

Final Paper

Zachary Six

Trey Tunell, CISO

Floor & Décor Holdings Inc.

CYSE 368: Summer 2025

Professor Duvall

August 4th, 2025

Table of Contents

<i>Introduction.....</i>	<i>3</i>
<i>Management Environment.....</i>	<i>5</i>
<i>Work Duties and Projects</i>	<i>6</i>
<i>Usage of Cyber Skills</i>	<i>11</i>
<i>Preparedness for Internship</i>	<i>13</i>
<i>Fulfilment of Objectives.....</i>	<i>15</i>
<i>Motivating and Exciting Aspects of the Internship</i>	<i>17</i>
<i>Discouraging Aspects of the Internship.....</i>	<i>18</i>
<i>Challenging Aspects of the Internship</i>	<i>20</i>
<i>Recommendations for Future Interns at this Company.....</i>	<i>21</i>
<i>Conclusion.....</i>	<i>22</i>

Introduction

For as long as I have been working and studying in college, I have found myself gravitating towards jobs that lean towards logistics and warehouse-related jobs. I originally started at Floor & Décor Holdings inc. (F&D for short) in 2021 as a warehouse associate after being laid off from another company relating to packing and shipping. I took some time to gain experience in this position and leveraged this experience to further pursue warehouse management positions for two other companies before returning to F&D in 2024 as a warehouse associate once again. This time, I was given better pay due to my recently acquired skills in warehouse management. After returning to this company, we had received a staff change in the position that oversees the entire physical store location and this new manager helped me apply for the position, get an interview, and finally receive the call an internship within the company's IT department. I personally believe that if it were not for this new manager, I would still be on the hunt for a first internship or entry-level position in my desired career path.

Floor and Décor Holdings, inc. is a hard flooring retailer that sells tile, wood, and stone at competitive prices and huge selections. The company started in the year 2000 under the name FDO holdings before changing its name to Floor & Décor Holdings, inc. in 2017. Unlike other hardware stores such as Home Depot and Lowes, our stores are stocked with almost nothing but different options of flooring to fill almost any cosmetic need for any new or soon-to-be renovated house. On top of selling affordable top-quality flooring, we also offer design services for our customers so they can get an in-depth view of how their tile decisions may look after installation. A majority of our customer-base are contractors, or "pros", who come in to purchase tile on behalf of the customer and take to a job site. Any customer can find, purchase, and pick up the flooring in the very hour they arrived if they so pleased with our quick and efficient team. Our

put the customer first by providing a one-stop-shop for everything they would need including the tile/flooring itself and all installation materials required for the job.

When I was first entering the internship there were a couple of things I had on my mind that I was personally hoping to accomplish over the course of the summer. My first objective I wanted to achieve was a good understanding of how an enterprise IT department performs to make the company perform better and how it interacts with the rest of the company. After being part of the internship for the last couple of months, I can confidently say I have a better understanding for how an IT department operates in a real-world setting. I have learned that it takes a large team with extremely good communication and trust among all the members to ensure everything gets done in a timely manner. A second learning objective I hoped to learn over the course of the internship was to learn how to configure a firewall with rules and policies. Although I did not get direct experience with our company's firewall, I was trained on a software that operates in a similar manner. Having a task on this similar software allowed me to get a solid foundation in how firewall rules are set and how detrimental they can be to the performance of the company. A third learning objective I wished to learn over the internship was the process that would take place in the event of a data breach or cyber-attack. The internship at this company allowed me to get a view into their Cyber Security Incident Response Plan and learn the processes and chain of command in the event of a data breach.

At the start of my Cyber Intern position, I was given next to no training for my position. Nearly all my training was done in real time or from learning new cyber security concepts of interest to myself and my career. A couple of training modules were presented to me for our regular cyber training on the newest adversarial techniques in my first couple of weeks as an intern. Although there was a lack of initial training for my position, I was given opportunities to

meet with the different areas within our IT department to get a feel for our day-to-day operations. These meetings allowed me to get a better idea of the software and techniques used by the different departments and gave me ideas for new concepts to look up and learn as part of my training.

