CYSE 368 Internship Final Paper

Spring 2025

Student Name: Christian Coleman
Employer: Digital Transformation & Technology
Course: CYSE 368/Internship
Term: Spring 2025

Table of Contents

1. Introduction

I decided to pursue an internship with Digital Transformation & Technology to gain practical experience in cybersecurity operations within a professional environment. As a cybersecurity student, I recognized that bridging the gap between classroom learning and real-world application would be essential for my professional development. Through this internship, I hoped to achieve three specific learning outcomes: first, to develop practical skills in security monitoring and incident response; second, to understand how security protocols and policies are implemented and maintained in an enterprise environment; and third, to improve my ability to communicate security concepts effectively to both technical and non-technical stakeholders. This paper outlines my internship experience at Digital Transformation & Technology, reflecting on my growth, challenges, and the valuable insights I've gained during this time.

2. Beginning of Internship

Digital Transformation & Technology is a division within Old Dominion University that supports the university's technological infrastructure and digital security needs. This division plays a crucial role in maintaining secure IT operations across campus, protecting sensitive academic and administrative data, and ensuring compliance with educational privacy regulations. The division serves various departments within the university, providing essential security services to protect student information, research data, and administrative systems from increasingly complex cyber threats.

My initial orientation began with an introduction to the division's mission, structure, and security operations. During the first week, I participated in training sessions covering the university's security platforms, internal ticketing systems, and communication protocols. I was assigned a mentor who guided me through basic security monitoring tasks and helped me understand the workflow of the security team. My initial impressions were extremely positive – the division had a structured yet collaborative environment, with team members who were both knowledgeable and willing to share their expertise. The internship seemed well-organized, with clear expectations and a progressive path toward more complex responsibilities.

3. Management Environment

The management structure at Digital Transformation & Technology follows a hierarchical yet approachable model. The security operations team I was placed in is led by the Chief Information Security Officer, who oversees the security team leads, each responsible for different aspects of security: Security Operations, GRC, and Cloud operations. These team leads supervise analysts and engineers who handle day-to-day operations.

My direct supervisor was the Security Analyst team lead, who provided weekly check-ins to review my progress and address any questions or concerns. The supervision style was supportive, and I was given clear guidance on tasks but also encouraged to think independently and propose solutions. The management effectively balanced oversight with growth opportunities, allowing me to take ownership of projects while providing a safety net of expertise when needed.

The overall management environment fostered both accountability and creativity. Regular team meetings facilitated knowledge sharing and collaboration, while the open-door policy of managers created a comfortable space for seeking guidance. This management approach was particularly effective for my internship as it provided structure while allowing flexibility for learning and exploration.

4. Major Work Duties and Projects

During my internship, I worked on several key duties and projects that helped the organization's security efforts. One of my main responsibilities was firewall management, which included watching logs, looking at traffic patterns, and handling rule change requests. This job was important for keeping the organization's security boundaries safe and stopping unauthorized access to important resources. The daily review of firewall logs needed careful attention to spot possible security events among normal traffic. I got better at seeing patterns that might show scanning attempts, unusual access requests, or possible data theft. When I found concerning patterns, I would write down what I found and pass it to senior team members for more investigation.

I also worked on security tickets about possible phishing attempts, suspicious network activity, and access management issues. This job needed good investigation and documentation skills, since each ticket had to be correctly sorted, addressed, and documented for future reference. Solving these tickets quickly affected both the organization's security operations and how productive users could be. A typical phishing ticket involved looking at email headers, checking suspicious links or attachments in a safe environment, and figuring out if the threat was just one email or part of a bigger campaign targeting many employees. For access management tickets, I checked user identity, confirmed authorization levels, and made sure access requests were properly documented according to company policy.

An important project I helped with was creating Crowdstrike documentation, which involved making detailed guides for endpoint detection and response procedures. This documentation helped the team respond better to threats found by the Crowdstrike platform, making security work more efficient. The documentation included step by step procedures for sorting alerts, doing first investigations, and containing compromised endpoints. I added flowcharts to show decision paths and created detailed appendices with command references for common

investigation scenarios. Later on, I got to present this documentation to supervisors, showing how it added value to security operations. The presentation meant explaining technical procedures as business benefits, highlighting how standard response procedures reduced the time needed to fix problems and improved overall security.

