Farbod Farhour

Senior Software Engineer · Application Security · AI-native

Montreal, QC, Canada | farbod@farhour.com | +1 438-408-4833 | farhour.com | linkedin.com/in/farhour

SUMMARY

Senior software engineer at Security Compass, whose SD Elements platform maps security requirements to standards such as PCI DSS and SOC 2. I build the parts that decide which requirements apply to an application, check them with security scanners and report the evidence. I work AI-native, and AI agents let me turn ideas into working products quickly: the company's first SDK, an AI agent harness for its 5 product repos, a multi-tenant SaaS with Stripe billing, and my own self-hosted agentic software factory. 13 years from mobile apps to ML research (FSE 2024) to application security.

EXPERIENCE

Security Compass Feb 2025 – Present
Senior Software Engineer Toronto, ON

- Lead AI engineering for SD Elements, the company's platform that maps 8,000+ security requirements to 100+ compliance frameworks, such as the Payment Card Industry Data Security Standard (PCI DSS), System and Organization Controls 2 (SOC 2), NIST 800-53 and ISO 27001.
- Turned scanner results into evidence: scanner imports now record a verdict for each security requirement, and the syncs to 8 issue trackers, Jira among them, report each failed item and why.
- Hardened the SD Elements AI service against prompt injection and patched its dependencies; enforced and tested tenant isolation in the SD Elements APIs.
- Built the company's first SDK, solo and AI-driven: typed Python clients for 338 API endpoints, with 96% test coverage.
- Built an AI agent harness that runs the full SD Elements stack on a Mac for engineers and AI agents: Docker services, guardrails for the agents, an MCP connection to the running app, and a 95% test-coverage gate.
- Led and built the integration tools of the SD Elements MCP server, so AI coding agents can sync security tasks to issue trackers and run scanner verification from the editor.
- Led the first SD Elements feature built with AI coding agents, and since 2025 made the case for agentic development across the company: more than 10 talks to management, developers, QA and product, and an AI development lifecycle brief to the CTO.
- Built the retrieval layer of Navigator, the SD Elements AI assistant: vector search over the security content library, and most of its TypeScript retrieval package (Vercel AI SDK, OpenAI).
- Trained the computer vision model (instance segmentation) that let AI threat modeling read architecture diagrams: components, text, connections and zones.
- Built an event-delivery engine: background jobs (Celery) that send project events, and an API with the history of every delivery attempt. Also sped up the compliance filtering of projects.
- Mentored junior and mid-level developers for 4 years; across 3 teams of 5 to 6 people, worked daily with product managers, QA and the security champion.

Security Compass Jun 2022 – Feb 2025
Software Engineer Toronto, ON

- Shipped features across the core security engine of SD Elements, its AI features and its integrations, such as Jira.
- Rebuilt core parts of the rules engine that decides which security requirements apply to each application, and made the All Tasks report explain why each one applies: a traceable reason for every requirement.
- Kept cardholder and personal data out of the LLM: wrote the filter that redacts card numbers and Social Security numbers (SSNs) from documents uploaded to AI threat modeling.
- Made security changes traceable: activity log entries record who changed a project's security weaknesses and when.
- Fed AI threat modeling with real-world documents: built text extraction for 10 file types, from PDF and Word to SPDX and CycloneDX SBOMs.
- Turned manual QA checks of risk-policy compliance scores into automated tests, and built dashboards, reports and data analytics.

Concordia University Sep 2019 – Aug 2021
Research Assistant Montreal, QC

Full-time.

- Built AlphaBot, a weak supervision framework that labels the queries posted to chatbots for code repositories and retrains the chatbots, on Rasa and Google Dialogflow. It improved the F1-score of the chatbot's natural language understanding (NLU) by up to 35%, and became my M.Sc. thesis and an FSE 2024 paper.
- Helped design and build a framework for the automated testing of deep learning libraries (TensorFlow, PyTorch, Keras and Theano), for a study of the oracle approximation assertions in them.

Housh Gostar Co Jan 2016 – May 2019
Full Stack Developer

Part-time and full-time.

- Built real-time collection and analysis of the tweets of 500,000+ Twitter users, with AI and natural language processing (NLP).
- Built a platform that deploys and manages servers securely across AWS, Google Cloud, DigitalOcean and Vultr.
- Built automated trading software and algorithms for the stock, futures and options markets that earned 2.5x profit.
- Delivered an online auction and tender platform for companies and sellers that became the largest in its market.

Khobregan Saham Brokerage Co Aug 2011 – May 2014
Web & Software Developer

Part-time.

- Built web and mobile apps for a stock brokerage, including an online trading platform whose users grew 3x, and configured the Linux servers they ran on.

Pichak Co Jan 2013 – Aug 2013
iOS Developer

Full-time.

- Built the Recordium app with the Pichak team. It became a top-10 app in more than 50 countries, featured by Apple, The Guardian, The Telegraph and The Next Web.