Management Environment

Understanding the interactions between management and different areas within the IT department, particularly the engineering team and the security operations center (SOC) team, was one of the more challenging aspects of the internship. Each area only consisted of a handful of people, but as my boss likes to say, “it takes a village.” The team I worked with the most only consisted of about 4 people at any given time, which makes it easier for collaboration and sharing information about a project we were working on. For the internship aspect specifically, I had two supervisors I could look to for any questions or guidance in any aspect of my position. A key aspect about the remote internship in contrast to an on-premises position is that I don’t have a boss hovering over my shoulder every minute and adding a level of stress to my workday. Twice a week I would meet with my two main supervisors to discuss my progress for the week and to see if there was anything I wasn’t experiencing that I wished to be part of. Along with these two meetings a week I also attended two mandatory SCRUM meetings a week with the majority of the Cyber Department. These meetings were meant to go over the week’s objectives as a team, so everyone is informed about the different situations happening across the Cyber Security Department. Something interesting I noted during my internship was during a large “IT Talk” meeting that consisted of about 50-60 attendees from the company’s IT department. I saw that there were many individuals I was unfamiliar with and had not seen during the entirety of the internship. I mention this specifically because they had job titles that were the same of other

team members that I see regularly in the meetings I attend. I have decided that there are probably many departments that I will never see in my time at Floor and Décor and that is one of the many hidden gears that allows the company to progress and perform.

Work Duties and Projects

During the very beginning of my internship, the company was in progress of implementing a new device/asset inventory software known as Forescout. This software would allow us to apply each store as a segment that would hold every POS, camera, and mobile device connected to the network of that store. The issue that was occurring is that each store would take about 20 minutes to onboard on this software and we have over 300 stores in the United States. Deployment for these stores onto the software would only occur once a week and ended up taking months just to get barely half of the stores. Due to this process being extremely slow, I was assigned to create a program that would automate the onboarding of new store segments onto the software. This would prevent the need to have several team members on the clock past midnight to onboard the new stores and ensure there are no misconfigurations occurring during deployment. During my time at ODU, I was taught to program in C++ but shown the syntax of other programming languages to gain familiarity. In the internship, I was told to code the automation program in the Python programming language for future changes and readability by the current staff. Being I had no prior coding experience in the Python language, I had to find a way to teach myself in the most efficient way possible. I used this opportunity to take advantage of my company's enterprise CoPilot AI license to help teach me what I needed to understand and learn the syntax for python. I made the decision to teach myself python by rewriting one of my old programs from C++ to Python. This would allow me to see the different techniques used in

Python vs the ones used in C++. Below are snippets of the relatively same function written in C++ and Python:

Figure 1: Python Code

```
def cr_master_list():
    global raceNum, TOTAL_avgLaptime

    with open("laps.txt", "r") as inData:

        for line in inData:

            # laps in text file must be formatted as 'lapCount, lap1 lap2 lap3 lap4'
            # takes the line and splits it into lap count and laps
            rawlapCount, laps = line.split(",")

            #conversion of str to int and form lap list
            lapCount = int(rawlapCount)
            lapList = list(map(float, laps.strip().split()))

            #update number of races input
            raceNum += 1

            #create tuple to pair number of laps with the laps recorded
            rawRace = lapCount, lapList, raceNum

            #function call to determine race analytics
            lapCalculation(rawRace)

            # calculate average lap
            totalNumLaps = 0
            for item in race_list:
                totalNumLaps += race_list[item][0]

            TOTAL_avgLaptime = round(TOTAL_lapTime / totalNumLaps, 3)
```

Figure 2: C++ Code

```
//organize all lap information into vector
void organizeLaps(raceChar raceInfo[], int& totallaps)
{
    double lap;
    ifstream inData;
    inData.open("LapTimes.txt");

    for(int i = 0; i < NUM_RACES; i++)
    {
        inData >> raceInfo[i].numLaps;

        for(int j = 0; j < raceInfo[i].numLaps; j++)
        {
            inData >> lap;
            totallaps++;

            raceInfo[i].laps.push_back(lap);
        }
    }

    inData.close();
}
```

