusionAuth, JWT

Secrets Management: Hashicorp Vault, AWS Secrets Manager, AWS Systems Manager Parameter Store

Observability: Prometheus, AlertManager, Grafana, Loki, Promtail, Thanos, Fluentd, Fluent-bit, ElasticBeats, ElasticSearch, Artifactory, Logstash, Kibana, CloudWatch, Splunk, DataDog

Networking / Service Meshes: TCP/IP, Routers, Gateways, NAT, DNS, Forward Proxies, Reverse Proxies, Istio, Consul, PXE, TFTP

CDNs: Fastly, Cloudfront

Compliance: FedRamp, SOC2, PCI, SOX, HIPAA, CIS, CVE, Inspec

Messaging: Kafka, Elasticache, SNS, RabbitMQ, MQTT, Slack

Blockchain / Crypto: Ethereum, Solana

AI Agents: Claude, claude-code, GPT

Profiles

GitHub <https://github.com/nikogura>

Linked In <https://www.linkedin.com/in/nikogura/>

Web Site <https://nikogura.com>

Open Source Projects

- [Dynamic Binary Toolkit](#) A delivery system for self-updating, signed tools. Listed in [Awesome-Go](#).
- [Go Mason](#) A tool for doing clean-room CI testing locally. Listed in [Awesome-Go](#)
- [Managed Secrets](#) A YAML interface on Hashicorp Vault that allows teams to manage their secrets, without being to access them in production.
- [K8S Cluster Manager](#) A command line tool for managing bare-metal and VM K8s Nodes on Talos Linux.
- [Hasura Operator](#) A Kubernetes Operator for declaratively managing Hasura instances
- [NamedReturns](#) A Linter for golang that enforces named returns for self documenting code.
- [KubectI-SSH-OIDC](#) A kubectI plugin that provides passwordless authentication using SSH keys and [Dex IDP](#).
- [geoip-cache-proxy](#) A transparent caching proxy for GeoIP data from MaxMind.