Final Paper

CYSE 368: Cybersecurity Internship

4/21/2026

Julian Samonte

Employer: James Zeigler

Company: UJFT

Spring 2026

Introduction

Over the course of the last few months I've been interning at a company called UJFT which stands for United Jewish Federation of Tidewater. According to their website, The "United Jewish Federation of Tidewater strengthens and perpetuates Jewish life. As a leader and facilitator of collective action, we develop human and financial resources to meet the evolving and vital issues of our world-wide community, partnering with local, national, and global organizations." Their vision is to "Nurture a vibrant, engaged, inclusive, and caring Jewish community whose collective action is guided by their values." This campus has many different branches which range from a gym membership, a charity organization, as well as a school to provide to jewish Americans in the tidewater region. I have been interning under another branch for information technology and security. This branch is in charge of keeping all of the networks and endpoints that are present in the environment safe. They are also responsible for any technological problems that people in the organization may have regardless of what branch they work under. Any branch of this environment is able to submit a ticket to them and receive help if it is under their jurisdiction. My mom currently works at this building and she was able to talk to the head of information technology and security and I was able to get an interview with him. I already knew the building pretty well and my initial impression of the environment was pretty good as I went to preschool there as well as used to use the gym that they have. In the beginning I was given an interview and off the bat I could tell I wanted to intern here. I felt that these guys knew what they were talking about and they are able to teach me more than just cybersecurity techniques and lessons I haven't already learned. I knew that they were able to teach me what an actual work environment would be like as well as how to solve problems outside of just the cybersecurity aspect. Which brings me to my three learning objectives for this internship. My first learning objective that I wanted to focus on was to apply cybersecurity principles in a real operational environment across various stages of IT support. The second was to develop hands-on experience with security tools, systems, and processes within an ITIL-aligned service management environment. The third and final learning objective was to strengthen documentation and professional communication skills through security focused email correspondence, service management platforms, and knowledge base development. These three objectives felt very important to learn as I have no prior experience in a work environment. Learning guidelines and principles in a classroom environment is very different from actually having to apply them in a real world/workplace environment. I was hoping that this internship was able to teach me how to do this.

Supervision and Effectiveness of My Internship

My internship's management environment was very collaborative making it a good productive and learning environment for me. As I was able to work on problems

myself with additional help from my supervisors if I needed it. A Director of Information Technology and Security led the team, with two additional IT specialists. Even though there is a clear chain of command, the team works together in order to solve the problems that are present to them. This management environment allowed for open communication making it easy for me to ask for guidance when it is needed and share some ideas that I had to solve vulnerabilities or problems that they had. They were also very open to hearing me out on ideas that I had, not letting any sense of ego get in the way of solving their vulnerabilities. The supervision in my internship was a very effective style of teaching for me because it was a perfect balance of guidance and independence. Rather than assigning tasks without context or just solving problems as I watched, they took the time to walk me through the processes step by step on how they would complete a task. They were also able to explain every step of the way why they would use a certain approach. After they walked me through the process they tasked me to solve problems by myself. They provided me with guidance when I needed it but they allowed me to have space to think critically and develop my own solutions with my own knowledge. This supervision style helped me towards one of my learning objectives of developing hands-on experience with security tools, systems, and processes within an ITIL-aligned service management environment. This improved my confidence in solving these problems as well as my technical abilities as I was constantly applying things I've learned in a real work environment. Another aspect of developing hands-on experience was learning the tools that they use in their environment. Some of these tools include Atera, Microsoft Defender, Microsoft Intune, and Wizer Training. These apps were used to monitor endpoints, manage devices, create patches for their environment, maintain network security, and teach their employees the importance of being aware of threats. Giving me access to these applications and systems really gave me effective exposure to the tools I could be using in the future as well as what a day in the life of an IT specialist would look like. The management environment was very effective for my time here as an intern. The leadership, open mindedness to collaboration, and teaching style were all aspects that created an environment of learning and active participation. I didn't feel limited to just observing what they do, I was given the opportunity to contribute and actually felt like a part of the team. They genuinely wanted me to find ways to make their cybersecurity more secure and it felt like they actually cared about me developing an understanding of what they do. I really appreciated this approach and it helped me to gain the knowledge of an IT specialist leaving a real impact on me.