The functions presented in the figures perform essentially the same task of organizing lap-time information into a list to be parsed later in the program. The python program parses the text one line at a time and then splits up the lap times. The C++ program reads the text file one word at a time, making it less efficient than the Python program I had written. Overall, rewriting the C++ code into Python was a very engaging and exciting way to teach myself an unfamiliar programming language. Because I was already familiar with the C++ program and knew the processes that needed to be completed, I only needed to figure out the syntax for Python.

With my new knowledge of Python I could work on my skills with APIs to write a Python program that would make use of the Forescout APIs. Further down the line of the project it was found that the implementation the company was looking for may not be possible and the automation they were looking for was not possible. Being that the automation was not possible, my project ended up being scrapped and the idea of implementing an easier way to deploy new software was now in question. Although this project ended up being scrapped, it introduced me to a new programming language and the Postman software that allows users to interact with application APIs. To get myself familiar with how APIs work and practice my python skills, I decided to make a program using Python that would allow me to interact with the APIs of some applications I used in my daily life. I used my reminders app, TickTick, to make a new reminder on my account and flash my Govee light in my room when this was complete. This gave me the experience with API keys and authorization methods that I had not been introduced to before. I have found that whenever I am met with a new major concept such as learning about APIs or a new programming language I turn to utilizing CoPilot instead of Google.

My second major task during this internship has been mostly involved in a software known as Cribl. This software is a data ingestion and manipulation application where logs from

many different sources get sent to a database with this service as the middleman to manage the data that gets sent to the database and stored. Currently, we have several routes to filter out the different logs and manipulate them depending on the source to add or remove items from the log. The department was looking for a way to develop a “universal route” that would be able to filter a specific type of log, make universal changes, make the necessary changes per source, and then send the log off to the destination database we have set up. When I was first attempting to solve this issue, I had a couple of solutions in mind. One solution was to create a secondary route list that the logs would pass into that would then be filtered off even further. For example, $\text{Log}_A \rightarrow \text{Main Log Route} \rightarrow \text{Secondary Route}_A \rightarrow \text{Destination}$. If the route was met with Log_B , then it would be passed through the secondary route_B because it is a different source. The main issue I faced with this setup was that I could not implement any universal changes because every log *must* pass through a pre-configured sub-route if I wanted any changes to be made to the log, otherwise the log would be sent straight to the destination without being changed. In the Cribl software, there is a feature called a pipeline that is attached to every route and allows for any number of changes to be made to a log before sending it off to its destination. My idea to ensure there could be universal changes made to the logs was to create a pipeline in which all the desired type of log will passthrough. The pipeline would make the universal changes and then additional changes based only off the source of the log. This solution was also a way to future-proof the routes by allowing for automated API calls to be made when a new source of logs gets added to Cribl.

Another major assignment I had over the course of the internship came about as I was completing the Cribl assignment. It was found by me and my team that nearly 25% of all our logs were being sent through the very last route and trashed. After this discovery, I was told to

resolve the issue by determining what kind of logs were being sent through this route to cause a large surge. To start this fix, I utilized a feature in Cribl that allows users to capture logs passing through a specific route to get a better idea of what was happening behind the scenes of the routes we have set up. I took different captures at 200, 500, 1000, 2000, and 10000 logs to get varying sample sizes and get accurate readings as to how many of each type of log were getting through. Cribl can filter through the results, however, the filters must use JavaScript regex syntax to work. After figuring out a little bit of JavaScript, I was able to filter and find out what types of logs were being sent through the route that trashes the logs. The team I was working with had decided that we don't have all the time in the world to look at every single log, so we went ahead and configured the route to send all the logs passed through this default route to the database for further analysis. After giving the database a couple of days to collect logs for analysis, we noticed that there was one service that was passing through 99% of all logs in this default route. To solve this issue is a very simple solution: we would create a new route that would filter out that log type and only have those 1% of logs we don't want sent to the trash bin. This will, in turn, take the route that has 25% percent of all logs passing through and drop that number down to about 1%. Being able to optimize the routes this way not only allows us to retain the routes we want to keep but also makes the routing list more efficient.

