Internship with GFT Inc.

Safety and Security Department

Cybersecurity Analyst

CYSE 368, Summer 2025

Nicholas Carter, 08/03/2025

Table of Contents

1.Introduction

I decided to do an internship with GFT for the Summer 2025 semester because they offered a wide range of learning opportunities such as working with multiple different companies and utilities, documenting networks, and gaining a better understanding of governance compliance and how they are used to support cybersecurity operations.

GFT is an AEC Firm (Architecture, Engineering, and Construction Firm) that works on a wide range of projects such as transportation, water, power, and building convergence. GFT started out as Ganner Fleming all the way back in 1915 and merged with Transystems (which was founded in 1966) just recently at the beginning of 2025. The company has many different sectors of operations such as industrial engineering, civil engineering, federal consulting, and safety and security. *(GFT.inc, 2025)*

My internship was done at the safety and security part of the company as a cybersecurity analyst. Going into my internship my top three objectives to learning were to learn as much as possible about cybersecurity governance, get experience out in the field seeing a SCADA system and documenting devices on the network, and gain technical experience with outlining and documenting a network's infrastructure.

My initial orientation of the internship started off a little rough. The first day I had to get my company computer up and running but there were thousands of interns starting at GFT who needed the same help. So, I had to wait to get connected with the personnel. After I got connected I worked with a member who was not typically at the helpdesk and he remoted into my computer in a way that was not conventional with how the company typically operates, which triggered a cybersecurity alarm on GFT's end. Due to this happening, I received a call from GFT's lead cybersecurity analyst who then called to talk to me about the "incident" and we cleared up that is was a misunderstanding. But this gave me the chance to meet a member of GFT's own cybersecurity team, and we ended up keeping in touch throughout my internship.

The rest of my initial orientation and onboard training was held in GFT's learning management system and Percipio. The LMS courses were mainly HR courses such as workplace safety training, active shooter procedure, required documentation, and sexual harassment training. The Percipio courses I was assigned were actually made to get me prepared for a CompTIA Security + certification and helped me refresh knowledge I have already know and gave me knew knowledge to apply towards the internship.

The next thing I learned in my onboarding was the correct procedure for making sure documents and work done are suitable to be submitted to clients. To teach me this, GFT set up a large interactive meeting for all interns and they walked us through the process.

The steps were to gather information, create a draft, revision, then to go through multiple quality checks from others, and collaborate to make a strong final document. This was the one of the most critical things I learned in my internship since I used it probably the most out of anyone of these procedures.

My initial impression of the company was how professional and helpful everybody I interacted with. I had the opportunity to have meetings and learn from a bunch of different people from separate sectors of GFT and they all happily walked me through what they do, how they got there, why it is important, and what advice they have for me. I was relatively confused and nervous at first but being able to meet and interact with so many people around the company was incredibly helpful.

With the internship being all remote, my biggest fear was there not being much structure in my internship. This was not the case, since on the first day I had an hour meeting with my supervisor where they laid out steps for me to gradually learn and get moved into doing hands on work. My supervisor laid out that as well as my schedule, which consisted of five 7–8-hour workdays a week and what I was going to be doing on each of those days. And I got told if I ever got to the point where I had no work left to do I could reach out and they would urgently find me something to do.

2. Management

The management environment was interesting because although there was supervision and accountability, it did not feel like I was being heavily managed because everybody including the department leaders collaborated with one another on tasks to get them done. I typically would be assigned tasks by my supervisor Kandace Jennings, who answered to our Safety and Security Director Bill Foos. But the main way work was monitored depending on who the project leader was. For example, if Bill was the project head and I got assigned work from him then he would reach out to me directly and I would directly send the work back to him. This happened through him and multiple different project leaders. So even though I was directly under Kandace, who I answered to depended heavily on who was leading the project.

My supervisor's main role was to make sure I and the rest of her team was doing enough work throughout the week to hit my utilization goal as an intern. Since she was the head of the cybersecurity team, she also was widely responsible for networking and finding the cybersecurity department more work to do. And Bill oversaw all the other branches of safety and security such as physical security, incident response, and recovery. One benefit

to all of these branches being under the same management umbrella was everybody being able to collaborate efficiently within the department overall. Which was very important because most of the time these clients were needing help from multiple different branches and there was a considerable amount of overlap of duties.

The main accountability at my internship would come at the end of the week where I would have a one-on-one meeting with my supervisor. Prior to the meeting I would fill out a weekly engagement report going over what I accomplished that week and how I did so. Then my supervisor would give me feedback and go over what was coming up next week.

