Ethan Corder
Digital Wave
CYSE 368
Summer 2023

Table of Contents:

After having issues finding a proper internship I decided to reach out to my friend and mentor Luke who had told me about his transition to Information Technology and then to Cyber security and asked him for help in finding an internship. He then offered me a volunteer position where I could work with him at his company however the position was to be fully remote as the office was located in Missouri. After getting rejected from local internships I jumped on this opportunity to get some real-world experience. As well as being able to take this class to graduate. At the time I was relatively new to the professional work for cyber security and as well as a business environment. Goal wise I wanted to take this opportunity to get a better understanding of how cyber security plays into a business role other than what I have been previously taught. I also wanted to learn about Endpoint Detection and response systems since they have been something that was mentioned but not taught in my classes. I also wanted to experience Cyber security policies and tools used by businesses to maintain a secure environment in a digital space.

Digital Wave is a small business that operates in the Ozarks of Missouri and is a local business that helps smaller local businesses step into the modern age of compliance and security as well as ease of access. Their normal demographic for customers is local businesses in the Ozarks like tourist attractions and hotels and resorts. They also do work for schools and state and local government as well as medical and legal businesses. They provide many services such as a dedicated Information technology team as well as network installment and tech expansion. They also do Security measures such as endpoint security which I was looking forward to learning more about.

The First day of my internship was rather interesting as it required me to go through orientation. I had worked an internship before this at Towne Bank however that was in person. This internship however was fully remote and our orientation was more or less a powerpoint presentation that was one on one instead of a room full of other interns. In this orientation, a few things were overviewed like expectations and a list of duties that I would need to do while working there. They also required us to read their cyber security policy which was twenty pages long. In it the discussed topics that I was familiar with like no tailgating and locking your computer whenever you leave your computer for any reason. They also showed me learning objectives for my work and what I'll be expected to learn by the end of my internship. Some of those objectives were understanding my team's role in the company and learning the importance of team-oriented projects. My initial training had me shadow my mentor Luke who worked remotely as well and he was working to mature the cybersecurity program by implementing SOAR. He is currently shopping for vendors or considering the open-source tool "The Hive". It appears that they are leaning towards using automation built into Logpoint, as that is the SIEM being used. My initial impression of the company was good. I felt that it being a small company made it a good fit for teamwork and someone like me who had little to no experience in the industry. I was excited to learn and ready to jump head first into work.

The managed environment at Digital Wave was split into teams and each team had a supervisor mine was Luke and each team tackled different tasks that would arise from our clients. I believe this was a great setup for the business for me at least as it made it so that the meetings held team-wise were not a bunch of talking faces on a screen. Each team was small and consisted of six people who all specialized in their work. This structure also allowed me to ask questions in meetings and would allow for examples shown or walkthroughs of a problem that was presented. Generally, I like this approach. I have not worked for a larger business as of yet however, for a learning process a smaller team is better than a twenty-plus person team that is always going and doing assignments and not leaving much time for questions or help with an issue.

I start my day and work alongside one of the members of the team depending on what tasks are going on each day. I join the morning meetings that start on Wednesday mornings at 8a central time where we discuss how the week's start went and what else there is left to do before the end of the week. I was put under a team that did Endpoint detection and response systems. As I did not have any certifications they did not have me do anything very technical for the client. Although they didn't want me to handle any detections, they did have me help verify if there were any deployment gaps and present an Excel file showing what devices were covered by their RMM tool, Automate, and their EDR tool, SentinelOne. They also made it my objective to look into a report it mailbox for our company and the company that we were working with had possible phishing emails sent to them. They first taught me how to spot a phishing email and gave me strict instructions on not clicking on any links or attachments. The main reason that they gave was that if I clicked on any links or attachments to let our Information Technology department they could lock my account and run a scan on my computer so that there isn't any malware or keylogging software on the device. My team first showed me how to spot an email by looking at the grammar in the text to see if there were any large errors. The second thing to look for was to look at the links sent in the email. In Outlook, you can hover over the link without clicking on it and it will tell you the full link of the email. This was incredibly useful for Docusign phishing emails as it showed a false link compared to how a normal Docusign link would look like. That was my first initial duty. My second duty was to verify detections on Endpoint systems using SentinelOne. SentinelOne was an important tool that we used to detect anomalous activity that may lead to a cyber threat. We used SentinelOne to not only detect anomalous activity but it has a very detailed system process timeline that shows what data has been used and/or manipulated. This is important to the business as it serves as an alarm for any malicious activity and this is tied into the report it mailbox as some people do fall victim to these phishing attacks and SentinelOne was a way for us to detect someone who fell victim to a phishing attack. This showed up on SentinelOne's Agents which shows us that they went to a website that was not secure as well as any attachments in the phishing email that were opened. With this detection, the following actions were taken. Firstly the account and possibly the device are locked. This is because if someone had either malware on their device or had willingly given their credentials over to the hacker they could then access the employee's account. We don't want to take that risk so when an employee clicks on any links on an email or an attachment we lock their account to prevent any further escalation of an attack. From there we examined the email in question and looked to see if it is a threat or not. We used some sandbox features through SentialOne to examine links that we deemed to be suspicious. We then looked at where the link sent the virtual machine to and looked for any inconsistencies in the layout of the webpage. This included URL, website design, and other links that would normally lead to terms of service. An example of what a phishing page website looked like will be found in Figure 1 of the Appendices. In cyber security and threat monitoring, there are a lot of false positives that will pop up however each one should be treated as a threat until proven otherwise.

