Kevin Landry

Spotsylvania, VA | 4406709866 | kevinlandrycyber@gmail.com
linkedin.com/in/kevinlandrycyber | github.com/DadOpsMateoMaddox | sitbackandattack.com

CYBERSECURITY PROFILE

Accomplished cybersecurity professional with over 20 years of combined military and technical experience securing critical defense and enterprise networks. Expert in network security operations, threat detection, and incident response with deep proficiency in Linux system administration, SIEM platforms, and Pythondriven SOC automation. Recognized nationally through U.S. Cyber Challenge and Commonwealth Cyber Initiative programs for excellence in cyber defense. Proven track record supporting DoD and Intelligence Community missions with active U.S. citizenship and prior TopSecret communications access. Experienced in classified and compartmented environments, aligning with DoD 8570 and FedRAMP compliance.

CORE TECHNICAL COMPETENCIES

- **Network Security & Analysis:** Packet analysis (Wireshark, Zeek), network forensics, intrusion detection (IDS/IPS), firewall configuration, protocol analysis
- **Security Operations:** Threat hunting, incident response, log analysis, SIEM operations (Splunk SPL, QRadar, Elastic Stack), EDR deployment
- **Frameworks & Standards:** NIST 80053, NIST Cybersecurity Framework, MITRE ATT&CK, CIS Controls, DoD RMF
- **Linux & Systems:** RHEL administration and hardening, Ubuntu, system virtualization, scripting automation
- **Programming & Automation:** Python, Bash, PowerShell, YAML/JSON, SQL querying, SOC automation pipelines
- **Cloud & Infrastructure:** AWS, Azure, GCP security architecture, VMware, Docker, Kubernetes, Terraform
- **Security Tooling:** Vulnerability assessment (Nessus, Burp Suite), malware analysis, reverse engineering, Shodan API, VirusTotal integration

PROFESSIONAL EXPERIENCE

U.S. Cyber Challenge | Teaching Assistant & Cyber Researcher — Remote

June 2025 – Present

- Delivered handson technical training in Linux/Windows forensics, cyber threat intelligence, incident response, malware analysis, and CTF strategy to 100+ national participants
- Guided live analysis of memory dumps, packet captures (PCAPs), and malware samples using Autopsy, Volatility, Wireshark, and industrystandard forensic tools
- Designed forensic and incident response scenarios for national CTF competitions and advanced training programs
- Contributed to opensource threat actor profiling and CTI workflows integrating MITRE ATT&CK framework mappings

Peraton Labs | Cybersecurity Apprentice / Software Developer (Research) — Reston, VA

September 2024 – November 2024

- Enhanced adversarial AI hardening frameworks through RF signal analysis and ML simulation testing, increasing model accuracy by 75% and visualizing anomalies in Power BI dashboards
- Participated in Agile research sprints and stakeholder briefings translating technical results into actionable cybersecurity insights

Independent Cybersecurity Researcher / Developer — Spotsylvania, VA

2011 – Present

- Architected distributed honeypot mesh (Cowriebased) deployed on AWS for realtime adversary tracking with AIdriven alerting and threatintel correlation
- Built Pythondriven SOC automation pipelines enriching attacker sessions with VirusTotal and Shodan data, reducing manual triage time by 40%
- Implemented mock SIEM dashboards with Splunk and Elastic Stack for testing SOC workflow efficiency and alert tuning
- Authored detection and response playbooks aligned with MITRE ATT&CK techniques and NIST incident response lifecycle stages
- Maintains active GitHub portfolio of network security automation scripts, forensic utilities, and threat intelligence research projects

United States Coast Guard | Operations Specialist 1st Class (CMCO / Crypto Custodian)

July 2002 – January 2011 | Worldwide Deployments

- Managed Top Secret communications systems and encryption keying materials across multiple operational theaters with zero security incidents over 9 years
- Directed secure multiagency communications (FBI, ICE, CBP, CGIS, FURA) ensuring uninterrupted data integrity under combat and emergency conditions
- Supervised and trained 15 junior operators per shift; recognized for leadership excellence and mission readiness
- Awards: Coast Guard Achievement Medal, GWOT Expeditionary Medal (Iraq), Humanitarian Service Medal, Special Ops Ribbon, Good Conduct (×2)

KEY PROJECTS

CerberusMesh — Distributed Threat Intelligence Platform

- Engineered automated system for subsecond threat correlation across 10+ TB network logs using ML pattern detection and SOAR integration, enabling 80% faster incident response for simulated SOC environments

HoneyBomb — Cyber Deception Framework

- Developed honeypot deployment suite integrating Python and Cowrie to simulate network environments, generate security alerts, and capture adversary tactics. Improved analyst training efficiency and playbook coverage by 40%

EDUCATION

Master of Science | Applied Information Technology – Cybersecurity

George Mason University – Fairfax, VA | Expected May 2026

Bachelor of Science | Computer Science – Cybersecurity

University of Mary Washington – Fredericksburg, VA | May 2025 | Cum Laude (GPA 3.55)

CERTIFICATIONS

- CompTIA Security+ (CE) December 2024
- Google Professional Cybersecurity Certificate December 2024
- Red Hat Enterprise Linux I May 2025
- CompTIA CySA+ In Progress
- Ethical Hacker Essentials (EHE) — In Progress

CLEARANCE & ACHIEVEMENTS

- Active U.S. Citizenship with prior Top Secret communications access (USCG)
- U.S. Cyber Challenge Cyber Bowl East (2025): 2nd place nationwide among advanced CTF participants
- USCC Cyber West Teaching Assistant (2025): Mentored 100+ students in forensics and incident response
- NSWC Dahlgren CRAM Competition (2024): 4th place for realtime malware triage solutions
- Commonwealth Cyber Initiative (CCINOVA) Trainee (2024): Selected for advanced training cohort