Internship Final Paper

Hailey L. Caram

Old Dominion University

CYSE368: Internship

Spring 2026

Navy Cyber Defense Operations Command

April 19, 2026

Table of Contents

Introduction

I completed my internship experience at the Navy Cyber Defense Operations Command. This is a military command working under the U.S. Cyber Command. The command provides CSSP services to the entirety of the Navy's networks. Since I have worked at this command for the last four years, I did not receive additional orientation or training for my internship experience. I completed my internship role as Security Information and Event Manager, or SIEM, developer under the guidance of my supervisor, Shannon Naughton. My established role at this command allowed for a seamless transition into my internship experience, and I maintained a professional working relationship with my team over the internship. My impressions of the command did not change over my internship experience.

The Navy Cyber Defense Operations Command, or NCDOC, developed from an incident response team. The command gradually grew into a 24/7 operation. NCDOC was founded in 2006 and has continued to grow over the years. When I first started working at NCDOC, I was a host analyst positioned on the watchfloor. From there, I transitioned into a lead analyst of my section. I began learning Tier II malware analysis, but I did not complete my training as I was selected for the SIEM team in a developer role. Since being selected for the SIEM team, I have been working as a SIEM developer.

Before I began my internship this semester, I developed four learning objectives to guide my learning experience over the next few months. Developing these objectives outlined a clear plan for the skills and knowledge I aimed to improve upon during my internship. Outlining my learning objectives also allowed me to create clear expectations for myself for the internship experience.

My first learning objective was to develop and apply professional communication and technical writing skills in a corporate environment, producing clear and effective documentation. Professional communication and technical writing skills are valuable assets in a corporate environment. By including this in my learning objectives, I ensured that I was continuing to develop these skills, which will benefit me over my professional career. I was provided many opportunities to address this learning objective over my internship, and I feel that I have thoroughly addressed these learning outcomes.

My second learning objective was to gain hands-on experience in integrating defensive cybersecurity operations into the SIEM development lifecycle. This practical experience is critical to becoming a well-rounded professional. As a SIEM developer, I was given daily opportunities to address this learning objective. By continuing to collaborate with my team and other professionals at the command, I effectively enhanced my knowledge and ability to integrate defensive cybersecurity operations into the SIEM development lifecycle. I successfully met this learning objective.

My third learning objective was to apply the foundational pillars of cybersecurity in a real-world setting, contributing to the protection and integrity of organizational assets and infrastructure. This learning objective allowed me to combine my academic experience and knowledge with my practical, hands-on experience and knowledge to apply the foundational pillars of cybersecurity. Coming into this internship with previous knowledge and cybersecurity experience enhanced my ability to contribute to the protection and integrity of organizational assets and infrastructure. Incorporating knowledge I have gained through my education at ODU further enhanced my practical ability to contribute to and protect organizational assets and infrastructure.

My fourth learning objective was to advance skills in detection engineering by creating, testing, and implementing threat detection mechanisms within a SIEM framework. My role as a SIEM developer provided me ample opportunities to address this learning outcome. My supervisor and members of my team are extremely knowledgeable about this process, and daily collaboration with my team improved my ability to create, test, and implement threat detection mechanisms within a SIEM framework. By highlighting this objective, I put forth conscious effort in my daily work to enhance my skills. I now feel more confident in my ability to create, test, and implement threat detection mechanisms within a SIEM framework. By addressing this learning objective, I am now more equipped to perform my daily role as a SIEM developer at the Navy Cyber Defense Operations Command.

Management Environment

My internship was completed with the SIEM team, which is a small team consisting of myself and a few other developers who have unique roles within the team. On my team, I work with both civilians and military members. The team reports to our immediate operational lead, a military officer. At the head of the chain of the command is Shannon Naughton, my internship supervisor and division officer. As division officer, Shannon Naughton oversees the SIEM team and makes final decisions. Ms. Naughton often delegates tasks to individual members or defers technical decisions to our immediate operational lead.

