Derek Arnold

Senior Platform Engineer | AWS | Observability | Security Infrastructure | Python | Agentic AI Automation

Saint Paul, Minnesota • recruitderek@minnesotazone.com • 763-300-0144 • resume.minnesotazone.com • US Citizen • Fully remote U.S.-based IC roles only

SUMMARY

Senior individual-contributor platform engineer with deep experience across AWS, observability, security infrastructure, and Python automation. Operate and improve large-scale telemetry and reliability systems spanning 20,000 Linux hosts and approximately 3 petabytes per day of data, growing 80% year over year. Known for building internal tools that reduce toil, improve reliability, and accelerate engineering workflows, including Claude-powered alert analysis, triage automation, structured summaries, and workflow tooling supporting 3 teams and 28 engineers.

3 PB/day	Operate telemetry and observability systems processing approximately 3 petabytes per day, growing 80% year over year.
20,000 Linux hosts	Improve reliability, automation, and monitoring across a 20,000-node Linux fleet in AWS and on-prem environments.
400+ incidents/month	Eliminated PagerDuty noise through Claude-assisted alert analysis, backtesting, and PR-generation workflows.
3,533 -> 38	Reduced one ticket triage pipeline to 38 actionable items with LLM-assisted triage and JQL scoping.
500+ clients / 30 trainings	Delivered consulting, enablement, and mentoring at scale in a firm serving 500+ clients; mentored 10 consultants and delivered 30 trainings.

EXPERIENCE

CrowdStrike | Senior Site Reliability Engineer / Engineering Manager

Oct 2019 - Present

- Operate and improve large-scale Splunk / LogScale telemetry systems processing approximately 3 petabytes per day, growing 80% year over year, across AWS and on-prem infrastructure supporting global threat-hunting workflows.
- Improved reliability, observability, and automation across a 20,000-node Linux fleet by building Python-based internal tooling, monitoring services, and workflow automation.
- Reduced PagerDuty noise by 400+ incidents per month across Thanos / Prometheus and LogScale alerting pipelines by designing Claude-assisted analysis and PR-generation workflows with backtested metrics.
- Built an AI-powered Zoom transcript processor from scratch in about 8 hours that outputs Slack, Google Doc, and Gmail-ready summaries, action items, and leadership coaching signals.

- Cut one triage pipeline from 3,533 tickets to 38 actionable items using JQL scoping and LLM-assisted description analysis, dramatically improving signal-to-noise for engineering follow-up.
- Automated the full 21-day sprint management cycle across 10 phases, removing 2-3 hours of repetitive Jira work per sprint for a 9-person team.
- Supported 3 teams and 28 engineers through internal platform tooling, observability improvements, and workflow automation designed for high-output remote execution.

Alchemy Security | Site Reliability Engineer

Apr 2018 - Oct 2019

- Launched Alchemy Defense Cloud, a managed Splunk service on AWS, and helped plan, build, and operate 10 customer environments.
- Supported a 20-member SOC with managed monitoring, Splunk operations, and Nessus-based vulnerability scanning across financial services, analytics, healthcare, retail, and government clients.
- Created 15 Ansible playbooks that improved repeatability, secure operations, and day-to-day engineering efficiency across customer and internal systems.
- Built and maintained Ansible-based automation used by engineers and developers to manage critical systems securely and consistently.

Optiv Security | Principal Consultant

Sep 2014 - Apr 2018

- Delivered SIEM, threat intelligence, and security operations consulting within a firm serving 500+ clients, contributing technical leadership across Fortune 1000 environments.
- Mentored 10 consultants, delivered 30 trainings, and developed reusable enablement content that improved onboarding and skill growth across the Splunk consulting practice.
- Earned two promotions from Consultant to Senior Consultant to Principal Consultant while contributing client delivery, labs, onboarding materials, and practice development.
- Created reusable technical content and training assets that scaled consulting delivery.

Abbott Laboratories | Senior Security Engineer

Sep 2008 - Sep 2014

- Supported enterprise security operations, intrusion response, vulnerability management, and reporting for a global medical device manufacturer.
- Led technical work across access control, surveillance, and security operations spanning global business and manufacturing environments.

SKILLS

Cloud: AWS (S3, EC2, Lambda, VPC, IAM, Kinesis)

Programming: Python (requests, urllib3, argparse, csv, os, re, json), Bash

Observability: Splunk, LogScale / Humio, Prometheus, Thanos, Grafana, PagerDuty

Automation: Claude API / CLI, internal tooling, workflow automation, Jira / Slack / Bitbucket integrations

Infrastructure: Linux, Ansible, Chef, Terraform, Jenkins, Cribl, cloud security services, incident response

Keywords: Platform Engineering, Site Reliability Engineering (SRE), Cloud Infrastructure, Security Infrastructure, Observability, Infrastructure Automation, Internal Tools, AI Automation, LLM Applications

EDUCATION

B.S., Computer Engineering - Milwaukee School of Engineering

CERTIFICATIONS

AWS Certified Solutions Architect - Associate | CISSP (Expired) | Splunk Certified Architect (Expired) | Splunk Certified Consultant II (Expired)