Derek Arnold

Engineering Manager — Platform, Infrastructure & Observability

Saint Paul, Minnesota | recruitderek@minnesotazone.com | github.com/ransomvik | U.S. Citizen | Open to fully-remote roles

SUMMARY

Engineering manager leading platform, infrastructure, and observability teams that operate petabyte-scale telemetry across multi-cloud environments. I own delivery, reliability, cost, and team growth — with a track record of cutting seven-figure infrastructure spend, shipping internal tooling engineers actually use, and holding 100% team retention. Twenty years across platform engineering, site reliability, and security operations.

CORE SKILLS

Leadership: Engineering management, team building, hiring, retention, career development, incident command, roadmap and delivery, stakeholder communication

Observability & SIEM: Prometheus, Grafana, Thanos, Splunk, Falcon LogScale, Next-Gen SIEM, Cribl, PagerDuty

Platform & Infrastructure: AWS, AWS GovCloud, Kubernetes, Docker, Terraform, Ansible, Jenkins, Linux, CI/CD, multi-cloud

Automation & AI: Python, Bash, LLM-assisted operations, Claude API/CLI, agentic tooling

EXPERIENCE

CrowdStrike — Engineering Manager, Platform Operations

October 2022 – Present | Remote

- Lead a 9-engineer team operating and scaling Falcon LogScale / Next-Gen SIEM clusters that process petabytes of security telemetry daily across multi-cloud infrastructure.
- Delivered approximately $1M/year in infrastructure cost savings through a log-storage waste-analysis initiative; roadmap extends impact to ~$1.6M/year.
- Shipped HawkEye, an internal self-service operations bot, 23 days ahead of schedule — 1,100+ invocations in 90 days, eliminating an estimated 40–50 engineer-hours per sprint of manual work.
- Drove 100% AI-tool adoption across the team; authored the team AI best-practices playbook and led monthly AI/ML knowledge-sharing.
- Directed a FIPS-compliant Ubuntu upgrade across 400+ production hosts with zero customer-impacting incidents; automated the 21-day sprint cycle and reduced alert noise by 400+ incidents/month.
- Supported CrowdStrike's 2025 MITRE ATT&CK Enterprise Evaluation (maintained evaluation clusters, fielded auditor questions); CrowdStrike delivered 100% detection and 100% protection with no false positives.
- Achieved 100% one-year team retention and 100% "I trust my manager" on engagement surveys.

CrowdStrike — Senior Site Reliability Engineer, Platform Operations

October 2019 – October 2022 | Remote

- Operated large-scale Splunk systems processing approximately 3 petabytes per day, growing 80% year over year.
- Improved reliability across a 20,000-node Linux fleet using Python-based tooling and automation.
- Built observability with Grafana, Prometheus, and Thanos that measurably reduced incident-response time.

Alchemy Security — Director of Engineering

April 2018 – October 2019

- Launched Alchemy Defense Cloud (managed Splunk on AWS) across 10 customer environments.

- Stood up managed monitoring and vulnerability scanning supporting a 20-person Security Operations Center (SOC).
- Authored 15 Ansible playbooks to make operations repeatable and onboarding fast.

Optiv Security — Principal Consultant
September 2014 – April 2018

- Delivered SIEM and security-operations consulting to 500+ clients.
- Mentored 10 consultants and delivered 30 trainings; earned two promotions while contributing to practice development.

Abbott Laboratories — Senior Security Engineer
September 2008 – September 2014

- Enterprise security operations and intrusion response for a global medical-device manufacturer.

EDUCATION

Bachelor of Science, Computer Engineering — Milwaukee School of Engineering

CERTIFICATIONS & CLEARANCES

CISSP; AWS Certified Solutions Architect – Associate; Splunk Certified Architect; Splunk Certified Consultant II (prior). Clearances: CJIS; AWS GovCloud (US).