Within the SIEM team, members are expected to perform independent work without requiring close supervision. Ms. Naughton trusts team members to update her accordingly as needed. SIEM team members are encouraged to consult with Ms. Naughton or our immediate operational lead for guidance or tasking. Ms. Naughton and our immediate operational lead often assist us with advocating for additional support or resources outside of our immediate team. For example, the SIEM team was requesting feedback from another team within the command on a tool required for the watchfloor. The team was not providing timely feedback, which was interfering with daily operations. Ms. Naughton and our immediate operational lead advocated on our behalf and consulted with the other team within the command to provide feedback on the critical tool needed within the watchfloor. Ms. Naughton and our immediate operational lead ensure the smooth operations of the SIEM team and support the overall Navy Cyber Defense Operations Command.

Their leadership has been effective as a SIEM developer, and their support has enabled me to successfully complete my internship. I appreciate the opportunity to work independently and develop confidence and resourcefulness. Knowing that I have support when I need guidance or extra assistance allows me to work more effectively. Their leadership has greatly benefited me throughout my internship experience.

Major Duties and Assignments

Throughout my time at NCDOC, my major work duties, assignments, and projects have varied greatly. My internship experience was completed with the SIEM team, and I worked as a SIEM developer. Therefore, my major work duties, assignments, and projects are completely different from my duties as an analyst, even though both roles were completed at the same command. My main work duties as a SIEM developer consist of maintaining the SIEM/SOAR platforms, ensuring the watch floor maintains 24/7 operational capabilities, responding to tickets that report bugs or breaks and capability requests, and detection engineering. I have been given daily or weekly opportunities to complete these duties over the course of my internship experience at NCDOC.

Over my internship experience, my main project has been unifying SIEM platforms to have bidirectional communications. This allows analysts to use one single pane of glass to search across both tools. Currently, analysts must utilize both Sentinel and Splunk to search. To do so, we have conducted many joint collaboration meetings with the Sentinel and the Splunk consultants to brainstorm an effective solution. At this point in the project, all alerts in Splunk are sent to Sentinel using a webhook. The analysts can now respond to both alerts in Sentinel. However, Sentinel does not have the ability to update Splunk once the analysts respond. I am continuing to work on setting up the response from Sentinel to Splunk. I am also continuing to work on developing the ability of Sentinel to search all of Splunk's data. Completing this project will benefit the watchfloor and support the security and operability of Navy Cyber Defense Operations Command.

Skills in Use

Before beginning the internship, I had experience with host analysis, incident response, threat hunting, writing reports, and communicating events. I developed these skills during my time at JCAC when I joined the Navy. JCAC, or the Joint Cyber Analysis Course, is the Navy's cybersecurity military training course that all cybersecurity Navy personnel complete when they enter the Navy. I was enrolled in JCAC for about 8 months as I developed many of these skills, such as writing reports, host analysis, or incident response. My knowledge base began at JCAC. After graduating from the Joint Cyber Analysis Course, I began working at the Navy Cyber Defense Operations Command. I also developed these skills during my time at NCDOC and in my roles as an analyst and SIEM developer. These two different roles allowed me to strengthen different skill sets. Having both of these experiences has given me a comprehensive understanding of both roles and responsibilities. When I transitioned from the analyst role to a SIEM developer, I am now able to envision what I would have found most helpful as an analyst. This experience informs my practice as a SIEM developer and I am better able to support the watchfloor.

After completing my internship, I have learned or advanced many skills, including automation, detection development, API integration, and creating documentation. Developing my automation skills was critical when working at NCDOC, as the SIEM team monitors many sensors and a global network. The SIEM team is responsible for creating tools for analysts to protect the global network. By using automation to detect or analyze threats, threat detection is enhanced and conducted more quickly. As discussed above, API integration is a skill I reinforced through my major project during my internship. Unifying the SIEM platforms was a chance to integrate the use of APIs within automations to create a single pane of glass for the analysts on the watchfloor. Additionally, throughout all of my tasks during internship I maintained effective and timely documentation. Ensuring documentation is standardized and timely reduces risk and provides structure. Documentation also aids in effective and structured communication across NCDOC.

