Jake Richard Meyers - Information Technology & Cybersecurity Architect

Profile

Background

Principal-level cybersecurity and cloud architect with 22 years of experience designing and hardening large-scale infrastructure, identity, and security systems across finance, healthcare, public sector, and enterprise environments. Microsoft alumnus and practitioner of AI-assisted engineering who specializes in red-teaming safety and security controls and building deterministic guardrails with immutable attribution. Recent work has produced measurable reductions in standing privilege, detection volume, and residual risk while standardizing secure patterns that accelerated cloud adoption for thousands of applications. Brings architectural rigor and adversarial testing discipline to strengthen AI safety systems and complex cloud environments under real operational constraints.

Contact Information

- Phone: (626) 988-6620
- Email: resume@askjake.pro
- Website: https://askjake.pro
- LinkedIn: https://www.linkedin.com/in/jakermey
- GitHub: https://github.com/jakermey

Work Experience

Scoria Software Solutions | March 2025 – Present

Founder & Principal Software Architect

- Designed every tool to operate inside explicit, deterministic guardrails with codified approval and immutable attribution for any divergence, producing clearer audit trails, faster incident response (seconds or milliseconds instead of minutes), and a 1–2 order-of-magnitude reduction in attempts to bypass safety controls.
- Reduced false positives by more than 50% (reaching over 95% in mature deployments) and cut human-intervention escalations from 20–30 per month to

roughly one per quarter at one client, freeing security specialists to resume long-shelved SASE work.

- Built the XLM engine and MCP toolkit family that turns a single prompt into a complete, deterministic, multi-platform application stack while remaining fully model- and platform-agnostic, enabling early adopters to collapse POC cycles from months to weeks, double win rates, and increase inbound leads tenfold.
- Made the suite model- and platform-agnostic so the same tools run interchangeably across consumer apps, enterprise platforms, Azure AI Foundry, Ollama, and local models; one customer cut Azure spend 65% while dropping application latency from 3–5 seconds to 10–150 ms.
- Created the DevOps orchestration engine with built-in AI-development guardrails that reduced technical debt 65–95% of the codebase and compressed feature and patch delivery from weeks or months to days or hours, supporting daily stable releases at one client.
- Developed a single canonical JSON schema front-end engine that deploys cohesive applications across web, native mobile, desktop, APIs, CLIs, and MCP toolkits, reducing each interface's codebase 25–30% through shared components and enabling one team to manage all interfaces instead of dedicated teams per platform.
- Built the vendor- and OS-agnostic infrastructure engine spanning Azure, AWS, private cloud, bare metal, and OpenStack, enabling consistent portable deployments and stronger vendor negotiation leverage that contributed to the observed 65% cloud-cost reduction.
- Engineered the back-end data engine for live, byte-perfect interconversion and normalization across major relational, document, and file formats, allowing agents to work exclusively in JSON and eliminating the token overhead normally spent on formatting and translation.
- Designed and implemented a proprietary Rust conversion engine delivering byte-perfect bidirectional Markdown/MDX ↔ DOCX/PDF translation, eliminating branding and styling errors and collapsing white-paper and sales-collateral production from 1–2 weeks to 1–2 days (more than half same-day including human review).
- Reduced token consumption in LLM-driven document generation by 60–90% across four workflow steps, enabling models to produce publication-ready output with zero post-processing.
- Marketed and deployed the suite to technology companies, MSPs, and consulting firms, enabling functional hands-on POCs before competitors could pitch, single-source vendor status on multiple public-sector bids, 20–40% lower delivery cost to

end customers without eroding margins, and significantly accelerated revenue recognition.

