STEVEN TUSCHMAN

Sunnyvale, CA | (763) 746-6185 | steventuschman2@gmail.com
linkedin.com/in/steven-tuschman | **intelligent-architecture.com**

PROFESSIONAL SUMMARY

Enterprise Identity Architect and Systems Engineer specializing in Microsoft Entra ID ecosystem defense, Workload Identity Federation (WIF), and machine identity configurations. Applying systems-level diagnostic rigor, I leveraged Generative AI to reverse-engineer cloud vulnerabilities and construct the ***Enterprise Field Manual***—a closed-loop, deterministic playbook fully documented and showcased at **intelligent-architecture.com**. By uploading this rigid schema directly back into the AI, the model transforms from an open-ended assistant into a highly focused orchestration engine that anticipates the exact engineering workflow.

The system forces a strict, reproducible sequence: it first executes the **AI & Cloud Pipeline Hardening Framework (ACPHF)** to establish the core Zero-Trust bedrock, immutably recording those states in the **Identity Architecture Ledger (IAL)**. Next, it performs **Dual-Interface Auditing** via active telemetry, logging the cryptographic proof in the **Audit Results Ledger (ARL)**. Only after this core is fully verified does the AI-backed system advance to **Modular Capability Expansion**, selectively deploying from a 35-tool Microsoft Entra taxonomy to deliver a tailored **Final Configuration Package**. Holding SC-300 and CySA+ certifications and applying formal Project Management Professional (PMP) principles, I deliver modernized architectures that replace reactive, ad-hoc cybersecurity with governed, AI-driven defense.

TECHNICAL SKILLS & COMPETENCIES

- **Identity & Access Management:** Microsoft Entra ID, Workload Identity Federation (WIF), Service Principals, User-Created & System-Assigned Managed Identities, OpenID Connect (OIDC), OAuth 2.0, Conditional Access, Privileged Identity Management (PIM), Data-Plane Role-Based Access Control (RBAC), Zero Trust Architecture.
- **Diagnostic Auditing & Security Operations:** Kusto Query Language (KQL), Azure Log Analytics, Dual-Interface Auditing, Non-Interactive Sign-In Telemetry, "Silent 403" Diagnostics, Threat Vector Analysis.
- **Automation, CLI & Cloud Infrastructure:** Azure CLI (Primary Interface for Enterprise Automation), Programmatic Configuration, Python, GitHub Actions CI/CD, Cross-Platform Execution (Windows/macOS), Generative AI Orchestration.
- **Governance, Frameworks & Compliance:** NIST SP 800-207 (Zero Trust), SOC 2 Type II, AI & Cloud Pipeline Hardening Framework (ACPHF), Identity Architecture Ledger (IAL), Audit Results Ledger (ARL), Systems Lifecycle Management.

PROFESSIONAL EXPERIENCE

Enterprise Identity Architect / Systems Engineer Intelligent Architecture | Sunnyvale, CA | May 2024 – Present

Phase 1: AI-Driven Market Forecasting & Skill Acquisition

- Leveraged Generative AI using formal project management principles to forecast and target modern cybersecurity's highest-value vulnerability: unmanaged machine identities.
- Utilized this AI-assisted methodology over two years to rapidly master Python, data engineering, network cybersecurity, and the complete CompTIA CySA+ and Microsoft SC-300 curriculums.
- Reverse-engineered cloud vulnerabilities to build a fully operational, closed-loop AI compliance engine centered on the AI and Cloud Pipeline Hardening Framework.

Phase 2: System Execution (The Enterprise Field Manual) Orchestrated the ***Enterprise Field Manual*** (fully documented and showcased at **intelligent-architecture.com**), a cohesive compliance system designed to optimally leverage Generative AI. The system eliminates ad-hoc guesswork by executing a strict, reproducible progression:

- **Component 1: Configuration Engine (ACPHF):** Executes its four phases to establish a zero-trust bedrock and enforce passwordless OIDC federation via programmatic CLI execution.
- **Component 2: Identity Architecture Ledger (IAL):** Records all hard validation states and data-plane RBAC assignments into an immutable configuration file prior to runtime.
- **Component 3: Dual-Interface Auditing & ARL:** Executes active KQL diagnostics against mandatory gates, prompting the AI to output the Audit Results Ledger (ARL) as cryptographic proof of compliance.
- **Component 4: Modular Capability Expansion:** Acts as a diagnostic index to safely integrate precise toolsets from the 35-capability Microsoft Entra ecosystem based on exact business requirements.
- **Component 5: Final Configuration Package:** Delivers an audited, immutable core combined with adaptive security modules to completely eliminate manual configuration drift.

PROFESSIONAL CERTIFICATIONS

- **Microsoft:** Identity & Access Administrator (SC-300)
- **CompTIA:** Cybersecurity Analyst (CySA+)
- **Programming & Data:** PCAP Certified Associate Python | Dataquest Data Engineering Professional