Kevin McCarthy

kdmcyber00@gmail.com | kdmcyber.com | linkedin.com/in/kev-mac

Education

Rochester Institute of Technology Rochester, NY
Bachelor of Science in Cybersecurity Expected: Dec 2026

Experience

Lockheed Martin: *Cyber Systems Engineer Intern* Jun 2026 – Present

- Integrated NIST 800-53 security controls into system designs, authoring System Security Plans (SSPs) and Plans of Action & Milestones (POA&Ms) to obtain Authorization to Operate (ATO).
- Conducted STIG compliance scans, documented and remediated findings, and automated evidence collection to accelerate ATO approvals.
- Collaborated with key stakeholders to develop and align security control implementation strategies.

Technical Skills

Windows, Windows Server, Linux (RHEL/Debian), pfSense, Azure, Proxmox VE, KVM/libvirt, Active Directory, DNS/DHCP, Group Policy, VLAN Segmentation, Wazuh, Nmap, Metasploit, Burp Suite, Wireshark, Autopsy, NIST 800-53, RMF, STIGs, CIS Benchmarks, NIST CSF, Python, PowerShell, Bash, Git

Projects

Multi-Platform Cloud Infrastructure: *Cloud & Virtualization Engineer* Apr 2026

- Engineered a cloud and virtualization infrastructure suite across four lab environments, applying IaC, high availability, and Zero Trust principles across Azure, Proxmox VE, and KVM/libvirt.

Risk-Based Authentication Literature Review: *Contributing Author* May 2025

- Co-authored a systematic literature review on Risk-Based Authentication (RBA), evaluating machine-learning risk scoring, deployment challenges, and security-usability-privacy trade-offs.

Healthcare DR/BCP Technology Assessment: *Contributing Author* Dec 2025

- Co-authored a technology risk assessment on Identity, AI, Quantum Computing, and Cloud adoption for disaster recovery and business continuity; led the Cloud Computing analysis.

Segmented Enterprise Network: *Network & Systems Architect* Dec 2025

- Architected and deployed a segmented, two-VLAN enterprise network on Proxmox, integrating Windows Server 2022 (AD, DNS, DHCP) with RHEL 10 systems for web, database, and file/print services.
- Hardened all hosts against CIS Benchmarks and configured Wazuh for centralized log aggregation and threat detection across the environment.

Virtual Domain & Network Infrastructure: *Server Administrator* Dec 2024

- Established and managed core Windows Server infrastructure (Active Directory, DHCP, DNS, pfSense) to support Windows and Linux clients, including user, OU, and GPO management.
- Deployed a secure Apache web server with SSL/TLS encryption and configured a vsftpd server, evaluating rsync, FTP, Samba, and NFS protocols for secure file sharing.

Extra-Curricular Activities

RITSEC (Cybersecurity Club): *Active Member* Aug 2023 – Present

- Conducted mentorship-guided forensic analysis with Autopsy and applied the MITRE ATT&CK framework in adversarial emulation exercises.
- Contributed to building RIT's internal competitions, developing logging infrastructure and designing King of the Hill (KoTH) style challenges.

University at Buffalo Lockdown: *1st Place – Windows Incident Response Analyst & CTF Lead* Feb 2025

- Led Windows incident response, recovering compromised systems and implementing automated PowerShell scripts to streamline remediation.

CORA II: *1st Place – Penetration Testing Analyst* Oct 2024

- Discovered, exploited, and remediated critical web vulnerabilities (time-based SQLi, persistent XSS) using Nmap, Burp Suite, and Metasploit.