Work Duties and How They were Necessary

My major work duties, assignments, and projects included providing employees in the environment with a knowledge based document on basic security controls, a password policy improvement, investigating a suspicious application, coming up with a

plan for employees to complete security awareness training, and investigating a suspicious email for any kind of phishing attempts.

My first assignment was to provide employees with a knowledge based document on basic security controls. These controls include access control, multifactor authentication, endpoint protection, patch management, backup and recovery, network security controls, logging and monitoring, security awareness and training, and physical security controls. I had to state what the control does and why it is important. I was also tasked with noting which controls heavily depend on user behavior, where multiple controls work together to reduce risk, and any gaps or improvement that could be made.

My second task was to improve their password policy. The two improvements that they mainly wanted me to focus on in this project were to enforce a password history to 24 or more passwords and to set a minimum password age to 1 or more days. I was tasked with explaining why these changes were important and to outline the process I would follow to enable and enforce this policy. This was necessary in making sure that reusing passwords was prevented the best it could. As password reuse is a major concern for any organization, a lot of employees will want to use the same password for their accounts over a long period of time for convenience. Trying to use the same password could put the organization at risk and completely defeats the purpose of resetting and cycling passwords. This also makes brute force attacks much easier for attackers to get into an account. The set ‘Enforce password history’ to ’24 or more password(s)’ policy determines the number of unique new passwords that are required before an old password can be reused in association with a user’s account. Setting the minimum password age to 1 or more day(s) determines the number of days that you must use a password before you can change it, 1 day in this specific policy. Using these two improvements together could prevent an employee from reusing the same password as it would take them a minimum of 25 days to cycle back to the same password that they had. This task also showed me how to enable and enforce a policy. Letting them know what policy is changing, why this policy is changing, new guidelines that I’d like them to follow, and the exact date that it’s supposed to take effect. It is also extremely important to know how to communicate when a new policy is being rolled out.

My third task was to investigate a suspicious application that wasn’t updating when it should be automatically updating as patches are being implemented. This task had me use the application Atera to look into three specific devices to see the application and why it wouldn’t update automatically. When an application doesn’t update it could still contain known vulnerabilities that attackers are ready to exploit. That is why they thought it was important for me to look into to see why these weren’t updated potentially putting the environment at risk of attack. I was able to investigate and find out that two of the devices were laptops that had not been signed in for a while, meaning they wouldn’t have to update. The third device that I was told to investigate, I

was able to see that the user left the office for about a week and that is why their device hadn't received the patch yet. This project was necessary because it showed me that I need to be proactive on every vulnerability no matter how small in order to keep the environment safe from potential attackers. Teaching me how to monitor these applications and endpoints to make sure their software is up to date in order to protect itself from known vulnerabilities.

My fourth task was to come up with a plan for employees to complete security awareness training. Coming in they already had an idea of what program they wanted to use which was called Wizer training. This program is a free program that offers simulations for employees to complete showing them what a phishing attempt may look like. It also offers short videos to educate what potential attacks look like showing what red flags to look out for as well as what to do in response to these attempts. It offers short stories of real life scenarios that have happened showing that it could happen to just about anyone and it's not impossible to happen to them. It also gives the employees a short quiz at the end of each module in order to prove that they maintained the knowledge provided. I had to come up with a plan and hand pick which modules I were to assign employees of specific groups. I had to take into consideration which modules were most important and effective to not cause burn out for employees. I wanted to also make sure that employees are actually taking knowledge from the training rather than just going through it because it is required. Thankfully the module automatically pauses when going to another tab so they can't just hit play and do something else. It is essential for employees to also be aware of threats because if they're interacting with every link possible the technical level of security would just be ineffective. This was important in showing me what IT specialists have to go through in order to ensure an effective training program that can actually teach employees and strengthen overall security within the company.