The last assignment I had over the course of the internship was a programming assignment for an old program that was made by a former intern for the company. The goal of the program was to generate a report of the employees who had failed the current and/or previous phishing campaigns and then send an email to the managers of those employees. This was my first time ever looking at production code that was used by the company. My first task for this program was to update the email being sent to contain new verbiage that aligned with our

updated phishing policies. This would be a simple change of the text within the HTML message portion that would be inserted into the email. The second task I had for this program involves the number of months that is checked for a failure of a phishing campaign. My company has decided to increase the amount of time that it counts phishing campaign failures. The original timeline was six months but has been extended to a full year. Being that the size is doubled, I have been told to add a feature in the program that allows the user to select the number of months to be counted for failures. This requires a new button/label combination in addition to an entry field for the user to enter their desired number of months. The logic in how the program parses the different fields in the CSV file must be altered to only parse failures up to the number of months equal to the user input. This is a fairly straight forward implementation with a strategically placed for loop in the function that reads and counts the data in the CSV file.

Usage of Cyber Skills

Upon entering this internship, I was not prepared for the swift transition of using the knowledge I had been learning over the semesters. My first skill to be utilized in my internship was my ability to program and use logic to solve problems the department was having. This occurred when I was asked to write an automation script for the ForeScout application that would automate the process of adding appliances to the existing architecture. Before entering the internship, I was always curious about the environment of their developers and how the process would look in a real production environment. I was surprised to see that it was very similar to when I was doing programming assignments for my Computer Science classes. I used my knowledge of detailed documentation to ensure my program was well-documented and explained my program for the average person. Another skill I used from my learning at ODU was my knowledge of the basics of Firewall setup. Firewalls are set up with their rules in a specific order

to block traffic in the most efficient pattern and prevent unwanted users from accessing different software or systems. The Cribl service my organization used acts in a similar way in which the pipelines we create must be configured in a certain order to make the most efficient way of sorting through our logs. A specific skill I had to learn on the job was the processes of API keys and authentication when attempting to make an API call to any given service. I utilized a service known as Postman to teach myself how to handle the usage of API keys and use HTTP request messages to retrieve information from a website. Before being told that the automation project was not possible, I spent quite a bit of time looking at the API documentation for the ForeScout service I was preparing to make calls to. All, if not most, services that host an API also have documentation that explains how to use the API, the necessary parameters, and the method for authentication. I learned that every API call uses a certain method (GET, PULL, DELETE, etc.) and endpoint that signifies where the user is about to pull data from. Each endpoint is configured to send to or receive data from the user using the specified method. It is common for these endpoints to return data in the JSON file format that contains data in 'key': 'value' pairs. It is up to the service hosting the API to determine what the proper format of this JSON file will be in terms of assigning the different variables. After determining the proper endpoints, authentication, parameters, and figured out the proper JSON format for the service, I was able to transfer the requests to python code for the automation. When I was originally taught C++, I had not reached the point to use API calls in C++ and, because I had just started to learn python, I was able to learn this new skill in the language I was teaching myself. It was at this point where the project was scrapped, and I no longer had obligation to work on the project. Although the project was scrapped, I learned vital information regarding API calls and how to implement that logic into python code for future projects. Getting first-hand experience with authentication and receiving

keys cemented my teachings at ODU about symmetric and asymmetric keys as I had a lot of trouble understanding the logic behind what was going on to authenticate the user.

