

WAYNE O. MCDONALD

Email: wayneomc@outlook.com

Location: Huntsville, Alabama

Availability: 100% Remote

Active Public Trust

LinkedIn: linkedin.com/in/wayne-mcdonald-113a79248

GitHub: github.com/anticybertech

Portfolio: wayneomcdonald.com

PROFESSIONAL SUMMARY

Accomplished Senior IT Leader with over 30+ years of progressive experience in cybersecurity, information technology, vulnerability management, and solution architecture. Proven expertise in enterprise security operations, risk management, and technical leadership. Demonstrated success in leading cross-functional teams, implementing security solutions, and managing complex IT infrastructure for government and commercial organizations.

Core Competencies:

- Cybersecurity Operations & Vulnerability Management
 - Information Security Analysis & Risk Assessment
 - Enterprise IT Infrastructure Management
 - Vulnerability & Patch Management, POA&M, ATO
 - Microsoft IIS, Microsoft SharePoint & Office 365
 - Team Leadership & Project Management
 - Government Contracting & Compliance
 - Network Security & Endpoint Protection
 - Penetration Testing & Offensive Tooling (Burp Suite, Metasploit, Nmap, Nuclei)
 - Solution Architect, Technical Proficient
 - AWS Cloud/Azure Cloud/Azure Key Vaults/Azure IAM
 - AI LLM, ChatGPT, Claude AI, Copilot, Replit
-

PROFESSIONAL EXPERIENCE

Information Security Administrator

MKS2 Technologies, LLC | January 2020 – August 2026

Department of Veterans Affairs ITOPS TSS Contractor providing enterprise information security oversight and technical expertise for the Veterans Medical Devices Specialized Device Cybersecurity Department (SDCD).

Key Achievements:

- Security oversight of vulnerability management for medical devices and special purpose systems protecting over 152,000 medical information systems
- Audit systems configuration to ensure compliance with established cybersecurity policies, STIGs, and standards
- Architect of comprehensive SharePoint enterprise site with vulnerability remediation guidance, video tutorials, and automated scripts serving 400+ biomedical engineers
- Architect of Python software application (Netstat Visual Tool, Vulnerability data parser tool) leveraging Netstat and PowerShell for network troubleshooting and port analysis. Develop ERA design tool to automate PowerPoint graphic icons for network/server/switches along with port & data flows
- Build AI-powered chat agent in Microsoft Copilot Studio, integrated with Microsoft Teams and sourced from SharePoint libraries and Excel worksheets. Delivers remediation guidance, how-to documentation, and PowerShell remediation scripts mapped to Tenable Nessus plugin IDs on demand
- Develop iWAR, a C#/.NET 8 WPF application for weekly activity reporting, with Excel export that builds a separate worksheet per user. Object-oriented design, ongoing refactoring and feature updates across releases
- Architect of Power BI dashboard for the VA 19 medical boundaries
- Utilize IBM/HCL BigFix web Reports for enterprise vulnerability reporting and stakeholder communication
- Conduct quarterly OWASP ZAP web application security assessments and vulnerability analysis
- Maintain and update security documentation, standard operating procedures (SOP)
- Armis Centrix (IoT/OT) Security Solution, Elasticsearch using KQL inside Kibana

- RedSeal, Splunk Search & Reporting platforms
- Microsoft Sentinel to collect data from cloud services, on-premises systems, endpoints, network devices
- Passive Vulnerability Scanning (PVS) process for thousands of VA medical devices that cannot be actively scanned
- Create monthly Nessus vulnerability packages for 147 VA medical site locations, provide formal and informal reports to HTM biomed technical teams, and track remediation efforts to closure
- Provide bi-weekly Enterprise Risk Management, POA&M, ATO reporting and daily Tenable Nessus vulnerability remediation summaries
- Perform risk analysis on medical devices using four key security indicators. Track POA&M on medical devices
- ServiceNow ticketing platform, CAM, VR

Lead Senior Systems Security Engineer

Ankore Consulting, Inc. | August 2015 – November 2019

Lead cybersecurity operations for Veterans Integrated Service Network (VISN7) Continuous Readiness in Information Security Program (CRISP RSS Contract) serving the Department of Veterans Affairs.