I also went to an AWS event where I learned about cloud security principles and best practices. The event covered important topics like identity and access management in cloud environments, secure setup of virtual private clouds, encryption of data when stored and when moving, and cloud specific compliance issues. After this event, I helped review the organization's cloud security setups against industry standards, finding areas that could be improved. This project was necessary to keep the company's cloud resources protected as they used more cloud services. The review process involved using AWS security tools to check current setups, writing down findings, and preparing recommendations based on risk level and how complex they would be to implement.

Other duties included updating SMSing and vishing procedure documentation to make it clear and compliant with security best practices, helping with vulnerability assessment activities, and completing ongoing IT training to expand my technical knowledge. The procedure documentation needed close work with the security awareness team to make sure the content was technically correct while still being easy for non technical staff to understand. For vulnerability assessments, I helped scan network segments, analyze results to find false positives, and document real vulnerabilities for tracking their fixes. The IT training covered various topics including advanced network security concepts, security information and event management (SIEM) operations, and threat hunting methods. All these responsibilities helped the organization's security goals by either strengthening defenses, improving response capabilities, or increasing team knowledge.

5. Use of Cybersecurity Skills and Knowledge

Prior to the internship, I had developed foundational skills in network security concepts, basic threat identification, and security tool operation through my coursework. However, the internship environment required applying these skills in real time situations with actual consequences. For instance, my understanding of phishing tactics from classroom learning was enhanced by analyzing genuine phishing attempts targeting the organization, allowing me to recognize subtle indicators and evolving techniques used by threat actors. While academic exercises had familiarized me with common phishing indicators such as spoofed domains and urgent language, examining actual attacks revealed the sophisticated nature of modern phishing campaigns that blended legitimate and malicious elements to evade detection.

I also had to learn several new skills on the job. Operating the Crowdstrike platform required specific knowledge that I developed through mentor guidance and hands on practice. Learning to

navigate the Crowdstrike console efficiently took considerable practice, particularly understanding how to interpret the relationship between detection events, process trees, and potential indicators of compromise. Cloud security concepts, particularly related to AWS services, represented another area where I needed to expand my skills through both the AWS event and subsequent practical application. I had to quickly develop understanding of AWS security groups, Identity and Access Management (IAM) configurations, and security assessment tools specific to cloud environments. Additionally, I developed proficiency in security documentation writing, learning how to balance technical accuracy with clarity for different audience levels. This skill proved especially valuable when creating procedure documents that needed to serve both highly technical security analysts and general staff with limited technical background.

Furthermore, I expanded my knowledge of security information and event management (SIEM) systems, learning to create and fine tune correlation rules to identify potential security incidents from disparate log sources. This process required understanding log formats from various systems, identifying relevant fields for correlation, and establishing appropriate thresholds to minimize false positives while ensuring genuine security events were detected.

My on the job experience significantly changed my understanding of cybersecurity practice. While classroom learning had provided theoretical frameworks, the internship revealed the complexity of real world security operations, particularly how security decisions must balance protection, business needs, and user experience. In academic settings, security scenarios often have clear solutions with minimal constraints, but professional environments require navigating competing priorities, limited resources, and varying risk appetites across business units. I gained appreciation for the dynamic nature of cybersecurity work, where threats constantly evolve and security professionals must adapt continuously. Witnessing how quickly threat actors adjusted their techniques in response to defenses highlighted the importance of continuous learning and flexibility in security roles. The experience also emphasized the importance of soft skills alongside technical knowledge, as effective security work requires clear communication, teamwork, and critical thinking under pressure. I discovered that successfully implementing security measures often depended as much on effectively communicating their value to stakeholders as on the technical soundness of the solution itself.

6. ODU Curriculum Preparation

The ODU curriculum provided valuable preparation for my internship experience. Courses such as Windows System Management and Security gave me the foundation to understand enterprise security configurations and common vulnerabilities in Windows environments. This knowledge proved directly applicable when handling security tickets related to Windows systems and participating in vulnerability assessments.

Linux Systems for Cybersecurity similarly prepared me for working with various security tools and understanding server security principles, as many of the security platforms used by the organization ran on Linux infrastructure. Cyber Fundamentals established the core concepts and terminology that enabled me to comprehend security discussions and documentation within the organization. Cyber Techniques and Operations proved particularly valuable, as it introduced me to security monitoring and incident response procedures that closely aligned with my internship duties. The hands-on labs from this course gave me familiarity with security tools similar to those used in the organization's security operations center. Cyber Criminology provided important context about threat actors and their motivations, which helped me better understand the security incidents I encountered and the reasoning behind specific security controls. This sociological perspective complemented the technical aspects of my internship work.

