

Personal Narrative Essay

Jalen Walker

IDS 493 Electronic Portfolio Project

Professor Andrews

28 March 2026

Introduction

My name is Jalen Walker. I am a cybersecurity major at Old Dominion University, and I will be graduating this spring on May 16th. I decided to study cybersecurity because I have always been interested in technology since I was a kid. I knew technology would continue to advance and grow over the years, and I wanted to be part of that field. My real introduction to the field started in high school when my dad placed me into a computer science class. At first, I was confused because I thought it was going to be a traditional science class, which I wasn't very interested in. Once I realized it was more technical and focused on computers, I became interested and started learning more about cybersecurity.

What interests me the most about cybersecurity is that it requires problem solving every day. It almost feels like working on a puzzle that you have to figure out and complete. The problems you solve can help protect people, companies, and organizations from cyber threats. I also enjoy helping others understand good cyber hygiene because preventing problems is just as important as solving them. If people understand how to protect themselves online, it can reduce the number of security incidents that cybersecurity professionals have to respond to.

Right now, I am most interested in a Security Analyst role or anything related to security operations. This is where I gained my first real experience and where I learned about different areas of cybersecurity. During my degree I have developed both soft skills and technical skills. My soft skills include communication, public speaking, and preparing presentations. My technical skills include incident response, alert triage, and security investigations. I have also had the opportunity to use real industry tools such as CrowdStrike and IBM QRadar. Cybersecurity is

meaningful to me because it allows professionals to protect systems and make the digital world a safer place.

Key Experiences That Shaped My Path

One of the most important experiences during my academic journey has been my SOC internship at Old Dominion University. This internship is part of a first-year program where seven students were selected to work as security analyst interns on campus. We work about ten hours per week in person in Norfolk, Virginia. During this internship we handle many different types of security tasks including investigating phishing emails, reviewing risky user alerts, responding to firewall tickets, and analyzing alerts from tools like CrowdStrike.

Throughout the internship I have worked on different types of investigations ranging from low-level alerts to more serious incidents. At the beginning of the internship we mainly handled lower priority alerts while learning the systems and tools. As we gained more experience, we started working on more complex and higher priority alerts. Some of the tools we regularly use include Rapid7, Palo Alto firewalls, Microsoft Defender, and IBM QRadar SIEM. This internship gave me the opportunity to see how a real cybersecurity team operates. It helped me understand the responsibilities and expectations that come with working in a security operations center and gave me valuable experience before entering the workforce.

My coursework at Old Dominion University has also played a major role in developing my cybersecurity knowledge. Some of the classes that had the biggest impact on me were Microsoft Windows System Management and Security, Linux, and Cybersecurity Techniques and Operations. The Microsoft course especially helped me see cybersecurity from a different perspective because of how the professor explained the concepts and real-world applications.

The Linux and operations courses helped me strengthen my technical skills before gaining real work experience.

Several lab assignments also helped deepen my understanding of cybersecurity. For example, I completed a client-server programming lab that I was able to add to my resume. I also participated in an ethical hacking lab where I used industry tools like Metasploit and Wireshark. These hands-on experiences allowed me to practice analyzing systems and identifying vulnerabilities in a controlled environment.

In addition to coursework and my internship, I have also completed several cybersecurity projects. One project was a RAG SOC Assistant designed to help answer incident response questions using trusted sources such as NIST, CISA, and MITRE ATT&CK. Another project was an AI-powered cloud threat analysis pipeline that automated the processing of GuardDuty security findings. One of my most impactful projects was the Secure Cloud Services and AI Deployment Project. The goal of this project was to develop a stronger understanding of AWS and cloud security.

During this project I used several AWS technologies including IAM, VPC, EC2, GuardDuty, and WAF. I also worked with Infrastructure as Code technologies such as Terraform or CloudFormation. This project helped me learn important concepts like least privilege access, identity and access management, and cloud security monitoring. It introduced me to how cloud environments are secured and monitored in modern cybersecurity environments.

What I Learned Along the Way

Throughout my degree program I have developed many technical and professional skills. My coursework and internship helped me gain experience in areas such as incident response, threat hunting, security monitoring, and documentation. I also gained hands-on experience using industry tools including CrowdStrike, IBM QRadar, Rapid7, Microsoft Defender, Varonis, and Palo Alto firewalls. These tools are widely used in the cybersecurity industry and helped me understand how security teams detect and respond to threats.

One challenge I faced while learning cybersecurity was accepting that I would make mistakes while learning. Early on I realized that cybersecurity involves a lot of trial and error, and sometimes you will be wrong before you find the correct answer. Instead of letting that discourage me, I learned to ask questions, stay persistent, and keep trying until I understood the problem. This mindset helped me continue improving and gaining confidence in my skills.

My SOC internship taught me many important lessons about working in cybersecurity. I learned how important the work is and how much responsibility comes with investigating security incidents. I also learned how to communicate professionally, present findings, and maintain integrity in the work I do. In cybersecurity, your name is attached to your analysis and reports, so accuracy and honesty are extremely important.

Gaining hands-on experience also changed my view of cybersecurity in a positive way. At first it felt overwhelming because I did not fully understand what to expect. However, once I started gaining experience and understanding the tools and processes, I realized that this is something I enjoy doing and want to continue improving at. I also developed many professional skills including communication, teamwork, documentation, and participating in meetings and technical discussions. One thing that surprised me the most about cybersecurity work is how much you

think about the problems even after leaving work. Because I am detail-oriented, I often continue thinking about ways to improve my work and minimize mistakes.

Where I Am Headed

After graduation I would like to continue working in a security-focused role. My experience as a SOC analyst intern allowed me to develop strong foundational skills in security operations, and it also introduced me to several different areas within cybersecurity such as GRC, cloud security, security engineering, and networking. Because of that exposure, I feel that starting my career in a Security Analyst role would allow me to continue building my technical foundation.

What I enjoy most about cybersecurity is that it constantly challenges me to grow and learn. Technology is always evolving, which means cybersecurity professionals must continue learning and adapting. I enjoy solving problems that help protect organizations and individuals from cyber threats. One area that I would like to focus on in the future is reducing phishing attacks, since phishing continues to be one of the most common cybersecurity risks.

In terms of industries, I am interested in both government and private sector opportunities. I would eventually like to obtain a security clearance, which is common in government cybersecurity roles. However, I am also open to working in private industry where cybersecurity teams protect large organizations and infrastructure.

Looking ahead, I want to continue improving my security operations skills while also expanding my knowledge of cloud security. My internship helped me develop strong security investigation skills, and my cloud projects introduced me to AWS environments. My goal is to combine those

two areas and continue developing skills in cloud security. I also plan to pursue additional certifications in the future including the CySA+ certification and eventually the CISSP once I meet the required experience level. I currently hold the CompTIA Security+ and the AWS Certified Cloud Practitioner certifications.

When it comes to the type of work environment I prefer, I am open to remote work but I prefer a hybrid or on-site environment. I learn best when I can collaborate with others in person, ask questions directly, and observe how experienced professionals solve problems. Being able to interact with teammates helps me grow and develop my skills more quickly.

Cybersecurity work is important to me because it allows me to stay engaged in a field that continues to grow and evolve. I have always enjoyed working with computers and technology, and cybersecurity allows me to use those interests in a way that helps protect people and organizations. I care about helping others and making a positive impact, and cybersecurity gives me the opportunity to do that while continuing to grow in a career that I truly enjoy.