My fifth task was to investigate a suspicious email that was sent to a few employees in the environment. An email was sent to 10 employees at different times and I was tasked to investigate if it was legit or not. Off the bat I could tell that this email had all kinds of red flags. To start, I think that it looked insanely fake and suspicious. It was obvious that this was a scam or phishing attempt at our employees. Another red flag that jumped out at me was that the sender's IP address varied from all of the emails that were supposed to be the same. Usually legitimate bulk emails from vendors are from a consistent known IP range and don't randomly switch sending servers. Multiple sending IPs can indicate compromised email accounts or a spoofed domain sent through multiple mail relays. Another thing that we were able to do was file detonation. This is where we are able to take the suspicious link attached to the email and execute it inside an isolated sandbox environment to observe if it is safe or not. It was not safe. It had asked for personal information from the person that the email was sent to. This task

also taught me about ZAP-successed messages. ZAP-success rescans emails for up to 48 hours and when Microsoft updates its threat intelligence it can identify malicious emails and can remove it retroactively. Something that happened was that Microsoft Defender showed that only 1/10 emails were blocked and I was confused on why only one would be blocked and not just have all of them blocked. I was able to investigate this and realize that the one blocked was sent at 7:23pm compared to the other emails being sent from 1pm - 2pm. By that time the email had been reported and threat intelligence had been updated meaning the system was set to block this email by the time the later one was attempted to be sent. The fake emails are now ZAP-succeeded since the defender had learned it was a threat to the environment. I was also told that one person had interacted with this email, but had not submitted any personal information. I was then tasked to run an antivirus scan on their device and let one of the IT specialists know that they needed to reset their password as soon as possible. Thankfully nothing harmful was found on their device, but we went ahead and reset their password anyway since they interacted with the harmful link. This task was extremely necessary in teaching me what to look for when it comes to potential attackers and suspicious emails as well as what to do if an employee were to actually interact with one of these emails.

Use of Prior Skills On-The-Job Experience

During this internship I was able to use a lot of the skills that I had learned prior to working there. For example I was able to apply basic policies in order to reinforce their security like multi-factor authentication, knowledge on best password practices, knowing what suspicious phishing attempts look like, and having an overall understanding of all the basic security controls listed before. Using my knowledge I was able to understand some of their vulnerabilities and propose changes to fix them lowering their vulnerability score. Surprisingly, a lot of their users did not have multi factor authentication enabled and I was able to point that out to them. It is a simple fix, but it is something that makes it much harder for attackers to gain access to their environment.

The internship has also taught me a lot of skills that I did not have before. I have no prior experience with cybersecurity or any IT work in a work environment, so I was able to learn a lot about their day to day tasks while at work. I learned how to monitor endpoints and how to actually carry out and enforce any policies or ideas that I have for the work environment. Before the internship I had many ideas of how to improve a security system or knock down a vulnerability score, but I had no clue how I would be able to enforce the policies that I've come up with. Using Microsoft Defender, Microsoft Intune, and Atera I was able to learn how to implement patches and security fixes to the environment I was working for.

How has ODU Prepared Me for This Internship?

I made a lot of connections between what I've learned in school and the skills used at the internship. As stated before I was able to apply basic knowledge and standards that I have learned in school. Things like MFA, password policies, ability to recognize a suspicious email as well as the capabilities of a phishing attack just to name a few. Using my prior knowledge I was able to know what exactly to do, but I was just in the dark about how I was supposed to solve these problems. However, that's where my new skills come into play. I was able to learn how to implement my ideas on a technical level. I was also able to learn how I am supposed to let everybody know what policy I am implementing as well as why I am implementing it.

There were also some experiences that I had during the internship that reinforced what I have learned in school. For one, multi- factor authentication and strong passwords are very overlooked for how important they are. They are two simple policies that can prevent a lot of trouble for work environments. A great majority of the environment did not have multifactor authentication enabled and it brought down their secure score by a great amount. Multifactor authentication is something that was heavily emphasized in a bunch of my classes. It really surprised me that it was not used as much as it should be in this environment.

A new technique that I was able to learn during this internship was the use of advanced hunting. Using copilot, as instructed, I was able to use a code to find out which endpoint actually interacted with the suspicious email mentioned earlier. I had never used this technique before and was fascinated with the capabilities of this technique. I had no clue this technique existed to track hashes and finding attachment opens within the system. This is what led to me finding out which device needed an antivirus scan and password reset. This technique can also be used to track filenames or URLs, confirm malware execution, and find where else files appear.

How Has the Internship Fulfilled My Learning Outcomes?

The learning outcomes that I was expecting to learn were to apply cybersecurity principles in a real operational environment across various stage of IT support, Develop hands-on experience with security tools, systems, and processes within an ITIL-aligned service management environment, and Strengthen documentation and professional communication skills through security focused email correspondence, service management platforms, and knowledge base management. I can confidently say that my internship experience was able to fulfill all of these outcomes.

