Nomi J. Friday

InfoSec Growth Leader, Principal DevSecOps Engineer

friday@nomifriday.com
LinkedIn

EXPERIENCE

FlyLeaf, CTO - Founder

Jan 2024 - current

Founded an AI security company focused on compliance attestation. Flyleaf is a CISO's emotional support animal as they navigate helping ensure their company is ready to achieve FedRAMP certification. Flyleaf builds on the consulting experience we developed at HiNoon and encodes this knowledge in an assistant that learns about the customer, their business and security practices, and then helps them navigate the complex compliance process and ultimately produce a FedRAMP attestation. Flyleaf is in the seed stage right now and is in early beta with select customers.

HiNoon Technical Consulting - Infosec Consultant

Oct 2022 - current
Washington DC and Remote

Serve as a principal security consultant, specializing in compliance and security architecture for various standards including HIPAA, HITRUST, FedRAMP, and SOC2.

- Helped navigate multiple clients through retooling environments to meet the FedRAMP and HITRUST certifications, significantly improving their security posture and compliance readiness.
- Conduct comprehensive security assessments, identifying gaps and implementing technical remediation strategies across diverse client environments.
- Manage consulting teams of 3-4 professionals, overseeing project execution and client satisfaction.
- Co-founded an early stage startup with the owner of HiNoon aimed at automating compliance documentation processes.
- Contributed to business development by participating in client acquisition efforts, RFP responses, and legal negotiations.
- Implemented and optimized security solutions across multiple cloud platforms including AWS, Vultr, and Google Enterprise.
- Designed and implemented hardening strategies for Linux systems, networks, and AMIs, with a focus on FIPS compliance.
- Consulted on and provided design input a zero-trust network system for Amazon, showcasing expertise in advanced security architectures.
- Played a key role in expanding and hardening Hinoon's IT infrastructure, improving internal operations and security.
- Utilized a wide range of technologies including AWS, Azure, Google Enterprise, Linux, FIPS cryptography, NixOS, and Elixir.

ABOUT

My experience includes protecting major US and international security targets, manufacturing operations, and most recently a flying pharmacy. I love going deep on complex security problems and working out business-optimal solutions.

RESEARCH & OBSESSIONS

- FMRI neuroimaging project at Yale to track physiological changes in the brains of advanced meditators

- Built and lived full time in an off grid Yurt as a sustainable tech experiment.

PATENTS

- Systems And Methods For Tamper-Resistant Activity Logging

- Supervisory Control And Data Acquisition

Zipline - Lead Security Mammal

Mar 2020 - Sep 2022 • 2 yr 6 mos

San Francisco, CA and Remote

As ZipLine's first infosec hire, I built a security program from scratch. My programs helped ZipLine achieve FAA Part 135 certification, and lined up compliance with HIPAA and SOC2.

- **Built risk and vulnerability management processes from the ground up.** Built mechanisms to quickly surface and triage risk, automatically scan code for security flaws, identify vulnerabilities in all IT systems, and threat categorization and prioritization.
- **Built incident management processes.** Setup blue team and alerting.
- **Built IT security systems.** Implemented Zero Trust access with Google BeyondCorp, hardware two-factor authentication, SSO, SEIM and alerting, endpoint detection and response (EDR), remote endpoint management. Built a self-service IT acquisition process.
- **Secured AWS infrastructure.** Implemented SSO, converted to AWS Organizations, compartmentalized dev and prod stacks, implemented GuardDuty with ChatOps, built security reviews and controls.
- **Architected and deployed FAA-certified stateless servers for ZipLine airports**
- **Negotiated contracts with both vendors and customers**
- **Managed physical security at ZipLine airports.** Owned security guard contracts, physical barrier systems, and security cameras across multiple countries.
- **Oversaw all information security at Zipline**, including Engineering (Product, Quality, Infrastructure, Data Science), IT, Information Security and Pen Testing.
- **Provided guidance and leadership** for the IT org.
- **Acted as Chief Security Architect** over all engineering.
- **Hired and Managed a team of 6 individuals** plus multiple teams of contractors.
- **Primary tech used**: Google Workspace, AWS, various embedded Linux distros, SentinelOne, JAMF, StandardFusion.

Palantir - SecEng/SRE

2014 - Mar 2020 • 6 yrs

Washington, DC and New York, NY

- **Primary focus was on-prem DevSecOps for national security customers.**

- **Designed and implemented "CSTK"**, a product to rapidly secure on-prem systems for national security use.
- Built and defeated various iterations of tamper evidence for high security requirement customers.
- Supported the infrastructure and developed novel abuse detection strategies for the **National Center for Missing and Exploited Children**.
- **Supported the World Cup in Qatar** by developing novel anomaly detection strategies for OT (aka ICS) systems. This resulted in a few nifty patents.
- **Re-Architected AWS for SOC2 and FedRAMP.**
- **Built systems for automatic ATO generation.** These systems autogenerated all documentation needed to pass government audits.
- **Primary tech used**: AWS, Puppet, Palantir Gotham, Postgres, Oracle, ZFS, Various enterprise Linux distros

Shapeways.com - DevOps Lead

Apr 2013 - Jul 2014 • 1 yrs 4 mos
NY, NY

- **First DevOps engineer at Shapeways, owned all aspects of operations.**
- **Owned datacenter installations in US and NL**
- **Transformed home-grown server farm into modern architecture across multiple geographies.** Negotiated datacenter contracts, built server supply chain, installation, replacement, and retirement mechanisms, and guaranteed HA and DR.
- **Developed defense-in-depth security program for embedded systems**, including segmented, air-gapped networks. Connected security choices to financial outcomes, eliminated sources of regular security incidents.
- **Managed 5 individuals internationally,** both in New York and Eindhoven, NL.
- **Primary tech used**: KVM, ZFS, MySQL, Brocade, Ubuntu, Google Workspace

Samu Consulting / United Nations - Information Security Specialist / SRE

Sep 2009 - Oct 2013 • 4 yrs 2 mos
NY, NY

- **Sole owner/operator of Samu Consulting, with the United Nations as sole customer.**

- **Maintained server fleet for www.un.org** (hardware, software, configuration)
- **Built the primary monitoring system for tech at the UN.** Autogenerated nightly based on our CMDB.
- **Built and secured the tech stack for the RIO+20 conference,** one of the largest UN conferences on the climate crisis. Foiled a planned attack from Anonymous.
- **Helped build the primary United Nations data center in NYC.**
- **Primary tech used**: Apache, nginx, ZFS, puppet, nagios, drupal, SWIFT networks, and a staggering quantity of wireshark.

theLadders.com - Systems Engineer

Oct 2007 - Oct 2009 • 2 yrs 1 mo
NY, NY

- **Modernized home-grown tech stack to fully-virtualized (VMWare) environment in a modern datacenter.** Migrated with 0 downtime.
- **Built systems that could scale to handle a superbowl ad.**
- **Responsible for** email delivery systems, web and app servers, database servers, networking equipment, rack builds and other datacenter hardware.
- **Hardened all systems to NSA spec.**
- **Primary tech used**: VMWare, Tomcat, Ironport, Postfix