DAVID WOLF

PRODUCT SECURITY / AI ENGINEER

Builder-Breaker: A hands-on security engineer with an attacker's mindset.

Turns complex data, AI, and security constraints into trusted systems that work in real-world, regulated environments. Builds secure, production-grade platforms that scale across complex enterprise systems.

linkedin.com/in/davidwolf • research@davidwolf.org • Los Angeles, CA

PRODSEC ARCHITECT

Defines secure-by-design SaaS and multi-tenant patterns, reference architectures, and SDLC control standards.

APPSEC ENGINEER

Leads threat modeling, code review, penetration testing, and vulnerability management across enterprise applications.

SECURITY RESEARCHER

Investigates real-world attack patterns and publishes industry-cited findings that drive product innovation and security policy.

EXPERTISE: Secure SDLC • Threat Modeling • API and Platform Security • Incident Response • Vulnerability Management AI Guardrails • Agentic Workflows • Identity and Access Management • Cloud Security • CI/CD Tooling Statistics • Machine Learning • Natural Language Processing • Big Data Pipelines • Model Tuning

PROFESSIONAL EXPERIENCE

AI Engineer, Security & Platform — Independent Consultant — 2023 – Present

Independent consulting in AI and security engineering across multi-tenant SaaS, agentic systems, and containerized platforms.

- Architected LLM-augmented detection engineering with generative ATT&CK trees, converting realistic threat scenarios and enterprise asset context into high-fidelity SIEM rules and SOC runbooks for faster triage.
- Built and deployed multi-agent workflows exposing 300+ APIs as MCP tools; migrated business workflows between AI agent orchestration platforms, architected SaaS IAM controls (SSO, SCIM, RBAC/ABAC, MFA, tenant-scoped access) with guardrails aligned to ISO 42001, NIST AI RMF, and MITRE ATLAS, and trained/deployed MLflow models to 0.94 F1.

Security Research Engineer, Architecture — Devo — 2022 – 2023

Cloud-native SIEM platform recognized as a Gartner Magic Quadrant Visionary.

- Redesigned SIEM reference architectures and standardized taxonomy models across large-scale pipelines, aligning telemetry and metadata to Elastic ECS and OpenTelemetry standards.
- Built verification and validation practices for Devo Exchange detections; analyzed 300 enterprise and MSSP SIEM deployments to identify maturity patterns and turn findings into research accepted at RSA and industry conferences.

Principal Security Research Engineer — Forescout — 2017 – 2020

Zero-trust network and IoT/OT/ICS device security platform for global enterprises.

- Analyzed Forescout Device Cloud telemetry across 13M enterprise devices to identify device, network, product, and operational risk patterns across healthcare, financial services, manufacturing, energy, retail, and SLED.
- Established and led the Rapid Response program, cutting event-to-customer-policy go-live from >14 days to 48 hours through formal RACI and cross-functional execution across research, engineering, product, product security, legal, sales engineering, product marketing, PR, content, and technical docs teams.

Manager, Application Security — Cornerstone OnDemand — 2015 – 2017

Enterprise talent management SaaS platform for recruiting, performance, learning, and workforce development.

- Enabled FedRAMP ATO by translating regulatory requirements (FedRAMP, SOC 2, ISO 27001/27018, HIPAA, GDPR, PCI DSS) into reusable product security controls and multi-tenant SaaS architecture patterns.
- Architected authorization and data protection systems including RBAC/ABAC, SSO, IAM, MFA, OAuth, encryption/key management, and audit logging for 2,000 enterprise SaaS tenants across US, UK, EU, and FedRAMP environments.

Senior Product Security Engineer — Splunk — 2013 – 2015

Enterprise SIEM platform for machine data analytics, security monitoring, and operational intelligence.

- Drove product security for all Splunk-built apps and 450+ marketplace apps; scaled security design/code review, penetration testing, and incident response across customer-facing platform components.
- Established Splunkbase App Certification and “Splunk Certified” standards by defining verification and validation requirements and automating SAST/DAST checks; scaled bug bounty, triage, and root-cause workflows, authored sales enablement briefs and RFP responses, and achieved 100/100 Veracode for Splunk’s then-largest enterprise deal.

PROFESSIONAL EXPERIENCE

Management Consultant — Cyber Security Engineer — 2010 – 2013

Contractor to security-sensitive organizations in finance, defense, energy, and scientific research.

