NICHOLAS FERGUSON

727.266.8813 | nick@atlascrew.dev | github.com/NickCrew | linkedin.com/in/ncferguson

PROFILE

Platform engineer who treats infrastructure as a product. Delivered four production platforms in 11 months post-acquisition—an edge protection sensor with sub-millisecond detection latency (99.8% OWASP coverage), a fleet intelligence control plane, an internal security tooling suite, and a Linux endpoint agent for the company's AI Firewall product. Previously built an internal developer platform shipping $50M/year in software across 6 target platforms. Track record of identifying gaps, choosing the right technology for the constraint, and driving platforms from roadmap to production.

CORE COMPETENCIES

Languages: Python, C# / .NET, SQL, Bash, C++, PowerShell, TypeScript, Rust

Infrastructure: AWS (production, Serverless), Linux (RHEL, Ubuntu, KVM, systemd, SELinux), Kubernetes/EKS, Docker, VMware, Terraform, Ansible, Helm, Flux/Kustomize

Networking: TCP/IP, HTTP/S, TLS/SSL, DNS, routing/switching, load balancing, Nginx, Pingora

Data & Messaging: PostgreSQL, SQL Server, MongoDB, ClickHouse, Kafka (AWS MSK), WebSocket, REST APIs

Observability: Grafana, Prometheus, InfluxDB, ELK, Loki, PagerDuty

CI/CD: GitHub Actions, GoCD, GitLab CI/CD, Jenkins

PROFESSIONAL EXPERIENCE

A10 Networks *(acquired ThreatX)*

Senior Platform Engineer — Feb 2025 – Present

- Architected ThreatX Synapse, rebuilding the legacy SaaS-dependent WAF as a standalone edge protection sensor—moving detection and blocking inline at the edge, cutting latency 4,400x to sub-millisecond, and opening new customer classes (air-gapped, on-prem, hybrid). Sensitive data scanning runs concurrently with HTTP processing at zero added latency. Blocking uses campaign correlation and statistical anomaly detection, not just static rules. 99.8% OWASP CRS coverage.
- Identified a gap in API authorization observability—every competitor detects authorization attacks, but none provide continuous visibility into which endpoints enforce auth and how patterns change over time. Built the authorization coverage map MVP that auto-discovers endpoint auth posture from live traffic with zero configuration. Designed the roadmap for on-device behavioral learning and anomaly detection at the edge.
- Designed Signal Horizon, the central management platform for the Synapse sensor fleet—security operations, fleet management, and cross-deployment threat intelligence. Built for both SaaS and on-premise delivery, enabling the product to serve cloud-managed and air-gapped customers from the same platform. Multi-tenant intelligence sharing (HMAC-SHA256) allows cross-customer threat correlation without exposing tenant data.
- Created a real-time demo platform for sales engineering—live POC deployments couldn't guarantee advanced attacks would occur on-demand. Sales engineers could tailor attack scenarios per customer vertical, store blueprints in a shared catalog, and spin up configured environments with one click.
- Delivered an automated performance and security validation platform—auto-provisioned AWS infrastructure, industry-focused test suites (healthcare, finance), compliance framework support, and a visual test designer. Key enabler for the SaaS-to-on-prem transition: customers could self-validate without SOC involvement, opening a new class of on-prem customers who preferred self-support over vendor dependency.
- Designed the cross-platform endpoint agent architecture for the company's AI Firewall product—five platforms (Linux, Windows, macOS, iOS, Android)—and built the Linux agent (eBPF, Rust) as the production proof of concept. Authored v1 and v2 platform roadmaps. The endpoint agent unlocked the enterprise segment by maintaining protection without requiring a constant VPN connection.
- Established AI-augmented development methodology for the platform team—a multi-LLM workflow gating changes behind automated tests, linters, and multi-perspective analysis (security, performance, code quality). Includes behavioral test gap analysis that identifies missing or insufficient test scenarios based on expected system behavior, not just code coverage. Delivered four production platforms and an endpoint agent in 11 months.

ThreatX *(acquired by A10 Networks, Feb 2025)*

Senior Platform Engineer — Jan 2022 – Feb 2025

- Identified operational gaps in customer onboarding and sensor management—scattered scripts with manual steps frustrating both engineering and SOC. Built a unified CLI with a hot-reloading plugin architecture, cutting onboarding time and enabling self-service operations. Mentored SOC engineers contributing to the platform and eventually handed off full ownership. This led to my role as technical advisor for a new SRE team in the SOC that took over sensor development entirely.
- Rearchitected sensor fleet infrastructure after SOC platform work exposed systemic over-provisioning—cutting AWS spend ~50% (~$60K/mo savings). Consolidated per-customer VPCs into shared infrastructure with Fargate clusters and redesigned scaling from CPU-based to connection-based after identifying the fleet was scaling on the wrong metric.