While the curriculum created a strong foundation, there were some gaps that became apparent during my internship. The complexity of enterprise security tools often exceeded what was covered in coursework, requiring significant on-the-job learning. Additionally, cloud security concepts, particularly related to AWS, were areas where I needed substantial additional knowledge. The experience also revealed that coursework could benefit from more emphasis on security documentation and communication skills, which proved essential in the professional environment.

Despite these gaps, I frequently made connections between classroom learning and internship work. Analyzing network traffic patterns during firewall management directly applied concepts from network security courses. Incident response procedures reinforced and expanded upon frameworks introduced in cyber operations classes. These connections helped me apply theoretical knowledge to practical situations and deepened my understanding of both.

7. Achievement of Learning Outcomes

Regarding my first learning outcome – developing practical skills in security monitoring and incident response – the internship exceeded my expectations. Through hands-on experience with firewall management, security ticket processing, and participation in incident triage, I gained practical proficiency that would have been difficult to achieve in a classroom setting. By the midpoint of my internship, I was independently handling routine monitoring tasks and contributing to incident response activities, demonstrating significant growth in this area.

For my second objective, understanding how security protocols and policies are implemented in an enterprise environment and the internship provided comprehensive insight. Working with the security team allowed me to observe how policies translate into technical controls, how exceptions are managed, and how security requirements balance with business needs. Developing and updating security documentation gave me direct experience with the operational

aspects of security governance. This outcome was fully achieved, giving me a practical understanding of security management that complements my technical skills.

My third goal, improving communication of security concepts to various stakeholders was addressed through multiple experiences. Creating documentation for different audience levels required adapting technical information to various knowledge bases. Presenting my documentation to supervisors provided valuable experience in explaining security concepts clearly and answering questions effectively. Working on ticket resolutions further developed my ability to communicate security requirements in accessible terms. While I've made significant progress in this area, I recognize that effective communication is an ongoing development area that will continue to improve with additional experience.

Overall, the internship successfully fulfilled my learning objectives, providing practical skill development, insight into enterprise security operations, and opportunities to enhance my communication abilities. These achievements have significantly contributed to my professional growth in cybersecurity.

8. Motivating Aspects

The most motivating aspects of my internship centered around seeing the real world impact of security work. Particularly exciting was successfully identifying and helping to mitigate potential security incidents before they could cause harm. One memorable instance involved detecting unusual access patterns that indicated a potential compromise attempt, which was then blocked before any data could be accessed. This occurred during routine firewall log analysis when I noticed repeated connection attempts from an unusual geographic location targeting specific administrative interfaces. After reporting the pattern to my supervisor, we implemented additional blocks and verified that no successful access had occurred. The tangible protection this provided to the organization and its customers was deeply satisfying and reinforced the importance of diligent monitoring.

Another motivating experience came during a vulnerability assessment project, where I identified a previously undocumented security weakness in a legacy application. The discovery allowed the security team to implement compensating controls while the development team scheduled remediation. Knowing that my finding helped close a security gap before it could be exploited gave me a concrete sense of contributing to organizational security.

Presenting my Crowdstrike documentation to supervisors and receiving positive feedback was another highly motivating experience. The presentation required significant preparation, including creating visual aids and anticipating potential questions. Seeing my work recognized as valuable to the team affirmed my contributions and boosted my confidence in my technical writing abilities. Most gratifying was hearing from seasoned analysts that the documentation

clarified procedures they had previously found confusing. The subsequent implementation of this documentation into standard operating procedures made the effort feel especially worthwhile.

The AWS event was similarly engaging, as it exposed me to cutting edge cloud security concepts and connected me with professionals in the field. The workshops included hands on exercises in securing cloud infrastructure and managing cloud specific security challenges. Participating in discussions with experienced cloud security professionals provided valuable insights into real world implementation concerns not covered in academic settings. The opportunity to apply this knowledge directly to the organization's cloud environment afterward provided immediate relevance to what I had learned, allowing me to contribute to a cloud security assessment despite my relative inexperience with the technology.

Perhaps most motivating was the gradual increase in responsibility throughout the internship. As my supervisors recognized my growing capabilities, they assigned more complex tasks and greater autonomy, which created a rewarding sense of progression and professional development. By the final weeks of my internship, I was handling initial triage for certain categories of security alerts independently, conducting preliminary investigations, and making recommendations for response actions. This evolution from closely supervised basic tasks to more independent analytical work validated my growing expertise and provided a clear trajectory for further professional growth.

