~ whoami

Jonathan Major

Founder, Agentic Studio Labs · Senior AI Engineer · Ships systems that hold up

→jonathan@agenticstudiolabs.com →agenticstudiolabs.com →linkedin →github/agentic-studio-labs →github/riskresponse

$ cat summary.md

I build and deploy AI systems for teams where architecture, trust boundaries, and production handoff matter. I embed directly, ship real systems, and stay until they hold up without me.

✓MCP servers and Claude skills shipped across security, GRC, and internal tooling
✓ShellScan — pre-deployment security scanning for AI agent skills
✓Multi-agent LangGraph systems with human-in-the-loop
✓IngestGate — retrieval quality gate for RAG pipelines

Background combines enterprise platform engineering (BlackRock Aladdin, Crux Informatics MVP→Series B) with deep GRC and security architecture from a fractional CISO practice. Agentic Studio Labs grew out of the engineering side of that security work. I understand the business context, compliance constraints, and deployment pressure of the systems I build.

→ 0 → 1 engineer · San Francisco · GCP-native

EXPERIENCE

• deployment history

Founder

jan 2026 → present

Agentic Studio Labs

San Francisco, CA

AI engineering consultancy. I embed directly with client teams to build, deploy, and scale production AI systems. Fixed-price, outcome-scoped, full code ownership transferred.

POST /v1/scan-agent-skills-before-deployment — 200 shipped

ShellScan

Pre-deployment scanning platform for AI agent skills and MCP servers. 4 parallel engines (YARA, prompt injection/PipeLock, secrets, code injection). Event-driven GCP architecture. SARIF 2.1.0 output. Published PyPI SDK.

Python · GCP · Cloud Batch · YARA · SARIF

POST /v1/ingestgate — 200 shipped

IngestGate

Retrieval Quality Gate for RAG pipelines. Answers three questions before ingestion: is the document structurally healthy? Can its chunks actually be found by realistic queries? How should it be ingested? Produces weighted health scores, chunk-level retrieval benchmarks (Recall@5, MRR, nDCG@5), operational ingestion metadata via sidecar signals, and optional auto-fixes. Works upstream of any vector DB or retrieval stack.

Python · Claude API · Recall@5 · MRR · nDCG@5 · LiteParse

POST /v1/compliance-without-tab-switching — 200 shipped

grcer

Open-source GRC desktop companion for Vanta. 12 workflows, Claude Opus/Sonnet model routing with prompt caching. MCP security scoping — `withScope()` pattern makes it structurally impossible for prompt injection to trigger write operations.

Electron · TypeScript · MCP · Vanta · Claude API

POST /v1/ai-avatar-for-teacher-coaching — 200 shipped

Interactive Avatar Platform

Architected AI avatar coaching platform using Anam.ai + Brave Search API + Vertex AI for real-time claim verification. Designed zero data retention architecture, navigated university HECVAT procurement security review, delivered full security & technical assessment package.

Anam.ai · Brave API · Vertex AI · pgvector · GCP

POST /v1/agent-infra-and-context-layers — 200 shipped

Agent Infrastructure

Data extraction pipelines using LiteParse for local document parsing. Memory persistence layers with Supermemory for multi-agent context (profile + memory + RAG). MCP server development, agent orchestration patterns, and eval frameworks across client engagements.

LiteParse · Supermemory · LangGraph · MCP · Python

POST /v1/ai-sales-assistant — 200 shipped

AI Jumpstart Assistant

Conversational AI sales intake on Netlify Edge Functions + Claude Sonnet. Streaming SSE responses, fixed service catalog (no hallucinated offerings), rate limiting, input sanitization, adversarial prompt testing suite, graceful fallback to static quiz. $0.015/conversation. Built and shipped in under a day. jumpstart.agenticstudiolabs.com/how-we-built-this

Claude API · Netlify Edge · SSE · Prompt Engineering · Guardrails

POST /v1/semantic-search-for-marketing — 200 shipped

Content Intelligence Hub

Desktop app for marketing content intelligence. Electron + FastAPI sidecar. SQLite + sqlite-vss for vector search, sentence-transformers for local embeddings, Claude API for LLM features.

Electron · FastAPI · sqlite-vss · Claude API

Fractional CISO · AI Systems Builder

jan 2020 → present

Risk and Response LLC

San Francisco, CA

`security perimeter — grc & infosec practice`

- 18 SOC 2 Type I/II engagements delivered across SaaS, HealthTech, InsurTech, and Finance
- Led clients to ISO 27001 certifications and data privacy programs (GDPR, CCPA)
- STRIDE threat modeling for cloud-native applications and data pipelines
- MDR/DFIR architecture — automated incident response, evidence handling, investigation readiness
- M&A technical diligence — product/infra architecture, security posture, operational risk
- Built internal audit service (ISO 27001:2022, ISO 9001:2015) and conducted multiple internal audits across client organizations
- Deep operational expertise with Vanta and Drata — API integrations, MCP server development, platform configuration, evidence automation. Supported sales lifecycle and trained sales teams on security questionnaire response.
- Built and led data privacy programs — authored DPAs, engaged external counsel, automated Certificates of Deletion for data subject requests

SOC 2 · ISO 27001 · NIST CSF · GDPR · CCPA · HIPAA · STRIDE · MDR/DFIR

`POST /v1/mcp-servers-for-compliance-frameworks` `200 shipped`

MCP Servers

4+ MCP servers: NIST 800-53 (1,196 controls), NIST CSF 2.0 (740 questions, 40+ tools, Docker Hub published), Vanta integration, AWS CloudWatch.

