Greg Miller

AI Security Platform Architect

Seattle, WA | Greg@MillerSoft.org | (206) 535-4789 | LinkedIn | resume.millersoft.org

AI security platform architect with 12+ years building automated incident response systems — from enterprise SOAR platforms at Amazon to agentic AI with multi-agent orchestration and real-time threat response. Currently architecting AI security infrastructure at CARIAD and building an open-source agentic AI platform with 160+ tools, semantic search, and security-gated orchestration.

PROFESSIONAL EXPERIENCE

AI Security Platform Architect

Nov 2020 – Present

CARIAD Inc.

- Manage OpenAI Enterprise platform as internal security owner, establishing AI governance policies and access controls.
- Leading Microsoft 365 Copilot implementation, including governance, security controls, and enterprise rollout strategy.
- Implemented Zero Trust access using Zscaler ZIA/ZPA for enhanced security across the enterprise.
- Drove over $1.5M in annual cost savings through consolidation of Microsoft 365 and Azure licensing.
- Engineered SailPoint IdentityNow to ADP API integration for automated joiner/mover/leaver lifecycle management.
- Led enterprise-wide cloud-first digital transformation using Entra ID, Intune, Jamf, SailPoint, CrowdStrike, and 1Password.

Founder — AI Platform Engineering

2018 – Present

Millersoft LLC

- Architecting an open-source AI agent platform featuring 160+ registered tools, multi-agent orchestration with security gates, and an MCP server implementation.
- Designed and implemented a semantic search pipeline using fine-tuned BGE embedding models, ONNX Runtime, pgvector, and RAG for knowledge retrieval.
- Trained and deployed custom ML models including fine-tuned embedding models, ONNX Runtime optimization, and vector similarity search.
- Built a multi-provider LLM routing system with automatic fallback, local-first inference, and token optimization.
- Engineered container-based microservices infrastructure with FastAPI, asyncio, asyncpg, and Redis caching.
- Developed RS256 JWT license verification, bytecode-only distribution, and TOTP execution approval gates.
- Built container hardening pipelines aligned with CIS Docker Benchmark and NIST SP 800-190.
- Deployed Grafana/Loki/Promtail observability stack for centralized log aggregation and real-time infrastructure monitoring.
- Designed and implemented zero-trust network architecture using Tailscale mesh VPN across a hybrid fleet of 13 nodes.

Information Security TPM — Security Automation & SOAR Platform

Dec 2012 – May 2020

Amazon

- Led the design and implementation of a homegrown SOAR platform for Amazon Security, significantly decreasing operational overhead and enabling substantial automation of security workflows.
- Drove development of secure automation frameworks for access certification and joiner/mover/leaver processes, transforming manual audit processes from 40 hours/week to minutes daily — achieving nearly 99% efficiency.
- Managed large-scale identity and access programs across AWS and internal enterprise systems, including directory services for millions of domain controllers.
- Provided critical engineering solutions for Active Directory and LDAP systems at scale, decreasing system failures by approximately 80%.
- Partnered with engineering, audit, and compliance teams to align security programs with regulatory requirements.

Senior Associate – Security & Infrastructure

Jul 2007 – Nov 2012

Windsor Health Group

- Led Active Directory and Exchange Server migrations supporting HIPAA-compliant healthcare infrastructure.
- Designed backup and disaster recovery processes across multi-site operations. Provided Tier 3 escalation support.

CORE COMPETENCIES

Cybersecurity & Compliance

Zero Trust | SOAR | Security Automation | DevSecOps | Container Security | Incident Response | Microsoft Sentinel | Splunk | SIEM | KQL

AI/ML Engineering

Agentic AI | Multi-Agent Orchestration | MCP | RAG Pipelines | Embedding Fine-Tuning | ONNX Runtime | pgvector | LLM Routing | AI Governance

Cloud & Infrastructure

Azure/AWS/GCP | Kubernetes | Docker | Terraform | Tailscale | Zscaler ZIA/ZPA | Grafana/Loki | GitHub Actions CI/CD | Cloudflare

Backend & Identity

Python | FastAPI | PostgreSQL | Redis | SailPoint | Entra ID | Active Directory | SAML/LDAP | SCIM

EDUCATION & CERTIFICATIONS

MS, Cybersecurity & Information Assurance
Western Governors University — May 2025

BS, Cybersecurity & Information Assurance
Western Governors University — Sep 2024

Order of the Sword and Shield — Member since 2021

CompTIA PenTest+
SSCP (ISC2)
CompTIA CySA+
CompTIA Security+
CompTIA Network+
ITIL Foundation V4
CompTIA A+
Certified Scrum Product Owner (CSPO)