

JAKE MILLER

Technology Leader · Software Architect · Hands-On Engineer · Applied AI + Agentic Systems · AI Security

indy.jake.miller@gmail.com | linkedin.com/in/jakemillerindy | github.com/zivisai/maul | Indianapolis, IN (Remote)

PROFILE

Technology leader, software architect, and hands-on engineer with 20+ years building complex software systems, products, and teams, and the last several years building, securing, and evaluating LLM and agentic systems. Deep experience in distributed and event-driven architecture, graph and relational data, time-series systems, identity and authorization, API and platform architecture, and AI/agent infrastructure. I embed with customers, turn ambiguous business problems into deployable AI systems, and stay in the code. My greatest strength is synthesis: **bringing customers, engineers, models, and real-world constraints together into something cohesive that actually works.**

Proof points: helped build Salesforce Marketing Cloud's Journey Builder for brands like Nike, Uber, and Microsoft and led its 25-person engineering organization; grew a product studio to \$4M in revenue while taking 12+ companies from concept to in-market MVP; co-founded ZIVIS, an AI security and assurance company, and served as head of security for a customer through Salesforce's acquisition due diligence; holds a US patent for distributed data resolution; authored IETF Internet-Drafts (ZTIP/ZTNP) for agent intent binding and trust negotiation and released MAUL, an open-source red-teaming target for agentic systems.

CORE CAPABILITIES

- **Architecture:** Distributed and event-driven systems, graph, relational, and time-series data, API and platform architecture, identity and authorization, multi-tenant SaaS, telemetry and observability
- **Languages + Platforms:** TypeScript, JavaScript, Node, Python, C# / .NET, React, React Native / Expo, Kubernetes, Docker, GCP, Azure, AWS, Fly.io, WorkOS, Clerk
- **Data:** PostgreSQL, Neo4j and graph modeling, Google Bigtable, time-series databases, Redis, BullMQ, vector retrieval
- **AI + Security:** LLM applications, agentic systems, RAG, LangChain and LangGraph, MCP servers, tool use, agent memory and context, evaluation frameworks, model serving, Anthropic and OpenAI APIs, Claude Code, open-weight local models, penetration and exploratory testing, red teaming, threat modeling, OWASP LLM and Agentic Top 10
- **Go-to-Market:** Customer-embedded delivery, concept-to-MVP launches, solution architecture, executive communication, technical evangelism (YouTube, TikTok, LinkedIn, newsletter)

EXPERIENCE

ZIVIS

July 2025 – Present

Co-Founder, CEO & Principal Engineer

Lead architecture and hands-on engineering for a multi-tenant AI security and assurance platform that models security requirements, consumes live evidence and telemetry, evaluates system state, and produces verifiable assurance artifacts.

- Designed the versioned, machine-readable Security Assurance Model: a domain model for requirements, criteria, evidence, evaluation logic, and assurance state, with explicit draft/publish/version lifecycle, pinned installs, and previewed, consented upgrades.
- Architected the evidence and evaluation pipeline that normalizes telemetry, test results, and system signals into evidence, evaluates it against machine-readable criteria, persists findings and assurance state, and issues ZATs, signed machine-readable attestation tokens.
- Designed organization-scoped identity and authorization: tenant boundaries, ownership, and permissions across public and private models, installed versions, evidence resources, and publisher/consumer relationships.
- Built agent-facing infrastructure: an MCP server for onboarding, the @zivis/cli harness that gives coding agents security methodology and durable findings memory, and MAUL, a deliberately vulnerable agentic test system.
- Led security for MeshMesh through Salesforce vendor approval, AppExchange review, and acquisition due diligence, including deep penetration testing. Following Salesforce's acquisition, MeshMesh's founders publicly credited our work on security readiness and enterprise security.
- Designed and built the platform's recon, penetration-test, red-team, and monitoring agents and a 10-lens AI risk methodology used across assessments.

- Personally perform penetration and exploratory testing of production web applications, APIs, identity flows, cloud infrastructure, CI/CD pipelines, and AI/agent systems, built on threat modeling and attack chain analysis with SAST/SCA tooling and ZIVIS's proprietary testing harnesses.
- Run customer engagements end to end: scoping, threat modeling, testing, findings, remediation guidance, and retest, working directly with founders, CTOs, and security leaders.

PINK STACK STUDIO

2026 – Present

Founder / Creative Technologist

- Solo creative technology practice: created a 64-second AI-native film prototype and published an open case study of its exploratory design, from references, target and hinge frames, and generated bridges through continuity decisions, edit, and sound design (pinkstackstudio.com).
- Prototype AI-native creative pipelines and interactive experiences combining generative media, custom software, and physical hardware.

THE ENGINEERED INNOVATION GROUP

Nov 2021 – June 2025

Founder & CEO / Product & Engineering Lead

Founded and led a product engineering company building software for startups, enterprises, and private-equity-backed organizations.