9. Discouraging Aspects

While the internship was overwhelmingly positive, there were some discouraging elements. One challenge was the repetitive nature of certain security monitoring tasks, which sometimes felt monotonous despite their importance. Reviewing similar alerts daily occasionally made it difficult to maintain the high level of attention required to catch subtle anomalies.

Another discouraging aspect was encountering the same security mistakes repeatedly across the organization despite awareness efforts. Seeing users fall for similar phishing attempts or make the same security missteps despite training highlighted the human challenge in cybersecurity and the limits of technical controls alone. At times, resource constraints affected what security improvements could be implemented. Several worthwhile security enhancement suggestions were deprioritized due to budget or personnel limitations. This reality check revealed the business constraints that security teams often operate under, which can be frustrating when recognizing potential vulnerabilities that remain unaddressed.

Additionally, the learning curve for some enterprise security tools was steeper than expected, occasionally leading to feelings of inadequacy when I struggled to master complex platforms quickly. However, these moments of discouragement ultimately became learning opportunities that pushed me to develop resilience and perseverance.

10. Challenging Aspects

The most challenging aspect of my internship was balancing multiple responsibilities under time pressure, particularly when on-call duties coincided with project deadlines. Learning to prioritize effectively while maintaining attention to detail required significant adjustment to my work approach. One particularly demanding period involved managing multiple phishing tickets while simultaneously preparing my documentation presentation, which tested my ability to allocate attention appropriately across competing priorities.

Technical challenges included working with the more complex aspects of firewall management, where rule conflicts and dependencies created intricate troubleshooting scenarios. These situations required careful analysis and critical thinking to resolve without creating security gaps or disrupting legitimate business operations. Creating documentation that was both technically accurate and accessible to different audience levels presented another significant challenge. Finding the right balance between necessary technical detail and clear, straightforward guidance took multiple revisions and feedback sessions before achieving the right approach.

Perhaps the most challenging aspect was analyzing unusual network traffic patterns that didn't clearly match known threat signatures. These ambiguous situations required synthesizing information from multiple sources, collaborating with team members, and making judgment calls based on incomplete information – a complex but ultimately rewarding aspect of security analysis work.

11. Recommendations for Future Interns

For future interns at Digital Transformation & Technology, I recommend several preparations to maximize the experience. First, strengthen foundational knowledge in network security concepts, particularly firewall principles and common network protocols. Familiarity with these basics will help new interns understand security monitoring activities more quickly.

Develop basic proficiency with Linux command line operations before the internship begins, as many security tools operate in Linux environments. Even fundamental command knowledge will significantly reduce the learning curve for security platform operation. Future interns should also review cloud security concepts, particularly related to AWS services, as the organization increasingly utilizes cloud resources. Basic understanding of cloud security models will provide helpful context for related projects. Additionally, practice clear technical writing before the internship, as documentation is an important responsibility. The ability to explain technical concepts clearly will be valuable from the beginning of the experience. I also recommend that future interns approach the experience with an inquisitive mindset and willingness to ask questions. The security team is supportive and knowledgeable, but they expect interns to actively seek clarification when needed rather than making assumptions.

Finally, prepare to manage time effectively across multiple tasks with different priority levels. Developing a system for tracking assignments and deadlines will help navigate the varied responsibilities of the role successfully.

12. Conclusion

My internship with Digital Transformation & Technology has profoundly enhanced my understanding of cybersecurity beyond what classroom learning alone could provide. The opportunity to apply security concepts in a professional environment, work with enterprise-grade tools, and contribute to meaningful security operations has bridged the gap between theory and practice in invaluable ways. My main takeaway is the recognition that effective cybersecurity requires a blend of technical knowledge, analytical thinking, communication skills, and adaptability.

This experience will significantly influence my remaining time at ODU by shaping how I approach my coursework. I now have a clearer understanding of which skills and knowledge areas are most relevant to professional practice, allowing me to focus my studies accordingly. I plan to pursue additional coursework in cloud security and advanced threat detection, areas I've identified as particularly valuable based on my internship experience. I'll also approach team projects with greater emphasis on documentation and communication aspects, recognizing their importance in professional security work.

Looking toward my future professional path, this internship has confirmed my interest in security operations while also revealing new potential career directions. I've developed a particular interest in threat intellingence and compliance, areas I may pursue for specialization. The experience has also highlighted the importance of continuous learning in the cybersecurity field, reinforcing my commitment to ongoing professional development beyond graduation. Most importantly, the internship has given me practical experience to reference in job interviews and professional connections that may prove valuable as I begin my career. I feel significantly more prepared to enter the cybersecurity workforce with confidence in my abilities and clarity about my professional direction.