STEVE ZENONE

steve@zenone.org
linkedin.com/in/zenone | github.com/zenone

SUMMARY

Security and IT leader and hands-on AI engineer with 25+ years building security programs from the ground up in high-growth companies. Founded Netflix's Security Intelligence and Response Team (SIRT); first security officer at two healthcare startups, where I stood up security and IT from scratch and cleared HIPAA, HITRUST, and SOC 2 without slowing the business. I fine-tune and deploy large language models in production multi-agent systems - cloud or fully on-device, matched to the data and the risk - so sensitive workloads stay protected without giving up capability. I build the adversarial-AI and prompt-injection defenses most security leaders can't. Career spans Microsoft, Netflix, and Meta. Technical author on LLM security and security leadership.

SKILLS

AI and ML Engineering: LLM fine-tuning (QLoRA/LoRA, NF4 quantization, bfloat16), behavioral evaluation design, role-specific training data, Gemma 4 (31B dense, 26B MoE), multi-agent coordination, agent behavioral design, A/B testing AI workflows, self-healing infrastructure, semantic memory

AI Security: Adversarial AI, prompt injection, LLM security, multi-agent attack surfaces, injection defense architecture (4-layer), agentic risk, red teaming, AI governance, model security

Security Engineering: SIRT design, OSINT-driven detection, incident automation, SAST/CodeQL, secure code review, vulnerability management, bug bounty programs, static application security testing (SAST), application security, penetration testing, threat modeling

Security Operations: Splunk, CrowdStrike, Microsoft Sentinel, Defender for Endpoint, Carbon Black, SIEM and EDR deployment and operations (SIEM and endpoint detection and response), threat detection, incident response, intrusion detection and analysis (GCIA)

Systems and Infrastructure: Node.js, TypeScript, Python, Java, JavaScript, C#, Chrome DevTools Protocol (CDP), WebSocket systems, Docker, Podman, LaunchD, browser automation, distributed systems, npm publishing

Cloud: Azure, AWS, GCP, multi-machine orchestration, idempotent systems

IT and Collaboration: Google Workspace administration, Slack, Okta/SSO, SAML, MDM, endpoint management, SaaS security and vendor risk

Compliance: SOC 2, HIPAA, ISO 27001, HITRUST, PCI DSS, FedRAMP, NIST CSF

PROFESSIONAL EXPERIENCE

Security & IT Leader / AI Engineer

White Sands, LLC | Remote | Jan 2025 – Present

- Stood up a fully local 30B Qwen large language model on an AMD Strix Halo Framework Desktop, serving at ~80 tokens per second over Vulkan (no ROCm), reboot-persistent and bound to localhost only. Proved that inference needs no heavy GPU-compute driver stack, cutting infrastructure overhead and update risk.

- Fine-tuned and deployed Gemma 4 models (31B dense, 26B mixture-of-experts) with QLoRA in a production multi-agent system; built behavioral evaluation suites that validated deployment readiness at 80% to 88% pass rates on role-specific dimensions.
- Founded and built Nimbus, an end-to-end AI agent platform with multi-channel communication, browser automation, semantic memory, and an extensible 87-skill system, engineered with platform-scale operational security.
- Built Balisong, a private, local-only bug-bounty research toolkit; enforced validation-first findings with deterministic oracles, 75 passing unit tests, and in-code guardrails that block any cloud LLM or out-of-scope target.
- Research adversarial AI, multi-agent prompt injection, and LLM security; designed and documented a 4-layer injection defense architecture for multi-agent systems.
- Advise high-growth companies on standing up security and IT programs, compliance readiness (SOC 2, HIPAA), security operating model design, and AI risk for AI-integrated products.
- Published technical author at firstorder.zenone.org (security leadership for CISOs) and morphic.zenone.org (The Training Run series on LLM fine-tuning, behavioral evaluation, and agentic security).

