KYLE FIDUCIA

MAIL@KFIDUCIA.COM
941.650.9350

PROFILE

20+ years building and breaking systems across government intelligence, defense, enterprise consulting, and startups. Career spans bleeding-edge offensive security work as a subject matter expert for intelligence community and DoD programs, red team and penetration testing engagements for organizations from nonprofits to Fortune 100, and founding and scaling security products from the ground up. Deeply technical and hands-on, with equal fluency across engineering teams and customer-facing engagements — able to architect solutions and speak credibly to practitioner pain points from direct operational experience on both sides of the problem.

Currently CTO at Turngate, leading technology strategy, product direction, and hands-on engineering for a next-generation SIEM platform built by practitioners, for practitioners. Previously taught graduate-level offensive security at George Washington University. Nationally and internationally ranked competitive hacker. Active in the security community through DEFCON and BSidesNOVA.

EXPERIENCE

TURNGATE

CTO

2023 - PRESENT

CTO of an early-stage security SaaS company building a next-generation SIEM focused on high-end detective and investigative functionality that keeps pace with real adversary behavior, not checkbox compliance.

Technology strategy & hands-on leadership. Own the technical roadmap and lead cross-departmental product management spanning Engineering, Sales, Marketing, Design, and Customer Success — while remaining the leading individual contributor across the engineering team.

AI strategy — internal & product. Led company-wide AI adoption: evaluated tools, set usage standards, and integrated AI into development workflows. On the product side, shipped a proof-of-concept for AI audit data collection within days — giving customers visibility into their own AI usage before competitors offered anything comparable.

Prototyping & product R&D. Built functional prototypes for detection management and AI-powered investigation features, informed by active offensive security work and real-world adversary tradecraft. Created scaffolding that enabled the broader team to evaluate customer use cases and chart product direction.

Shipping reliability & platform stability. Drove measurable improvements: stronger regression coverage, richer error telemetry, security-focused CI pipeline hardening, and feature flags with preview builds. Led root cause analysis for production incidents and institutionalized blameless postmortems. Result: regressive bugs down, failures dropped substantially, and mean-time-to-remediation shortened.

Operational efficiency. Shrinking the engineering backlog with a smaller team than the company has had in years while driving down infrastructure costs through transparent, data-driven analysis — a strong velocity-per-engineer signal.

Engineering culture. Established open knowledge-sharing practices across the team, including blame-free incident analysis shared company-wide to normalize learning from failure. *Remote*

ALTUS CONSULTING

TECHNICAL FELLOW & CYBER SME

2012 - PRESENT

Currently serve as a technical fellow and cybersecurity subject matter expert. Earlier tenure included hands-on red team operations, penetration testing, and cyber defense across global networks.

CTF Competition. Core member of the team that placed nationally for 3 consecutive years at SANS NetWars Tournament of Champions, winning 1st place in the USA (2018, 2019) and internationally (2019).

Red Team Operations. Led offensive security programs including threat hunting and security posture enforcement across thousands of remote hosts.

Penetration Testing. Drove significant improvements to host, account, PKI, and database security through assessments spanning network/endpoint security, emerging technologies, mobile devices, and wireless systems (LTE, WiFi).

Cyber Defense & Insider Threat. Subject matter expert for global operations network defense.

Chantilly, VA

OODA
Red Team Lead
2019 - Present

Plan and execute Red and Purple Team security assessments for clients ranging from nonprofits to Fortune 100 companies.
Report findings to executive leadership with quantified risk evaluations and remediation roadmaps.
Manage a team of offensive security researchers and engineers. *Reston, VA*

NARWALL LABS,
Founder
2016 - Present

Founded a cybersecurity consultancy and product lab. Built a multi-tenant, cloud-based security platform processing high-volume host event data and telemetry — from SIEM-style log aggregation to contextualized threat intelligence — focused on reducing false-positive fatigue through machine-derived enrichment. Built on Apache Kafka, Elasticsearch, Python, Angular/TypeScript, and deployed across AWS, GCP, and Azure. *Arlington, VA*

GEORGE WASHINGTON UNIVERSITY
Adjunct Professor
2019

Designed courseware for and taught PSCS 4202: Attack Tools & Techniques for the College of Professional Studies. Senior-level course focused on hands-on offensive security scenarios using current threat actor tools and techniques. *Ashburn, VA*

LOCKHEED MARTIN
Systems Engineer
2009 - 2012

Lead engineer for Secure Mobile Platforms R&D covering secure wireless systems, enterprise mobility, and network security. Systems engineering role supporting complex classified missions requiring technical solution design, risk mitigation, and regular customer and management briefings. *Herndon, VA*

EDUCATION

MASTERS ELECTRICAL ENGINEERING	University Of Central Florida	2008
BACHELORS ELECTRICAL ENGINEERING	University Of Central Florida	2007

SKILLS

AI & Data LLM integration and evaluation, agentic architectures, retrieval-augmented generation (RAG), vector stores, prompt engineering, stream processing (Kafka, RabbitMQ), Elasticsearch/Logstash, graph databases, data ETL pipelines

Cloud & Infrastructure AWS (primary), GCP, Azure, infrastructure as code (Terraform), containerization (Docker), CI/CD pipeline design, feature flags, observability and error telemetry, microservice architectures, RESTful APIs

Languages Python, TypeScript, JavaScript, SQL (MySQL/PostgreSQL), PHP, Shell Scripting

Offensive Security Penetration testing, red/purple team operations, advanced exploitation, threat hunting, threat intelligence, CTF competition (1st place SANS NetWars nationally and internationally)

Security Engineering SIEM architecture, detection engineering, PKI, cryptography, network security, wireless security (LTE, WiFi, 802.1X), VPN, DNS security, incident response, root cause analysis

Security Tooling Kali Linux, Metasploit, Burp Suite, Wireshark, and broad familiarity with offensive and defensive security tooling

VOLUNTEER

Big Brother Big Sisters, Mentor	2016 - 2020
Youth Cyber Education, Mentor	2017-2018
DEFCON Goon	2019 - Present
BSidesNOVA, Volunteer (Network/CFP Board/CTFs)	2018 - 2021