Reflective Essay: Demonstrating Key Skills through Cybersecurity Artifacts

Mathieu Crosby

IDS 493

Professor Andrews

Old Dominion University

12/5/2025

Introduction

Throughout my degree program in cybersecurity and information technology, I developed a combination of technical knowledge and professional skills essential for career success. Three competencies stand out as the most influential to my growth: Leadership, Teamwork and Collaboration, and Problem-Solving and Critical Thinking. These skills were shaped through an interdisciplinary curriculum that merged technical subjects such as network security, intrusion detection, and digital forensics with communication, ethics, and organizational behavior. This blend helped me understand not only how security systems work, but also how human behavior and organizational structure influence cybersecurity outcomes. This essay reflects on how my academic artifacts demonstrate these skills and how they prepared me for a career in cybersecurity and IT.

Leadership

Supporting Artifact 1: Incident Response Simulation

During the Incident Response Simulation, I developed my leadership skills as a team leader through coordinating a simulated cyber-attack response by allocating roles, organizing investigative efforts, and establishing deadlines. I ensured that the essential tasks of analyzing logs, identifying threats, and documenting responses were completed effectively via the use of calm decision-making, adaptability, and clearly communicating under stressful situations. My ability to provide structure to the response and create a complete final report demonstrated my leadership capabilities in guiding a team during a high-pressure cybersecurity environment.

Supporting Artifact 2: Firewall Configuration Project

The Firewall Configuration Project allowed me to put my leadership into practice as I was the Project Manager (PM) responsible for coordinating the effort needed for the team to implement firewall rules that both provided secure connections and allowed systems to be usable by all employees. This was an extensive amount of technical decision-making for me but required me to gather input from my teammates when designing/Fabricating the firewalls, determining the best settings and configuring the firewalls. I led all discussions on the establishment of priorities, access controls and ensuring that both the Security and Operational requirements were met in the end solution. I was able to lead my team using both my technical expertise and my ability to work collaboratively with my teammates.

Supporting Artifact 3: Cybersecurity Event Reflection

The "Is Cybersecurity Enough?" Zoom event organized by Dr. Jonathan Avooske has significantly influenced how I view leadership within an industry. Dr. Avooske pointed out the importance of proactive leadership in addition to the traditional security approaches (e.g., multi-factor authentication and password policies). He also discussed how critical it is to share information related to threats and cooperate on a global level. The event led me to understand that cybersecurity leadership encompasses shaping the strategy and culture of an organization, rather than simply performing tasks.

Lessons Learned and Interdisciplinary Application

The integration of my technical courses and communication-centered classes throughout my program has provided me with leadership capabilities. In addition to providing me with a framework for managing individuals and teams, the courses in organizational behavior and

professional communication have enhanced my conflict resolution and peer motivation skills. As a result of these interdisciplinary experiences, I realize that a successful cybersecurity leader must also have a thorough understanding of people in addition to their technological expertise.

Teamwork and Collaboration

Supporting Artifact 1: Intrusion Detection System Log Analysis

As an example of my ability to work effectively in teams, I was part of an Information Defense Strategy (IDS) Log Analysis project with my peers. The purpose of this project was to review large numbers of network logs to find any anomalies. Working as a team allowed us to discuss each other's findings and share ideas about what we perceived as unusual occurrences in the network logs. This experience demonstrated the value of teamwork and collaborative communication within the Cybersecurity Operations realm.

Supporting Artifact 2: Group Vulnerability Assessment

The Group Vulnerability Assessment consists of identifying vulnerabilities on a simulated enterprise network and creating a detailed plan for mitigating risks. Each member of our team contributed unique technical expertise. My contribution was to compile and help conceptualize the final document. The experience of this project helped me to develop as a professional in my ability to work together to create a common outcome while being responsible for piece of the effort and maintaining a professional communication style.

Supporting Artifact 3: Internship Task Management

As an intern, I collaborated with my fellow interns to create a Client Risk Assessment and Incident Response Plan on behalf of an actual company. The division of task assignments

reflected our strengths, and we consistently communicated to meet our deadlines. The experience served as reinforcement for what I learned in class regarding teamwork as well as illustrating how the challenges of real life (unexpected schedule changes and differing client expectations) impacted my experience.

Lessons Learned and Interdisciplinary Application

In cybersecurity, working together requires effective communication, technical input and an effective organization. Training I received in communication, management of projects, and report writing provided me with more tools to be collaborative in a professional setting. As such, these multidisciplinary skills are a core requirement for many Cybersecurity roles where collaboration among a group of people is necessary.

Problem-Solving and Critical Thinking

Supporting Artifact 1: Wireshark Network Traffic Analysis

With this Wireshark Network Traffic Analysis project, I captured and analyzed network traffic to determine if any suspicious activity is occurring and used concepts taught in my Network Security courses to identify any anomalies in the captured packets and propose an appropriate response. This experience helped to further develop Analytic Thinking, and Structured Problem-Solving skills.

Supporting Artifact 2: Threat Modeling and Risk Mitigation

I assessed potential vulnerabilities to cloud environments and identified ways to mitigate those vulnerabilities. Using a systematic, critical thinking approach to identifying assets, threats

and attack methods, I was able to develop strategies to reduce risk. This reinforces the need for proactive security planning.

Supporting Artifact 3: Digital Forensics Investigation

Using digital forensic evidence from a laptop and smartphone, I used AXIOM, FTK Imager, and Cellebrite UFED to investigate of a simulated data breach. I examined and reconstructed timelines of the events surrounding this breach as well as reconstructed deleted files and established connections between the digital forensic evidence across both devices. I utilized a high degree of critical thinking skills and maintained a high degree of integrity with respect to legal and ethical standards during this investigation.

Lessons Learned and Interdisciplinary Application

Cybersecurity relies heavily on problem-solving and critical thinking skills. As I took my technical training courses, I also completed courses in law and ethical standards. My training prepared me to analyze and document my findings as evidence; I followed the same professional standards associated with conducting investigations. This combination of coursework strengthened my abilities to make informed decisions on securing systems.

Conclusion

Throughout my academic career in Cybersecurity, I have developed my skills in Leadership, Teamwork and Collaboration, and Problem Marking and Critical Thinking in preparation for entering the professional workforce of Cybersecurity, and Information Technology. Each of these artifacts demonstrate my ability to integrate Technical Knowledge into work through communication skills, management, ethical and legal issues. I also developed

my research and analytical writing skills in my IDS 300W as well as this course, IDS 493 learning about my ethical responsibility as a researcher. Interdisciplinary Learning has prepared me to view Cybersecurity from both the human aspect and from the technical aspect. Experiences have enabled me to Lead Effectively and work Well with Others and to develop a system for solving complex security issues. Cybersecurity is continually changing, and Adaptability, Collaboration, and Critical Thinking will continue to be necessary skills. My experiences within my Academics have provided me with the academic knowledge and the professional skills to achieve success within a Modern Cybersecurity and Information Technology Positions.