STEVEN GARY TUSCHMAN

Sunnyvale, CA | steventuschman2@gmail.com | linkedin.com/in/steven-tuschman
intelligent-architecture.com | github.com/Compcode1

PROFESSIONAL SUMMARY

Microsoft Certified Identity and Access Administrator (SC-300) specializing in Microsoft Entra ID and zero-trust machine identity foundations. To safely accelerate complex cloud deployments, I engineered the Zero Trust Interactive State Machine. By architecting a deterministic control loop, I harnessed generative AI into a strictly tethered execution engine. The AI is deployed to dynamically write configurations, patch code, and resolve syntax friction, but is systematically forced to return to the core framework, reporting its exact position in the execution pipeline to keep the architect and the execution engine fully synchronized step-by-step.

Operating within this interactive loop, I define the strategic intent for complex architectures, such as passwordless OpenID Connect (OIDC) workload federations. The framework is engineered with dynamic conditional logic, making it highly adaptable across varied execution agents, diverse data-plane assets, and multiple IaC payloads in both greenfield and brownfield environments. To secure this flexibility, I designed a decoupled logic engine to serve as the enterprise guardrail. This mechanism explicitly separates AI code generation from final deployment, mathematically neutralizing vulnerabilities across five critical vectors: preventing proprietary context leakage, enforcing strict declarative idempotency, restricting access exclusively to granular data-plane roles, rigorously pinning supply-chain dependencies, and masking terminal execution strings.

Crucially, this methodology autonomously translates infrastructure into immutable Compliance-as-Code. Rather than relying on manual checks, the system automatically generates customized cryptographic receipts to prove zero-trust governance. Every execution outputs an Identity Architecture Ledger (IAL) to record the exact target state configuration, alongside an Audit Results Ledger (ARL) and KQL telemetry to forensically confirm deployment success for immediate SOC 2 audit readiness. Anchored by a Defect & Patch Ledger (DPL) that continuously hard-codes operational refinements back into the core baseline, I utilize this framework as a secure, rapidly scalable launchpad for deploying advanced Entra ID enterprise modules.

To provide complete transparency into this methodology, the formal technical documentation and public proof-of-work are published at **intelligent-architecture.com**. This portfolio explicitly deconstructs the operational execution triad and breaks down advanced Entra ID deployments step-by-step, providing open-source visibility into the synthesized IaC payloads, reverse-engineered APIs, and final cryptographic ledgers.

PROFESSIONAL EXPERIENCE

Intelligent Architecture | Sunnyvale, CA *Principal Cloud IAM Architect / R&D Systems Engineer* | May 2024 – Present

- **Deterministic AI Orchestration (R&D):** Spearheaded an independent systems engineering initiative to fuse AI with enterprise cybersecurity, architecting a deterministic logic framework that forces probabilistic LLMs to execute as strictly tethered, zero-trust infrastructure compilers.
- **Cognitive Framework Engineering:** Reverse-engineered Microsoft Entra ID backend behaviors to program the Zero Trust Interactive State Machine, utilizing advanced memory configuration and state-tracking constraints to autonomously optimize against execution friction.
- **Passwordless Workload Federation:** Dynamically synthesized and executed complex IaC payloads (Terraform, Bicep, Native PowerShell REST API) to establish OIDC trust matrices across GitHub Actions, GitLab CI/CD, and Azure DevOps.
- **Complex Edge-Case Remediation:** Programmed native structural bypasses for severe cloud deployment friction, including Entra ID Graph API eventual consistency (race conditions), local terminal MFA token drops, and GitHub OIDC Node-ID token volatility.
- **Automated Compliance Validation:** Enforced an audit-first mandate by deploying asynchronous Kusto Query Language (KQL) telemetry and generating immutable Cryptographic Ledgers (IAL/ARL), mathematically proving data-plane isolation for immediate SOC 2 readiness.

TECHNICAL SKILLS & COMPETENCIES

- **Identity & Zero Trust:** Microsoft Entra ID, Conditional Access (CAWI), Workload Identity Federation (WIF), OpenID Connect (OIDC), Managed Identities, Service Principals, Data-Plane RBAC, Azure Key Vault.
- **IaC, CI/CD & Automation:** Terraform (HCL), Azure Bicep, GitHub Actions, GitLab CI/CD, Azure DevOps, Native PowerShell REST API, Microsoft Graph API, Azure CLI, Python.
- **Systems Engineering:** Deterministic AI Orchestration, Prompt-Driven Execution Pipelines, Cryptographic Ledgering (Compliance-as-Code), Kusto Query Language (KQL), SOC 2 Technical Readiness.

CERTIFICATIONS

- Microsoft Certified: Identity and Access Administrator Associate (SC-300)
- CompTIA Cybersecurity Analyst (CySA+) & Security+ ce
- Project Management Professional (PMP)
- PCAP-31-03 Certified Associate in Python Programming