3. Major Assignments

My work duties had a large range from writing and reviewing documents, collaborating on technical cybersecurity-based projects, and attending meetings for note taking and team reviews. A great part about the internship was how many different projects I got to work on and how my assigned tasks would heavily vary depending on the project I was working on.

Unfortunately, I am not able to show samples of any work I did because it is all restricted access for our clients that I am not able to share as it has been made to be kept private for their operations.

Governance Documents

A large part of my internship consisted of reviewing governance documents for different utilities and going through them to make sure the information was correct and also written to where these documents could be used effectively. The documents I worked with the most were incident response plans, secure document handling procedures, and network monitoring plans.

Incident Response Plans

I was given the opportunity to write multiple cybersecurity incident response plans for water utilities all over America. This was a great learning task since I was able to reference and learn more about governance standards such as NIST's OT Cybersecurity framework and ISA ISO/IEC 27001 standards. One thing I was surprised to see was how much detail went into these documents. Because in the procedure it had to be written for multiple different departments, and they all had unique roles in their responses. Then I had to take the different information and scenarios of each utility to successfully make a draft of the document that was specific to them.

Secure Document Handling Procedures

Secure document handling procedures were a big emphasis on these projects. Most OT facilities do not have proper cyber hygiene when it comes to the way they handle documents. So, I would be given the task of taking information we gathered from touring facilities and interviewing their personnel to make a practical secure document handling procedure. While they all followed the same procedures, they did not all operate the same way. Sometimes the I&C operators played a large role in securing documents and other times it was DIT's job to make sure that documents in the facility were secured correctly.

Regardless of how the facility was laid out, the standards applied the same way. The main principles to keep were that documents needed to be transferred over secure network protocols (such as TLS or SFTP), there needed to be consistently updated and verified backups locked in a separate location, and role-based access control based on labeled sensitivity for each document. *(National Institute of Standards and Technology., 2025)*

Network Monitoring Plans

Every OT system that we worked with needed a lot of work on how they monitored their OT networks. Monitoring OT networks is not quite as simple as monitoring IT networks. A large reason for this is that a lot of the devices on these networks are very old and use old protocols to communicate with one another. The OT network is also very fragile so it is a must be very passive when monitoring the data being sent around.

In the majority of the documents, a big emphasis was manually going through the devices that use the network and setting up a network diagram of the entire utility. So, we would document the steps to take to do so, then we would take the tool that the utility intends to use and go over how it can be most effectively utilized.

Technical Cybersecurity Projects

The most exciting tasks I got assigned were easily the more technical projects for me to do. A few of these tasks were going out on site and doing packet captures, mapping out networks, and passively scanning OT networks.

Packet Captures

Although it was not a main focus for many of the projects, it was still assigned to me a couple times to go out and do packet captures for a utility. The packets that I captured were then saved and taken back for the rest of the team to review and help us get an idea of what the typical network flow was for the utility. While reviewing these packets there was never anything overly exciting to look at like a live cyber-attack, but mainly just PLC's and

RTU's communicating across the network. It was still beneficial to gain hands on experience doing it over multiple different systems in a real-world environment.

Mapping out Networks

I worked a lot on networking with a cybersecurity expert named Gus. He has been working on a large project in California over the past few years, and he emphasized to me how much learning networks has helped him in his career. Even though I was not assigned to his project he gave me some hands-on networking things to do. With the main project being mapping out an entire rail systems network.

In this project, we went and used Cisco configurations to gather all the devices and IP addresses and what router they were sending their traffic through. This started out as a daunting task, and I needed his assistance when we first started. But over time as I worked through it my understanding rapidly expanded and now I feel confident I could do it for just about any network that has a documented Cisco configuration.

Passively Scanning OT Networks

OT networks are incredibly fragile, so when learning about these networks we cannot just go through and do an NMAP scan to find out the open ports and what protocols get used. A large part of our data collection was through packet captures. But this is not always going to tell the full story. To fix this, we got the utility to install and use an OT detection Network called Claroty that did a mix of passive and active scanning.

Although the scan was active, it was not your typical ARP request spamming across the network. It instead sent out a set of lightweight queries throughout the network to detect devices without breaking the network like a large NMAP scan would.

Team Collaborations

While it was not the most exciting part of the job, a portion of the time I spent with GFT was listening in on meetings and note taking. Then after the meeting was finished I would throw together a report and send it out to the rest of the team. This was beneficial to the team since it was a way for them to keep track of what had and had not been discussed yet. My favorite collaboration we would do was just a cybersecurity team meeting that would occur biweekly. In these meetings we would all go around and say what we have been working on and then Bill and Kandace would go over what we were lining up for future work.