When it comes to my first learning outcome I feel like I was really able to feel what it was like to apply my knowledge of cybersecurity principles in a real work environment. As I have stated many times in this paper already, I was able to really apply my ideas and knowledge to policies that they had. When I saw a vulnerability in

their policies or an anomaly within their system I was able to apply cybersecurity principles and let them know of simple solutions they could implement to solve these issues.

For my second learning outcome of developing hands-on experience with security tools, I felt that this was the outcome that was touched on the most. I have never felt what it's like in a work environment for this field so I was introduced to a lot of their software when I was first brought on. As stated before, I spent a lot of my time looking into Microsoft Defender, Microsoft Intune, and Atera to monitor and implement patches for the environment. I was also introduced to a ticketing system that I was unfamiliar with before coming into the internship. I learned how employees of the environment reported their problems and how the IT team assigned and tended to these problems. This was very educational for me as I knew ticketing systems existed, but I never knew how they worked or what they even looked like. I was able to shadow one of the IT specialists and learn how they react and responded to these tickets as well as being able to solve a few on my own.

For my third learning outcome of strengthening documentation and professional communication skills this was probably touched on the least. When I was coming up with policies and changes for the environment I had to email everybody that these patches would affect. Letting them know when the policy would be rolled out, why this policy was being implemented, and what it does. I also created a knowledge based article in order to educate employees on basic security controls. I was able to strengthen my ability to communicate with other employees in the environment.

Describe the Most Motivating, Discouraging, and Challenging Aspects of This Internship

For me, the most exciting aspect of this internship was the opportunity to get hands-on experience with the actual equipment and software used in a professional IT and cybersecurity environment. Before working at this internship, most of my knowledge came from courses that I have taken here at ODU. Being able to work with real systems made a huge difference on how I understood the field. I was especially excited to learn how they analyze endpoints and network activity. Most of all I really was interested to see how they are supposed to respond to potential security threats. Being able to see how everything works in a real work environment gave me a much better understanding of what a career in this field actually looks like on a day to day basis. As someone that doesn't have a ton of experience, getting the chance to get my hands dirty and actually participate in tasks rather than just watching was very effective for me. It gave me the opportunity to apply what I learned in school while also gaining new skills that I feel cannot just be taught in the classroom. Another motivating aspect of this internship was my conversations with the head of the IT department. After speaking with him I learned

that we shared a very similar background and math into technology. He was also introduced to devices at a young age and developed curiosity that turned into a career. Hearing his story made the idea of pursuing a career in cybersecurity feel much more attainable.

Something that was discouraging to me during this internship was realizing how much I still don't know about the IT and cybersecurity field. Coming into the internship, I felt like I had a decent foundation from school, but once I was exposed to a real work environment it became clear that there is a much deeper level of knowledge required to fully understand and secure a system. There were countless vulnerabilities that I had never encountered before and at times I didn't know how to properly address or fix them. This made me feel like I had just scratched the surface of cybersecurity. Everytime that I learned how to solve a vulnerability, it seemed like there were even more coming up that I hadn't even heard of yet. The number of potential vulnerabilities in a system made it feel overwhelming at times and made me question how it's even possible for organizations to maintain a safe environment for their employees. This reality was discouraging at first, but it also motivated me to keep learning in order to be more capable of handling these challenges in the future.

The most challenging aspect of the internship honestly was learning to get used to the schedule that was given to me. My internship started somewhat early and that was hard for me to adjust to. Another challenging aspect was that I am still in school so this made it hard sometimes for me to balance my life out socially, academically, and internship wise. Sometimes I had to drop some events that were going on that I really wanted to go to so that I could meet the hour requirements for this course.

The most challenging aspect of the internship for me was adjusting to the schedule that came with it. My internship started pretty early in the day which was difficult for me at first since I was not used to consistently waking up that early. It took some time to build a routine that allowed me to be productive at the start of each day. In the beginning, I found myself feeling tired and less efficient, but as the weeks went on I adapted and became more comfortable with the schedule. This adjustment taught me the importance of discipline especially in a professional environment where being on time and ready to work is expected. School is pretty forgiving when it comes to being on time however my job in the future will be a lot less forgiving when it comes to this. Another major challenge I faced was balancing the internship with my responsibilities as a student. Since I was still taking classes, I had to manage my time carefully academically and socially while still meeting internship hour requirements. There were moments when deadlines from school and responsibilities from the internship overlapped which made it extremely stressful to stay on top of everything. It required me to improve my time management skills and prioritize tasks more effectively than I had before. For example there were times where I had to miss out on events that I really wanted to go to at

school just to meet the hours that this course requires. At times this was very frustrating, but I knew I was making the right decision as part of the commitment I made and I knew it would help me to achieve my long term goals. These challenging aspects force me to adapt to a new schedule and although it was not easy I still think it was an important lesson to learn.

