Christian Coleman
Secret Clearance
Warrenton, VA
(540) 878-8143 | chrisacoleman23@gmail.com | LinkedIn

SKILLS

- **Security Operations**: CrowdStrike EDR, IBM QRadar, Microsoft Defender, Microsoft Sentinel, Palo Alto Panorama, ServiceNow, Snort IDS, Varonis
- **Cloud & Infrastructure**: AWS, Azure, Active Directory, Azure AD, Linux (Rocky & Kali), Windows Server
- **Compliance & Frameworks**: CIS Benchmarks, DISA STIGs, DoD Risk Management Framework, MITRE ATT&CK, NIST 800-53, SCAP, Nessus, Rapid7 InsightVM
- **Scripting & Automation**: Python, PowerShell, Bash, KQL

CERTIFICATIONS

CompTIA Security+ | Certified Ethical Hacker (CEH) | DoD RMF Certificate

EXPERIENCE

Old Dominion University – Security Analyst
Norfolk, VA (08/2025 – Current)

- Investigate security incidents using CrowdStrike EDR and Microsoft Defender, analyzing endpoint security data across 25,000+ endpoints and mapping threats to MITRE ATT&CK framework for threat intelligence reporting.
- Triage 220+ monthly phishing alerts using Microsoft Defender, maintaining 1-minute acknowledgment and 20-minute resolution SLAs.
- Lead team of 7 student SOC analysts, conducting weekly training on phishing triage, threat detection, and incident response procedures.
- Manage security infrastructure including 30+ weekly Panorama firewall requests via ServiceNow.

Commonwealth Cyber Initiative Coastal Virginia (COVA CCI) – Undergraduate AI Researcher
Norfolk, VA (08/2025 – 11/2025)

- Researched security vulnerabilities in AI development tools (MCP servers) and presented findings on behavioral detection methods at COVA CCI showcase.

Deloitte – Cyber Summer Scholar
Arlington, VA (06/2025 – 07/2025)

- Deployed 3-node Rocky Linux 9 IDS infrastructure environment with Snort IDS for network threat detection and centralized rsyslog for state government client.
- Analyzed 100+ weekly security events in IBM QRadar, correlating alerts with MITRE ATT&CK techniques to identify attack patterns.

Old Dominion University – IT Security Intern
Norfolk, VA (10/2024 – 05/2025)

- Investigated 50+ DMCA violation reports by correlating network logs to identify responsible endpoints.
- Detected and investigated MFA bypass attempts by analyzing Duo Mobile logs and Azure AD sign-in activity for 25,000+ users.

Mission Technologies – System Administrator Intern
Newport News, VA (05/2024 – 11/2024)

- Managed Active Directory for 500+ users including automated account provisioning and group policy.
- Performed SCAP scans on 50+ DoD terminals and remediated findings to maintain 95% DISA STIG compliance.

PROJECTS

Azure Sentinel Detection Engineering (02/2026**):** Engineered a cloud-native SIEM deployment with custom KQL detection rules to identify identity-based attacks including password spraying and privilege escalation.
AI-Powered Cloud Threat Analysis Pipeline (11/2025**):** Deployed automated incident response system using Amazon Bedrock, S3, DynamoDB, SNS, Lambda, and EventBridge to process GuardDuty findings and generate AI-powered incident summaries.

EDUCATION

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