Samuel Reed
Application Security Professional
Seattle, WA | crysys@gmail.com | CV at https://samuelreed.info

Summary
Application Security leader with nearly two decades of experience, including several years of direct people management leading teams of up to 15. Most recently led a security review organization through its transition from traditional SDLC gates to AI agent-assisted workflows — building agents for pre-review triage, threat modeling support, and automated feedback grading. Skilled at designing the measurement systems (vulnerability tracking dashboards, metrics programs, FedRAMP compliance automation) that turn security data into fast, evidence-based decisions, designing company-specifiic SDLC programs, and building the automation, tooling, and paved-path processes that let security teams scale.

Core Competencies
AI Agent-Assisted Workflows & Automation • Custom SDLC Program Developement • Security Evaluation, Metrics & Dashboards • Vulnerability Management • Threat Modeling • SAST/DAST Tooling • CI/CD Security Integration • Team Leadership & Cross-Org Partnership • FedRAMP / SOC 2 Compliance • Application Security Program Design

Professional Experience

Manager, Proactive Security (Application Security) — Amazon Web Services (AWS)
March 2025 – February 2026

- Led an 8+ person team performing security reviews for new product launches across Identity, Observability, Monitoring, Analytics, Region Services, and Messaging/Streaming services.
- Directed the team's shift from traditional SDLC security reviews and manual approvals to AI agent-assisted workflows — using agents to perform pre-review triage and generate baseline threat models that supported human reviewers, increasing engineering velocity without lowering the review bar.
- Built agents to support management workflows: feedback on self-evaluations, escalation emails, and team agendas; created a guide and matching feedback agent for writing Situation-Behavior-Impact (SBI) statements that graded quality and flagged missing elements.
- Used GenAI tooling to monitor active workstreams and surface issues needing correction, and introduced structured engineering practices (Asana tracking, documented 1:1s, action-item burn-downs) to raise team operating rigor.
- Balanced shifting launch schedules and cross-team escalations, exercising judgment on the right level of visibility and decision-making to resolve conflicts while keeping review throughput aligned to customer launch needs.

Staff Security Engineer — Pave Inc.
January 2023 – September 2024

- Built and ran Pave's application security program: dynamic testing (annual penetration tests, bug bounty program, DAST), static analysis (Snyk Code, Semgrep in CI/CD), and lightweight security reviews.
- Automated test-environment provisioning — including synthetic HRIS and cap-table datasets — cutting environment setup from days to under an hour and giving pentesters and the security team a consistent, reproducible environment.

- Authored custom Semgrep rules and rolled open-source rulesets into CI/CD in blocking mode; established SAST baselines and drove code-review burn-down to meet SOC 2 requirements.
- Owned the bug bounty program and pentest engagements end to end — triage, fix-drive, vendor migration, external communications — and ran the company's incident response tabletop exercises.

Staff Security Engineer — MongoDB Inc.
October 2020 – November 2022

- Third hire on MongoDB's Cloud Security team; helped build the application security function from the ground up, including architecture reviews, static analysis strategy, and penetration testing for Atlas, Realm, and Charts.
- Designed and built the CSEC vulnerability tracking project: analyzed vulnerability data back to 2019 and built a dashboard (JIRA data surfaced through MongoDB Charts) to track origin, status, and time-to-close, informing team strategy and a recurring engagement cadence with product teams.
- Led the approach to FedRAMP Continuous Monitoring (ConMon) for application security, creating a repeatable, documented process that helped achieve FedRAMP Ready status in May 2021; built a custom Burp plugin to automate scanning through the product's custom authentication flows.
- Evaluated commercial and open-source static analysis tools (gosec, Semgrep, CodeQL) to inform rollout strategy, and implemented initial Splunk detection alerts based on observed attack patterns.

Director, Security Engineering (Application Security) — Credit Karma Inc.
January 2019 – February 2020

- Led the Application Security team through major product launches (Savings Account, Noddle re-brand, UK launch), growing the org from 6 to 15 across engineers in North Carolina and the UK.
- Founded the Security Design Review Group (SDRG), a panel-based architecture review model that cut review time from 3+ hours across multiple meetings to a single 30-minute session.
- Built the real-time AppSec Metrics Dashboard to unify team results and target bug burn-downs, and launched Project Insight, a custom static analysis framework combining company-specific rules with open-source scanners.
- Created the AppSec Engagement Model and a structured onboarding/mentoring program with a new title ladder, developing engineers into SDRG advisors and defining promotion criteria; owned hiring, promotions, 9-box, OKRs, and the team's risk register.

Founder & Principal Security Consultant — Vallation Security, Inc.
December 2015 – December 2018

- Founded and ran an application security consultancy delivering penetration testing, code/architecture review, and program-strategy engagements, including secure AWS storage architectures.
- Produced third-party security assessments and white papers with follow-up testing to verify remediation; handled the full business lifecycle — incorporation, compliance, contracting, and outsourced accounting/legal operations.

Engineering Manager, Security Intelligence & Response — Netflix, Inc.
November 2014 – August 2015

- Promoted to lead Netflix's security intelligence, investigations, and incident response function; built threat intelligence capabilities using OSINT and commercial feeds, including a Facebook Threat Exchange partnership.
- Standardized incident response procedures around NIST 800-61 — on-call rotations, war-room coordination, and recurring cross-team tabletop exercises.

Earlier Roles

- **Senior Application Security Engineer, Netflix, Inc.** (2012–2014) — led security reviews, built security tooling, a vulnerability metrics program, and co-designed Netflix's patented cloud vulnerability-scanning framework (Patent No. 10769282).
- **Application Security Architect & Principal Application Security Engineer, Zynga, Inc.** (2011–2012) — designed Zynga's formal SDLC program; led architecture/security review of platform APIs and payment systems.
- **Security Consultant, iSEC Partners, Inc.** (2010–2011) — led security reviews, penetration testing, and source code review engagements across web, mobile, and financial systems.
- **Security Researcher, Adobe Systems, Inc.** (2007–2010) — led security reviews, redesigned Adobe's SDLC and threat modeling program; delivered company-wide static analysis and code-signing tooling.
- **Software Engineer, LynuxWorks, Inc.** (2005–2007) — security hardening with SAST and Common Criteria EAL4+ certification work on a real-time embedded OS.

Full details on all roles: https://samuelreed.info

Education

B.S., Computer Science, Minor in Mathematics — San Jose State University, CA (2005)
Honors Humanities Program Alumni