Bedrock Information Systems LLC | January 2019 – Present

Principal Architect

- Established NIST CSF 2.0 Tier 3 (Repeatable) as the new baseline for onboarded systems across all core functions, replacing prior Tier 1 awareness-level practices and enabling automated, single-click audit reporting that reduced typical municipal IT audit effort from 40–120 staff hours to under 30 minutes.
- Delivered measurable advances in CJIS compliance for multiple public-sector customers, strengthening security controls while reducing administrative burden on sworn officers by 1–2 hours per day and allowing more time for street-level public safety work.
- Led a Microsoft Teams implementation for a municipal customer that expanded into a five-year city-wide AI adoption roadmap, aligning 26 major IT priorities across modernization, security enhancement, compliance enforcement, user training, AI adoption, and legacy phase-out; projected initial ROI within 6–8 months and full ROI by year three, with seven-figure annual savings expected from year four onward.
- Built and deployed a custom microfilm digitization tool that converted more than a century of legacy government records (dating to the 1800s) into OCR/ICR-optimized, PDF/A-compliant digital assets with full metadata in a single 21-hour continuous run—collapsing an estimated 10-year multi-person full-time effort—and reduced pre-digital public records request turnaround from weeks or months to days or hours.
- Applied structured guardrails and deterministic processes to AI-assisted development, enabling non-developer infrastructure and application engineers to safely expand into development work; accelerated project timelines 50–75%, allowed teams of 2–3 to deliver what previously required teams of 6–12, eliminated engineer overtime (previously 50–60 hours/week), and increased per-engineer revenue and profitability while expanding overall market footprint without added headcount.
- Directed a large-scale public-sector MDM migration completed in 45 days with one part-time engineer (versus a prior 6–9 month estimate requiring five engineers), achieving 100% success, zero data loss or service interruption, and only five support requests from a 2,300-user organization after a 15-minute training session.
- Designed and operated Azure DevOps and GitHub-based CI/CD pipelines and repository standards that automated deployment and release management for

multi-environment application fleets while embedding security and compliance requirements as first-class, non-negotiable constraints alongside functional and budgetary needs.

- Provided architectural leadership for secure web and application solutions across internal and client environments, expanding Bedrock's capabilities from family-office technology support into a full managed-service provider model serving public-sector and regulated clients while consistently managing concurrent teams averaging 6–12 people.

Los Angeles County Employees Retirement Association (LACERA) | August 2023 – June 2024

Principal Cybersecurity Architect

- Led a five-person dedicated cybersecurity engineering team as the senior-most technical authority under the CISO, shifting the team from reactive whack-a-mole on user reports and Netskope alerts to consistent daily workflows focused on fundamentals and holistic remediation; user-submitted incidents and business disruptions fell from dozens per day to a handful per week, while GRC moved from constant chasing of IT staff to dashboard-driven work, reducing audit compliance effort from a dedicated full-time auditor to a monthly inter-team checkpoint with largely automated report generation.
- Implemented Entra Privileged Identity Management with Just-in-Time access, eliminating 45 standing privileged accounts and all persistent admin access except a monitored break-glass account, while unifying a single audit trail and introducing M-of-N controls integrated with change management.
- Stopped a successful phishing compromise of a high-value, high-privilege executive account with zero data extraction, zero lateral movement, and no impact to business systems, validating the effectiveness of the new privileged access and monitoring controls.
- Deployed Pentera as a continuous red-team capability that initially surfaced hundreds of findings (thousands when correlated with Defender), consolidated after MITRE-aligned triage to approximately 360 actionable items; Critical and High severity issues (roughly 10–15 percent of the total) were closed within the first month's change cycles, and the residual backlog was driven down to an average of 10–12 active findings, with zero-day exposures typically detected within 1–24 hours of CVE assignment and more than 80 percent remediated inside a single change cycle.

- Paired Pentera (red team) with the Microsoft Defender / Purview suite (blue team) to institutionalize regular red-team / blue-team war-game exercises, producing a two-order-of-magnitude drop in Defender events (from hundreds of thousands to thousands per week across the enterprise) and closing nearly all historical vulnerabilities within one quarter of joint operation.
- Integrated security tooling and processes into existing fire-drill and disaster-recovery exercises, creating a unified operational cadence that enabled full business continuity during a real high-privilege account lockdown with zero impact to internal users, external consumers, or public-facing services.
- Led RFP, demonstration, and proof-of-concept processes for SIEM, SOAR, and SASE platforms while simultaneously advancing the organization's compliance maturity more than 30 percent across key frameworks through prioritized controls and programmatic governance.
- Drove ServiceNow-based GRC and change-management integration that increased legitimate change tickets from a handful per month to dozens per week, established a weekly Change Review Board with security as an equal participant, and reduced change delivery cycles from weeks to days or hours with almost no post-change security regressions.
- Delivered real-time security dashboards and live monitoring that compressed project charter and board-approval cycles from multi-quarter processes to a standard monthly cadence, unlocking faster budget and resource decisions and organization-wide visibility into posture and progress.

Wells Fargo Bank | July 2022 – July 2023

Senior Cybersecurity Architect

- Led the Service Enablement Task Force that validated and approved secure architecture and infrastructure blueprints across 128 cloud resource provider types, creating a library of pre-approved patterns that allowed thousands of downstream business applications to adopt standardized designs and largely eliminated the need for custom infrastructure architecture.
- Accelerated security and infrastructure review cycles from an average of 3–12 application approvals per month to 40–50 completed reviews per week, unblocking the bank's first successful large-scale public-cloud migration program after multiple prior failed attempts and enabling application teams to move into Azure architectures in volume for the first time in years.
- Designed and implemented multi-layered Hold-Your-Own-Key (HYOK) cryptography with external key providers that eliminated all third-party cryptographic

dependencies and delivered 100% bank-controlled operations with zero exceptions; this removed an entire class of key-management risk, strengthened audit posture under high securities-regulation and FISA scrutiny, and served as a decisive requirement that finally unblocked enterprise cloud adoption.

