# NICHOLAS JAMES VIDAL

Portales, NM 88130
(618) 799-3850| Vidal@NicholasVidal.tech
https://www.linkedin.com/in/NicholasVidal/

## PROFESSIONAL SUMMARY

15 years of experience leading cyber defense strategy, incident response, and secure infrastructure design across complex enterprise environments. Proficient in DFIR, malware analysis, vulnerability management, and securing hybrid cloud systems in alignment with NIST, RMF, and FedRAMP frameworks. Hands-on expertise building automated DevSecOps pipelines, cloud security architectures, and AI-driven tools for threat detection, config auditing, and policy enforcement. Trusted leader in high-pressure environments, known for driving technical execution, leading red/blue team efforts, and translating risk into actionable outcomes for senior stakeholders.

- Digital Forensics
- Cloud Security
- Risk Mitigation
- Threat Hunting & Analysis
- Vulnerability Management
- Complex Problem Solving
- Cyber Incident Management
- SIEM Integration (Wazuh, Grafana)
- AI-Augmented & Auditing

## EDUCATION | CERTIFICATIONS

**Master of Science, Digital Forensics & Cyber Investigation** | University of Maryland Global Campus | 2026
**Bachelor of Science, Computer Networks & Cybersecurity**| University of Maryland Global Campus | 2023

**Certified Information Systems Security Professional (CISSP)** | (ISC)$^2$| Expected 9/2025
**CompTIA Security+ |** CompTIA
**CompTIA A+ |** CompTIA

## PROFESSIONAL EXPERIENCE

**United States Air Force | Various Domestic and Global Locations** **5/2006 – Present**
**Senior Cybersecurity Director | 8/2023 - Present**

- Spearhead cybersecurity strategy and operations, ensuring adherence to NIST and AFI standards across a multi-million-dollar network infrastructure.
- Lead a division-wide cyber defense initiative, coordinating cyber incident responses, risk assessments, and continuous threat monitoring.
- Serve as the executive point of contact for cybersecurity-related incidents, providing leadership during high-pressure situations to maintain secure network operations.
- Managed cybersecurity inspections and risk mitigation for critical IT systems using NIST SP 800-53 and SP 800-37 standards, enhancing the organization’s security posture.
- Conducted post-incident analysis, collaborating with cross-functional teams to drive process improvements and develop proactive defense measures.

**Cybersecurity Analyst | 8/2021 – 8/2023**

- Managed and secured 260 classified and unclassified cyber systems across 9 bases, supporting 46,000 users with mission-critical IT services.
- Led Defense Cyber Operations, implementing proactive security measures and responding to real-time cyber incidents to prevent further system breaches.

- Directed a $500K cybersecurity budget, allocating resources effectively to improve network security and incident response capabilities.
- Conducted incident analysis and remediation, ensuring compliance with cybersecurity frameworks and improving organizational readiness for cyber threats.

**Enterprise Communication Operations Lead | 6/2017 – 3/2021**

- Led the secure deployment of communication packages for a major U.S. Air Force network, collaborating with security teams to strengthen network defenses.
- Performed network security assessments and contributed to the implementation of secure VPN solutions, enabling robust communication for 400,000 simultaneous users.
- Assisted in the integration of advanced security technologies to enhance the security infrastructure and improve response times to potential threats.

**Senior IT Program Manager | 8/2006 – 6/2017**

- Managed complex IT programs focused on vulnerability management, system security, and cyber defense strategies across global Air Force bases.
- Led vulnerability management initiatives using advanced scanning tools like Retina and ACAS, performing incident response and reporting in compliance with IT security standards.
- Oversaw the management of SharePoint environments, ensuring the secure integration of IT systems and improving operational efficiency.

## CURRENT IT PROJECTS

**AI-Augmented DevSecOps & IaC Lab** **5/2025 – Present**

- Built a local AI-powered security automation framework using Ollama (Mistral model) and LangChain agents. Designed workflows to analyze and remediate YAML, IaC, and Docker misconfigurations. Integrated GitHub Actions for CI/CD pipeline security gates, including static analysis and secret scanning. Dashboard in progress to track IAM privilege drift, CVE exposure, and policy violations.

**Cyber Range Lab & Cloud Security Architecture** **3/2025 – Present**

- Built an enterprise-grade cyber range using Proxmox and pfSense to simulate red/blue team ops across segmented VLANs. Deployed Windows/Linux VMs for threat emulation and IR testing. Integrated Wazuh SIEM, with Grafana + InfluxDB in progress for live telemetry. Using AI agents to automate setup, config audits, and threat modeling. Expanding with a Pi-hole DNS firewall layer for DNS filtering and exfiltration defense.

**Cybersecurity CTF Development for eSports Students** **In Progress – 2025**

- Developing a hands-on cybersecurity training track for high school eSports students, blending CTF-style challenges with real-world skills like password cracking, forensics, and threat detection. Built in Docker-based labs with gamified scoring to boost engagement and teach fundamentals in a competitive format.

## TECHNICAL SKILLS

**Incident Response & Digital Forensics**: Malware Analysis, NIST SP 800-53, Incident Coordination
**Cybersecurity Tools**: Nmap, OpenVAS, SIEM, Zenmap, Encryption Technologies
**Network Security**: Firewall Management, IDS/IPS Systems, VPN Security
**Infrastructure & Cloud:** Proxmox, pfSense, VLANs, Windows/Linux, Terraform (basic), Docker
**Risk Management & Compliance**: NIST, AFI Standards, Vulnerability Assessment
**Security Awareness & Training**: Endpoint Security, Identity & Access Management (IAM)
**DevSecOps & Automation:** GitHub Actions CI/CD pipelines, OpenAPI + SDK integrations
**Local AI & Security Augmentation:** Ollama + Mistral LLM setup, AI agents using LangChain + CrewAI, YAML/config file auditing, AI-generated SAR/report templates, natural language remediation analysis.