Preparedness for Internship

The teachings offered at ODU provided me with exceptional knowledge for the professional field, however, I do not recall one class teaching about common IT infrastructures and how they operate within an organization. I believe my biggest wake-up-call was discovering that I did not know how each of the services within an IT department talk to each other. For example, ODU had not taught me that there are dedicated syslog servers that send data logs to then be saved within the company's datacenter or a third-party cloud storage. When I first entered the internship, I felt that I could spit a fair amount of technical knowledge at my superiors, but I had next to no knowledge or even a general sense as to how the different technologies interacted. After spending some time on the internet and using Google/AI to my advantage, I found that there are some common configurations that organizations may use to set up their IT infrastructure. Technologies such as Network Access Control (NAC), log ingestion, and how data may move to or from data centers/servers to different branches of the organization. This configuration could be applied in many different situations whether it is government or non-government and could have been beneficial if introduced in one of my classes.

I did make several connections from my teachings at ODU, and I believe the biggest one to be authentication techniques and multi-factor authentication (MFA). During my first week of the internship, there was a big push towards to policies on MFA for employees who have access to sensitive parts of the company. The company, at the time, was only using push-notifications through an authenticator application where the user would just have to click 'Accept' to get

through to the sensitive material. There was also a ransomware group known as Scattered Spider going around and making swings at retail companies in the United States. Being that we wanted to defend against this group, we had decided to make our authentication policies stricter by making all employees with access to sensitive info type in a generated code that gets refreshed every 30 seconds to ensure security throughout the department. I was introduced, again, to authentication with the Forescout project as mentioned previously. As stated before, that project allowed me to gain a significant understanding of real-time usage of API keys, authentication tokens, and taking into account that I must provide security for the user's username and password.

Another aspect of the internship I believed was assisted by my learning at ODU was my general knowledge of the concepts brought up in different meetings I had attended. Concepts such as ransomware, intrusion detection systems (IDS), firewall policies, and even knowing some of the most basic concepts had helped me in my internship to understand the different ideas presented by my coworkers. Although it is very easy to overlook, having a solid foundation on these basic concepts allowed me to comprehend and follow along in the meetings much better than if I had just been introduced to the concepts.

One of the more profound areas that ODU had prepared me for was the ability to logically think through the problems and develop plans of attack to approach the issues. Being that the first half of my college career at ODU was set on Computer Science, I was geared towards programming, computer architecture, and theoretical Computer Science. I believe the latter class prepared me the most as I believe it required the most amount of logical thinking. I

believe that having this skill helped me in my projects where I needed critical thinking skills to properly solve the issue in an efficient way.

Fulfilment of Objectives

Upon reflecting on the internship, all but one of the goals presented to me in the beginning were met. The one objective that was not met that I believed could have had more focus on was the objective concerning incident response and how that may benefit with AI assistance. Being that AI is a rapidly growing industry and technology, it is important for the company to know the potential risks or benefits that may come with this technology. In the little time I did spend on this objective I learned that there are underground AI forums that are selling their models they have trained on specific adversarial things such as phishing, data extraction, and prompt generation. These risks pose a huge threat against the company as threat actors can develop more convincing phishing campaigns against associates to potentially gain access to our systems.

The internship offered much more insight to the other learning objectives including network/infrastructure security, retail cybersecurity, and incident response as a whole. Of the three objectives most of the time in the internship was spent on network/infrastructure security and monitoring the logs coming through our systems. As stated previously, I had worked with a service called Cribl that would manage the logs to be saved in a database. I spent a lot of time looking through the logs coming through system to identify any anomalies and helped ensure that we are collecting the appropriate logs according to security auditing standards. I was also introduced to many of their security monitoring applications such as the Tanium endpoint manager and the Forescout device auditor and NAC. Tanium allows the company to keep eyes

