

Patrick O'Doherty

TEAM-FOCUSED SECURITY ENGINEERING LEADER

San Francisco, California

✉ hello@patrickod.com | 🏠 www.patrickod.com | 📧 patrickod | 📺 podoherty

Summary

Security Engineer with a decade of experience developing, securing, and orchestrating software at scale. I enjoy employing product engineering and security expertise to solve real-world problems. I have experience in security engineering, infrastructure security, full-stack product engineering, cloud security, and compliance. I am seeking staff+ level engineering roles helping teams work sustainably to deliver durable impact and results.

Work Experience

Oso Security, Inc

San Francisco

ENGINEER, SECURITY LEAD

October 2021 - Present

- Built and operated Oso's security and compliance program. Responsible for SOC2 Type 1 implementation.
- Led Oso's annual third-party penetration test engagement and managed the remediation of findings.
- Designed AWS cloud architecture underlying Oso Cloud production environment. (Pulumi, Github Actions, AWS SSO, AWS IAM, OIDC, ECS Fargate).
- Delivered Yubikey WebAuthN multi-factor for all Oso employees and critical systems including training, documentation, and onboarding material.
- Extended Polar language with dynamic rule type checking and rich query logging to assist users writing correct authorization policies (Rust).
- Created Oso's subscription billing and metering infrastructure (Python, Airflow, Jupyter, AWS MWAA, Stripe).
- Established written rubrics for Oso's engineering hiring process. Conducted dozens of interviews with candidates for engineering roles.
- Authored multiple documentation chapters and blog posts ["Authorization in Microservices"] ["Authorization Patterns in GraphQL"].

Intercom, Inc

San Francisco

SENIOR SECURITY ENGINEER

June 2016 - September 2021

- Built Intercom's critical asset monitoring using streamalert to monitor CloudTrail, GSuite, Okta, and other data sources.
- Created a Google OAuth based SSH certificate authority server and accompanying command line client for convenience certificate issuance. Delivered a company-wide migration to SSO-based, centrally audited, ephemeral remote access using SSH certificates and Duo in 6 weeks.
- Designed Intercom's AWS SSO deployment using Okta, ActiveDirectory, and Duo to provide access to AWS assets and development environments.
- Developed Intercom's "Secure Rendering Strategy", a complimentary system of strong framework defaults, safe rendering APIs, and strict static-analysis designed to eradicate XSS across Intercom. Led the successful deprecation of exploitable DOM sinks across Intercom codebases over 3 months.
- Mentored two teammates in successful security engineering role transitions and promotions within Intercom Security.
- Authored a column encryption ORM integration to provide a default solution for protecting sensitive data in Intercom's relational datastores.
- Developed data access controls based on explicit customer consent gathering to authorize temporary access to sensitive data for support workflows. Achieved a 70% reduction over 3 months in the number of employees with sensitive data access by migrating to just-in-time grants.
- Served as primary Security contact for Intercom's Finance and Legal teams.

Intercom, Inc

San Francisco

GROWTH

April 2013 - June 2016

- Built Intercom's first alternative sign-up flows that allowed customers to bootstrap accounts with imported data (Ruby, Rails, MySQL, AWS SQS).
- Created Intercom's internal billing service that powered subscription billing, feature provisioning, and commission-based sales compensation. Scaled this service through 12 pricing models and nine figures of annual recurring revenue (Ruby, Rails, MySQL, Stripe, AWS SQS, AWS EC2).

PageLever, Inc (acq. 2013)

San Francisco

ENGINEER

May 2012 - April 2013

- One of two building tools for real-time monitoring of ad performance on Facebook for Fortune 500 brands (express.js, MongoDB, PostgreSQL).

Extracurricular experience

Noisebridge Hackerspace

San Francisco, California

TREASURER

2014 - 2018

Served as Treasurer for an educational 501(c)(3) non-profit hackerspace in San Francisco's Mission district. Operated the largest Tor exit node in the USA, handling fundraising, bookkeeping, infrastructure, and legal interactions arising from exit node traffic.