Key Achievements:

- Managed team of 7 security engineers supporting 54 CRISP contractors across three states
- Provided security oversight for 8 Veterans Affairs Medical Centers managing 31,100+ devices
- Achieved monthly vulnerability remediation rate of 13,500 vulnerabilities across enterprise infrastructure
- Implemented standardized security processes and technology configurations across VA enterprise
- Conducted comprehensive risk assessments and enforced IT security policies and baselines
- Developed and delivered vulnerability remediation status reports to governance boards

- Performed remote and on-site troubleshooting of government furnished equipment (GFE)
- Analyzed security logs, events, and incidents from multiple system sources
- Trained local IT specialists on VA remediation tools and security procedures
- Received recognition as top performer for customer-focused innovation

Project IT Technician

Precision Resources (Trimarc Group Inc.) | May 2015 – August 2015

Conducted on-site enterprise upgrades and configurations for major financial institutions including Regions Bank and Trustmark Bank.

Key Responsibilities:

- Performed Linux & Windows 7 Enterprise desktop and Windows Server 2008R2/2012R2 deployments
- Executed DoD 5220.22-M compliant hard disk wiping procedures
- Provided troubleshooting for commercial off-the-shelf software applications (COTS)
- Maintained detailed service documentation and client communication
- Delivered high-level on-site technical support and project consultation

Lead IT Specialist

Rapid Global Business Solutions, Inc. | August 2014 – April 2015

Led IT operations team managing network infrastructure, server administration, and end-user support.

Key Achievements:

- Supervised team of 2 IT specialists for comprehensive infrastructure management
- Managed enterprise security infrastructure including Symantec Endpoint Protection and PGP encryption
- Implemented security monitoring with Nagios and managed firewall configurations
- Monitor Linux servers with Nagios Core
- Manage enterprise SQL Server 2012, conduct weekly maintenance and backups
- Led security patch management using LANDesk Management Suite

- Conducted security assessments and vulnerability remediation

Systems Engineer

Randstad USA/Randstad Technologies, Inc. | October 2013 – January 2014

Implemented server infrastructure for Department of Navy C.A.N.E.S contract.

Key Responsibilities:

- Fulfilling Consolidated Afloat Networks and Enterprise Services (CANES) contract for the entire NAVY by upgrading cyber security, command and control, communications and intelligence (C4I) systems across the fleet.
- Deploy and configure Virtual machines using vSphere and VMware and vCenter Configuration Manager
Configuring, optimizing and securing SQL Databases using SQL Server 2008 R2
- Deployed Haivision encoding systems and Cisco networking equipment
- Managed Windows 2008, Unix/Linux operating systems and SAN configurations
- Executed application deployments and patch management using Microsoft SCCM 2012
- Create and update procedures in support of the CANES contract specifying in SMS, BVM, SHSA, ESX, Networker, FTS, SRC on CVN's, DDG's and LHD's

Senior IT Consultant

TABAM Innovations, LLC | January 2011 – October 2013

Key Achievement:

- Led testing and development of Try2See mobile application for Android and iOS platforms
- Designed QR code integration features enhancing user engagement and experience

IT Administrator/Manager & Security Operations Lead

Alabama A&M University Research Institute (AAMURI) | January 2003 – August 2010

Managed comprehensive cybersecurity and technical operations across Windows enterprise platform.

Key Achievements:

- Designed and implemented enterprise cybersecurity policies and procedures for 200+ users

- Managed security infrastructure including firewall configurations, IDS/IPS systems, and access controls
- Led security incident response and forensic investigations
- Conducted quarterly security assessments and vulnerability scans
- Implemented SSL certificate management and secure communication protocols
- Developed and enforced security policies for MS SQL Server 2000 and Exchange Environments
- Managed security aspects of Deltek Costpoint including role-based access controls

IT Manager

McSys Technology Corporation | November 1993 – December 2003

Designed and managed enterprise IT configurations and custom hardware solutions.

Key Achievements:

- Configured and integrated custom desktop, workstation, laptop, and server hardware
- Implemented Novell Netware, Microsoft Windows NT, IIS, and LAN/WAN wireless security
- Managed cybersecurity, vulnerability remediation, and mitigation strategies
- Developed enterprise IT systems supporting business operations
- Supervised team of 4 technicians and established client support contracts
- Researched and responded to RFQs and RFIs for government and educational institutions

Computer Technologist

Tupelo Public School District | June 1993 – October 1993

- Installed Apple hardware and software systems across entire school district
- Managed AppleTalk Network installation and administration
- Provided technical support and computer lab instruction

Manager Trainee

Tandy Corporation (Radio Shack) | February 1992 – June 1993

- Managed computer department sales and daily store operations
- Supervised team of 2 employees and achieved 100% project completion rate

