WADE WOOLWINE
703-342-2416 | wade.woolwine@gmail.com | wadewoolwine.com

PROFESSIONAL SUMMARY

Product Security Leader & Distinguished Engineer with 20 years of experience bridging C-level strategy and code-level implementation. A hands-on practitioner who has founded $60M+ managed services and architected DevSecOps frameworks for 800+ engineers. Expert in operationalizing cutting-edge tech from defining early MDR methodologies at Mandiant to engineering autonomous AI agents today. Passionate about leading high-performance teams, writing code, and solving complex architectural challenges.

TECHNICAL SKILLS & LEADERSHIP

- **Security Architecture & DevSecOps**: Threat Modeling, Zero Trust, OWASP SAMM/DSOMM, Snyk, SonarQube, TruffleHog, Burp Suite Pro, GitHub Advanced Security, DefectDojo.
- **Cloud Native & Infrastructure**: AWS, GCP, Azure, Proxmox, Kubernetes (Talos Linux), Cilium (Networking/Service Mesh), GitLab, GitHub, Flux CD (GitOps), Docker, Terraform, Cloudflare Tunnels.
- **AI & Machine Learning Engineering**: Local LLM Hosting (vLLM, Ollama), Model Fine-tuning (SLMs), Computer Vision, MCP Server Development, Python (PyTorch/Pandas), Claude Code, Agentic workflows.
- **Executive Leadership**: Board Reporting, P&L Management ($60M ARR), ISO 27001/SOC2 Compliance, Team Development, Strategic Roadmap Planning, Coaching, Organizational Design.
- **Certifications**: (in progress) AWS Solutions Architect, AWS Security, DevSecOps Professional, DevSecOps Expert

PROFESSIONAL EXPERIENCE

RAPID7 | Boston, MA (Remote) | 2015 – Present
Senior Director of Product Security (Distinguished Engineer) & Deputy CISO | 2022 – Present

- **DevSecOps Architecture**: Architected the shift from traditional AppSec to DevSecOps for 800+ engineers across 7 product lines, implementing a custom governance model based on OWASP SAMM/DSOMM.
- **Engineering & Automation (Hands-On)**: Personally developed a CVE validation agent using Claude Code and Python that intercepts Snyk/SonarQube alerts, autonomously validates exploitability against the codebase, and automates risk adjustment.
- **Tooling Development**: Engineered a proprietary "Repository Trust Validator" web application to assess third-party dependency risks and deployed custom AI-driven tooling for automated threat modeling and vulnerability triage within the CI/CD pipeline.
- **Security Culture & Scale**: Established and led the "Security Champions" program, embedding 37 engineering leads across 7 product lines to decentralize security ownership, resulting in faster remediation cycles and widespread adoption of secure coding standards.
- **Interim CISO Leadership**: Served as Deputy CISO for 14 months, bridging three CISO transitions; managed the InfoSec program for a 2,500-person organization, briefed the Board of Directors, and maintained regulatory compliance (ISO 27001, SOC2, FedRAMP).

Principal Security Researcher (Threat Intelligence) | 2020 – 2022

- **Data Engineering & ML**: Developed a threat analysis pipeline using Python, PyTorch, and NLP to parse unstructured SOC analyst reports, map behaviors to the MITRE ATT&CK framework, and correlate findings

against petabytes of alert data in Amazon Athena/ELK.
- **Thought Leadership**: Produced the Rapid7 Quarterly Threat Report based on this analysis, directly supporting marketing campaigns and elevating the company's brand reputation through regular press interviews and webcasts.

Director & Founder, Managed Detection & Response (MDR) | 2015 – 2020

- **Zero-to-One Scale**: Founded and scaled the service to $60M ARR and 250+ customers in three years, designing the "vCISO" service model to provide strategic guidance to SMB executives.
- **Service Design & Strategy**: Defined the technical requirements and service architecture for the endpoint agent and rules engine, directing a small engineering team to build the proprietary detection stack while personally leading pre-sales, go-to-market strategy, and public evangelism.

INDEPENDENT RESEARCH & ENGINEERING (Home Lab) | Ongoing

- **Private Cloud Architecture (Proxmox/Talos)**: Designed a bare-metal cloud on 4U hardware (4x Tesla V100s) running Kubernetes on Talos Linux with Cilium. Implemented an enterprise-grade GitOps pipeline using Self-Hosted GitLab and Flux CD to automate security scanning (SAST/SCA) for all commits.
- **AI Agentic Workflows (MCP)**: Developed custom Model Context Protocol (MCP) servers to interface Claude Code with local infrastructure (Nginx/SonarQube), enabling natural language autonomous deployment. Engineered an app to fine-tune Small Language Models (SLMs) to map threat reports to MITRE ATT&CK.
- **Computer Vision**: Built a custom home automation integration intercepting Ring video, processing it through a custom-trained image classification model to trigger granular events in Home Assistant.

PREVIOUS EXPERIENCE

MANDIANT | Alexandria, VA | 2010 – 2014
Manager, Threat Analysis & Hunting / Threat Assessment Manager | 2012-2014

- **Elite Team Leadership**: Directed a team of Principal Analysts delivering advanced threat hunting against nation-state actors; selected as a speaker for Mandiant's annual conference (MIRcon) on advanced detection methodologies.
- **Executive Advisory (vCISO)**: Acted as a dedicated Virtual CISO for 20 enterprise clients, translating forensic findings into executive risk strategies and guiding Boards through post-breach remediation roadmaps.

Senior Threat Analyst (Founding Team, Managed Defense) | 2010 - 2012

- **Service Design**: As a founding analyst for Mandiant's Managed Defense, authored the technical service delivery methodology and SOPs for auditing environments using Mandiant Intelligent Response (MIR).
- **Forensic Operations**: Managed 30 simultaneous clients, bridging Incident Response and continuous monitoring to ensure zero recurrence of compromised assets.

EARLY CAREER OVERVIEW

- Senior Product Security Engineer | Aol | Dulles, VA | 2006 – 2010
- Cyber Threat Analyst | Mantech/Dept. Of State | Arlington, VA | 2004 – 2006