Principal Security Engineering Manager

Microsoft | Remote | Jul 2022 – Jan 2025

- Led security engineering across Windows, Office 365, Xbox, and core Microsoft services as part of the Security First Initiative.
- Drove CodeQL and static analysis (SAST) adoption across critical product lines; increased secure code coverage 70% and reached 90% of critical assets.
- Built AI-assisted vulnerability triage workflows using Microsoft Copilot; increased developer participation in security review across globally distributed teams.
- Maintained zero attrition across a globally distributed team through two-plus years of industry-wide layoffs.

VP, Information Security and IT

Dispatch Health | Remote | Jun 2021 – Oct 2021

- First security officer at a fast-scaling healthcare company delivering in-home medical care; built the security AND IT function from scratch.
- Led HIPAA and HITRUST compliance and delivered a clean first external audit while the company grew rapidly.
- Managed a lean team of eight; owned security posture, IT operations, and executive risk reporting.
- Implemented practical, low-friction controls - secure by design, not audit theater - so security enabled the business instead of slowing it.

Head of Information Security

Mindstrong | Remote | Jun 2020 – Jun 2021

- Built and led security from the ground up for a regulated healthcare (mental health) startup during rapid growth.
- Led SOC 2, HIPAA, and ISO 27001 efforts in parallel while supporting active product development.
- Stood up continuous monitoring, automated controls, and a vendor risk program from zero.

Director of Information Security

Pulse Secure | San Francisco Bay Area | Jul 2019 – Jun 2020

- Led corporate and product security at a zero-trust network access vendor serving government and enterprise customers globally, including FedRAMP-regulated organizations.

- Managed an 8-person team; launched private bug bounty programs and drove secure code initiatives; led incident response that retained high-risk government clients.

Senior Information Security Engineer

Facebook (Meta) | San Francisco Bay Area | Apr 2019 – Jul 2019

- Supported CERT operations at production scale; rebuilt forensic workflows and automated analysis pipelines to increase investigation throughput.

Senior Security Engineer — Security Intelligence and Response Team (SIRT)

Netflix | San Francisco Bay Area | Aug 2013 – Jan 2019

- Joined when there were four engineers on the security team; helped scale the function to more than 100 as Netflix expanded globally.
- Founded the Security Intelligence and Response Team (SIRT) and built it into a standing, durable organizational capability used across the company.
- Built OSINT-driven tooling for credential theft and account abuse detection; reduced investigation time from days to hours.
- Created BotSwanson: a Slack-based automation platform for repeatable, low-friction incident response, adopted across the security team.

EARLIER EXPERIENCE

Information Security Manager | University of California, Santa Cruz | May 2000 – Mar 2012
Information Security Consultant | Brocade Networks | May 2012 – Aug 2013
UNIX Security Consultant (Contract) | Wells Fargo Bank | Apr 2001 – Jan 2003
Security Consultant (Contract) | TiVo | Apr 2001 – Sep 2001
Senior Security Consultant (Contract) | CAT Technology | Dec 2000 – Apr 2001
Senior Security Administrator | OnRadio / Avevo | Nov 1999 – May 2000
Senior Security Consultant | Internet Security Systems (ISS) | Jan 1999 – Jan 2000
Senior Sales Engineer / Security Administrator | Data Fellows (F-Secure) | Jan 1998 – Dec 1998
Senior Support Engineer | NETCOM Online Services | Jan 1997 – Jan 1998

PUBLICATIONS

Morphic (morphic.zenone.org) - "The Training Run" series on LLM fine-tuning, behavioral evaluation, and multi-agent injection defense. 24 additional pieces on AI systems, distributed architectures, and autonomous security.

First Order (firstorder.zenone.org) - Security leadership publication for CISOs and executives.

EDUCATION

California State Polytechnic University, Pomona
Philosophy | Minor: Artificial Intelligence | 1991 – 1994

CERTIFICATIONS

CISSP, ISC2 | 2005
Cyber Leadership Program, Cyber Leadership Institute | 2020
GIAC Certified Intrusion Analyst (GCIA), GIAC