Computer Lab Technician

Huntsville City Schools | August 1989 – June 1991

- Maintained computer systems and provided training to students and teachers
 - Ensured smooth computer lab operations and technical troubleshooting
-

EDUCATION

Bachelor of Science in Computer Science (Pursued)

Alabama A&M University, Normal, AL

Advanced Cybersecurity Program Certificate (In Progress)

Stanford University School of Engineering, Professional Education

Completed Coursework:

- XCS100 - Introduction to Web Security
- XACS100 - Advanced Cybersecurity Program Preview
- XEE100 - Introduction to Internet of Things
- XACS101 - Foundation of Information Security

Cisco Networking Academy Certifications:

- Networking Devices and Initial Configuration
 - Cisco Packet Tracer
 - Networking Essentials
 - Introduction to Cybersecurity
 - Cybersecurity Pathway
 - Cyber Threat Management
 - Network Defense
 - Endpoint Security
-

CERTIFICATIONS

Current Certifications:

- Cisco Certified Support Technician Cybersecurity (CCST)
- CompTIA Server+ CE Certification
- Armis Centrix™ Foundations Certified
- Armis Centrix™ Medical Device Security Foundations Certified
- Scrum Fundamentals Certified (SFC)
- Business Analysis Fundamentals with AI Certified
- IBM Artificial Intelligence Fundamentals
- IBM Cybersecurity Fundamentals
- Fortinet NSE Level 1/2/3 Network Security Expert
- Fortinet Certified Cybersecurity Associate
- Tenable Nessus Fundamentals Certification
- Tenable Nessus Expert Advanced Certification
- Qualys Certified Specialist - Vulnerability Management
- Qualys Certified Specialist - Patch Management
- VA Enterprise Mission Assurance Support Service (eMASS)

In Progress:

- CompTIA Security+ Certification
- Microsoft Azure Fundamentals Certification (MPC)
- AWS Cloud Practitioner

Additional Training:

- Pearson VUE Cybersecurity Certification
- StationX Nmap Ethical Hacking Course
- Microsoft Pre-Installation Specialist (Windows 98/XP/Windows NT Server)
- Symantec Sales Expert Plus Endpoint Solutions

TECHNICAL SKILLS

Security Tools & Platforms:

- Tenable Nessus, Qualys VMDR, IBM/HCL BigFix, OpenVAS
- Burp Suite, Metasploit, Nmap, Nuclei, OWASP ZAP
- Armis Centrix, RedSeal, Forescout
- Splunk, OWASP ZAP, Symantec Endpoint Protection, Microsoft Defender EDR
- Tenable Nessus Vulnerability Management

Operating Systems:

- Windows Server (2003/2008/2012/2016/2019/2022/2025), Windows 7/10/11
- Linux/Unix, VMware ESXi, Novell Netware

Networking & Infrastructure:

- Cisco Networking (Catalyst, ISE, Unified Communications)
- TCP/IP, DNS, DHCP, WINS, VPN Configuration
- Storage Area Networks (SAN), Network Attached Storage (NAS)
- Wireless Security, Fiber Connectivity

Development & Scripting:

- C#/.NET 8 (WPF, Office/Excel automation), Python, PowerShell, Batch Scripting
- SharePoint Development, Web Development, Power BI
- Database Management (SQL Server, MySQL)

Project Management:

- Microsoft SCCM, LANDesk Management Suite
- ServiceNow, CA Service Desk Manager
- Deltek Costpoint, IBM Cognos Business Intelligence

PROFESSIONAL AFFILIATIONS

- IEEE Computer Society
- Cyber Huntsville Alabama

PERSONAL PROJECTS & PLATFORMS

Independently design, build, and manage 15+ production cybersecurity and technology web platforms, handling full-stack architecture, security hardening, and ongoing operations:

- Cybersecurity scanning & threat intelligence: wincyberscan.com, spatcyber.com, urlcybersecurity.com, cybertaip.com, jextscanner.com, dark27web.com
- Consumer security awareness & resources: top8cyber.com, fyicyber.com, antibodycyber.com
- Privacy & compliance tooling: cookieft.com
- Security Operations Center services: socsoutheast.com, socbama.com
- Specialized/vertical platforms: medfda.watch (medical device security advisories), sixty3energy.com (health & wellness), mcsystech.com (IT services)
- Professional portfolio: wayneomcdonald.com