I have also developed a proactive approach to cybersecurity. My internship experience strengthened my proactive approach and my perspective has shifted from reactive to proactive. Proactive cybersecurity is incredibly beneficial and prevents attacks before they occur. A reactive approach can help to address attacks once they occur, but systems remain vulnerable to attacks. Switching my mindset to a proactive approach reduces risks and saves costs by addressing vulnerabilities before any breaches occur.

In addition to these hard skills, I have also continued to develop soft skills that have benefited me in the workplace, including decision-making, problem solving, collaboration, and

critical thinking. My work often requires collaboration with team members or outside teams, such as with the Microsoft teams or the countermeasures team. My improved communication skills have also aided me in explaining technical terms or concepts to non-technical personnel with whom I collaborate with or report to. Problem solving and critical thinking skills support my work to find or analyze vulnerabilities and then address these vulnerabilities. I have also continued to improve my decision-making skills, as I am often called upon for quick responses that require independent and effective decisions. Cybersecurity requires continual problem solving to address vulnerabilities, respond to attacks, or resolving incidents in a timely manner while ensuring security.

ODU Curriculum

During my time at ODU, I have taken relevant classes such as networking and security, cyber law, Windows system management, cybersecurity technology in society, and cybersecurity in social science. The ODU curriculum reinforced my existing knowledge in preparation for the internship. The networking class provided a particularly helpful refresher before my internship, as I had not reviewed that material since attending JCAC several years ago. The cyber law class that I took at ODU educated me on laws surrounding security and data that I would not have previously considered but are important to know during research and creation. The cyber law class prompted me to analyze my experience and knowledge in new ways, and the class provided me with a helpful lens to utilize during my internship experience. The technology and society class better prepared me for real-world events to affect my daily work. After taking the technology and society class, I analyzed and formed connections between real world events and my work during my internship.

I did have opportunities to connect what I have learned in school and the skills or knowledge used at the internship. In the Windows system management course, I learned about Windows servers and logs and how they are configured. I also learned about where the Windows servers are placed in the network and how they interact with other network devices. One of the detections I recently wrote at work analyzed Windows logs. The course I took at ODU reinforced my knowledge and directly benefited me as I wrote this detection recently during my internship. During my internship, I was not tasked with setting up a Windows server, but I was responsible for writing a detection for searching security logs from Windows domain controllers. Because I previously took the Windows system management course, I knew where the domain controllers likely were in our network and I had an idea of how the traffic should look coming in and out of the domain controller. Connecting my ODU curriculum and my skills used at the internship was a motivating and rewarding moment.

Another example of a connection I encountered between my ODU curriculum and my internship experience came up when I determined whether a detection belonged to the host or the network analyst using information I learned during the networking and security course I took at ODU. A ticket was submitted by an analyst after a network alert was firing more than usual. The analyst and watchfloor argued that the detection that was firing the alert should be tuned. Furthermore, the watchfloor argued that they should not be responsible for responding to the alert and that the Endpoint division should respond instead. The watchfloor thought the detection and response should fall to Endpoint because the detection was connected to a self-replicating file on a host. After analyzing the detection using what I learned in the networking course, I determined that although the detection was connected to the self-replicating file, the detection was not concerned with the file being on the host. Rather, the detection was looking for the file

traveling through the network. This is outside of the host analysts' purview and falls to the analysts on the watchfloor. I utilized my knowledge gained in the ODU network security class to come to this conclusion.

During my internship experience, there were experiences that revealed new concepts, techniques, or skills that I have not yet encountered in school. The ODU curriculum did not sufficiently prepare me for working with SIEM platforms or development lifecycles. Instead, I learned those concepts on the job. My coworkers and team provided on the job training that helped to fill in the gaps from the ODU curriculum. I also did not have any hands-on experience with search languages from the ODU curriculum. This knowledge was developed through hands-on experience at my internship. For example, I learned search languages by reading other searches that were already built out and analyzing each line. I completed independent research if I did not know what a specific line meant. Being more prepared for writing my own queries would have been helpful when beginning at NCDOC and would be a helpful addition to ODU cybersecurity curriculum.