- Grew revenue \$1M → \$2M → \$4M in the first three years, scaling to a 40-person team including offshore contractors.
- Took 12+ companies from concept to in-market MVP, in several cases designing the core technology the business was built on.
- Built across unfamiliar domains: software for a nephrology lab, cybersecurity and data-protection products, a state government contract, venture studio launches, and AI startups.
- Helped build a generative-AI sales enablement platform combining simulations, coaching, assessment, and AI-generated insight.

METAIMPACT

Feb 2018 – Nov 2021

Co-Founder & CTO

Co-founded MetaImpact and built MetaCX, a multi-tenant enterprise platform that created persistent shared spaces between companies for defining, measuring, and managing business outcomes.

- Architected a graph-based model of interconnected businesses, relationships, outcomes, and enterprise data.
- Built time-series metric infrastructure that continuously recalculated customer and business metrics with approximately minute-level latency.
- Designed the multi-tenant data and application architecture integrating enterprise systems, APIs, customer data, and workflows.
- Owned technology strategy and architecture, built the engineering organization, and stayed closely involved in product, data, and system design.

SALESFORCE MARKETING CLOUD / EXACTTARGET

Aug 2012 – Feb 2018

Director of Software Engineering, Journey Builder

Oct 2016 – Feb 2018

Senior Engineering Manager, Journey Builder

Apr 2013 – Sep 2016

Software Engineer, Journey Builder (ExactTarget)

Aug 2012 – Mar 2013

- Helped build Journey Builder from its early engineering stage into a large-scale event-driven orchestration platform for real-time, cross-channel customer experiences: visual workflow authoring, distributed services, contact data, APIs, event processing, and automation.
- Progressed from early software engineer to Director of Software Engineering, leading a 25-person engineering organization across three product teams.
- Coordinated platform architecture and delivery with 6–8 partner teams such as Contacts, building for enterprise-scale reliability in regulated environments; customer brands included Nike, BBVA, Uber, Lyft, and Microsoft.

PATENTS, OPEN SOURCE + RESEARCH

US Patent 10,872,097 B2. Data resolution system for management of distributed data (Salesforce, granted 2020): resolves data requests by identifying sources through a schema registry and querying distributed data sources.

Local Security Harness (in progress). A locally runnable security testing harness built on open-source, open-weight models.

ZTIP + ZTNP. Authored the Zero-Trust Intent Protocol (verifiable delegation and intent binding for AI agents) and Zero-Trust Negotiation Protocol (session-scoped trust negotiation between services and autonomous workloads), submitted as IETF Internet-Drafts, with reference implementations and test vectors in agent-trust-protocols.

ZAT. ZIVIS Attestation Token, an open spec for signed, machine-readable compliance attestations: outcome-level claims, Merkle-committed evidence, selective disclosure, and post-quantum ML-DSA-65 signatures verifiable against published JWK Sets. github.com/zivisai/zat

MAUL. Open-source, deliberately vulnerable AI application for red-teaming agentic systems, with gap analysis against OWASP's agentic security frameworks (LLM Top 10, Agentic Top 10, Agentic Skills Top 10, MCP Top 10). github.com/zivisai/maul

AI Safety Research. Conspiracy Cascade, a multi-agent false-consensus failure mode (published; submitted to DEF CON 34), and Eight Outlaws, an attack taxonomy for classifying how AI and agentic systems are exploited.

Processing Chain Attestation. Conceptual work on attesting to what a chain of AI processing actually did, feeding the ZIVIS assurance model.

EARLIER ENGINEERING EXPERIENCE

Senior .NET Developer · Indiana University Health	Jan 2011 – Aug 2012
Senior .NET Developer · Allison Transmission / TGI	Mar 2010 – Jan 2011
Software Engineering Lead · Ooviso	Aug 2007 – Aug 2010
Freelance Software Developer · MeSync	May 2002 – Jul 2007

EDUCATION

B.A., English and Linguistics · Indiana University Indianapolis	May 2007
---	----------

SELECTED R&D

Interactive AI Hardware. NVIDIA Jetson Orin Nano and Raspberry Pi systems combining cameras, microphones, computer vision, and AI models; prototyped a camera → face recognition → LLM → speech interaction pipeline and explored moving it onto embedded hardware.

AI-Native Creative Production. Workflows combining generative imagery, video, music, sound design, and custom software with human creative direction on every frame.

HOW I WORK

Customer first	Embed with the people who own the problem, then build the thing they actually need.
Prototype fast	Get ideas into a form people can see, test, and react to quickly, then iterate relentlessly.
Deep work	Go heads-down, all the way into a hard problem, and come back with something that feels like magic.
Production matters	Prototypes must survive users, edge cases, deployment, support, and security review.
Generalist by design	Walk into unfamiliar territory, get fluent fast, and ship something real.