- Developed SDLC policy-enforcement roadmaps that shifted the organization from an exception-driven culture to standardized architecture selection; application teams' effort dropped from dozens of hours spread over weeks or months to roughly one to two hours of asynchronous work, while security and infrastructure teams achieved substantially higher output volume with near-universal consistency of results.
- Operated as a cross-functional cybersecurity resource influencing groups of 12 to 100+ engineers, GRC specialists, product teams, and cryptography experts; drove the senior-most executive decision to select the cloud provider and compel organization-wide adoption, eliminating longstanding resistance and entire categories of security and compliance risk across tens of thousands of endpoints and approximately 12,000 ATMs globally.

Microsoft Corporation | March 2021 – November 2021

Senior Customer Engineer, Global Tech Team

- Operated as a Senior Customer Engineer on the elite Global Tech Team supporting Fortune 500, U.S. government, Microsoft internal, and high-technology customers; managed 37 dedicated accounts (12 persistent for the full tenure) while serving as a broader escalation resource and the final technical authority for Microsoft IT and product-group escalations—resolving issues that had no remaining internal escalation path.
- Mentored approximately a dozen engineers and contributed to more than six internal training programs and over twenty standardized customer delivery programs; the volume and variety of customer demand directly led to requesting and shaping production features that later shipped in Exchange Online Bookings.
- Served as a primary post-incident remediation resource for Microsoft's Detection and Response Team (DART); after DART contained a global ransomware attack against a Fortune 500 transportation company, led the subsequent worldwide identity-management overhaul spanning Active Directory forests, Microsoft 365 tenants, Azure and Azure Stack deployments, and private-cloud regions across tens of thousands of endpoints and users, permanently closing the privilege-escalation and leaked-privilege lateral-movement vectors that enabled the original attack and

rapidly deploying FIDO-token plus Microsoft Authenticator multi-factor authentication to the entire global user base.

- Averaged one to two critical-situation escalations per week (frequently joining proactively); most notably diagnosed a Windows Server 2016 Storage Spaces Direct (S2D) bug that was causing cascading SQL Always-On, Exchange Online, Remote Desktop Services, DFS, and failover-cluster outages; the resulting global patch resolved long-standing, multi-year issues for six of twelve dedicated customers and every organization running high-availability Windows Server workloads on S2D worldwide.
- Participated in the critical remediation team for a major global service outage at a hyperscale technology company, helping identify an infrastructure-as-code workflow that triggered the event, providing guidance for the rollback and permanent fix, and contributing to both customer-facing and Microsoft-internal postmortems; the internal postmortem drove backend process changes that improved geo-resiliency protections against rapid global rollouts and influenced standardized geo-resiliency and disaster-recovery planning for Premier and Unified Support customers.
- Delivered customized Well-Architected Framework engagements for the complex minority of customers whose scale or operating model exceeded the standard program (ten of twelve dedicated accounts), driving nearly nine figures in multi-year Azure commitments (including one customer above eight figures), Azure Reserve Instance purchases, and multiple Unified Support renewals and expansions.
- Authored and published reusable PowerShell and ARM-template assets to Microsoft's public GitHub repositories and learn.microsoft.com (cybersecurity, identity, Azure infrastructure, Modern Workplace, and Microsoft 365); these assets were systematically linked from the AskJake.ms technical blog, which reduced repeat customer request volume and freed capacity for higher-value escalation and architecture work.
- Acted as a rare broker between customer escalations and product groups; contributed multiple production features to the Outlook / Exchange Online personal Bookings experience (categories, private booking-link behavior, security and permissions for anonymous links, and Power Platform / inbox-rule integrations), all of which shipped, resulting in standing weekly check-ins requested by the product group.
- Provided continuity for LACERA after leaving the earlier engagement: as their Microsoft engineer, launched Year 1 of the previously authored three-year roadmap, completed all identity and endpoint cloud-management objectives, stood up greenfield Active Directory and Microsoft 365 environments that closed the prior

backdoor-account incident, designed Azure landing zones and SD-WAN foundations, and established the operational momentum that enabled the full multi-year program to finish on schedule years later.

- Co-founded an elite cross-organizational "Super Pod" that grew from two engineers to nearly one hundred subscribers and more than fifty active participants within three months, overhauling Unified Support intake, triage, and communication processes at a time when backlogs had become unmanageable.

