

# ERIK KRISTENSEN

Director of Engineering & Hands-on Platform Architect · Cloud Infrastructure, Cybersecurity, Open Source

Remote, US · erik@ekristen.dev · linkedin.com/in/erikkristensen · github.com/ekristen

## SUMMARY

I build the platforms other people work inside, and I lead the teams that run them. Across a career that began in Air Force network defense and ran through mobile security startups to the SANS Institute, the throughline has been the same: take infrastructure that is fragile, manual, or built once by hand, and turn it into something declarative, reproducible, and disposable — whether that is a rack of physical phones, a cyber range that exists only for the length of a class, or a video pipeline nobody had touched in fifteen years.

Today I direct the engineering organization behind every student-facing platform at SANS. I still own the architecture of the cyber range platform I designed and I ship code on it every week, because I think the best technical leaders stay close enough to the work to be wrong about it in public. Outside work I maintain open source tooling that other teams depend on daily, and I treat stewardship of other people's projects with the same care as my own.

## EXPERIENCE

**Director of Engineering & Research Operations Center** — SANS Institute Jun 2025 – Present

- Lead a 20+ person engineering organization across five teams — curriculum engineering, courseware, on-demand learning, cyber ranges, and workforce development — covering all student-facing technology at SANS, after a 2025 scope expansion that consolidated four previously separate groups under one technical vision and grew the organization from ~9 engineers.
- Modernized a 15-year-old video production and delivery pipeline serving 138 course versions and 10,555 active students, taking it from discovery to organization-wide buy-in in 30 days and to full cutover in nine months.
- Replaced a CPU-bound, seven-pass lossy render chain with GPU encoding to a single high-bitrate master, moved delivery to Cloudflare Stream and transport off Dropbox — cutting render turnaround from ~24 hours to ~70 minutes and ~\$235K/year in infrastructure and vendor spend.

**Director, SANS Research and Operations Center** — SANS Institute Jun 2023 – Jun 2025

- Led SROC, an organization of ~9 engineers responsible for cyber range research, delivery, and operations serving 50,000+ students per year across hundreds of courses.
- Ran range delivery at that volume with a 95%+ build success rate, with residual cloud-provider failures absorbed by automatic retry rather than operator intervention.

**Chief Engineer & Cloud Architect, Ranges** — SANS Institute Feb 2021 – Jun 2023

- Architected and built the multi-cloud platform that provisions, monitors, and retires realistic cyber training environments on demand across AWS, Azure, and GCP — replacing manually built, non-reproducible environments behind a single shared network entry point with a reproducible, per-environment-isolated system.
- Authored the Terraform-based range specification that course authors build against, so content teams ship complex multi-host environments without touching platform internals.
- Designed the observability layer: every environment self-monitors and self-alerts, federating metrics over mutual TLS into a single live and historical view across every environment, with automated remediation on environment-local alerts.
- Owned the cloud account lifecycle strategy that lets curriculum grant learners full administrative access to real cloud accounts, with deterministic reclamation and automated sanitization between uses.

**Director of DevOps** — NowSecure (formerly viaForensics) Dec 2013 – Feb 2021

- Led DevOps for a mobile application security company: hundreds of servers, mobile devices, and IoT devices across cloud, on-premise, and hybrid environments, at hundreds of deployments per week — on LXC before Docker existed and on Kubernetes years ahead of mainstream adoption.
- Led design and build of a Kubernetes-orchestrated mobile device lab scaling to 160+ physical Android and iOS devices: each 48U rack ran as its own cluster of PoE-powered single-board computers, one per handset, sustaining ~2 automated app analyses per device per hour.
- Replaced a prior ~100-device fleet multiplexed 4–8 handsets per host with a 1:1 device-to-node architecture, eliminating the contention and shared-failure modes that had made it unreliable; the platform has since doubled in footprint on the same design.

- Planned, architected, and implemented Fixmo's cloud systems for global 24/7 availability, and drove the architecture that moved the flagship mobile security product to a cloud-native deployment with linear horizontal scaling.

**Computer Network Defense / Boundary Protection** — United States Air Force

May 2004 – Nov 2011

- Seven and a half years across forensics, intrusion detection, firewalls, and proxies.
- Consolidated half of the Air Force's boundary protection under a single cohesive managed policy, writing the tooling that merged multiple proxy and firewall configurations into one.
- Led the technical implementation of mobile security for smart devices during the final two and a half years of service.

**OPEN SOURCE**

---

**aws-nuke** · Lead maintainer · 1,400 stars · 174 contributors · 737k+ downloads

The standard tool for removing every resource from an AWS account. Began contributing upstream for range teardown, forked to add resource types, then rewrote the core around libnuke for v3. When the original maintainers offered to hand it over, proposed they archive and redirect instead so they kept their history and credit.

**libnuke** · Creator · 95%+ test coverage

Provider-agnostic Go library for discovering, dependency-ordering, and deleting cloud resources — the shared core that makes a three-cloud suite sustainable for one maintainer.

**azure-nuke / gcp-nuke** · Creator · 79k+ combined downloads

Tenant-level Azure and project-level GCP teardown tools built on the shared libnuke core.

**SIFT Workstation** · Maintainer since 2013 · 500,000+ downloads

The premier Linux digital forensics and incident response distribution, used across DFIR training and practice.

**cast** · Creator · 139 stars · 84k+ downloads

Go CLI that installs SaltStack-defined Linux distributions in one command; the install path for SIFT and REMnux.

**distillery** · Creator · 26k+ downloads

Binary installer that pulls directly from GitHub, GitLab, and Codeberg releases, verifying checksums and signatures — no package manager, no central metadata.

**Atlas** · Creator · production across hundreds of clusters

Kubernetes operators that build a self-configuring Envoy mutual-TLS mesh for distributed Thanos across clusters.

**terraform-provider-pgp** · Creator · 1.1M+ Terraform Registry downloads

Terraform provider for PGP key generation and encryption.

300+ public repositories · GitHub Arctic Code Vault Contributor

**TECHNICAL SKILLS**

---

|                                  |                                                                                                                    |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Languages</b>                 | Go, Python, TypeScript/JavaScript, PHP, Bash                                                                       |
| <b>Infrastructure</b>            | Kubernetes (operators, CRDs), Docker, LXC, Terraform, Nomad, Rancher, GitOps/Flux, PXE and bare-metal provisioning |
| <b>Cloud</b>                     | AWS (EC2, IAM, S3, RDS, Lambda), Azure, GCP, Cloudflare (Workers, R2, D1, Stream)                                  |
| <b>Observability</b>             | Prometheus, Thanos, Alertmanager, Grafana, Splunk, Consul                                                          |
| <b>Security &amp; Networking</b> | Envoy, mutual TLS and PKI, OIDC/IRSA, DNS, load balancing, PoE, boundary protection, digital forensics             |
| <b>Data &amp; Messaging</b>      | PostgreSQL, MySQL, SQLite/libSQL, Redis, RabbitMQ, MQTT                                                            |
| <b>Delivery</b>                  | GitHub Actions, GitLab CI/CD, GoReleaser, semantic-release, Renovate                                               |

**EDUCATION & CERTIFICATIONS**

---

**B.S. Computer Science** — University of Arkansas Grantham

2010

**A.S. Information Technology** — Community College of the Air Force

2007

**GIAC Certified Forensic Analyst (GCFA)**