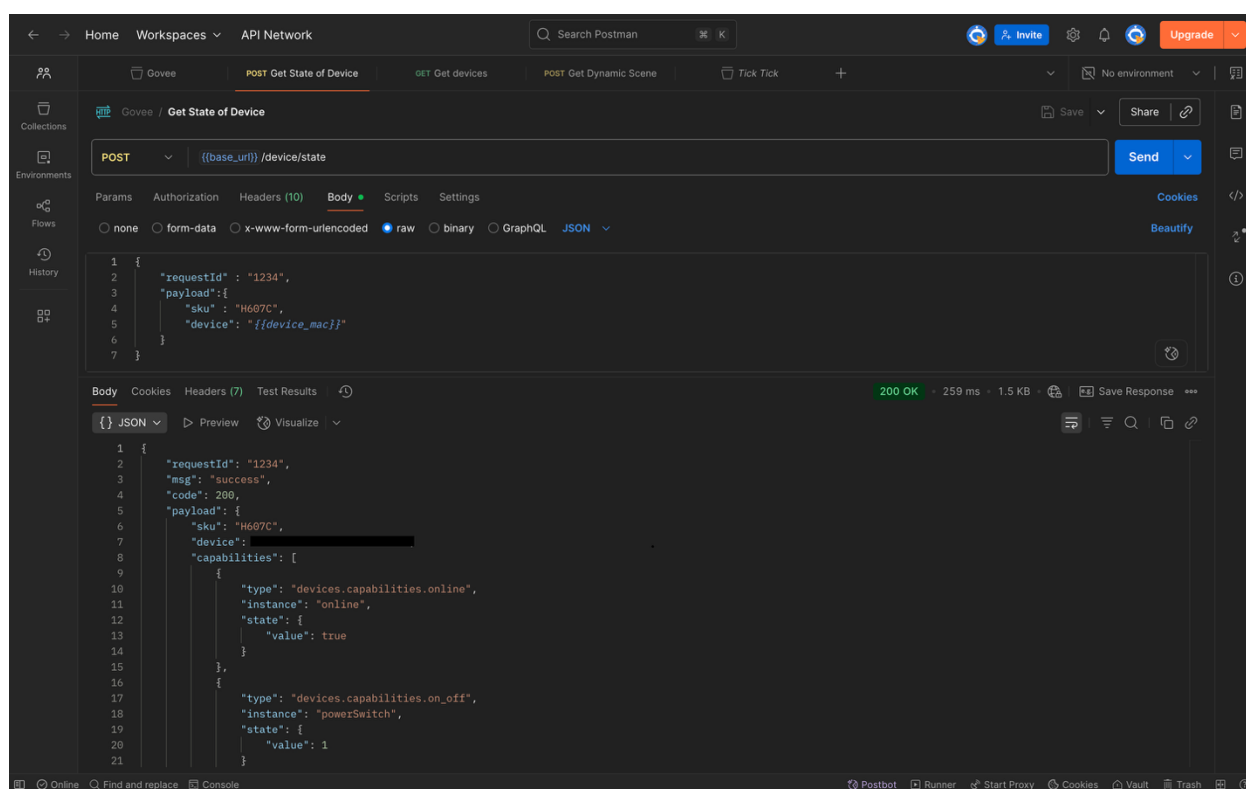
on the devices connected to the company network and ensure all devices are running the proper security updates and applications. One of the biggest surprises that came with learning these new services was the scale at which they operated at. Logging into a service for the first time and seeing tens of thousands of devices connected to a server really hit me like a bus. I understood that now I wasn't just working on a homework assignment, I was helping defend an entire nationwide company. When given access to Forescout and met with similar numbers of devices, I was shown how network policies came into play within the store to ensure every camera and POS system was accounted for and compliant. This service was similar to Tanium in that it took a device count for all connected devices, but different in that Forescout acted as a Network Access Controller (NAC) and Tanium ensured compliance of the connected devices.

When I was being introduced to incident response within the company, I had spent a good amount of time discussing the Cyber Security Incident Response Plan with my supervisor. This document contains all the necessary information the IT department needs in the case of a data breach. Some of the more important areas in the document are where chain of command and chain of info sharing are defined. This tells the team who to contact and about what aspect of the situation at hand. Another important section shown to me was the playbook explaining how many days it should take to resolve certain aspects of the issue. Aspects such as making sure POS and clock-in functions are working first to keep money flowing into the company. While being introduced to incident response, I was simultaneously introduced to governance, risk, and compliance. This entire area seems to be handled by a single person at my company and is a central place that determines if an individual's actions are considered compliant. For example, this individual is responsible for gathering the phishing campaign results and using the program I am editing to send emails to the managers of those individuals that failed the campaign.