Los Angeles County Employees Retirement Association (LACERA) | December 2020 – March 2021

Senior Cybersecurity Architect

- Served as the organization's first dedicated cybersecurity engineer and primary architect of a comprehensive three-year technology and security maturity roadmap spanning eight domains that was formally adopted by the CISO, IT leadership, and the Board; established a NIST CSF baseline at Level 1 with a formal target of Level 3 and secured a funded multi-year program that immediately opened three new security engineering roles.
- Discovered and fully remediated hidden super-privileged Active Directory backdoor accounts that held the highest possible rights—built-in administrator, domain, enterprise, and schema administrator in Active Directory, plus synchronized Global Administrator access in Microsoft 365. These accounts were invisible in standard tools, completely excluded from audit trails and authentication records, and carried suspected logic-bomb associations; they were eliminated within two weeks of discovery.
- Designed and deployed Entra and Netskope across the entire organizational footprint of approximately 550–600 users and endpoints, converting the environment from zero visibility on remote endpoints (beyond legacy VPN tunnel traffic) to full visibility, full-tunnel VPN, firewall, web filtering, and endpoint security controls.
- Stabilized and hardened remote access for the entire workforce during the COVID crisis, eliminating frequent unexpected downtime (previously one to two hours of partial or full impact several times per week) so that only scheduled maintenance remained; zero unexpected incidents occurred in the first quarter after implementation, restoring pre-crisis customer service metrics for the populations the organization served.
- Established the initial identity, access, and visibility foundations that produced the organization's first clear view of previously unknown shadow IT and high-risk access

patterns, and initiated five formal RFP processes for core platforms (including ServiceNow, PMO tooling, and Microsoft security solutions) that locked in the next phase of the maturity program.

City National Bank | March 2020 – July 2020

Vice President, Azure Infrastructure

- Led a core infrastructure team of approximately six engineers (expanded to roughly eighteen during the crisis response), serving as the bank's only pre-existing remote-access capability and the first group transitioned to full remote work in March 2020.
- Executed rapid remote-work enablement that moved all IT staff to remote within one week and emptied the bank's downtown Los Angeles and New York facilities to align with the governor's emergency closure mandate; achieved 100% workforce remote transition within 30 days, with only minor adjustments required for branch-based colleagues.
- Designed and scaled corporate VPN, Microsoft Teams / Microsoft 365 collaboration, and VDI infrastructure to support the full national workforce, while implementing updated multi-factor authentication (Ping Federate + Azure AD + Microsoft Authenticator with continuous RADIUS) and Azure availability monitoring—foundational capabilities preserved for subsequent enterprise adoption.

Molina Healthcare | February 2019 – February 2020

Senior Solutions Architect (Consultant, Infosys)

- Architected and led the Azure Landing Zone and hybrid-cloud migration program for a healthcare environment of approximately 16,000 production servers (≈40,000 total environments including non-production), more than 630 business applications, and a data footprint exceeding 2 petabytes; completed migration of roughly one-quarter of the footprint within the year.
- Selected the organization's single most business-critical application—an SQL Always On cluster protecting 450 TB of data with 2.7 TB of daily transactions and one of the most complex SDLC cycles (up to 12–15 environments)—as the first major workload to move; designed and executed the full migration in four to five months, establishing a fully repeatable pattern that reduced subsequent application migrations from months to days or weeks.
- Authored the majority of the Infrastructure-as-Code and orchestration frameworks that provisioned and governed all Landing Zone resources (networking, Virtual WAN, storage, gateways, firewalls, and Zero Trust network security) as well as the ongoing

deployment and maintenance of the critical SQL Always On workload; integrated the frameworks into the organization's existing Terraform processes so that operational teams experienced zero change to day-to-day maintenance and management, while end-to-end automated cutovers (including a perfectly clean production SQL Always On migration) required only human monitoring.

- Treated security and compliance as first-class requirements from the outset, embedding HIPAA controls, comprehensive audit trails, and ready integration points for existing SIEM/SOAR tooling; the design received full CISO and security-team approval and satisfied 100 percent of the security organization's stated requirements.
- Led a combined delivery team of approximately twelve onshore and two dozen offshore Infosys consultants plus a core group of fifteen permanent Molina stakeholders, coordinating Infrastructure-as-Code work with application refactoring (including a significant SQL version upgrade) performed by team developers to make the critical workload cloud-native; the coordinated effort delivered a successful, clean migration of the organization's most complex and business-critical application while maintaining influence across the full server, data-center, and application footprint.