After I got accustomed to working with my team and attending team-related meetings they gave me a new responsibility of Verifying and logging all detections from SentinelOne. These detections were all false positives however we treated them as real threats until we had confirmation that proved them to be otherwise. One case example of this was when there was a detection at four am which was irregular as it was when the company that we were servicing was closed. The detection came from an alert about a Teamviewer session that had connected to a tool called Automate. This was alarming because this tool was vital for running automated programs and with this being a potential threat we had to investigate what was run through Automate. We used the Deep visibility function on Sential One to investigate and scrutinize every command written in the program. With some communication with the company and no apparent malicious code after our initial investigation, we found that the detection was set off by a legitimate technician working on an issue with Automate. This was a false positive as the person who was running a diagnostic of the program ran it at an irregular hour. This goes to show how important Sential One is but also how important it is to have an Endpoint team examine these detections as the majority of the time they end up being a false positive however in the chance that they are not a false positive and require immediate response. Unfortunately during my time at the internship, there was not an event that was not a false positive. However, for every single detection that happened, we treated it as a false positive. Even when we had used SentialOne's Deep visibility function and we found nothing we still treated this as a potential threat as it could be a risk factor for an attack that either we did not see or the system failed to pick up. However, after we received verification from the company we then determined it was a false positive.

I believe that everything I did working for the team was important to the business that I was working for as well as our clients. Because without it there would be no one to one determine whether a false positive was a false positive and if it was a real and active threat to go through the proper channels to respond to this threat and limit the damage done. I also believe that running a report it mailbox is important to mitigate threats as it's an easy entry point for a hacker to get into a system. By trying to block emails and shift through the false positives and real threats I believe that I provide an essential role to protect the company from threats and a pile-up of false positives.

I have learned a lot of information from ODU's Cyber security curriculum. During my time at ODU, I have learned about the importance of an organization's security as well as how to develop a basic network and how to secure the network from threats. I also knew how detrimental phishing emails can be to an organization as well as how fast an attacker can get access to a system and manipulate it to accomplish their goals. One thing that I noticed working at this internship is that my classes taught me about these threats but it didn't prepare me for how to stop and prevent these threats. For example, SentinelOne was a program that was never mentioned in class and I had no clue how it worked until I asked questions and did individual research outside of work to fully understand how the program worked. I believe that the ODU Cyber security curriculum prepared me for a basic understanding of how cyber security is generally best applied however it lacked specifics and this internship was about those specifics needed to address each different client. I feel that in the case of specifics I was unprepared. I understood the theoretical approach but the appliance of what I learned was difficult because it was different and looking into the details of data manipulation I had no idea how to determine what that looked like unless it was very apparent. However, with the help of Luke and my team, I was able to learn how to use SentialOne as well as understand what a threat looked like and what patterns existed to determine if data was maliciously being manipulated. I also noticed that I did not have a great deal of professional skills in communications and when I was at those meetings I felt I wasn't asking the right questions to answer the question that I was looking for. I also felt that I did not have experience working as a team as in class we rarely ever worked as a team to tackle a problem or question. However, after I got more and more exposure to the team experience, I got better at asking the right questions as well as being able to communicate with my team and ask for help when needed.

Overall I feel that I have gained a lot of knowledge from this opportunity and I believe that The cyber security curriculum prepared me for a theoretical approach to the problems and challenges that I faced working for Digital Wave however the how when fixing these issues became a challenge in itself to learn how to learn and adapt at a moments notice. I believe that while college has somewhat prepared me to examine these problems it is up to me to solve them and approach them with a critical-thinking mindset to find the best solution to the problem. Another difference that I found in working at Digital Wave was the new technology that is available for companies to use. Before in class, we discussed using anti-viral detection software however it was regarded as less effective because it lacked the technological innovation that current anti-viral detection software has now. In the past anti viral detection software had a definition list to look for when conducting a scan and is updated regularly. However, newer software like SentinelOne uses machine learning and Artificial intelligence to keep a constant update of threat definitions as well as closely monitor user behavior and can tell when a user is deviating from a defined “normal user behavior.