PROJECTS

Agentic software factory Mar 2026 – Present

- My own self-hosted platform, where AI coding agents such as Claude Code build and ship software through policy gates, and I approve every merge.
- **AI Harness:** a standalone, versioned product (7 releases since October 2026, 191 deny rules for the agents) that any repo installs with one command. It stops agents from editing main, leaking secrets or pulling in packages less than 7 days old, and merges only on a green pipeline for the exact commit.
- AI Harness also gives agents a full engineering process: a spec, plan and review workflow that logs every decision; 5 read-only AI reviewers (security, correctness, tests, docs, spec compliance) that check each change in parallel; and research missions where separate agents try to refute every claim before a human signs off. 537 tests keep it honest.
- **Development infrastructure:** more than 50 containerized services on one machine (GitLab with CI and a registry, a secrets platform, databases, monitoring, automation), reachable only over a private network. It's run like a compliance program: least-privilege secrets on OpenBao with short-lived CI credentials through OIDC, digest-pinned and hardened containers, drift checks in CI, and encrypted backups proven by weekly restore drills.
- Shipped about 1,800 merge requests and 9,500 pipeline runs across 16 projects since March 2026, built with AI coding agents.

SC Sentinel May 2026 – Aug 2026

- A multi-tenant SaaS (Next.js, Supabase, Stripe, Vercel), live in demo mode at sc-demo.xyz, with Stripe subscriptions, license seats and a usage dashboard.
- Designed it around one idea: turn a team's security policy into live context that AI coding agents check over MCP while they write code. Built its core: the MCP server, license gating and rate limits, key revocation, custom rules, and usage analytics with export.

RefactorGuard AI Dec 2025

- Turns a codebase into a dependency graph so an LLM's refactoring answers are checked against the real code structure. Gemini 3 Pro answers questions like "can I delete this class?" by calling tools that query an AST-built graph, then returns a confidence score and a visual impact map. Solo entry in Google DeepMind's Gemini 3 hackathon on Kaggle (writeup).

PUBLICATIONS

A Weak Supervision-Based Approach to Improve Chatbots for Code Repositories 2024
Farbod Farhour, Ahmad Abdellatif, Essam Mansour, Emad Shihab
10.1145/3660812 (Proceedings of the ACM on Software Engineering, vol. 1 (FSE), pp. 2378–2401)

EDUCATION

Concordia University Sep 2019 – May 2022
M.Sc. in Computer Science Montreal, QC
Thesis-based. GPA 3.90/4.00.

- Thesis: A Weak Supervision-Based Approach to Improve Chatbots for Code Repositories, defended in May 2022 and published at FSE 2024.

Amirkabir University of Technology Sep 2013 – Dec 2015
M.Sc. in Computer Science

Thesis-based. GPA 3.90/4.00.

- Thesis: Controllability Discovery of Biological Networks. Proposed and built a method to discover controllability in biological networks, with a framework to model the networks.

Shahid Beheshti University Sep 2009 – Sep 2013
B.Sc. in Computer Science

TEACHING

Concordia University, Teaching Assistant (2021–2022): Introduction to Software Engineering and Software Process, for undergraduate students

Jahesh Co, Instructor (2016–2017): Linux System Administration

Shahid Beheshti University, Instructor (2012–2013): Web Design and Web Development, for graduate and undergraduate students

Shahid Beheshti University, Teaching Assistant (2011–2013): Programming in C++, and Algorithm Design and Analysis, for undergraduate students

SKILLS

Security and compliance engineering: security requirements and controls, verification evidence and traceability, scanner and issue tracker integrations (SonarQube, Jira Cloud), threat modeling, secrets management, least-privilege access with OIDC, tenant isolation, redaction of cardholder data and PII, supply-chain security (SBOM, SPDX, CycloneDX, dependency pinning and patching), prompt injection defense

Automation and data: compliance automation in Python, policy-as-code gates, CI/CD with GitLab, dashboards, reporting and data analytics, SQL (PostgreSQL)

AI engineering: agentic development with CLI coding agents (Claude Code, OpenCode), AI agent harnesses, MCP servers, RAG, LLM security, multi-agent orchestration (crewAI), OpenAI SDK, Vercel AI SDK, computer vision (instance segmentation)

Stack: Python, TypeScript, SQL, Bash, Django, React, Next.js, Jest, Celery, FastAPI, Flask, PostgreSQL, MySQL, Redis, MongoDB, Supabase, Docker, GitLab CI, Vercel, Stripe, AWS, Google Cloud, Linux

Machine learning and data: PyTorch, TensorFlow, Keras, scikit-learn, Pandas, NumPy, Matplotlib, NLTK, OpenCV, Rasa, Google Dialogflow, weak supervision with Snorkel

Ways of working: spec-driven development, agentic code review with a human check of every critical change, mentoring, technical talks to engineers and leadership

Languages: English (full professional proficiency), Persian (native or bilingual proficiency)

Continuous learning: more than 30 online courses, such as Machine Learning, Deep Learning, Machine Learning with Python, Advanced Machine Learning and AWS Fundamentals

AWARDS

International Tuition Award of Excellence, Concordia University 2019 – 2022
Awarded for 3 academic years: 2019–2020, 2020–2021 and 2021–2022.

21st of about 15,000 in the national M.Sc. entrance exam Jul 2013

Our student scientific association ranked 1st among all associations at Shahid Beheshti University May 2011