Resume

Kobe Coleman
Phone Number: 757-338-4398
Email: Kobe.coleman227@gmail.com
Clearance Level: TOP SECRET (TS)//Special Intelligence (SI)//TALENT-KEYHOLE (TK) (Since August 2022)

Executive Summary

- **Risk Management Framework (RMF)**
- **Software/Tools**: SEAR, Splunk, Nessus, Biscotti, Kali Linux
- **Scholarship For Service Scholar**

Certifications

- Security +
- AWS CCP
- Certified Ethical Hacker

Degrees

- B.S. in Cyber Security and minor in Cyber Crime at Old Dominion University

---

Honors and Awards

- Dean's List 2021 – current

Work Experience

NSA ISSO/ISSE Intern August 2022-December 2022

- In Accordance with (IAW) ICD 503, supported the Information System Owner (ISO) through the Risk Management Framework (RMF) steps for ATO and Re-Authorizations of Information Systems (ISs)
- Ensured that the government policies and procedures are followed to protect the Confidentiality, Integrity, Availability (CIA) of the IS
- Assisted in creating the SECONOP, Privileged User Guide (PUG), and Contingency Plan
- Worked with RMF ISSE to Complete the Security Controls Traceability Matrix (SCTM)
- Reviewed and updated System Security Plans (SSPs) in XCATA to reflect system changes
- Conducted Self-testing with System Administrators (SAs) and System Engineers (SEs)
- Prepared Pre-SCA Analysis (PSA)
- Utilized NESSUS to review vulnerability and compliance scans
- Acknowledged SEAR and Splunk audit logs daily and worked with SAs to investigate any findings or anomalies
- Conducted Continuous Monitoring activities for all ATO'd Systems on behalf of the ISO, to ensure continued compliance

- Racked and Unrack servers and switches
- Cabled switches as well as host Ips

NSA System Vulnerability Analyst May 2023-August 2023

- Performed Analysis of U.S. Government Unclassified Communications
- From an adversarial perspective, identify and reported instances of disclosures of sensitive information and possible network vulnerabilities in relation to customers' critical information lists.
- Participated in weekly research reports with small teams.
- Researched current cyber-related news and vulnerabilities for team to review. Once topic was selected for the week, used low-side and high-side resources to further research the topic, and used tools to search for instances of topic in our customers' traffic.
- Participated in bi-weekly cyber syncs with cyber team.