Fulfilling Goals

My first learning objective was to develop and apply professional communication and technical writing skills in a corporate environment, producing clear and effective documentation. My internship experience at NCDOC provided ample opportunities to fulfill this goal and continue developing and applying professional communication and technical writing skills. Throughout my internship experience, I was expected to produce and maintain clear and effective documentation on major work duties, assignments, and projects. After completing my internship, I feel more comfortable developing and applying professional communication. My technical writing skills have also improved, and I feel comfortable operating in a corporate environment to produce clear and effective documentation.

My second learning objective was to gain hands-on experience in integrating defensive cybersecurity operations into the SIEM development lifecycle. Completing my internship at NCDOC allowed me to gain hands-on experience and integrate defensive cybersecurity operations into the SIEM development lifecycle. My daily tasks and responsibilities as a SIEM developer allowed me to gain hands-on experience. Although I began the internship with prior experience and knowledge about the SIEM development lifecycle, externalizing my goal and expectation to learn more about the SIEM development lifecycle provided extra motivation. Additionally, writing this learning objective motivated me to be more intentional in my daily tasks. I set forth intentional effort to focus on the SIEM development lifecycle and analyze each step to ensure I was gaining valuable experience and knowledge. Completing the reflection papers throughout the internship encouraged me to process my experiences, and writing about my internship hours allowed me to organize my thoughts and knowledge into a cohesive narrative. Having processed my thoughts and knowledge in this way has benefited the way I interact with the SIEM development lifecycle, and I feel as if I more fully understand the roles and responsibilities I have as a SIEM developer. Although the workload may have felt draining at times, being forced to stop and reflect will benefit me as I continue to work as a SIEM developer at NCDOC.

One recent example of becoming more familiar with the SIEM development lifecycle occurred recently when I was asked to create detections for computer activity that I was not familiar with. I received support from my supervisor, who provided me with a list of detections. After realizing I was lacking important knowledge, I completed independent research to

familiarize myself with best practices for creating these new detections. My supervisor provided initial, necessary support, but she trusted me enough to allow me to complete independent research and come up with the answer on my own. I appreciate the opportunity to foster resourcefulness and confidence in my skills while increasing my own knowledge through independent research.

My third learning objective was to apply the foundational pillars of cybersecurity in a real-world setting, contributing to the protection and integrity of organizational assets and infrastructure. Recent real-world events have affected my workload at NCDOC. These situations can be stressful and overwhelming, especially as the pressure and workload continue to mount. However, encountering these types of situations with the support of a functioning team alleviates some of that pressure and helps prepare me for future situations. Cybersecurity is interlinked with real-world events and global conflict, and I recognize this fact. I firstly recognize my mission to contribute to the protection and integrity of organizational assets and infrastructure. This often means staying aware of current events and remaining vigilant to ensure full protection and integrity.

My internship provided plenty of opportunities to apply the foundational pillars of cybersecurity in a real-world setting. Since I work on a specialized team, I am expected to complete daily tasks and uphold my responsibility to apply the foundational pillars of cybersecurity. I appreciate being able to complete my internship in a critical role, despite occasional feelings of pressure. A recent example of applying the foundational pillars of cybersecurity in a real-world setting occurs in my work with the watchfloor. As the SIEM development team, we are responsible for ensuring that the tools the watchfloor uses are available. The watchfloor operates 24/7, and their work is critical to network security for the whole of NCDOC. The watchfloor is responsible for 24/7 monitoring over the sensors. To apply the foundational pillar of availability in a real-world setting, the SIEM team developed a tool that automatically monitors the sensors and provides the status of all sensors. The tool also monitors when a sensor is down and alerts the watchfloor when a sensor has been down for a certain amount of time. This tool provides critical indicators and assists the watchfloor with constant monitoring. The development and use of this tool is a prime example of one way I apply the foundational pillars of cybersecurity in a real-world setting.

