

SHUBHAM JOSHI

Forward Deployed AI Engineer | San Francisco, CA | (202) 440-8445 | shubhamjoshipro.mail@gmail.com

[Tacet, live product](#) | [AgentDock demo](#) | [Pitch deck](#) | [Portfolio](#) | github.com/shubhamjoshipro/mail-svg | linkedin.com/in/shubham-joshi1

SUMMARY

Client facing AI engineer who sits with the customer, turns an ambiguous workflow into a working system, and stays until they actually adopt it. I have been the person in the room for five years: four running my own studio where I found the clients, scoped and priced the work and answered when a campaign underperformed, and a year on a national client engagement that ended with me presenting in person to their leadership, who changed where the organization spent its resources. I pair that with deep hands on building, 508 commits and 92,448 lines of code in the last year with 8 applications deployed and live, including an agent platform that takes real actions on real accounts behind a permission layer I designed and then attacked myself. Now I am building Tacet, my own company, which captures the judgment an expert never wrote down so agents and new hires can act on it.

SKILLS

Client Delivery and Discovery: Consultative technical discovery with business and non technical stakeholders, partnering directly with companies from startups to national organizations, turning ambiguous business challenges into scoped technical solutions I then design, build and deploy myself, requirements gathering and goal clarification, rapid prototyping in front of a customer, live demos and walkthroughs, written specifications and implementation documentation, launch runbooks and explicit release boundaries, executive and client readouts delivered in person, workshop design and enablement, teaching and mentorship, pricing and scoping ownership, developing long term customer relationships, relentless initiative, willing to travel to customer sites

Agentic AI and LLM Systems: Designing agent behaviour end to end: prompt engineering, reasoning and planning, tool calling and function calling, multi agent orchestration, Model Context Protocol servers and clients, retrieval and context engineering, structured output, multi provider routing; Large Language Models from Anthropic Claude, OpenAI GPT and Codex, and Google Gemini; AI powered development with Cursor, Claude Code and Codex

Applied Computer Science and Software Engineering: Applied computer science and software development across emerging technologies: Python, TypeScript, JavaScript, SQL; Next.js, React, Node, FastAPI, PostgreSQL and Prisma, REST API design, system design, real time streaming over server sent events, durable job queues, idempotency, crash recovery, concurrency control, observability and per run cost tracking, automated testing, Docker, Git, CI/CD, deploying and operating software in production on Railway, Chrome extension and Tauri desktop packaging, PyTorch fine tuning with a public model

Evaluation, Trust and Deployment Safety: Evaluation harnesses and benchmark design, scenario and regression testing, adversarial and red team testing including prompt injection defense, deny by default permissions, human in the loop approval gates, encrypted credentials and budget caps, audit trails, confidence gating and abstention, failure mode analysis, honest reporting of negative results, the judgment to say what a system cannot do

EXPERIENCE

Founder, Tacet - San Francisco, CA

Oct 2026 - Present

- Founded Tacet and built it solo from a HackNation and ElevenLabs hackathon prototype into a live multi tenant product. It watches an expert work, predicts each decision before they make it, asks one question only when it cannot explain what they did, and compiles the answer into an executable rule in the expert's own words that AI agents can call over API or MCP and new hires are coached against.
- Let evidence pick the first release: when screen capture failed on a real third party accounting app, rebuilt the first release around the CSV export bookkeepers already have, so a firm sees its own rules learned and tested from last month's ledger before installing anything.

Analytics Consultant, Johns Hopkins University, Client: Alliance of Community Health Plans - Washington, DC

Jul 2025 - Jul 2026

- Embedded with a national organization representing nonprofit health plans for a year, ran the discovery that turned a vague concern about a federal reimbursement change into a measurable economic question, and led technical execution for a six person team.
- Built and deployed the solution end to end: a four stage Python and SQL pipeline reconciling four inconsistent federal sources into 138,263 matched records across 208 variables, an econometric model isolating the consumer cost impact at p below 0.001, and a competitive benchmark across 875 county markets. Caught a twelvefold enrollment overcount before it reached a single reported figure.
- Closed the loop: Tableau exhibits, a data dictionary so the client could run it without me, and a written report presented in person to their leadership. The client said it would change where the organization directed its advocacy, and the team placed top three school wide.

Founder, Digital Marketing and Web Studio, self-employed - Nagoya, Japan

Jan 2021 - May 2025

- Ran a studio single handed for four years for international clients in a third language and carried the entire commercial loop myself: found the clients, ran discovery, scoped and priced the work, delivered websites and campaigns, reported on performance, and answered for the result when something underperformed. Four years of being the person the customer calls is where I learned to run a room and say no to the wrong scope.

Co-Founder and Vice President, Business Analytics and AI Organization, Johns Hopkins University - Washington, DC

Jan 2026 - Present

- Co-founded and lead a 100 member organization alongside my degree, a part time role built on enablement, which is the same skill as driving adoption: recruited the founding team and successor leadership, and designed and delivered a 3 hour hands on workshop on agents and modern AI development to 35 registrants, publishing the guide open source so it outlived the session.

PROJECTS

AgentDock, Agent Platform That Takes Real Actions on Real Accounts

[Live app](#) | [Demo](#) | [Pitch deck](#) | [Code](#)

- Built the whole product solo: model backed planning that compiles a plain language goal into a validated multi step workflow over the real Model Context Protocol wire, first party connectors for Gmail, Calendar, Docs and Search, and a catalog that syncs and classifies the official MCP registry so new tools drop in without a rebuild. 225 commits and 35,539 lines in two months with 11,000 lines of tests across 66 test files.
- Solved the thing that actually blocks a customer from letting an agent near their account: permissions resolve and clamp server side so prompt text can request capability but never grant it, every outbound action passes a human approval gate, credentials are encrypted and budgets capped, and I wrote the adversarial suite proving prompt injection arriving through tool output cannot fire an unapproved send.

Vibe Curator, Nimbus and FridgeChef, Products Shipped to Users

[Vibe Curator](#) | [Nimbus](#) | [FridgeChef](#)

- Vibe Curator is a generative product across 104 commits and 19,913 lines shipping as a web app, a Chrome extension and a signed macOS desktop build, taken to an invited beta on a written runbook that names what is deliberately out of scope. Nimbus is an AI companion for student burnout that answers with one useful next step, and FridgeChef turns a fridge photo into a personalized recipe streamed live.

EDUCATION

Johns Hopkins University, Carey Business School - MS, Business Analytics and Artificial Intelligence, STEM designated, Dean's Scholarship Aug 2026

Nagoya University of Commerce and Business - BBA in Management, **GPA 3.63** (WES evaluated), Dean's Scholar honors, Monash exchange 2025

Coursework: Generative AI, Practical Machine Learning, AI-Driven Sequential Decision Making, Analytics Consulting Project, Responsible AI. **Certifications:**

Anthropic Claude 101, Anthropic AI Fluency, Azure AI-900, SAS SQL Essentials. **Languages:** English, Japanese, Nepali, Hindi.