I enjoyed these meetings because it really helped me understand what was going on if I ever felt behind or out of the loop on something. But I also enjoyed it because it gave me the chance to speak up and tell everybody what I had accomplished over the past couple weeks and if anybody requested help I could speak up to get myself enough work to stay

busy. And being able to keep the notes I took was beneficial as well because if I needed help on a project I could just check the notes to see who was assigned to the project I was working on as well. These meetings and collaboration projects gave me great insight on how to work as a team in a professional cybersecurity environment.

4. Skills and Knowledge Learned

During the internship I was able to progress on many of the cybersecurity skills and some of the knowledge I already had. Some of the skills I branched out my knowledge on were cybersecurity governance compliance, networking, and business writing.

Governance Compliance Application

Going into the internship I thought I had a firm grasp on the governance side of cybersecurity since a few of my classes have covered it. But in reality I had no idea how granular it truly was and how deep the standards were. When it came to standards such as NIST Cybersecurity Framework I knew most of the components of it. But I never had to actually apply or use these standards to put into practice. When I was given the task of doing so at first I froze and ended up throwing together documents that were subpar. But by going through the review process and seeing the comments from professionals on how I could improve I was able to sharpen my application skills drastically. One thing another analyst named James showed me was that for something to be applicable you need to have a firm grasp of what is going on at the facility and see what micro steps that can be taken overtime to get to a good standard. By taking advantage of the people around me, I gained what would take people years of experience to learn in just a few months.

Networking

During my time at ODU, I have had the chance to use controlled environments to practice the technical side of networking. While this did give me a solid set of foundational skills it did not prepare me to go work in a live setting to the extent I needed. The first time I took the packet capture on the OT network I had no clue what I was looking at when the data came swarming through. Thankfully I had my supervisor and a couple other colleagues to guide me through what we can filter out to make it less overwhelming. And they also showed me in a step by step what these packets mean on a live network such as where they are going, what outside communication looks like, and what suspicious behavior looks like on a large live network.

Business Writing

One thing this internship required a lot of is writing. Going into the internship I was very confident that the writing skills I had would translate well towards my work. But early on I realized that my writing in comparison to everybody else was inefficient. I barely used headers on my work, did not get to the point quick enough, and wasted a lot of time using filler words. By seeing the way everybody else communicated I was able to adapt my writing to be more sensible in a professional environment. Small things such as sending emails with the appropriate tone or communicating with a client in the comments in a Word document were all skills I assumed I already had down. Even though it seemed like an easy skill to master, it took a lot of time and effort, and I still feel that I have more work to do before I can call myself an expert in that area. But at least now I can say I know I have improved significantly and can see the areas of my writing that still need to grow.

5. Learning Objectives Results

Overall, I would say that I have completed the objectives I set at the beginning of my internship. My objectives were to learn as much as possible about cybersecurity governance, get experience out in the field seeing a SCADA system and documenting devices on the network, and gain technical experience with outlining and documenting a network's infrastructure.

Learning About Cybersecurity Governance

Learning about cybersecurity governance was a big goal of mine and I would easily say I reached it. While there is certainly more for me to learn, I am beyond pleased with the progress I was able to make in just a few months. Going into the internship I did not even know what a draft to most of these procedure documents looked like, now I can go through a facilities list of documents and say what is missing from their archive.

Exploring SCADA Facilities

Another goal of mine was to go onto the field and visit SCADA sites to see how they operate. I had the opportunity to go and do this with about 5 sites total and interview the employees who worked there about the operations. They gave me more of a detailed rundown of the components such as the RTU's, PLC's, and HMI's and how they applied for the specific utilities. This was more than I expected to get and I was very pleased with the number of in-person visits that GFT set up for me to go to.

Outlining Network Infrastructure

One of my weaker points in cybersecurity always seemed to be the networking side for me. I wanted to grow and deepen my understanding about the layout of networks and how to go about mapping it out. I expressed this to Gus over a call, and he took the idea of putting me under his wing to help me grow my understanding and get hands on experience. In the process, it achieved my goal of deepening my understanding of networks and being able to document and map out how a network is set up.

After going through the projects completed, it is easy for me to say I hit each of these objectives and some. Going into the internship I was a bit naïve on how much I did not know, and it was really nice to see how much room for growth I had. Gaining my experience through these learning objectives were great, but I now know I have a lot more to learn about and am excited for another year of school to be able to refine my skills and continue growing in the field of cybersecurity.