Motivating and Exciting Aspects of the Internship

I was fortunate enough to have excellent motivation throughout the entire internship from my boss and coworkers. During my first assignment as the intern, I had quite a bit of learning to do about the company and many new processes to ensure I provide value to the company. I found myself to have the most excitement towards a project when there was actual forward momentum with it. During my learning of APIs I took advantage of smart home devices I owned to make my own program and teach myself at the same time. Making the first calls to an API and authenticating everything correctly feels like magic as I was now looking at another world of the devices I already own.

Figure 3: Postman GET request of personal smart home devices



Above is a screenshot of a GET request I made to these smart devices in my process of learning how to use APIs for future API manipulation for my company. This process got me familiar with

authenticating through a third-party service and sending singular requests to form the handshake between client and server. The most exciting part for me was the first time I was able to turn off my light using the Postman application shown in Figure 3. This kind of progress is what I consider to be forward momentum and is the source of my motivation through my projects. In the program focusing on the internal phishing campaign, most of my excitement came when I successfully created my first ever GUI element. My implementation was a checkbox that would then enable the user to enter the number of months they wanted to record for the report. The program was not written by me and took several days to learn and understand how the data flows through the program.

Throughout the internship I was also lucky enough to have supervisors consistently praising the work I was presenting to them as solutions. I made sure that I would not present a solution or sound over-confident until I knew the capabilities and features of my project like the back of my hand. I believe that if I don't have a 110% understanding of the scope and surrounding area of the problem, I won't be able to properly implement a solution.

Discouraging Aspects of the Internship

Although the internship presented many exciting and motivating opportunities, they did not come without their own share of disappointments. I believe one of the most discouraging aspects of this internship was the amount of work I was given over the summer. There were many times during the internship when I would complete a task rather quickly or get to a spot that requires attention from another department and then not have anything to do for several days. To keep myself busy, there were other activities I could do such as learning new cyber security concepts, techniques, and taking notes on my CompTIA Network+ certification. It did

not take long for many of these side-activities to become very old and boring, causing me to lose motivation and become discouraged. A couple of times when this would happen, I would reach out to one of my bosses or someone in another department and ask them a question on a topic I have been recently thinking about. Nine times out of ten they would have a meeting relating to that topic and send the invite for the meeting for me to listen in. Another discouraging aspect about the internship was the lack of areas that I was able to experience in the IT department. For the majority of the internship, I was sticking with the Security Operations Center (SOC) team to help improve their logging and data ingestion. This allowed me to gain a lot more knowledge in this area and next to nothing in the other areas of the IT department. I was only given an introduction to the responsibilities and a quick overview of the tools each area of the IT department used to complete their daily tasks. I would have liked to have had a week within each area of the IT department to really cement the processes each area does and help me better understand the role each area has into making the company more secure.

In the beginning of the internship, I had a meeting with my two bosses to review the general structure of how the internship will play out over the summer. In this review, I was told that there is a high probability of performing an internal penetration test on our VA beach store for any security vulnerabilities within the physical store. Unfortunately, this was the only time this project was ever mentioned over the entirety of the internship. I was very excited to perform real-world penetration testing techniques on the store and test my “hacker”-type thinking on a store I used to work at.

Challenging Aspects of the Internship

Reflecting back on the internship, there were not a lot of instances where I felt the internship was too challenging for me to continue or complete my tasks. The most challenging aspect of the internship that I am still figuring out today is working out how all of the different systems we have in place work together to form a cohesive infrastructure that allows the network devices to remain secure and allow the company to operate. Upon my entering of the internship, I was met with what seemed like nearly a dozen different services that all provided a different function necessary to the security of the company. The aspect of this that made it so challenging is that many of the software and services we use also can provide functions that are already provided by other services we use. For example, the software Tanium and Forescout were mentioned previously and both of them offer device auditing. From a high-level view and no working experience on either, these services felt like comparing Google Search to Bing Search. In my mind they felt like the same service, but after spending time with the people who use them the most and asking a lot of questions, I was able to figure out the key differences in these two pieces of software.

