

G. Daniel Schillinger

AGI Cybersecurity Architect | GenAI Ambassador+

Miami / Fort Lauderdale, FL | Authorized to Work in the U.S. and EU | Open to Relocation

gdaniel.schillinger@gmail.com | 305-316-4578

gdanielschillinger.com | champlain.joinhandshake.com/profiles/5krkgk | github.com/gdanielschillinger

Professional Summary

AGI cybersecurity architect and enterprise GenAI practitioner with experience in AI-enabled compliance workflows, agentic-system security, RAG architecture, and cyber risk management. At Visa, contributed to an in-house LLM and compliance automation initiative that drove case-summarization accuracy from 37% to more than 90% within 30 days while supporting OFAC-related workflows. Recipient of Visa's 2024 Client Care Excellence Award and GenAI Ambassador+. Completing a B.S. in Cybersecurity with a 4.0 GPA while delivering secure AI systems, client-facing agentic platforms, and private procurement-intelligence workflows.

Professional Experience

Client Care Senior Support Specialist & GenAI Ambassador+

Visa Inc. | Miami, FL (Hybrid) | 2023–April 2026

- Architected and built Visa's first in-house LLM from the ground up, trained on production-grade, compliance-controlled sensitive data using reinforcement learning and continuous retesting; supported OFAC compliance automation.
- Drove case-summarization accuracy from 37% to more than 90% within 30 days, reducing regulatory risk and operational overhead.
- Selected as a GenAI Visa Ambassador+; trained cross-functional teams on responsible AI use and enterprise AI tooling.
- Received the 2024 Client Care Excellence Award for contributions to the internal 365 Copilot LLM lifecycle, including suggestive and proactive reasoning frameworks.
- Served as a Subject Matter Expert, delivering training and recruitment programs across risk, compliance, CCPA, GDPR, OFAC, FinTech regulations, tokenization, and global financial procedures.
- Directed penetration-testing engagements and malware-analysis cycles; applied zero-trust cryptographic practices across internal systems.
- Built a Python suggestive-reasoning module adopted for production use in the Visa 365 Copilot LLM pipeline.

President, VAST — Visa Asians Standing Together

Visa Inc. | 2023–2026

- Led culinary, cultural, philanthropic, and community events representing Asian heritage across Visa's Miami operations.
- Championed LGBTQIA+ inclusion, diversity, equity, and Visa Foundation charity initiatives.

Independent Researcher & AGI Security Architect

Self-Directed | Miami, FL | April 2026–Present

- Advance the Sentient Sync Engine and [auditor.py](#), focusing on agentic-AI security, AI integrity, and cyber-risk reduction.
- Design Llama-based LLM workflows for algorithmic-trading research through Edge API integration, emphasizing system design, data-informed reasoning, and controlled automation.
- Complete B.S. Cybersecurity coursework while pursuing AGI, cybersecurity-architecture, and AI-security roles in financial services and related sectors.

Key Projects

Sentient Sync Engine — AGI Collusion Detection Architecture

Founder & Lead Architect | 2025–Present

- Build a security-focused framework for detecting and responding to multi-agent collusion, including coordinated prompt-injection chains and policy-evasion behavior.
- Address six OWASP LLM Top 10 categories: prompt injection, insecure output handling, model denial of service, sensitive-information disclosure, excessive agency, and overreliance.
- Implement [auditor.py](#) for cryptographic signing and tamper-evident action logging.
- Build with Python, LangGraph, Gemini 2.5 Pro, Next.js, Tailwind CSS, TypeScript, SQLite, HMAC-SHA256, and Vercel.

Sterling Realty Group — Agentic Real-Estate Platform

Lead Architect & Engineering Lead | Client Capstone Engagement | May–June 2026

- Led a three-person team through a seven-week, \$15,000 client engagement, delivering an agentic real-estate platform from project initiation through client proposal and handoff.
- Owned system architecture, user experience, AI orchestration, data integrations, security controls, and delivery planning.
- Built with Next.js App Router, TypeScript, Tailwind CSS, Python, LangChain, LangGraph, vector retrieval, Redis, Vercel Pro, live MLS data integration, and CRM pipeline connectors.

- Designed autonomous lead qualification, real-estate context tooling, and human-in-the-loop intercepts for high-value client interactions.
- Applied SAST, OWASP-aligned review, API security testing, prompt-injection guardrails, and PEP 8 quality controls.
- Earned an A / 98 out of 100 from Dr. Barker and delivered the client proposal.

