Upcoming in Cybersecurity: A Reflective Essay

by

Galen Cole

A Reflective Paper

Submitted to IDS 493

Old Dominion University

Professor Carin Andrews

August 2025

I am currently pursuing a Bachelor of Science in Cybersecurity at Old Dominion University (ODU). Throughout my time in the program, I have been exposed to a wide range of ideas, practices, and learning environments across multiple disciplines. One of the most compelling aspects of the cybersecurity field, and a significant reason I chose it, is the constant growth of knowledge and the increasing demand for expertise in cyberspace. This evolving landscape has allowed me to develop essential skills in technical problem solving, cybersecurity analysis and awareness, and professional communication. Through hands-on projects, interdisciplinary coursework, and professional experiences, I have learned to think critically and conduct myself with professionalism in cybersecurity-related roles.

Throughout my academic and professional experiences, I have had to adapt to a variety of technical environments, each with unique approaches to maintaining confidentiality, integrity, and availability. One of the most formative experiences that shaped my problem-solving ability was creating and maintaining my network and Docker-based server stack. Through this personal project, I learned how to configure systems from the ground up, resolve dependency issues, and identify performance bottlenecks. My artifact, titled "Hastily Constructed Docker Stack File," demonstrates my ability to troubleshoot, adapt, and refine solutions through hands-on experimentation.

In a professional context, I further developed these skills while working at the ODU Information Technology (IT) Help Desk and interning at the City of Virginia Beach (CoVB) Office of Information, Security, and Privacy. These roles introduced me to enterprise infrastructure, including the use of ticketing systems for real-time troubleshooting for hardware, software, and user account issues. My "Help Desk Ticket Resolutions" artifact outlines the responsibilities I managed and the successful resolution of some service requests. At the Help Desk, I frequently worked with account lockouts, password resets, email configurations, software issues, and fundamental networking issues. These common but critical issues gave me insight into the user side of cybersecurity and highlighted the importance of balancing security with usability. I also had exposure to Active Directory management and ticketing system workflows, which deepened my understanding of enterprise operations.

To automate repetitive tasks and improve efficiency, I developed a custom script known as the 'Keyboard WASD Jiggler,' which simulates keystrokes for the 'W, A, S, D' keys on a keyboard at random intervals — typically used within online games to avoid being labeled as inactive. While not directly used in enterprise systems, this project showcases my initiative in scripting and task automation, which is helpful in systems administration and cybersecurity operations.

Job postings for roles such as IT technician, cybersecurity analyst, and system administrator frequently list troubleshooting and diagnostic skills as essential. These experiences have prepared me to meet those expectations by helping me develop confidence and logic-based approaches to problem-solving.

Another critical skill I have developed is the ability to analyze threats and maintain cybersecurity awareness in both technical and organizational contexts. My coursework and field experience have taught me that cybersecurity is not limited to technical defenses but also includes understanding user behavior, policies, and the broader risk environment.

One artifact that represents this is my tabletop exercise on Domain Name System poisoning. I evaluated potential attack paths, system weaknesses, and mitigation strategies using both technical training and knowledge from behavioral theory at varying levels of compromise. I also created a "Risk Evaluation Brief" on the MOVEit Transfer breach, CVE-2023-34362, by applying a professional template I became familiar with during my internship. This self-directed analysis helped me examine the real-world implications of software vulnerabilities and data exposure.

My artifact, titled “Nessus Scans and Comprehension,” showcases my use of a vulnerability scanner to evaluate systems based on Common Vulnerabilities and Exposures and the Common Vulnerability Scoring System. This work involved interpreting severity scores, assessing risk, and organizational remediation strategies in a practical format. Additionally, earning the CompTIA Cybersecurity Analyst Plus (CySA+) certification validated my understanding of these core skills and practices. Preparing for the CySA+ exam pushed me to refine my knowledge of intrusion detection, vulnerability management, and threat mitigation. I studied various frameworks and security models, such as the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework and the NIST Cybersecurity Framework. Passing the certification validated not just theoretical knowledge but also practical skills like analyzing logs, prioritizing threats, and building incident response strategies. These are skills I now feel confident in any entry-level security role.

These activities strengthened my ability to perform threat assessments, an essential skill in roles of threat intelligence, security operations, and compliance. They also helped me apply knowledge from courses that covered technology, ethics, and human behavior, reinforcing the interdisciplinary nature of cybersecurity.

In both academic and workplace settings, the ability to communicate clearly and document technical information effectively has been one of my most important and transferable skills. Whether drafting internal memos or preparing instructional content, I learned that accurate communication across various language barriers is essential for successful teamwork and operational consistency.

One artifact that highlights this skill is a knowledge base entry I contributed to during my time at the Old Dominion University Help Desk. The article, formatted in a question-and-answer style, helped staff manage email migrations between Eastern Virginia Medical School and the university. It was designed to be clear, accessible, and reliable for daily use. While working on training materials and knowledge base articles, I became more aware of the language needed for non-technical users who may be unfamiliar with IT terminology. This experience has taught me the value of analogies and clear formatting to avoid confusion. It also prepared me to engage with clients or executives in a professional setting where clarity is essential.

Another example is a formal report I completed for my CYSE 368 internship course, which included sections such as a table of contents, definitions, and detailed documentation of tasks. I also participated in preparing training materials and reviewing onboarding procedures for new hires. My privacy policy titled "Legalnese by My Lawyer (Chat-GPT) and I" demonstrates my initiative to maintain ethical standards even in my projects. It explains how data is collected, used, transformed, and managed, offering transparency and accountability in line with industry norms.

Professional communication skills are mentioned in nearly every job listing, especially cybersecurity roles focused on governance, auditing, and technical support. My writing experiences, especially in courses like IDS 300W, helped me build the ability to translate technical ideas for diverse audiences.

Cybersecurity is by nature an interdisciplinary field. The skills I have developed through my coursework, projects, and work experience reflect how different areas of knowledge intersect with one another. Technical problem-solving was built on logic, experimentation, and system configuration. Cybersecurity analysis requires both hands-on tools and an understanding of policy, ethics, and organizational behavior. My communication and documentation skills were improved through academic writing, professional practice, and real-world responsibilities.

Courses such as IDS 300W encouraged me to think across subjects and to integrate knowledge from various domains into a complete understanding of my field. These methods were critical for completing assignments and for preparing to solve complex problems in the workplace. Whether responding to incidents, configuring secure systems, or writing reports, I now approach tasks with an awareness of how different fields contribute to the success of cybersecurity efforts. As threats continue to evolve and new challenges emerge, the ability to think and act across disciplines will remain one of the most valuable strengths I bring to any future role.

References

CompTIA. (n.d.). *Cybersecurity Analyst (CySA+)*. Retrieved from https://www.comptia.org/certifications/cybersecurity-analyst

MITRE. (n.d.). *MITRE ATT&CK Framework*. Retrieved from https://attack.mitre.org/

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). https://www.nist.gov/cyberframework

Common Vulnerabilities and Exposures. (2023, July 2). *CVE-2023-34362*. https://www.cve.org/CVERecord?id=CVE-2023-34362