My fourth learning objective was to advance skills in detection engineering by creating, testing, and implementing threat detection mechanisms within a SIEM framework. My internship experience created many opportunities to continue advancing my skills in detection engineering. My daily responsibilities often include creating, testing, or implementing threat detection mechanisms within a SIEM framework. These daily opportunities ensure that I am constantly developing my skills in detection engineering, which will benefit me in my current role as SIEM developer. These skills will also benefit me as I transition out of the military and into my future civilian career.

I recently had an example to advance my skills in detection engineering when I was asked to use logs I was unfamiliar with. To become more familiar with these logs, I conducted a broad search of what the logs looked like in our data to become more familiar with how everything was formatted and displayed. After conducting an initial broad search, I conducted open search research on attack vectors and common indicators of this kind of data. This narrowed my search on what I needed to look for so that I could create my detection based on what I was seeing. After conducting research, I built out my search that would be used in my detection. To do so, I needed to determine how often the data was ingested into our systems so

that I could configure the detection to run at certain times and intervals. By configuring the detection at set times and intervals, I ensured that there were no gaps and the detection would fully catch all data without any gaps in coverage.

Motivating Aspects

My internship experience was hands-on and required practical, real-world knowledge. I dealt with real situations and threats daily, which motivated me to perform at a high level. The ability to see immediate feedback on tools or detections also provided motivation to continue learning. For example, if a tool we developed does not work, we are often able to see errors in the tool immediately. This immediate feedback makes the process feel more involved and rewarding, rather than having long intervals between the work and the ability to see the results. I appreciate being able to see the impact of my dedication and labor. If a tool does not initially work and I can problem solve to find a solution, this provides a feeling of accomplishment that continues to motivate me to provide successful and effective tools.

Additionally, providing the watch floor with tools was an exciting aspect of the internship. Being able to see the watch floor use what we developed was extremely rewarding, as we saw the immediate benefit of our hard work. Knowing that what we developed was effective and useful is one of the most motivating aspects of the internship. I appreciate the feeling of a completed task, particularly when the task benefits the team or allows the team to support the overall mission.

The impact of real world events is also a motivator during this internship. When global events occur, such as the conflict in Iran or Russia, the command is usually affected in some way. Knowing what is occurring globally is also a great motivator to perform well and learn new skills during my internship. Cybersecurity is interlinked with national and global conflicts, so staying current with world events or tensions can allow me to perform better during daily tasks and responsibilities at my internship or job. I am able to analyze and protect against likely threats as I am aware of what to look for.

An additional motivating aspect of my internship was the ability to network and collaborate with other professionals, particularly within my team. Being able to work with competent professionals who have more or different knowledge and skill sets than me is extremely motivating. I appreciate working with others who can motivate me to learn and perform in my role more effectively, and this internship provided me the opportunity to do so. Networking is a professional skill that I am continuing to develop, and working with others in a close setting is a great opportunity to become more comfortable networking in a safe, learning environment.

Discouraging Aspects

Firstly, adjusting my expectations and accepting the fact that we can’t catch every single malicious attempt can be discouraging at times. Although I strive to keep networks as secure as possible, the unfortunate reality is that there will be things that get by. This is mostly due to the sheer number of malware or attempted hacks. Over my internship experience, I have learned to readjust my expectations in order to take pressure off myself and my team. Instead of expecting absolute perfection, I aim to provide the best cybersecurity possible and continue to learn and improve my skills daily. I have adjusted my expectations to ensure that the most damaging hacks or malware are prioritized, therefore protecting the networks as best as possible. Although we may not catch every attempted hack or piece of malware, my team and I strive to keep networks secure and ensure safe cyber practices.