Procurement Intelligence RAG & Guardrails Platform

Project Manager | Client: IB Lux | Beratender Ingenieur | 2026–Present

- Manage delivery planning for a secure German-language procurement knowledge platform supporting private consulting, training, compliance research, and supply-chain decision workflows.
- Define hybrid retrieval with dense embeddings, BM25 keyword search, reciprocal-rank fusion, cross-encoder reranking, hierarchical chunking, and metadata filtering.
- Coordinate LangGraph-based routing for commercial analysis, procurement controlling, strategic sourcing, supplier risk, and structured advisory workflows.
- Implement safeguards for prompt injection, topical routing, evidence sufficiency, grounded-answer validation, and citation enforcement.
- Establish evaluation and hardening criteria through retrieval benchmarks, context-quality measurement, grounded-answer assessment, and adversarial prompt testing.

Ethical Hacking & Penetration Testing — Authorized Isolated-Lab Assessment

Summer 2026

- Executed an authorized enterprise-style security assessment within an isolated laboratory environment, applying NIST SP 800-115, PTES, OWASP Web Security Testing Guide, and MITRE ATT&CK-aligned methodology.
- Performed OSINT and reconnaissance, host and web-application discovery, Nessus and OWASP ZAP scanning, manual validation, exploitation-path analysis, privilege-escalation testing, and remediation planning.
- Documented 13 confirmed vulnerabilities—7 critical, 5 high, and 1 medium—and produced a risk-ranked remediation roadmap.
- Validated SQL injection, OS command injection, reflected XSS, and stored XSS strictly within the authorized environment.

2025 Visa Hackathon — Python Suggestive-Reasoning Module

Individual Contributor → Production | Visa Inc. | 2025

- Designed and built a Python-based suggestive and proactive-reasoning module during Visa's internal hackathon.
- Selected for production deployment into the Visa 365 Copilot LLM pipeline, strengthening proactive recommendations in enterprise AI workflows.

Education

Bachelor of Science, Cybersecurity

Champlain College | Burlington, VT (Online) | Oct. 2023–Expected Dec. 2026 | GPA: 4.0

- Class President and Honors League member.
- Completed Coursework: Ethical Hacking (CYBR-335), Advanced Python (CMIT-235), Digital Forensics & Investigation (CFDI-240), Intrusion Analysis & Response (CYBR-320), Networking & Security (CYBR-240), Security Scripting with Python (CYBR-260), Mobile Security (CYBR-310), TCP/IP (NETW-215), Wireless Networking (NETW-210), Sysadmin & Network Services (NETW-255), Project Management (MGMT-260), Web Development I (WEBD-125).
- Planned Fall 2026 Coursework (12 Credits): Cloud Computing Security (CMIT-280); Operating System Security (CYBR-330); Emerging Threats & Defenses (CYBR-410); Cybersecurity Policy Analysis & Implementation (CYBR-420).

Technical Skills

AI & Agentic Systems: LLMs, Llama, LLM Design, Edge API Integration, Algorithmic-Trading Workflow Design, Generative AI, Gemini API, Reinforcement Learning, RAG, LangGraph, LangChain, Hybrid Retrieval, Vector Databases, Agent Collusion Detection, Prompt-Injection Defense, OWASP LLM Top 10

Cybersecurity: Penetration Testing, Vulnerability Assessment, Web Application Security Testing, OWASP WSTG, PTES, MITRE ATT&CK, OWASP ZAP, Nessus, Metasploit Framework, Kali Linux, Malware Analysis, API Security Testing, SAST, Zero-Trust Architecture, NIST CSF, NIST 800-53, NIST 800-61, OWASP Top 10, OWASP ASVS, CISA KEV, Remediation Planning

Engineering & Platforms: Python, TypeScript, Next.js, Tailwind CSS, REST APIs, SQLite, Redis, GitHub, Vercel, Docker, Kubernetes, GitHub Actions, Google Cloud, Vertex AI, VMware, Bash, SQL, HTML/CSS, JavaScript, MySQL, Power Automate

Cryptography & Compliance: HMAC-SHA256, Ed25519, Cryptographic Signing, Post-Quantum Cryptography, Kyber-768 / ML-KEM-768, OFAC, CCPA, GDPR, PCI-DSS, FinTech Regulations, Tokenization, Risk & Compliance Frameworks, IEEE P2842

Leadership: Project Management, Client Delivery, Stakeholder Communication, Cross-Functional Training, SME Facilitation, Full-Cycle Training & Recruitment, Organizational Leadership