Justin Graham

CYSE 368

Summer 2024

Dominion Energy Internship

Table of Contents

1. Introduction……………………………………………………………………...3
2. Internship Beginning………………………………………………………….…3
3. Management Environment………………………………………………………4
4. Work Duties……………………………………………………………………...4
5. Cyber Security Skills…………………………………………………………….6
6. ODU Curriculum………………………………………………………………...6
7. Internship Objectives…………………………………………………………….7
8. Exciting Aspects…………………………………………………………………8
9. Discouraging Aspects….………………………………………………………...8
10. Challenging Aspects……………………………………………………………..8
11. Recommendations……………………………………………………………….9
12. Conclusion……………………………………………………………………….9
13. References………………………………………………………………………10

**Introduction:**

This internship was a position assigned to the Energy Management Systems Team (EMS) as part of their compliance team. In this position, I helped to ensure that all compliance related standards were being met as well as supporting the server administrators. Many of these standards were related to cybersecurity and involved managing which ports were open, submitting firewall rules, running scans to remediate vulnerabilities, and managing software on cyber assets.

The reason I decided to take an internship with Dominion Energy was because they are a large well-known company that plays an impactful role in the state as well as knowing a few people who already work at Dominion Energy. I was given this opportunity as a reference from a friend who works at Dominion Energy. After applying for the internship and doing an interview, I was accepted for the Summer of 2024.

The learning outcomes that I was given from my manager included learning and understanding the Northern Electric Reliability Corporation (NERC) Critical Infrastructure Procedures (CIP) requirements for Energy Management Systems, Supporting the team so that the NERC CIP compliance is being maintained, gathering evidence and doing reviews to ensure all compliance standards are being met, and using tools such as Nessus and OpenAudit to run cybersecurity scans and remediate vulnerabilities that were found.

**The Beginning:**

The business I was interning for was Dominion Energy. Their mission statement is “To provide the reliable, affordable, and increasingly clean energy that powers our customers everyday”. At a basic level, Dominion Energy generates and provide electricity or natural gas to more than four and a half million customers across 13 states. [[1]](#endnote-1)

Dominion Energy has been around for quite some time. They used to be called Virginia Electric and Power Company (VEPCO) in 1925. This serviced mostly the state of Virginia. They were later branded as Virginia Power.[[2]](#endnote-2) At the same time, they owned businesses in North Carolina called North Carolina Power. As they expanded and purchased other companies in other states, they realized it was time to pull the company together. In the year 2000 that they re-branded all their operations to Dominion Resources to create a unified company. It was in 2017 that they re-branded once more to finally be called Dominion Energy. [[3]](#endnote-3)

Currently, Dominion Energy services electricity to Virginia, North Carolina, and South Carolina. They also service natural gas to Utah, Idaho, Wyoming, West Virginia, Ohio, Pennsylvania, North Carolina, South Carolina, and Georgia.

The beginning of my internship started out very slowly. The first day was fascinating. My new boss had to always escort me around the building while I had my badge created and completed some basic orientation guides. At first, he showed me around the common areas and where my desk would be located. He also introduced me to the other members of the team I would be working on. The cool part was when he took me to the protected areas, and showed me the server rooms, power generators, and Systems Operation Center (SOC). This is the area in which operators continually monitor and manage the electrical distribution of all the substations throughout Virginia, North Carolina, and South Carolina.

I was also treated to lunch on the company and then left to do some orientation training at my new desk. After the first day I was amazed and overwhelmed. My manager through a lot of information, new terms, and more acronyms than anyone should ever have to know at me. He did let me know that learning all of this would come with time and experience.

For the first two weeks of the internship, I was left to complete various online orientation videos and guides. I was also sent to watch and start learning from some of the other members of my team. They were all very nice and helpful. None of them had any problems showing me what some of their basic work tasks looked like and what I would be doing soon. I was definitely looking forward to my summer working here.