Another discouraging aspect of my internship experience has been a lack of being consulted for Microsoft tools. As part of my role on the SIEM team, I am mainly responsible for Microsoft tools and knowledge. However, NCDOC has in-house Microsoft consultants. Many people within NCDOC automatically seek advice or information from the in-house Microsoft consultants. This can feel discouraging at times, as I know I am capable of providing assistance or answering questions. However, this pattern is likely due to name association rather than a disregard for my knowledge. Associating Microsoft questions with the in-house Microsoft consultants is natural, and I do not take these situations personally. Instead, I offer help to individuals or other teams where appropriate, collaborate with the in-house Microsoft counsel, and continue to be available when needed to ensure that all parties are fully supported as best as possible.

An additional discouraging aspect of my internship experience has been the occasional feelings of monotony. Although I appreciate the low-stress days and periods, these can sometimes feel repetitive and lead to discouragement. I prioritize continued learning and I enjoy challenging myself. I pay close attention to each task to avoid making mistakes due to monotony or inattention. To address the repetitiveness of tasks, I actively seek out new learning experiences, such as networking with other teams or learning more about other tools and platforms. During my internship experience at the Navy Cyber Defense Operations Command, I researched independently to become more familiar with Splunk, although my primary responsibility is Microsoft. Learning more about Splunk helps to refresh daily tasks and keep me interested in the work. Completing this independent researcher also makes me a more valuable team member and will hopefully benefit me in the future. As I begin to apply for jobs and further my professional career, I am now equipped with knowledge of multiple different tools and platforms.

Challenges

Although I have had a successful and motivating experience during my internship this semester, some aspects have been challenging. At times, collaboration can be difficult, particularly when others are unwilling to collaborate. Part of my role as a SIEM developer involves close and frequent collaboration with other teams, including the Microsoft team or the IT team. Slow or reluctant feedback on tools we have disseminated can impede our work and makes the job much more challenging. Often, other teams are not purposefully avoiding collaborating, but rather do not know how to do so effectively. Poor communication and prioritization is a challenge that I face often. I have reflected on my part and have tried to improve the way I communicate with other teams to facilitate this process in the future. Communication goes more smoothly when both parties are willing and open to listen and improve.

Similarly, outside expectations are difficult to navigate at times. There are situations I have faced in which others have asked for a task to be completed which is not immediately possible or may take longer than the individual had in mind. Individuals outside of the SIEM team may not have all the information, such as limiting factors, other priorities, or a full understanding of the process for SIEM development. Explaining the SIEM development process to others who do not work for the SIEM team can be challenging at times. Learning how to explain this process in a concise, helpful way has been a skill I have had to consciously develop over my internship and is a skill I am continuing to improve. Although I work with many talented teams and individuals who have plenty of technical background and expertise, individuals who do not work closely with the SIEM development process may come with unclear

or unrealistic expectations. Continuing to develop my collaboration and communication skills has been critical for addressing this challenge. By being better able to explain technical concepts to others who do not work in a critical role, I am more equipped to collaborate and complete projects.

An additional challenge that I have faced during my internship is a lack of direction at times. A part of our job is seeking out threats and evaluating whether systems have been compromised. Being proactive in addition to defense ensures that networks are secure. Since we do not usually know where the attack is coming from, this sometimes results in a lack of direction. Constantly monitoring all potential sources of attack can be challenging and initially resulted in feelings of intense pressure or worry. When I first began working with the SIEM team, I found myself placing unnecessary pressure on my tasks and holding myself to unfair expectations, such as expecting to catch all malicious activity or threats or being very disappointed when this was not possible. This obviously raised my stress levels and made the transition to the SIEM team more difficult. I have learned to accept the reality of the job and I have tried to place less pressure on myself, which makes the work more enjoyable. This challenge grows easier with time and teamwork, and has become easier as I have continued to develop my skills over the course of my internship. Alleviating some of the pressure that I have placed on myself will make for a more sustainable career, and I will be able to continue to work with passion and care in all my daily tasks.

Recommendations

Future interns beginning this internship should enter the internship with a curious attitude. By being willing to learn, interns can take advantage of the opportunity provided and capitalize on the learning experience. Completing an internship provides students with the space to ask questions, gain hands-on experience, and benefit from leadership and collaboration with professionals. Future interns should practice being willing to ask for help, ask questions, and incorporate feedback from other professionals. Acknowledging that you are a student and may need guidance at times is a beneficial and positive mindset. Others are likely to provide positive guidance and feedback to interns who are willing to learn.

