Steven Richards

resume@rookdynamics.com | linkedin.com/in/stevenlrichards | Greater Cincinnati Area

PROFESSIONAL SUMMARY

Cybersecurity and presales engineering leader with over 20 years of experience across enterprise security architecture, complex solution selling, and applied AI systems work. Currently serving as Domain Consultant at Palo Alto Networks, focused on Cortex XDR and XSOAR across a broad range of enterprise verticals. Career spans presales and solution engineering roles at Cylance, Optiv, IBM, Juniper Networks, and Internet Security Systems, building on a foundation in network and security infrastructure dating to the late 1990s. Outside of the day job, actively building agentic AI systems, autonomous infrastructure, and AI-integrated tooling, developing practical expertise in LLM routing, context and memory management, RAG pipelines, and multi-agent coordination.

ENTERPRISE CYBERSECURITY EXPERIENCE

Palo Alto Networks, Cincinnati, OH

Domain Consultant, Cortex (Pre-sales) | 2019 – Present

FY23: 145% · FY22: 187% · FY21: 117% · FY20: 212% · FY19: 123% | Century Club 2019-2023*

- Lead design and technical sale of advanced security solutions across Financial Services, Healthcare, Government, Education, Manufacturing, and Critical Infrastructure.
- Developed custom Insider Risk Management solution with Cortex XSOAR, replacing a failed Exabeam implementation for the region's largest financial customer.
- Applied practical AI/ML knowledge to position AI-SPM, XSIAM, and Cortex analytics; advised on AI security posture and governance.

Cylance Inc., Cincinnati, OH

Security Engineer (Pre-sales) | 2015 – 2019

FY18: 127% · FY17: 223% · FY16: 167%

- Early adopter of AI/ML-driven endpoint security, serving as technical lead for product evaluations using machine learning models for predictive threat prevention.
- Developed dynamic live-malware demonstration methods; delivered technical expertise enabling expansion across 5 states.

Optiv (formerly Accuvant), Cincinnati, OH

Senior Solutions Engineer (Pre-sales) | 2009 – 2015

FY14: President's Club · FY13: #1 Account Team, President's Club · FY12: President's Club

- Delivered enterprise pre-sales engineering across a full cybersecurity product portfolio, supporting multimillion-dollar sales cycles through RFP responses, architecture sessions, and executive presentations.
- Led RFP responses, executive-level presentations, and technical architecture sessions.

FULL CAREER HISTORY

IBM (Internet Security Systems), Cincinnati, OH

Security Solutions Architect | 2007 – 2008

- Served as Solutions Architect for ISS following IBM acquisition, positioning the full ISS security portfolio across enterprise accounts in the Midwest region.

Consentry Networks, San Jose, CA

Consulting Systems Engineer | 2005 – 2007

- Consulting systems engineer for an early network access control startup. Worked directly with customers on NAC architecture, policy design, and deployment across complex enterprise environments.

Juniper Networks (NetScreen, OneSecure), New York, NY / Chicago, IL

Consulting Systems Engineer | 2002 – 2005

- Consulting systems engineer through the NetScreen acquisition by Juniper and the OneSecure integration. Supported enterprise firewall, VPN, and IDP deployments across financial services, healthcare, and government accounts.

SecureInfo Corporation, San Antonio, TX

Security Engineering Consultant | 2001 – 2002

- Security engineering consultant supporting federal government clients with compliance, risk assessment, and security architecture work.

Internet Security Systems, Chicago, IL

Systems Engineer | 2001

- Systems engineer supporting ISS intrusion detection and vulnerability management products across enterprise accounts in the Chicago region.

CNG Financial, Cincinnati, OH

Security Engineer | 1999 – 2001

- In-house security engineer responsible for firewall management, intrusion detection, security policy, and incident response across a multi-site environment.

DLP Technologies, Cincinnati, OH

Network Administrator | 1997 – 1999

- Network administrator responsible for infrastructure design, maintenance, and support. Early entry point into enterprise networking and security operations.

AI SYSTEMS PROJECTS

Independent work spanning agentic AI systems, autonomous infrastructure, and applied security tooling. Built and operated under Rook Dynamics since 2024.

- **AI Operations Platform (Rust):** Multi-tenant agentic orchestration platform with secrets management, CI/CD pipelines, and HashiCorp Vault integration across 21+ engineering phases.
- **Multi-Agent AI Infrastructure:** Five-agent system using Anthropic-native MCP tooling with dynamic tool discovery.
- **AI Security and Applied ML:** Isolated AI red team training enclave with vector DB integration, OWASP targets, and adversarial testing tooling.
- **Persistent Agent Daemon (Rust):** Multi-agent coordination daemon with PostgreSQL/pgvector for RAG and Python/SQLite context management for long-running agent state.
- **Browser Extension (TypeScript/WXT):** Automated text routing, IOC lookup, and indicator defanging with LLM integration.
- **Infrastructure and DevOps:** Full ESXi to Proxmox migration. Multi-node private lab orchestrated via MCP-based remote execution.

TECHNICAL PROFICIENCY

AI Engineering and Operations: Agentic AI, MCP, Claude Code, Anthropic SDK, RAG, Prompt Engineering, AI-SPM, LangGraph, OpenRouter, Prompt Injection Defense, Context Window Management, Agent Memory Architecture, LLM Routing, Multi-Agent Coordination

AI Project Stack: Rust (Axum, Tokio), TypeScript, React, Next.js, WXT, PostgreSQL, SQLite, Qdrant, pgvector, Ollama, Podman

Languages and Scripting: Python, Ruby / Rails, SQL, REST APIs

Infrastructure and DevOps: HashiCorp Vault, Docker, CI/CD, Proxmox / ESXi, Active Directory, DNS / DHCP, MySQL / MariaDB, Oracle DB, Infrastructure-as-Code, Git

Security Domains: NGFW, EDR / XDR / EPP, SIEM / XSIAM, SOAR / XSOAR, Zero Trust, CSPM / ASPM, Threat Intelligence, AI Red Teaming, Pen Testing, UEBA / ITDR

Platforms: Rocky Linux, RedHat, CentOS, Ubuntu, FreeBSD, OpenBSD, UnixWare, SCO Unix, Windows Server 2019+, Windows 10/11

MILITARY EXPERIENCE

United States Air Force Reserve, 906th Tactical Fighter Group

F-16 Weapons Systems Specialist (462x0) | 1989 – 1995

- Maintained and serviced F-16 aircraft weapon systems ensuring operational readiness.
- Held Secret clearance (expired).

REFERENCES

> *I've served as CISO of several large organizations. Wherever I go, I view Steve Richards as a trusted advisor and consider him a part of our team. His view of what is happening in the industry is both deep and broad and his focus on problem-solving is truly unique.*

Marc Yoder, Former CISO of Texas.gov and Texas Department of Transportation