Adam Dye

Principal Security Architect

Zero Trust · Cloud Security · AI System Security

Chesapeake, VA · Open to relocation and remote
adamsdye@outlook.com · GitHub · Credly · Substack

PROFILE

Security architect and leader with 10+ years designing, building, and validating security for classified, critical infrastructure, and regulated environments. Hands-on with Zero Trust segmentation, tiered administration, PKI, SIEM, and Microsoft 365 / GCC security, and builds adversarial AI testing environments for prompt injection and data leakage assessment. Led the security design and delivery of a 325-person organization's cloud tenant migration, coordinating the MSP and third-party integrations. Previously governed security for 13,000+ users across 17 countries in nuclear energy, and served as senior technical authority on security validation for classified naval combat systems.

Core competencies

Zero Trust & network segmentation · Cloud security (Microsoft 365 / GCC) · AI / LLM security testing · Identity & tiered administration (AD, PKI) · SIEM & detection (Wazuh) · Security automation (PowerShell, Hyper-V) · Data protection (Purview, DLP) · NIST 800-171 / 800-53 / CSF 2.0 · Incident response & DFIR · Third-party & supply chain risk · Disaster recovery & continuity · Executive & board communication

EXPERIENCE

Chief Information Security Officer (CISO) — 2026 – present

T-Solutions, Inc.

- Led the security design and delivery of a 325-person organization's enterprise tenant migration to Microsoft Government Community Cloud (GCC), Microsoft's government cloud, coordinating the managed service provider (MSP) and third-party integrations to meet contractual security requirements.
- Fully implemented the NIST SP 800-171 control environment, positioning the organization for CMMC Level 2.
- Deployed and administer Microsoft 365 security and compliance controls: Purview data governance, DLP, information protection, insider risk management, and audit/eDiscovery.
- Set enterprise security direction and advise executives on risk posture and investment.

Supervisor, IT Governance, Risk Management & Security — 2021 – 2026

Westinghouse Electric Company

- Directed enterprise cybersecurity governance for 13,000+ users across 17 countries in nuclear energy critical infrastructure.
- Led compliance alignment across NIST CSF 2.0, NIST 800-53, ISO 27001, SOC 2, NIS2, CRA, GDPR, and NERC; guided the organization through three independent NIST assessments and earned external recognition from PwC for program maturity.
- Built and led a global team executing 300+ risk assessments and 100+ policy exceptions annually; spearheaded enterprise GRC platform implementation.
- Integrated cybersecurity into third-party risk governance across 300+ vendor relationships; designed an enterprise phishing resilience program.

Information Systems Security Officer / Intelligence Analyst
2018 – 2020

T-Solutions, Inc.

- Administered a 2,000+ user enterprise environment with 100% availability across 200+ accounts, and led business continuity through multiple parallel disaster recovery scenarios.

Earlier career: Electronic Warfare, Program Management, and Doctrine
2016 – 2021

Warrant Technologies, Stratascorp, Prevailance

- Senior technical authority on security validation for classified naval combat systems; directed delivery of technical intelligence libraries and expanded production capacity 10x; developed doctrine across 12+ programs.

Chief Cryptologic Technician / Technical Leader
1996 – 2016

United States Navy

- 20-year career as an award-winning information security and operations leader across global deployments; managed cross-functional teams and multi-million-dollar system installations, including a $15M emerging technology integration.

PROJECTS

Zero Trust Compliance Enclave & GRC Lab

Built and scripted (PowerShell, Hyper-V) a segmented 11-VM environment aligned to NIST SP 800-171 / CMMC L2: default-deny OPNsense boundary, dual domain controllers with tiered admin model, offline-root and issuing PKI, Wazuh SIEM, and encrypted, audited file shares. CISO Assistant GRC platform tracks assets, evidence, risk, and POA&M. Source on GitHub

AI Governance & Security Testing Lab

Adversarial AI testing environment for model risk validation, prompt injection testing, data leakage assessment, and governance policy development aligned to NIST AI RMF.

Cloud Resume Challenge on Azure

This site. Static hosting on Azure Storage behind a Cloudflare Worker with HSTS and a strict CSP, a serverless Python visitor-counter API on Azure Functions and Cosmos DB, Bicep infrastructure as code, and GitHub Actions CI/CD with passwordless OIDC, an SBOM, dual vulnerability scanning, CodeQL, and enforced signed commits. Frontend · Backend · Write-up

CERTIFICATIONS

CISSP **CISM** **CRISC** **CompTIA SecAI+**

EDUCATION

Bachelor of Arts, Biblical & Theological Studies · Regent University