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

PROFESSIONAL SUMMARY

Cybersecurity professional and United States Air Force Veteran with a Top-Secret SCI Clearance leveraging extensive leadership in developing and executing comprehensive cybersecurity strategies, enhancing network security, and managing complex incident response (IR) activities. Proficient in digital forensics and incident response (DFIR) with hands-on expertise in malware analysis, vulnerability assessments, and compliance with NIST and industry frameworks. Skilled in coordinating cyber defense operations, conducting thorough investigations, and delivering actionable insights for risk mitigation. Adept at working in high-pressure environments, collaborating with cross-functional teams, and providing clear communication to senior stakeholders.

- Digital Forensics
- Network Security
- Risk Mitigation
- Threat Hunting & Analysis
- Vulnerability Management
- Complex Problem Solving
- Cyber Incident Management
- Incident Response Automation
- Security Compliance & Frameworks

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 4/2025
Practical Network Penetration Tester (PNPT) | TCM Security | Expected 9/2025
CompTIA Security+ | CompTIA
CompTIA A+ | CompTIA

TECHNICAL COMPETENCIES

Vulnerability Assessment | Active Directory | Endpoint Security | OpenVas | Zenmap
Security Awareness Training | Patch Management Nmap | Encryption Technologies
Security Policies and Procedures Identify and Access Management (IAM)
Linux/Unix Windows System Administration

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.

IT PROJECTS

Nicholas Vidal Tech | https://NicholasVidal.tech **1/2024 – Present**

- Developed a professional cybersecurity website to showcase skills and projects, integrating security best practices for web development and hosting.

Virtualization on Raspberry Pi **4/2024 – Present**

- Configured ESXi on Raspberry Pi 4B to run multiple virtual machines, exploring cloud technologies and containerization through Docker, emphasizing hands-on cybersecurity techniques.

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
Operating Systems: Windows, Linux/Unix
Risk Management & Compliance: NIST, AFI Standards, Vulnerability Assessment
Security Awareness & Training: Endpoint Security, Identity & Access Management (IAM)