Another challenging aspect of the internship was the amount of “corpo-talk” and acronyms used in regular speech. Being an existing employee for the company but new to this department, I was attempting to figure out the meaning of the acronyms in relation to things about the company that I already know. Acronyms such as SSC (Store Support Center) were tossed around with such ease in nearly every sentence, a lot of what my coworkers were saying felt like gibberish and was difficult to follow along in conversations. A couple times I have been told “hope you got all of that” after a coworker was talking about another implementation and I have had to ask them to repeat it because I did not understand a decent chunk of the vocabulary

used in their speech. This felt very inefficient to me because I was unfamiliar with all of their vocabulary and had to get them to repeat it but also not use the acronyms when they repeat it. I am sure that over time I will learn these acronyms and won't need clarification, but for now I am stuck looking up acronyms on Google after meetings to make sure I understand what was said.

Recommendations for Future Interns at this Company

Maneuvering through the internship has been fairly straight-forward without many niche concepts required or the company expecting you to be a genius from the start. My first recommendation for a future intern at this company would be to come into the internship with a huge list of things you want to learn. Coming into the internship with only a couple of potential items to learn will not be enough as I had an immense amount of free time on my hands to learn about nearly any cyber-related topic I felt necessary. Although I did make sure all my assignments were either completed or needed to be examined by someone else due to an issue, there were still many times that I had nothing to do and wanting to fill my brain with as much knowledge as I possibly could. Making sure that you have plenty of material to expand your knowledge base is extremely beneficial and may get bonus points from a supervisor. Another recommendation for future interns at this company is to make sure you are prepared to work entirely remote; have an office space set up prior to your first day to make the transition as smooth as possible. Thankfully I was able to have this kind of set up in place long before the internship, but I believe that not having an "office space" is crucial to having the right mentality and work ethic on the clock. I also found it very easy to become distracted by the things around me because I am not in the traditional work environment. After some time, though, I was able to capture my attention and focus on my work every day instead of getting distracted by the closest thing to me.

Conclusion

As an employee who once used to work in a warehouse but now works in the IT department for the same company, I can safely say that I would much rather work in the IT department than the warehouse. Entering the internship was an extremely different experience than working in the warehouse where you are lifting 50-80 pounds at all times, walking an estimated 10 miles a day, and dealing with difficult customers. My duties within the IT department included gaining a generalized idea of how the operations of the IT department create a secure environment for the customers/employees in the stores, creating automation techniques for different areas of the IT department to increase efficiency, and learning about the newest techniques used by threat actors taking advantage of AI systems to run their exploits. Learning about all the different systems, techniques, and departments within the F&D IT department was the most challenging and least technical aspect about the internship. I found myself spending more time attempting to understand how the different software talked to each other than working on the different tasks because I wanted to know how the data flowed from the second the client connects to the second the client leaves the network or how requests made to one server get passed through the firewall and through other services. My experience in the internship has finally shown me how the corporate world operates in their IT departments. It has shown that my initial thoughts of an IT department are severely overexaggerated and that most of the time the IT department is a busy, yet relatively calm environment. Although everyone is frantically moving from one meeting to another, when I can sit down and get some actual work done, I am able to feel a sense of calmness.

Participating in this internship has also made me realize the kind of career path I would like to take after I graduate and get some experience under my belt. In this internship, I spent all

my time in a DevOps engineering role to help provide efficiency, security, and automation to our department. I found that this role fits my interests, however, it doesn't meet my need for a physical job. Working in the warehouse I was always moving and in the IT department I am sitting for 6-8 hours a day typing away at a computer. This will influence how I look at future jobs when applying and will make sure my next job has more physicality than the internship. Working within this internship has given me a lot of hope and excitement for after I graduate. This excitement will help encourage me to perform my absolute best in my last semester at ODU to graduate with an acceptable GPA and begin my life in the world of Cyber Security.