Résumé for Kirk Strauser

632 Pacific Avenue, Alameda, CA 94501 • 510-496-9333 • kirk@strauser.com
https://www.linkedin.com/in/kirk-strauser-2638b/

Objective

Lead role in a security engineering team at a scrappy company, responsible for solving complex, vaguely specified problems in ways that make both compliance teams and engineering teams happy.

Summary

I've done everything that needed to be done for 20+ years at startups through medium-sized companies. I'm a hands-on software and infrastructure engineer, and I've built and run security programs to meet strict enterprise customer, regulatory, and compliance framework requirements. I do what it takes to make my employer secure and profitable.

Experience

Languages: Python, SQL, shell scripting, Rust, JavaScript / TypeScript
Platform: Linux, Docker, Terraform, GitHub, Jenkins, CircleCI, Slack API, Ansible, Packer, Aviatrix
App development: Flask, Django, PostgreSQL, broad experience with the Python ecosystem
AWS: EC2, ECS, S3, ELB, VPC, IAM, SSO, KMS, Security Hub, Config, Inspector, Route 53, CloudWatch, Lambda, RDS, WAF, Aurora, API Gateway, SES, Certificate Manager, Transfer Gateway
Security: Jamf, Okta, Netskope, Endpoint Protector, Burp Suite, Hyperproof, pen testing project management, HackerOne
Regulatory frameworks: HIPAA, SOC 2, HITRUST

Employment

Coda / Grammarly

Staff Security Engineer • October 2023 — present • San Francisco, CA

- Wrote automation and auditing tooling
- Reviewed code and designs
- Used Terraform to deploy infrastructure changes to achieve a 100% CIS AWS Foundations Benchmark score
- Met with customers in sales calls to help close deals

- Managed annual pentesting
- Responded to customers' security questionnaires
- Advised Legal on security issues
- Ran the HackerOne bug bounty program.

After Grammarly acquired Coda, worked with their Platform Security team to integrate Coda's security program with Grammarly's:

- Deployed Sumo Logic logging, Semgrep SAST, and Wiz auditing
- Documented Coda's practices to identify and prioritize gaps for remediation

Amino Health

Lead Security Architect / CISO • September 2015 — September 2023 • San Francisco, CA

Reported to the CTO and CISO to deliver cross-department compliance projects on time and on budget.

- Completed enterprise customer-driven technical audits helping land Amino's first large customers with over $20M annual revenue.
- Created reporting and technical controls for successful SOC 2 certification, enabling shorter sales cycles.
- Planned and guided engineering-wide projects to achieve HITRUST certification on budget and on time.
- Helped interview, hire, and train an IT department.
- Designed and implemented Amino's most sensitive technical backend and cloud systems storing HIPAA-covered personal and healthcare data, with designed-in security controls that passed rigorous audits.
- Spearheaded and completed privacy- and security-sensitive initiatives, becoming a subject matter expert and advisor in related fields.

Earlier career

Coverity • Architect, R&D DevOps • August 2014 — September 2015 • San Francisco, CA

- Operated, maintained, and upgraded Coverity's complex build system to create deployment packages for multiple OS and hardware combinations.
- Reduced unplanned developer tooling downtime and manual intervention, resulting in increased developer productivity and less frustration.

Crittercism • Senior Software Engineer • February 2014 — August 2014 • San Francisco, CA

- Redesigned a large, monolithic application into a distributable service-oriented architecture.

Kwarter • Platform Engineer • July 2013 — February 2012 • San Francisco, CA

- Used Python, Linux, AWS, and NoSQL databases (including MongoDB, Couchbase, Cassandra, and Redis) to build APIs capable of sustaining hundreds of thousands of requests per second.

Projects

The Policy Wonk (https://github.com/aminohealth/wonk)
Wonk is a tool for combining a set of AWS policy files into smaller compiled policy sets.
- Designed, wrote, and published the tool as an open-source project.

Veilid (https://veilid.com/)
Veilid is an open-source, peer-to-peer, mobile-first, networked application framework.
- Wrote an app to demonstrate the platform's functionality
- Demonstrated and explained the app's functionality at the DEF CON 31 conference
- Interviewed by Washington Post about the project (https://www.washingtonpost.com/technology/2023/08/02/encryption-dead-cow-cult-apps-def-con/)

Education

Missouri State University, Springfield, MO — B.S., Computer Science / Physics Minor

Volunteering and Hobbies

- Member of Missouri State University's Computer Science Department Advisory Board.
- Amateur radio operator, "extra" class license KM6OCD.
- Wrote a bulletin board system for the Meshtastic radio mesh networking system.

Patents

US20160196398A1, "Data analysis mechanism for generating statistics, reports and measurements for healthcare decisions"