- Integrated 100+ APIs into microservice-based security workflows; implemented SAST/DAST tooling, secrets extraction, and secure refactoring workflows; designed KYC investor-screening for PCI DSS Level 3 requirements.
- Retained by Splunk to continue the program as a contractor, then converted to FTE.

Director, Product Manager — Syntryx — 2006 – 2010

Open-source intelligence platform for multi-channel web and behavioral data.

- Led an 11-person product and engineering team serving 100+ enterprise clients and driving $2M ARR, and built and operated a >2B-page PostgreSQL OSINT platform with high-throughput crawling, ingest, ML, and search pipelines.
- Used NLP, ML, clustering, and factor analysis to reverse-engineer search-ranking factors, and pioneered graph visualizations of semantic relationships across domains, keywords, ads, and links.

Management Consultant — Cendant Travelport (Orbitz) — 2004 – 2006

Global travel conglomerate with Blackstone roots and a private-equity Travelport carve-out.

- Advised product and marketing leaders across the $6B Travelport portfolio on technical marketing strategy; engineered Markov-style route-ranking models over waypoint graphs that generated £400–600K monthly gross profit by surfacing high-value niche itineraries, and corrected thousands of mislocated Galileo properties.

Prior Experience & Education — 1999 – 2004

Founded a tech startup acquired in 2002.

- Built autonomous browser agents for evolutionary content generation, crawling, and traffic experiments; authored and marketed technical content across SEO/SEM/PPC funnels and grew a portfolio to ~30K daily visitors.
- B.S., Business Administration — Business Information Systems | University of Colorado at Boulder
- M.S. Thesis: How North African Desert Warfare Models E-commerce | American Military University

RESEARCH AND PUBLICATIONS

A selection of conference-accepted and industry-cited work in security, AI, and applied machine learning.

WIRED Magazine
Hackers Could Use Smart Displays to Spy on Meetings

RSA Conference
Aligning Values, Purpose, and Meaningful Work in Cyber

Vedere Labs
Banking on Security: Leveraging Device Data for Financial Risk

Vedere Labs
Putting Healthcare Security Under the Microscope

Security Boulevard
Controlling Zoom: Telework in Healthcare, Government, and Finance

Bloomberg Law
Cyber Insurance as a Line Item in Security Budgets

CyberScoop
Malware Causes Significant Disruption in German Manufacturing

NextGov
Huawei, ZTE Devices Still Running on Government Networks

Cloud Native Security Conference
Mapping Motives: Analysis of 2,000 Enterprise Cloud Detections

BrightTALK
Banking on Security: Malware and the Financial Sector

Devo
Mapping SIEM to Zero Trust and MITRE ATT&CK Cloud Matrix

Forescout
Connected Medical Device Security: Healthcare Network Deep Dive

Forescout
From Events to TTPs: OT Incident Response with MITRE ATT&CK

Forescout
Cybersecurity in M&A Diligence

Australian Cyber Security Magazine
10 Riskiest IoT Devices in 2020

Splunk .conf
Splunkbase App Certification: Security Verification and Validation

TECHNICAL STACK

AGENTIC AI & GUARDRAILS

Claude, Codex, Cursor
MCP, Ollama, Agents SDK
n8n, LangChain, AutoGPT
CrewAI, Flowise, Sim Studio
Presidio, NeMo, Garak, Vigil
Supabase, pgvector, Qdrant
MLflow, Hugging Face, WASM
Model Armor, Mindgard, PyRIT

SECURITY ENGINEERING

ISO 42001, NIST AI RMF, AIMS
Splunk, Devo, Elastic, SIEM
SSO, OAuth2, SAML, SCIM
Semgrep, SonarQube, Trivy
Coverity, Checkmarx, Snyk
MITRE ATT&CK and ATLAS
Mattermost, Slack, Chatbots
Burp, ZAP, Tenable, Qualys

DEVELOPER TOOLKIT

Next.js, React, Shadcn
Rust, Go, Tauri, Electron
TypeScript, Python, Bash
GitLab, Jira, Linear, Notion
Helm, Docker, Vercel, AWS
Puppeteer, Playwright, CDP
OpenAPI, Swagger, Postman
Browser extensions, proxies

TRAINING & CERTIFICATIONS

CISSP, ISSAP, ISSMP, CSSLP
CRISC, CISM, CCSK, CPHIMS
PMP, PRINCE2, Scrum Master
SANS Pen Testing, Forensics
AWS Architect, Big Data, ML
Splunk Certified Architect
Elastic Certified Analyst
CPR/AED, ASA Skipper