

MO SADEK

Security Leader, AppSec + AI Security

Security programs from zero · Customer-facing security

San Francisco Bay Area · mo@makesecurity.fun · [linkedin.com/in/msadek1](https://www.linkedin.com/in/msadek1) · blog.makesecurity.fun

SUMMARY

Security builder with director-level scope, scaling security functions at a fast-growing company and writing their first playbooks, processes and governance. Hands-on across application and AI security, with experience standing up programs, cross-functional reviews and enterprise trust. Contributes to the field beyond the day job, through industry standards work, published research, open-source tooling and conference speaking.

EXPERIENCE

Alice (formerly ActiveFence) — Technical Director

Jul 2025 – Present · San Francisco Bay Area *AI security company.*

- Technical evangelist for Alice's AI security platform: explain model behavior, risk frameworks and product capabilities to enterprise customers, partners and executives.
- Built the **research-to-publication pipeline** that turns Alice's security research into published work.
- Turn customer feedback and field observations into **working prototypes** that product leadership uses to prioritize features.
- Built **Caterpillar**, an open-source scanner that audits AI agent skills for malicious behavior before install, with LLM-as-a-judge or rule-based modes, offline support and CI/CD gating.
- Co-led the **Rogue Agents (ASI10)** risk area of the **OWASP Top 10 for Agentic Applications (2026)**; represent Alice in OWASP, CoSAI and ISACA.

Roblox — Chief of Staff to the Chief Scientist

Jun 2024 – May 2025

- Established and chaired a companywide **AI Review Board**, reviewing **80+ internal AI initiatives** in the first year against a risk framework covering cost, ethics, performance, infrastructure and age-appropriate user safety.
- Implemented automated intake and triage across information security, data privacy, patent review and IP.
- Evaluated **third-party AI integrations and open-source models** against internal security standards and regulatory requirements, with legal and compliance.

Roblox — Sr. Application Security Engineer (Security Partner)

Sep 2019 – Jun 2024 *Early security hire during the company's growth toward its direct listing.*

- Helped build the application-security practice from the ground up, writing its first playbooks and processes: CI/CD integration, code review and architecture assessments.
- Led and supported **incident response**, building the IR process and leading live incidents across account takeover and session management, insider threat (vendor and employee), and anomalous transactions and fraud.
- Took over the bug-bounty / vulnerability-disclosure program in 2020: response rate from **~60% to 90%**, average time to close from over a month to **~2 weeks**.
- Led early compliance and regulatory conversations ahead of the direct listing, translating requirements into engineering guidance.
- Re-architected RBAC for the trust & safety platform with its engineering team, rationalizing **400+ role IDs** across a **5,000+ person outsourced workforce** toward least privilege.
- Threat modeling and architecture reviews for high-impact systems, including the voice-chat system, region-specific apps for China and Vietnam, an authentication refactor supporting console quick-login and LMS SSO, and a platform-wide safety-system redesign across 30+ components and 7 engineering teams.
- Ran security program management for AI features across 4 teams (15 major features): reviews, testing and mitigation.
- Built parts of and maintained the internal ProdSec scanning platform.

- Set up the open-source security process: automated review for internal projects up for release, a governance framework with Engineering Efficiency, supplemental dependency scanning, and GitHub workflow automation for release compliance.
- Built a security partnership program that made AppSec the front door for engineering; the function grew from 3 to 12 engineers.
- Interviewed across InfoSec through its first ~40 hires, then was first point of contact for onboarding and mentoring new security hires as the org grew from 7 to 90.

Bosch — Security Engineer, Bosch Center for AI Research

Nov 2018 – Aug 2019

Secured Bosch's AI research and enablement environment: led ISO 27001 compliance initiatives, threat-modeled autonomous-driving systems and their software supply chain, built Kubernetes security policies and RBAC for a GPU cluster, and built an early ML-for-SOC threat-detection capability with the SOC team.

Warner Bros. — Lead Application Security Engineer

Apr 2018 – Oct 2018

Restructured the security-assessment program around risk-based architecture reviews and improved third-party risk review.

NBCUniversal — Sr. Application Security Analyst

Sep 2016 – Mar 2018

Led security testing across broadcast and on-air systems, including a PCI compliance program; built a mobile application review program from the ground up.

Cigital (now Synopsys) — Security Consultant

2015 – 2016

OWASP Top 10 vulnerability assessments, remediation guidance and developer security training.

SELECTED SPEAKING

RSAC 2025 · The Official Cybersecurity Summit 2025 · HumanX 2026 · GOSIM Paris 2026 · *The Application Security Podcast*, "Building an AppSec Program from Scratch" (2025)

EDUCATION

B.S., Computer & Information Sciences, SUNY College at Fredonia