- Stabilized the platform's critical failure point—database saturation under production load—by deploying Kafka (AWS MSK) with custom connectors as a protective buffer, buying time to architect the Synapse and Signal Horizon replacements. Built the first version of what became ThreatX Labs as a serverless attack traffic platform (Lambda, Step Functions) that modeled kill chains and bot detection scenarios through a chatbot-controlled interface. Featured during Black Hat keynote.
- Enabled a $1M enterprise contract by diagnosing Wayfair's failed sensor onboarding (1 prior failed attempt, 400+ self-hosted sensors). Designed a distributed load testing framework generating 150K+ RPS that revealed conntrack table exhaustion. Tuned the Linux TCP stack, built dynamic conntrack sizing, and developed a scaling policy that improved efficiency 40%.
- Recognized that the company lacked a professional services capability after repeatedly being the engineer who could drop into complex customer environments—coordinating across customer teams, CDN providers, and internal engineering to solve deployment problems no single team could own. Proposed the service model, organized the delivery structure, and personally delivered 4 enterprise engagements including Microsoft-ecosystem integrations, a VMware appliance for a customer that wouldn't run Linux containers, and pre-sales technical translation that opened new market segments.
- Replaced a manual documentation bottleneck—engineers handing Confluence pages to one person for bespoke rewrites—with an automated publishing platform versioning docs alongside every release. Designed the information architecture (Diataxis), built custom AsciiDoc components and generators, and enforced quality through PR checks and pipeline gates. Scaled from a single-author dependency to a system anyone could contribute to with consistent output.

Vispero

Senior Platform / Build Engineer Oct 2018 – Dec 2021

- Position created after meeting leadership at a 30-year-old assistive technology company with no platform engineering function. Walked into NAnt-based Windows-only builds, spinning-disk servers, agents created by copying VMDKs, and builds promoted by moving folders on a CIFS share. Built a cross-platform build engine and DSL in PowerShell 7 with self-bootstrapping buildfiles and semantic versioning—reproducible builds across six target platforms. Used build telemetry to justify a dedicated cluster with local SSDs, dropping CPU WAIT from 1–7 seconds to under 8ms. Recognized with quarterly award (1 of 450+ employees).
- Replaced the release engineering team's role as gatekeeper for all pipeline and build configuration. Gave developers sandbox pipeline environments with release-engineer-provided templates as guardrails, automated the entire release candidate process (branch management, pipeline creation, build promotion, CDN publishing), and built a database-backed artifact repository with dependency mapping and safe CDN cleanup. Built targeted developer tools that eliminated ~1 day/week of engineering toil: pipeline diff/merge for 600+ pipelines, multi-pipeline orchestration, and a static analysis tool that diagnosed build failures with 100% accuracy on compiler errors.
- Reverse-engineered license generation logic out of an ancient C++ application backed by XML flat files and rebuilt it as a database-driven platform with a modern web interface and automated approval workflows—managing $2M+ in active government licenses and reducing turnaround from 3+ days to immediate. Removed a hard dependency on the one person who understood the original code and made the system usable by non-engineers for the first time.
- Led post-acquisition technical integrations contributing to 3 new product lines. Designed hybrid CI/CD architecture (AWS control plane, on-prem ephemeral agents) and migrated dev services to AWS—a decision that isolated the team from a ransomware attack that incapacitated the rest of the organization.

PROJECTS

Apparatus — AI-augmented network security platform for validating detection logic and incident response workflows against realistic attack scenarios. Automates red/blue team exercises with scenario-driven traffic generation, LLM-powered honeypots, and chaos engineering. Built internally; extracted from monorepo for open-source release. TypeScript. github.com/NickCrew/apparatus

Crucible — Attack simulation engine used internally to regression-test Synapse edge sensor detection rules. 119 scenarios covering OWASP Top 10, APT kill chains, HIPAA/PCI compliance boundaries, and nation-state threat models. TypeScript. github.com/NickCrew/crucible

Chimera — Vulnerable application platform for validating WAF/sensor coverage across realistic attack surfaces. 450 endpoints spanning 22 verticals across 13 industry-specific web apps. Includes an OWASP LLM teaching environment with guided hints, vulnerability code diffs, and detection x-ray view. Python Flask and TypeScript. github.com/NickCrew/chimera

EDUCATION

St. Petersburg College, Clearwater, FL — AAS, Computer Information Systems, 2020