**Management Environment:**

The management environment with this internship was very relaxed. My boss would check in on me a few times throughout the day for the first week or two, but then I only talked to him a couple times a week after that. I thought that I would have more interactions with him, but instead he had a hands-off approach and let me learn from the other members of the team. I think this was partly due to the fact that he was the manager for six different teams and was always very busy. This was actually nice in my opinion as I would get stressed out if he was constantly checking in or quizzing me on things that I was just learning.

He did have an open-door policy. His office was almost always open and anytime I had a question he would make time to explain things to me. He seemed very well respected by every member of the team but was also very friendly and would create conversation if he had time to spare.

**Work Duties:**

The major focus of my work duties was to complete compliance tasks for my team. These tasks came from multiple NERC CIP standards. Some of the more important compliance tasks were managing baselines, completing Cyber Security Test Plans, and Performing Cyber Risk Assessments.

The baseline process consisted of managing all the software that was on a “NERC” cyber asset. I had to create a list of all the software on the systems and check to make sure they were all authorized software. I also had to add new software to the baseline if it was recently installed on a system as well as track all the security patches that were installed onto the systems. This was an extensive process as there were 88 cyber assets classified as NERC that I was working on. Fortunately, I was able to use a tool called OpenAudit. By having scanners in different VLANs, it was able run different queries we set up to look for things such as software, open ports, and local accounts and groups. This made is possible to create those reports utilizing data collected from OpenAudit. I then still had to go through all the data to ensure it was accurate and that if something on the baseline changed, there was an associated Change Order (CO) that was approved for the change. After completing all of this, I had to label and store the evidence in a secure repository for future audits.

I also had to do something similar for a ports baseline. I had to manage a list of all approved ports on each device and spot check the assets by reading all the current open ports after any changes were made to the system. This was to ensure no new unauthorized ports were opened by new software or that nothing was open as a cyber vulnerability. I then had to make a report of all this to store as evidence as well. If for some reason an unauthorized port was open, I had to report it to a Cyber Risk team and find vendor documentation stating what the business reason is for needing the port open, otherwise we would have to go in and block the port. These reports were important to the business as part of one of the CIP standards was to only allow authorized ports to be open on NERC cyber assets. They also relied on the accuracy of these reports for future audits to show evidence that the company has been compliant with NERC CIP standards throughout the audit period.

The next major task that I performed for my team was the Cyber Risk Assessment. This was a task performed at the beginning of each month to evaluate all the security patches that were supposed to be pushed to the cyber assets throughout the month. Different teams would send me files with all the patches that they wanted to push onto my team’s assets for the month. I would also take any software or patches that my team wanted to push and turn it into a report that showed each asset linked with the specific patches. I would then have to go through the list and make sure that each software or patch has gone through a verification process. This process had a script that would compare the software downloaded from the site with what the vendor expected it to be. For example, the script would check the hash values to ensure that they match, or it would check for a valid digital signature form the vendor. I also had to ensure that the sites the software came from were on an approved list from the cyber risk team. This is important to ensure that only the proper software packages are being installed onto these assets that help run our state’s critical infrastructure. The business takes cyber security very seriously and would not allow any software that might contain a virus to be installed onto their systems.

The third major task I would perform for me team was the Cyber Security Controls Test (CSCT). This was an extensive set of tests I had to perform on the servers after any patch cycle or change to the baselines had been made. The list of tasks included in a CSCT were checking for changes in the IP addresses, local accounts and groups, backing up installed media and the assets themselves, checking for unauthorized ports, verifying that the servers are still communicating with InTrust, a logging software, Truesight, a patching software, and OpenAudit. The main purpose of this test was to ensure that the functionality of all the cyber assets was still the same following any changes. I used different scripts as well as some excel macros to help automate some of the process since running reports on 88 different servers takes quite a long time. If there were any unauthorized changes to any of these tests, I had to report it and investigate which software was causing the change. We would then need to remove the software until we figured out why it was causing issues.

These three tasks are just some of the assignments I had to do or help with during my internship. The team has too many different tasks to count and thirteen different NERC CIP standards to comply with, each having many sub-standards that required work to be done.