Recommendations for Future Interns at this Internship

For future interns, I recommend that they have a really good understanding of basic cybersecurity principles and come in with some ideas of how an environment's security can be improved. This is what a great majority of my work looked like. As stated before I was able to look into password policies, MFA, and implementing employee training. It would also be very beneficial for future interns to be exposed to common cybersecurity tools even if at a basic level. It's not expected to be an expert, but it is important to have a little knowledge on tools with endpoint detection, patch management, ticketing systems, as well as an application to monitor emails. This will help the intern to get past the introduction of these applications quickly to make the work easier to understand as well as being able to contribute much earlier than I was able to. This will also give interns a strong understanding of how their tasks are going to be handled in a real work environment. I would also recommend that interns come in with questions. The internship and supervisors here are a great opportunity to learn from, and the supervisors are always open to questions as well as being able to explain what they're doing as well as why they are doing it. Interns need to be engaged and comfortable with asking for help or confirmation from the supervisors that work here in order to make the most of their experience. I'd also say that time management is an important factor as interns could likely also be juggling school and other responsibilities. It's important to come up with a plan for the week as well as staying on task in order to meet the internship requirements without becoming too overwhelmed.

What are Some Key Take-Away Thoughts From This Internship?

My main take away thoughts from my internship experience is that real world cybersecurity is way more complex than what I had originally thought or experienced in my courses. My time at school provided me with a strong foundation in very basic concepts of cyber security like the password policies and MFA, but this internship really showed me that those principles are just the surface of a completely different level of security. I was able to learn how these principles are implemented in a real life environment as well as some other principles that are a little more in depth. Another thing that I took away from this internship was that cybersecurity and IT is more than just finding technical solutions to problems, it is also about how you communicate with other employees and how you can teach them to protect themselves. Another big take away I had from this experience was that it is important to be able to adapt to things and

continuously learn about new vulnerabilities as they are popping up all the time all over the work environment. Attack attempts could be happening daily and it is important to stay on top of that as an IT or cybersecurity specialist. For example, phishing attempts happen all the time making communication that much more important between you and your employees reporting the attempt.

How Will This Internship Influence the Remainder of Your Time at ODU?

I do not have much time left here at ODU, but this internship has really influenced the way that I will use my knowledge for when I graduate. I can see now that it is extremely important to connect my knowledge in my courses to real world situations. I plan on getting my certifications so that I am able to do more hands-on work as soon as possible. I want to be able to strengthen my technical skills as I can now see that I need to improve my understanding of tools and systems that are commonly used within this field. I really liked the endpoint management and security monitoring platforms that they were using at this internship, but I also want to familiarize myself with other platforms that could be used to be more useful to more companies. I am also still spending time with this internship and it has motivated me to ask more questions and take more initiative knowing that these questions can have a direct impact on what I want to do in the future.

How Will This Internship Influence Your Future Professional Path?

Thankfully, this internship has confirmed my interest in pursuing a career in cybersecurity and IT as I am moving towards a professional path. This experience has given me a better understanding of potential career paths that I could go for as well as an idea of some skills that I need in order to succeed in these careers. The internship has also shown me that both technical and professional skills are equally needed in order to succeed in IT. Not only do I need great technical skills, but I will also need to know how to communicate and document problems that I come across. I feel that this internship has taught me how to do well in both aspects. As stated before, I don't have any certifications so I feel that is the logical next step in order to get my technical skills on par with the new professional skills that I have gained from this internship. I want to be able to secure an entry level position that will allow me to continue building on the experience that I've gained during this internship experience. Overall I feel that this internship has made my goals feel more attainable as I did not even know where to start as a senior with no experience. I felt somewhat hopeless but it has given me a stronger sense of direction in planning for my professional future. I am excited to see what I can do in this field as I love technology and find cybersecurity very interesting.