Within NCDOC, there are many more teams than expected within the command. Collaborating with them early and often will set future interns up for success. By collaborating with others in different roles, interns have the opportunity to learn many skills and form connections. This can set interns up for future opportunities by building a professional network and developing diverse knowledge. I have appreciated the opportunity to learn from professionals who work in very different roles than I do, and therefore have immense knowledge and skills to teach me. By forming connections, interns could possibly secure or open future employment opportunities by building a professional network. Interns would also benefit from the guidance of seasoned professionals in the cybersecurity field who have navigated many challenges.

Before beginning the internship, future interns should refresh themselves on the background and structure of the command. Since NCDOC has many teams and departments, becoming familiar with the structure of the command will allow for a smoother transition and easier collaboration with other teams. When I first began working at NCDOC, I felt slightly overwhelmed by the many varied teams, departments, and responsibilities at the command. Additionally, becoming more familiar with the chain of command can make future interns feel more comfortable when asking for help or collaborating with outside teams and departments. The military chain of command is hierarchical and strictly outlined, so future interns should feel

comfortable knowing who to ask for help and who they will often be collaborating with during daily tasks.

An additional recommendation I have for future interns is to become more familiar and knowledgeable about search languages. This will greatly benefit interns who are working at NCDOC. Future interns should also become more familiar with development lifecycles. This is particularly important for future interns working with the SIEM development team. Future interns should learn how data is ingested into SIEM platforms, as this will be a part of daily tasks and responsibilities.

Conclusion

My internship experience was extremely rewarding and provided me many opportunities to compound my existing skills and knowledge. I gained more hands-on experience in the cybersecurity field and established a firm understanding of the foundational pillars of cybersecurity. I successfully met all of my learning objectives that I originally outlined for the semester. My first key take-away from the internship experience is the importance of networking. I had the privilege of completing my internship at NCDOC, which is a large cybersecurity command in the U.S. Navy. I work with many knowledgeable and skilled coworkers, who eventually transition out of the Navy or beyond NCDOC to a variety of employers. By maintaining the connections I made during my internship, I will have built a foundational professional network that will hopefully benefit me in future endeavors and as I transition out of the Navy in the near future. Relying on my professional network may lead to career opportunities or social support during the potentially difficult transition, as I have never worked as a civilian in the cybersecurity field.

My second key take-away from my internship experience is increased career clarity. I have thoroughly appreciated my overall experience at NCDOC, and I am looking forward to continuing to grow in my career in cybersecurity. Although there were some negative or discouraging aspects of my internship experience, my time as a SIEM developer has confirmed that I will seek out similar employment roles once I transition out of the Navy and into civilian employment. Completing my internship has also provided needed confidence for my career progression. I feel more confident and assured in my knowledge, skills, and work. This confidence and experience will propel me to continue learning and developing with a newfound passion.

During the remainder of my time at ODU, I will prioritize maintaining communication and relationships. Over my time at ODU, I have not always made an effort to forge relationships with classmates or professors as the majority of my classes have been online. This has seemed like a barrier to forming meaningful connections at times. However, part of my internship experience was remote work, which allowed me to experience a different aspect of online communication. Moving forward, I will make an effort to maintain relationships or form connections even if I am only taking online classes. This will help me to continue to hone this skill.

Additionally, the remote aspect of my internship has influenced my future professional planning. I have found remote work harder to concentrate on or I have been less productive at home than I typically am when I am in the office. Although I appreciate the flexibility and comfort of remote work, the experience has made me realize that I would not like to pursue remote work again in the future. I also appreciate the social aspect of working in the office. As a self-proclaimed introvert, I typically get part of my socialization from collaborating with

coworkers. Once I began working remotely, I was surprised that I found myself missing this socialization aspect of office work.