**Cyber Security Skills:**

I was able to understand many of the network diagrams and what roles different components were playing in the Energy Management System. This network is very large with many different types of servers including both Linux and Windows. They also had different routers and critical switches that helped route the connections to were they needed to go. I could see where the Electronic Security Perimeters (ESP) were as well as the different firewalls to limit traffic in and out of the ESP. I also had access to see the various firewall rules in place and could identify what most of the rules were doing.

On the job I was able to learn how to use vulnerability scanners and their various purposes in protecting systems. I learned how to scan the systems, view the vulnerabilities, and find the solutions to fix them. This was helpful to understand as it was more along the lines of what I would like to be doing in the future.

**ODU Curriculum:**

The ODU curriculum prepared me more than I thought it would for this internship. The cyber security major requirement classes were helpful in some ways, but also lacking in others. Two important classes that I took were CYSE 270 and CYSE 280. These classes focused on Windows Server Management and Linux Server Management. The EMS team that I worked with for this internship managed both Windows and Linux Servers. The cyber assets were probably seventy percent Windows and thirty percent Linux. Although I was not on the team as an administrator, I worked alongside the administrators on the EMS for many of the tasks. I was able to understand what they were doing as well as help with some of the tasks because of what I learned in the classes.

Another important class was CYSE 250, the python coding class. This was helpful in learning the basics of coding that I was able to use to fix scripts or macros that were not working. I was able to go through the code and understand most of what it was supposed to be doing and, in some cases, figure out where it was breaking down. On the other hand, it was the only coding class I had to take, and I am not able to write much code myself. It would have been very helpful if I was able to have a better understanding of coding and be more efficient at it. I could have written my own macros, scripts, or code to automate some of the processes I had to do to save time and sanity.

CYSE 300 was also a helpful class as it introduced many important cybersecurity topics. Since I was able to understand how communication between assets and websites work, monitoring network traffic, and the different types of cyber-attacks, I knew what to look out for while running the different security scans and following traffic to determine if something was vulnerable or not.

I could also say that the various research classes I had to take and my ability to write papers helped with all the reports I had to create. It also helped with writing and updating various procedures for my team.

**Internship Objectives:**

I believe I was able to accomplish each internship objective to some degree. The first objective was to learn and understand the Northern Electric Reliability Corporation Critical Infrastructure Procedures and Standards for the energy management systems. I was able to learn and understand a lot about many of the standards, but each standard consists of many sub-standards, and it is a lot of information to absorb. The NERC standards are organized into thirteen main standards with each having its own set of sub-standards. These are all cyber security standards organized by numbers. Some examples include CIP-002 Critical Cyber Asset Identification, CIP-005 Electronic Security Perimeter, CIP-006 Physical Security of Critical Cyber Assets, CIP-007 System Security Management, CIP-009 Recover Plans for Critical Cyber Systems, CIP-011 Information Protection, and CIP-013 Supply Chain Risk Management. [[4]](#endnote-4)

As you can see, there are many different aspects to all these different standards. My manager said that the only way to fully understand them all is to work in the business over a long period of time. There are some people who spend over a year working and still don’t know all the different standards. So, I would say in my brief time with the company, I learned quite a bit.

The second internship objective was to support the team so that compliance was being maintained. I also believe that the internship fulfilled this goal. I truly felt part of the team towards the end of the internship. After a few repetitions of performing evidence gathering and running reports, they would rely on me to complete some of them on my own and then peer review it. It felt fulfilling to be helping the team.

The final objective was to use tools such as Nessus and OpenAudit to run cybersecurity scans and remediate vulnerabilities that were found. This task was not as fulfilling as I would have hoped. Entering the cyber security field, I was hoping to spend more time focused on defensive strategies and protecting networks. However, this job is more about maintaining compliance then it is doing specific cyber security related jobs. As part of an annual NERC CIP Standard, the team must run a cyber security scan on all their systems and then create action plans to start remediating the issues. However, this seems to be an ongoing task that members do whenever they get spare time, which doesn’t seem often. They showed me the list of vulnerabilities form their last scan and had me investigate a couple of them to be fixed. I was able to submit ServiceNow Tickets to the proper teams to have the issues solved. An example of this was using old certificates and adding in new firewall rules.

