

# Joshua Russell

Norfolk, Virginia 23502

[jmrussell202@gmail.com](mailto:jmrussell202@gmail.com) | (202)-471-0545 | [jruss020@odu.edu](mailto:jruss020@odu.edu)

## Objective

My objective is to obtain a career in the areas of penetration testing, risk assessment, risk analysis, and risk management. By assessing the risks and analyzing their potential impacts, I would be able to display, through penetration testing, how the threats and weaknesses can be exploited for gains by malicious actors. After which, I can provide organizations with the proper tools to manage the risks, reduce harms associated with them, and mitigate attacks against their assets.

## Education

*Old Dominion University*, Norfolk, Virginia (08/2023 – Anticipated date 05/2025)

Bachelor of Science in Cybersecurity

GPA: 3.96

Dean's List: Fall 2023, Spring 2024, Fall 2025

*Tidewater Community College*, Virginia Beach, Virginia (01/2021 – 12/2022)

Associate of Applied Science in Cybersecurity, Summa Cum Laude

GPA: 3.894

Dean's List: Spring 2021

President's List: Fall 2021, Spring 2022, Fall 2022

## Experience

Valor Cybersecurity, Norfolk, Virginia (1/2025-05/2025)

*Intern*

- Provide local small business free cybersecurity risk assessments
- Utilize Valor Cybersecurity's Top 10 Digital Security Checklist to assess cybersecurity postures, policies, and procedures
- Analyze risk assessments for gaps in people, operations, and technology
- Analyze cybersecurity efforts using a SWOT Analysis
- Formulated recommendations using SWOT Analysis

CM Technology Inc., Surry, Virginia (1/2025-5/2025)

*Intern, Research Lead*

- Perform comprehensive SWOT Analysis

- Perform risk assessment and analysis for private sector SATCOM provider
- Utilize NIST CSF 2.0 and NIST 800-171 frameworks to create best practices for cybersecurity efforts
- Analyze cybersecurity efforts using a SWOT Analysis
- Formulated recommendations based on SWOT Analysis
- Created an employee training program, best practices guidelines, Continuity of Operations Plan, and a software improvement plan

## **Related Experience**

CyberForge Capture the Flag (CTF) Challenge (04/2022, 03/2025)

- Identify network details by using sniffing tools and commands in the terminal
- Perform packet sniffing using Wireshark and command line tools
- Execution and reconnaissance of social engineering attacks and spear fishing campaigns
- Solve cryptographic challenges based on cyphers, hashes, and encryption
- Forensic analysis of data gathered via social engineering and packet/network sniffing
- Perform penetration testing through command line interfacing

## **Skills**

- |  |  |
|--|--|
| • Linux / Unix (Ubuntu, Kali)                      | • Virtual Private Networks (VPN) setup and maintenance   |
| • Python/PyCharm                                   | • Firewall setup and maintenance   |
| • Microsoft PowerShell                             | • Utilization of network security tools (Aircrack, Tcpdump, John the Ripper, Metasploit, Nessus, Snort, Cain and Abel) |
| • Virtualization (Oracle Virtual Box, VMware)      | • Risk Assessment and Management   |
| • Wireshark packet sniffing and analysis           |  |
| • CISCO Networking Hardware (Routers and Switches) |  |
| • CISCO Networking Software (Packet Tracer)        |  |

## **Organizations**

Tau Sigma National Honors Society

PTK Phi Theta Kappa International Honors Society

CS2A Cyber Security Students Association of Old Dominion University