

Christian Coleman

Warrenton, VA

(540) 878-8143

chrisacoleman23@gmail.com | [LinkedIn](#)

PROFESSIONAL SUMMARY

Cybersecurity professional with DoD Secret Clearance and hands-on experience in threat detection, incident response, and enterprise systems administration. Proven experience working in agile environments with requirements development and system integration capabilities.

SKILLS

- Security Tools: CrowdStrike EDR, IBM QRadar, Microsoft Defender, Nessus, Rapid7 Nexspose, ServiceNow, Splunk
- Virtualization & Cloud: AWS, Azure, Hyper-V, VirtualBox, VMware
- Programming & Automation: Python, PowerShell, SQL
- Operating Systems: Kali Linux, Rocky Linux, Windows Server, Ubuntu
- Compliance & Frameworks: CIS Benchmarks, DISA STIGs, DoD Risk Management Framework, ISO 27001

EXPERIENCE

Old Dominion University – Security Analyst

Norfolk, VA (08/2025 – Current)

- Analyzing CrowdStrike alerts for potential malicious activity and security threats, maintaining over 85% resolution accuracy across enterprise endpoint detection and response operations.
- Triaging and investigating 220+ monthly phishing alerts with a 1-minute MTTA and 20-minute MTTR using Microsoft Defender for email threat mitigation.
- Supervising 7 SOC analysts in weekly operations including phishing alert triage, threat detection training, and incident response procedures.
- Managing Palo Alto Panorama firewall processing 10+ weekly ServiceNow tickets for security rule changes, access control modifications, and enterprise network policy enforcement.

Commonwealth Cyber Initiative Coastal Virginia (COVA CCI) – Security Researcher

Norfolk, VA (08/2025 – 11/2025)

- Developed behavioral detection methodology for identifying vulnerabilities in Model Context Protocol (MCP) servers, focusing on security risks in AI-powered development environments.
- Presented research findings on AI infrastructure security to cybersecurity professionals and academic stakeholders at COVA CCI conference.

Deloitte – Cyber Summer Scholar

Arlington, VA (06/2025 – 07/2025)

- Built 3-box Rocky Linux 9 IDS environment with Snort and centralized rsyslog, supporting integrated security solutions for state government clients.
- Analyzed security events in IBM QRadar for compliance with government security policies.
- Conducted vulnerability assessments using TenableSC and Nessus scanning platforms, analyzing scan results and prioritizing remediation efforts

Old Dominion University – IT Security Intern

Norfolk, VA (10/2024 – 05/2025)

- Processed DMCA violations by examining network logs and identifying responsible IP/MAC addresses.
- Supported 24x7 security operations including log analysis, incident triage, and threat investigation procedures

Mission Technologies – System Administrator Intern

Newport News, VA (05/2024 – 11/2024)

- Administered Hyper-V virtualization infrastructure supporting server deployment and resource management
- Administered Active Directory for 500+ users with automated provisioning and group policy management.
- Conducted STIG (Security Technical Implementation Guide) compliance assessments on Windows Server environments, ensuring adherence to DoD security configuration standards.

Certifications:

CompTIA Security +
Certified Ethical Hacker

RMF Curriculum
AWS Certified Cloud Practitioner

PROJECTS

CIS Benchmark Infrastructure Assessment (September 2025 - Present): Configured automated CIS policy compliance scanning across university Linux server infrastructure using Rapid7 Nexpose, analyzing security posture gaps and developing standardized remediation workflows for enterprise-wide security baseline enforcement.

Multi-Node IDS Lab (June 2025): Deployed Snort intrusion detection system with dual-stream rsyslog centralized logging across 3 Rocky Linux servers, achieving real-time network monitoring and hostname-based log organization for enterprise security infrastructure.

EDUCATION

Cybersecurity - Bachelor of Science
Old Dominion University (May 2026)