**Exciting Aspects:**

One of the most exciting aspects of this internship was towards the beginning of the job. When my manager took me around the building and showed me all the servers, we had along with all the protections and the ways the company generated all the electricity to be sent to the substations and then houses around, I found it fascinating. He also showed me the Systems Operation Center, where operators around the clock are controlling the substations and managing electricity throughout the state. It made this job feel important and that I was doing something worthwhile. If my team was unable to operate effectively, then the operators would be unable to their job and everyone using Dominion Energy’s power would be helpless. This motivated me to want to be successful with the team.

**Discouraging Aspects:**

There were a few discouraging parts to learning this job. One of the main parts was the sheer amount of information I had to absorb in such a small amount of time. I am the type of person who wants to do a good job and be above average when it comes to working. I wanted to be able to understand the NERC CIP standards and be as helpful as possible. It was discouraging that it would inevitably take me over a year to understand the standards and become self sufficient if this was my full-time job.

Another aspect that was discouraging was how much paperwork I had to do. I have been told that the cybersecurity field is vast and there are many different types of jobs within it. I would guess that most people want the “cool” jobs where they can practice penetration testing or dive into the systems and utilize codes and firewalls to protect networks from attacks. This job is not like the movies, which I knew heading into it, but it could be very dry at points. There was a lot of updating procedures, running reports, and analyzing information. I could see this becoming tiresome over a long period of time.

**Challenging Aspects:**

This job was not all that challenging compared to other jobs I had. One thing I had to get used to was being in an office all day. My previous job was in the United States Navy fixing helicopters. I was outside working most of the day and it kept me busy. This was a real change of pace having my first office job.

Another thing that challenged me was the NERC CIP Standards as I have previously mentioned. The standards go in depth on so many topics and it was difficult to try and remember which ones applied in certain situations. It was also difficult to just read through them all and understand what each standard was asking for as evidence of compliance. I think once an employee can figure out what the standards are asking for, the job is not the difficult.

**Recommendations:**

The biggest recommendation I would give future interns in this internship is to be patient and have an open mind. There are many different types of cyber security jobs in the industry and sometimes getting the one you want might be limited. Getting a foot in the door is a great way to start networking and building a resume for the ideal job. This job is not the most fun and can be very tedious at times. A large company like Dominion Energy does have other cyber security departments with different jobs such as managing firewalls or building networks. I have been told that they also promote changing roles within the company to gain experience in different departments to become more knowledgeable and qualified employees.

I also suggest that they be prepared to study and be able to read through the standards required for this job. It takes effort to learn the NERC CIP Standards. There is a lot of information for the intern to go through and start learning. It also takes time to get your access approved to start performing the duties of your job. This is a great time to start diving into the standards.

**Conclusion:**

This internship was an overall beneficial experience for me. This was the first opportunity I have had to do an office job as well as work in normal office conditions. I was able to understand what it will take to start out in the cybersecurity field. I made good connections there and hope to possibly work there in the future.

This internship has helped motivate me to finish out my time at ODU strong. I want to finish the rest of my classes, learn some new skills, and transition into the workforce to start earning money.

I have reaffirmed that I want to follow the path into the cyber security field. I enjoy working with computers, networks, and security. Although this is not my ideal job, I know that it is a great entry point to build experience and skills that will help translate into a more ideal job in the future. I plan to try to work my way up to something that is more interesting and less paperwork.

**References:**

1. https://www.dominionenergy.com/our-company [↑](#endnote-ref-1)
2. https://www.powermag.com/history-of-power-dominion-energys-fluid-transition [↑](#endnote-ref-2)
3. https://en.wikipedia.org/wiki/Dominion\_Energy [↑](#endnote-ref-3)
4. https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx [↑](#endnote-ref-4)