Python · TypeScript · MCP · Docker Hub

`POST /v1/multi-agent-systems` `200 shipped`

Agentic Systems

SEC Filing Intelligence Agent (LangGraph, HITL, EDGAR ingestion). Sales Account Concierge (Supermemory, 4 coordinating agents). AG-UI/MAESTRO security demo (multi-agent financial advisor, Neo4j context graph).

LangGraph · Supermemory · Neo4j · FastAPI

`POST /v1/cloud-forensics-pipeline` `200 shipped`

DFIR Cloud Forensics Pipeline

Cloud-native digital forensics pipeline. Processes Velociraptor collections through automated timeline generation with Plaso, threat hunting with Chainsaw, and EVTX log analysis — visualized in Aiven-hosted OpenSearch with pre-configured DFIR investigation views. Infrastructure managed with Pulumi. Reduced time to first incident search from days to under one hour.

forensics · Plaso · Aiven OpenSearch · Pulumi · GCP Cloud Batch

`POST /v1/api-gateway-for-mdr-platform` `200 shipped`

Kong API Gateway

Kong-based Public API gateway layer for a managed security platform. Hybrid deployment mode, multi-tenant rate limiting, per-consumer quota tracking for billing, and tiered access controls across Basic, Standard, Premium, and Enterprise tiers.

Go · Kong Gateway · Cloud Run · OpenAPI

`POST /v1/multi-tenant-siem-rules` `200 shipped`

Panther SIEM Detection Rules

Multi-tenant detection rules repo serving multiple client environments. GitHub Actions matrix strategy auto-discovers environments and deploys shared + client-specific rules in parallel with per-client overrides and cross-environment validation.

Python · Panther SIEM · GitHub Actions · Multi-tenant CI/CD

`POST /v1/internal-audit-as-code` `200 shipped`

ISO 27001:2022 & ISO 9001:2015 Audit Toolkits

End-to-end internal audit toolkits with Claude skills for AI-assisted audit workflow. 93 Annex A controls + Clauses 4–10 (27001:2022), 301 audit questions across all certifiable requirements (9001:2015). Includes working paper generators, evidence intake automation, Vanta API bulk export scripts, 9-phase communication templates, CAR tracking, and formal report templates.

Claude Skill · Python · ISO 27001:2022 · ISO 9001:2015 · Vanta API

VP of Engineering & CSO

oct 2017 → jan 2020

Crux Informatics

San Francisco, CA · Backed by Citi, Goldman Sachs, Morgan Stanley, Two Sigma

- Founding engineering team member. Built the company from MVP through Series A and B funding.
- Hired and led Engineering, Operations, and InfoSec departments.
- Architected and launched enterprise data operations platform.
- Established InfoSec program: ISMS, SOC 2 Type II 'no exception' report, CIS Benchmarks, incident response, vendor management.

SVP of Engineering

aug 2013 → sep 2017

Incapture Technologies

San Francisco, CA

- Led development, testing, and devops for Rapture — Java-based enterprise application platform.
- Product management contribution and client support across the platform lifecycle.

Global Head of Testing

dec 2009 → jul 2013

BlackRock

San Francisco, CA · Aladdin Platform · $10T+ AUM

- Built and scaled global test engineering team from 10 to 100+ members (post BlackRock acquisition of BGI).
- Developed global testing strategy across functional and performance testing for the Aladdin platform.

ITTO — Principal oct 2005 → nov 2009

Barclays Global Investors

San Francisco, CA · IT Transformation Office (pre-BlackRock acquisition)

→ Internal consultant to business lines — designed and implemented automated frameworks for functional and performance testing.

Consultant Test Manager feb 1999 → oct 2005

Arsin Corporation (at Charles Schwab)

San Francisco, CA

Lead Tools Engineer may 1995 → jan 1999

Lotus Development Ireland (IBM)

Dublin, Ireland

CAPABILITIES

• stack

ai/agents	Claude API (Opus/Sonnet/Haiku), LangGraph, MCP server dev, agent orchestration, HITL, prompt injection detection, RAG, evals, sentence-transformers, vector search	coding harness	Claude Code, Cursor, GStack (role-based AI engineering), Beads (agent memory/task graphs), custom Claude skills and slash commands, AI-assisted code review, CLAUDE.md architecture patterns
languages	Python, TypeScript, Go, Rust, Java, SQL, Shell	cloud	GCP (Cloud Run, Workflows, Batch, Firestore, GCS, Pub/Sub, Eventarc, Artifact Registry, Secret Manager), AWS, Cloudflare, Terraform, Docker, GKE
backend	FastAPI, Express, Gin (Go), event-driven architecture, microservices, Pub/Sub, CI/CD	frontend	Electron, React, Chrome Extensions (MV3), TailwindCSS, shadcn/ui, Preact
data	PostgreSQL, Firestore, SQLite, Neo4j, Weaviate, sqlite-vss, knowledge graphs	grc	ISO 27001, SOC 2, NIST CSF 2.0, NIST 800-53, GDPR, CCPA, HIPAA, HECVAT, OWASP, STRIDE
security	Threat modeling, AI red team, vendor risk, agent guardrails, tool scoping, MDR/DFIR, SARIF, penetration testing		

EDUCATION

• credentials

— B.Sc. Computer Science, 1991–1995

```
$ echo $STATUS
✓Taking on new engagements and selective full-time opportunities
✓Scoped builds, sprint embeds, fractional AI leadership, or the right permanent role
→ San Francisco · In-office, hybrid, or remote · No visa required
```