6. Most Motivating Aspects

The most motivating aspect of the internship was definitely the amount of positive feedback I would receive from the people I was working with. Everybody was aware that I was an intern with little experience, so they did not expect me to be perfect, but instead just liked that I gave all of my assignments a strong effort. All of the critiques for my work was constructive and never done in a harsh way or with a negative connotation. And in meetings they would always give me a chance to speak or voice my input. Even if what I was asking seemed simple to them, they never had a problem with going over it in a step-by-step manner to make sure I understood.

7. Most Discouraging Aspects

The most discouraging aspect of my internship was probably the lack of instruction I was used to receiving in school. Throughout school, all of the assignments I have been given had clear guidelines to give me suggestions for how I should go about completing assignments. I never realized how helpful these direct guidelines were when it came to starting and completing projects. At the start of the internship, I was a bit caught off guard at how little direction I was given for assignments.

They would say something like “research these software platforms used by this electric water utility.” And then my job would be to go about how the best way I could condense my research into reports that would be used to communicate with others easily. I would not be given guidelines, an expected format or word count, or anything in that realm. So at first it

was a bit frustrating, and I felt a bit confused. But the more I worked at it the more comfortable I felt. Now I have absolutely no problems establishing my own guidelines and using my intuition as the best way to approach an assignment.

8. Most Challenging Aspects

The most challenging aspects of my internship was communicating with clients, keeping up with and finding work, and learning how to effectively communicate in a remote environment.

Communicating with clients

Communicating with clients in itself never seemed challenging to me. But then when it came time for me to be asking them interview questions or work with them to figure out the next steps in the project to help benefit them I got really nervous. The reason was because I knew that it was incredibly important to represent GFT in a positive way. And that if I had any negative interactions with clients it could lead to the department losing work. While it has gotten easier, there is still a large amount of pressure for me when I interact with clients.

Finding Work

One interesting part about being on the consulting side of cybersecurity was the search for work. There was not always a clear path for me on what I would do week after week even if my supervisor went over it with me. For instance, if I finished my work early and still had 3 hours of work I needed to do in the day I would have to frantically search around to find ways I could contribute to the team. This was certainly a more stressful part of my internship.

Communicating in a remote environment

Being in a remote environment for my internship was not easy for me, especially in the beginning of my internship. A small part of me felt very isolated at some points because I did not know the steps to take to be a part of what was happening with the team since we were not in an office together. Over time, I saw the value in taking initiative and setting up meetings with everyone as often as possible to make sure I kept myself in the loop and not just relying on my supervisor to reach out with work to do.

9. Recommendations for Future Interns

My recommendations for future interns in my position would be to polish up on professional writing skills, be bold in reaching out for help, and to know the OT cybersecurity standards going into the internship. These were skills that I heavily underestimated the importance of, but if I would have made it more of a focus I may have had a much easier time throughout my internship.

10. Conclusion

My overall takeaway from my time interning at GFT would be that experience and growth in the field of cybersecurity goes much further than I thought it did. I have a lot to learn and grow still, so seeing the way seasoned professionals operated and how much knowledge they had was an eye opener. By being able to work alongside them I gained so much wisdom from them that I will certainly be able to apply to my career as it is kicking off.

The internship will have a very positive impact on the remainder of my time at ODU. I now know much more about what real life cybersecurity work is like and how the assignments and what I learn in school will apply. Instead of doing assignments to check off the notification on canvas, I now know what I can take from them and put forward towards sharpening my skills in cybersecurity.

One valuable thing the internship showed me was that I want to be well versed throughout cybersecurity. There are many sectors of cybersecurity and if I as a professional cannot speak to each one then I will not be as valuable an asset towards whatever team I am a part of. So, in my career I will make sure to always stay well informed in every aspect of cybersecurity as it evolves.

I cannot thank GFT enough for giving me the opportunity to intern with them and I hope that one day I get the chance to work for them again.

References

GFT Technologies. (2025). *Ingenuity that shapes lives*. GFT. https://www.gftinc.com/

National Institute of Standards and Technology. (2025). *Framework for improving critical infrastructure cybersecurity* (NIST Cybersecurity Framework, Version 2.0). U.S. Department of Commerce. https://www.nist.gov/cyberframework

International Organization for Standardization. (2025). *Information technology—Security techniques—Information security management systems—Requirements* (ISO/IEC Standard No. 27001:2025). https://www.iso.org/standard/27001.html