Aaron Kawer

San Francisco, CA
aaronkawer@gmail.com | aaronkawer.com
linkedin.com/in/aaronkawer

SUMMARY

Senior Security Engineer with 7+ years across detection engineering, offensive security, and software engineering. Former Microsoft Red Team engineer who combines adversary tradecraft with hands-on detection development across identity, SaaS, cloud, endpoint, collaboration, and infrastructure telemetry. Builds Python and LLM-assisted security tooling, improves detection lifecycle quality, and partners closely with incident response and engineering teams to turn attack paths and investigation findings into durable defensive coverage.

CORE SKILLS

Detection & Response	Detection Engineering, Threat Hunting, Incident Response, Detection Lifecycle Management, Detection-as-Code, Security Analytics, Detection Validation and Tuning
Offensive & Defensive Security	Red Teaming, Purple Teaming, Threat Modeling, Adversary Tradecraft, Attack-Path Analysis, Secure Code Review
AI & Engineering	Python, Security Tooling, LLM and Agentic Workflows, Prompt Engineering, AI-Assisted Security Workflows, Log Analysis, Splunk/SPL
Domains	Identity, SaaS, Cloud, Endpoint, Collaboration, Application, and Enterprise Telemetry

EXPERIENCE

Workday

San Francisco, CA

Senior Security Engineer — May 2026 - Present

- Lead detection engineering initiatives across identity, SaaS, cloud, collaboration, endpoint, and infrastructure telemetry, translating realistic attacker behavior and incident-response requirements into high-signal defensive coverage.
- Drive improvements to detection lifecycle and detection-as-code processes, including review, testing, deployment safety, quality measurement, tuning, and long-term maintainability.
- Establish detection-quality practices that use investigation outcomes, purple-team findings, validation results, and analyst feedback to improve precision, reliability, and operational usefulness.
- Build Python and LLM-assisted security workflows for investigation enrichment, knowledge retrieval, detection development, pull-request review, and repetitive analyst tasks.
- Partner with incident response, red and purple teams, threat intelligence, platform engineers, and telemetry owners to investigate attack paths, close logging gaps, and define durable detection and response requirements.

Security Engineer, Detection Engineering — Jan 2023 - May 2026

- Built, tuned, and operationalized attacker-informed detections in Splunk across identity, cloud, SaaS, collaboration, endpoint, and infrastructure telemetry.
- Used red-team experience and adversary tradecraft to model attack paths, identify defensive blind spots, and strengthen coverage against realistic attacker behavior.
- Supported high-priority investigations through rapid analytics development, cross-source log correlation, telemetry validation, targeted threat hunting, and incident-informed detection improvements.
- Improved telemetry onboarding and environment sign-off processes across production and regulated environments by validating log availability, schema quality, coverage assumptions, and deployment readiness.
- Converted purple-team findings, incident lessons, and logging gaps into durable improvements to detection coverage, operational runbooks, and monitoring quality.

Microsoft

Security Software Engineer, Red Team — Redmond, WA | Jan 2021 - Jan 2023

- Conducted adversary-driven security assessments across Azure services, identifying exploitable weaknesses in web and native applications, identity and authentication flows, databases, distributed systems, and network protocols.
- Led threat modeling and security reviews with product teams to identify architectural weaknesses, validate practical exploitability, and translate findings into prioritized engineering fixes, control improvements, and detection opportunities.
- Built internal software and automation to standardize assessment workflows, improve repeatability, and accelerate red-team operations.
- Partnered with engineering teams to reproduce findings, communicate technical risk, validate remediation, and strengthen services at scale.

Software Engineer, Geographical Disaster Recovery — Vancouver, Canada | Mar 2019 - Dec 2020

- Optimized end-to-end geographical failover pipelines, reducing failover duration by 40% across large-scale production services.
- Redesigned bot and automation components to reduce CPU and memory usage while improving operational reliability and maintainability.
- Built distributed systems supporting service resilience, disaster recovery, and production operations, establishing the software-engineering foundation for later offensive-security and detection-engineering work.

Motorola Solutions

Tel Aviv, Israel

Software Engineering Intern — Jun 2017 - Aug 2017

- Reduced live video-streaming latency by 90% by refactoring a VR/AR application to run natively in Unity with GStreamer on Microsoft HoloLens.
- Built an early TensorFlow prototype to identify the active device user from interaction-derived behavioral features.

EDUCATION

ITESM | B.S. in Computer Science | Graduated May 2018
University of Illinois at Urbana-Champaign | Civil Engineering and Computer Science Exchange Program