Additional Historical Roles

- **Senior Solutions Architect****Senior Solutions Architect* | _**Coretek Services**__*Coretek Services*_* | August 2018 – January 2019
- **Principal Consultant****Principal Consultant* | _**Obsidian Availability Solutions**__*Obsidian Availability Solutions*_* | September 2016 – December 2018
- **Senior Solutions Engineer, Engineering Team Lead****Senior Solutions Engineer, Engineering Team Lead* | _**Orion Technology Services**__*Orion Technology Services*_* | June 2015 – August 2016
- **Senior Systems Administrator****Senior Systems Administrator* | _**Detroit IT / Core 3 Solutions**__*Detroit IT / Core 3 Solutions*_* | June 2014 – February 2015
- **Senior Systems Analyst, Helpdesk Lead****Senior Systems Analyst, Helpdesk Lead* | _**Detroit Country Day School**__*Detroit Country Day School*_* | June 2013 – June 2014
- **Systems Analyst****Systems Analyst* | _**University of Michigan, Information & Technology Services**__*University of Michigan, Information & Technology Services*_* | June 2011 – September 2012
- **Information Technology Specialist****Information Technology Specialist* | _**Battery Giant / Energy Products**__*Battery Giant / Energy Products*_* | January 2007 – December 2010

- **Systems Analyst***Systems Analyst* | _**Detroit Country Day School**__*Detroit Country Day School*_* | June 2005 – August 2006

Education

The University of Michigan, Ann Arbor, MI

- College of Literature, Science, and the Arts (LSA) | Biochemistry, Economics, and Data Science
- School of Music, Theatre, and Dance (SMTD) | Design & Production, Stage Management, Lighting Design & Electrics, Sound Engineering, and Music Production

Detroit Country Day School, Beverly Hills, MI

- High School Diploma | College Preparatory Curriculum

Skills

AI / LLM Safety & Red Teaming*AI / LLM Safety & Red Teaming** Deterministic guardrails, immutable attribution, continuous red-team/blue-team exercises, adversarial testing of safety controls, model- and platform-agnostic XLM (LLM/SLM) orchestration, MCP toolkits, Azure AI Foundry, Ollama/local models, hybrid multi-model routing, token optimization, AI-assisted development guardrails

Identity & Privileged Access*Identity & Privileged Access** Microsoft Entra ID / Azure AD, Privileged Identity Management (PIM), Just-in-Time access, Conditional Access, FIDO / MFA, Bring-Your-Own-Key (BYOK) & Hold-Your-Own-Key (HYOK) cryptography, RBAC & least-privilege design, Active Directory (schema-level) Domain/Certificate/Federation Services, identity governance, Netskope / Prisma / CASB patterns

Cybersecurity Architecture & Operations*Cybersecurity Architecture & Operations** Zero Trust, Microsoft Defender / Purview, Pentera, SIEM / SOAR, SASE, XDR & vulnerability management, endpoint protection, incident response & post-incident remediation, privileged-access overhauls, shadow IT discovery, change-integrated security scanning

Cloud & Infrastructure Architecture*Cloud & Infrastructure Architecture** Azure Landing Zones, Virtual WAN, Azure Stack, hybrid cloud, Well-Architected Framework, AWS, private cloud / bare metal / OpenStack, geo-resiliency, high-availability patterns, vendor-agnostic infrastructure schemas

Infrastructure as Code & DevOps*Infrastructure as Code & DevOps** Terraform, ARM / Bicep, PowerShell, GitHub, Azure DevOps, CI/CD pipelines, Infrastructure-as-Code engines, repository governance, full lifecycle automation, SecOps automation

Languages & Data Systems*Languages & Data Systems** Rust, Python, C# / .NET, Node.js / Next.js, PowerShell, SQL (multiple dialects), R, C/FFI; Microsoft SQL Server Always On, PostgreSQL, MySQL, Cosmos DB / MongoDB, Oracle, large-scale (petabyte-class) data environments, live interconversion & normalization

Networking, Storage & Core Infrastructure*Networking, Storage & Core Infrastructure** SD-WAN / SDN, Virtual networking & firewalls, Storage Spaces Direct (S2D), DFS, Windows Failover Clustering, VDI, VPN scale-out, Active Directory infrastructure

Compliance & Governance*Compliance & Governance** NIST CSF 2.0, CJIS, HIPAA, securities-regulation environments, audit automation, enterprise architecture review boards, GRC / ServiceNow integration, SDLC policy enforcement

Microsoft 365 & Modern Workplace*Microsoft 365 & Modern Workplace** Teams, Exchange Online, SharePoint / OneDrive, Bookings, Conditional Access for M365, large-scale remote-work enablement