

Patrick Selamy

New York, NY | (210) 704-7370 | pselamy@gmail.com | selamy.dev | linkedin.com/in/patrickselamy | github.com/pselamy

VP Developer Experience / Agent Deployment Engineering, MCP Tooling, and Guardrailed AI Platforms

Summary

Senior software engineer focused on deploying agentic AI systems into real engineering workflows: MCP-style tool servers, secure runtime boundaries, evaluation harnesses, observability, CI gates, and developer experience for AI-assisted software delivery. Former Meta and Google engineer who built one of the first Gemini-based software-engineering agents at Google Cloud Office of the CTO, including SWE-bench-style eval harnesses and planning-versus-execution metrics. Runs a live autonomous-agent fleet with credentialed tools, reusable skills, human-review thresholds, and production-style monitoring across repos, CI repair, scheduling, documents, and messaging.

Selected Agent Deployment Engineering Portfolio

Agent Runtime, MCP Tooling & Guardrails

- Built a multi-agent operating model where MCP-style servers expose callable capabilities, skills encode reusable procedures, and broker-held credentials keep high-risk actions behind explicit approval gates.
- Designed guardrailed orchestration loops for long-running engineering tasks, including dispatch/fan-out workflows, tool contracts, recovery behavior, and human-in-the-loop thresholds for external actions.
- Implemented CI-backed verification for autonomous coding work, including SWE-bench-style harnesses, planning-versus-execution metrics, and tests that separate runnable artifacts from plausible summaries.

Developer Experience, Observability & Enterprise Fit

- Instrumented agent workflows with OpenTelemetry-style traces, logs, and metrics across tool calls, latency, cost, retries, and task outcomes so operators can debug agent behavior rather than trust black-box output.
- Built internal platform and product systems across Google Cloud Office of the CTO, Google Internal IAM, Citi, Lumeris, and Meta Marketplace, including secure APIs, workflow systems, ranking/ML-backed product improvements, and enterprise identity surfaces.
- Developed customer-facing and internal developer tooling where reliability, auditability, permissions, and clear failure modes mattered more than demo-only automation.

Experience

Meta, Software Engineer

New York, NY | 2025 to 2026

- Expanded Facebook Marketplace third-party partner APIs and shipped-listing workflows for partner and seller-facing commerce.
- Shipped an ML-assisted listing flow that removed manual item-weight entry for shipped listings; predictions were evaluated against user-entered weights and carrier actuals, met the launch threshold near 80% accuracy, and lifted new-listing creation about 8%.

Google, Software Engineer

Pittsburgh / Austin / Remote / Atlanta | 2018 to 2025

- Worked across Google Shopping (Engineering Productivity), Google Play, Google Cloud Office of the CTO, and Internal Identity and Access Management.
- In Google Cloud Office of the CTO, built early agentic-coding systems: a Gemini-based software-engineering agent, SWE-bench eval harnesses, and planning-vs-execution metrics that guided funding and staffing; benchmarked vector-search frameworks at scale (ScaNN, FAISS, pgvector) to position GCP's AI competitively.
- In Google Play, helped build [Play Games Leagues](#) from the ground up on a five-engineer team and designed a configurable fuzzer for third-party Play APIs.
- Built Insider Risk systems for internal security, enterprise identity, and trust-sensitive access.

Earlier, Backend / Platform / Healthcare Engineering

Citi, Lumeris, ClearDATA, and others

- Built backend, platform, cloud, and healthcare systems in Python and Java across APIs, data workflows, and regulated environments.

Selected Systems & Public Work

- [Public agent-skills](#): reusable agent procedures, authoring patterns, and an MCP-vs-skills framework.
- [Operating Agent Fleets](#): an evidence-backed field guide for durable agent systems and bounded authority.
- [polymarket-insider-tracker](#): a Python tool that flags suspicious wallet activity on Polymarket prediction markets.
- AI instructor and speaker: led an [Ayiti AI](#) bootcamp session on MCP, AI-assisted coding, and deployment, and [addressed lawmakers on AI policy](#) at the NHAEON National Leadership Summit.

Technical Skills

Languages:	Python, Java, Kotlin, JavaScript/TypeScript, Hack, PHP, Bash, SQL
AI / Agent Systems:	AI agents, skills/playbooks, MCP-style tools, tool calling, evals, agent harnesses, autonomous coding loops, context engineering, RAG, model routing, secure tool execution, state management
Product & Systems:	API design, backend platforms, distributed systems, workflow orchestration, product metrics, experimentation, launch analysis, developer infrastructure
Security & Enterprise:	internal IAM, auth boundaries, insider-risk systems, credential brokering, trust-sensitive workflows, privacy/security review gates
Infrastructure:	Kubernetes, OpenTofu/Terraform, Argo CD, Docker, Linux, GitHub Actions, Actions Runner Controller, CI/CD, observability, multi-cloud
Data & Cloud:	PostgreSQL, Redis, Kafka, InfluxDB, Google Cloud, AWS