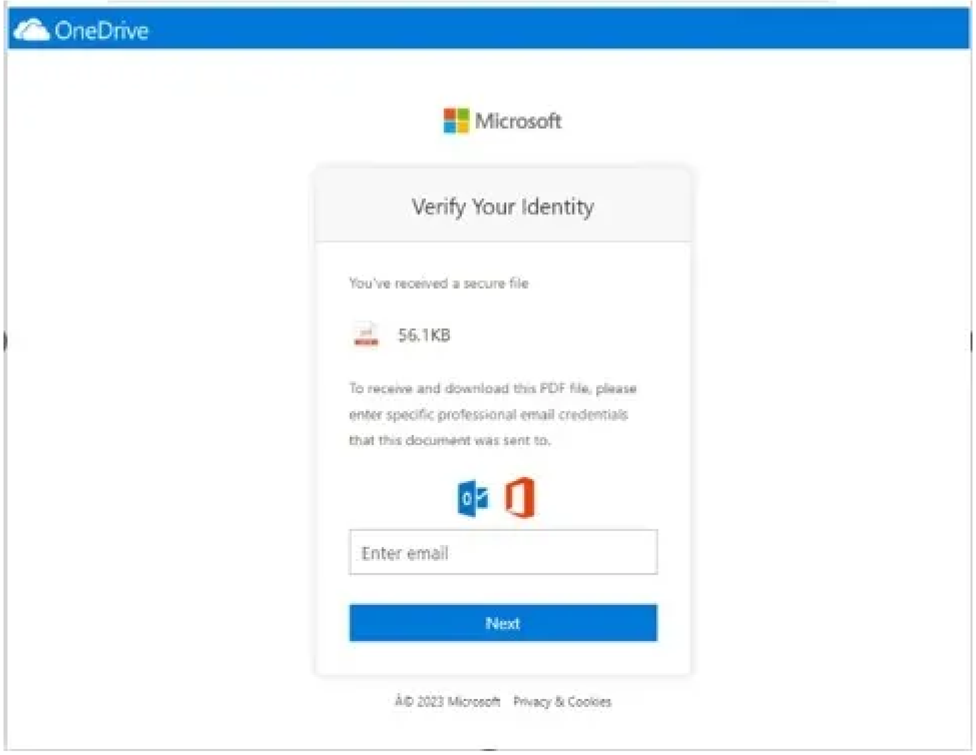
Previously In the introduction of this paper, I defined my learning objectives for this internship. They were: a better understanding of how cyber security plays a business role, learning about Endpoint Detection and response systems, and experiencing Cyber security policies and tools used by businesses to maintain a secure environment in a digital space. I can happily say that I accomplished all three of these learning objectives in my time working for Digital Wave. For “better understanding of how cyber security plays into a business role I learned how important cyber security is to a business even small business. Without cybersecurity, there would be free reign on information that is processed or produced by a company by hackers. I believe that cybersecurity is a line in the sand against business from attackers. I now appreciate the work that other cyber security teams do for business as they not only keep my information safe from hackers but also allows business to engage in online commerce. As for “learning about Endpoint Detection and response systems” I learned a lot about SentinelOne and how important of a tool it is to an Information Security analyst as it alerts a team to a possible threat. It also has great investigation tools with its deep visibility feature which allows us to take a deep dive into a system's usage and is an essential tool for investigating potential threats to a system. As for the response side, I did not experience a cyber attack or a realistic threat that was not a false positive. The only realistic threat that we encountered was phishing emails and employees clicking on those emails. We reacted by locking their computer and account to run scans and had them reset passwords to protect their account. However, that's all I experienced on that end. For the goal of “experience Cyber security policies and tools used by businesses to maintain a secure environment in a digital space. “ I saw the policies that we used when during the begging of the internship where I had to read their twenty-page cyber security policy and noticed some interesting points such as no tailgating at the entrance of the office, locking your computer when not at the desk, and have an independent password which not used anywhere else on the internet. I understand why these policies are in place and they give an idea of what real-world events can happen that may lead to a cyber attack. As I have heard of pen testers using tailgating tactics to get into a secure building and then finding an already logged-on computer and injecting hack programs into a system. As for tools used by these companies, I found that using Outlook and Microsoft Teams was very interesting as Outlook had a great tool for email filtering. My email had tickets and other reports from things that I did not use sent to my email flooding my inbox. Microsoft Teams were great for working in a small team environment and allowed for an open group chat that we would post to for events or questions. From there we also had the option to launch a meeting at any time. SentinelOne was the most important tool that I used at my internship and it took time to get used to as I was not familiar with the program but it was an essential tool for my work. It had machine learning and Artificial intelligence to track user behavior to determine if any actions that they were doing or any background programs were anomalous behavior and if they were they would send a notification to us and we would investigate the computer for any malicious behavior. Overall I feel that my goals were met while working for Digital Wave and I think that I learned a lot in my time there.

Every day I was very motivated to jump in to work and look at any phishing emails and determine if the email was legitimate or not. I will say that I was excited when a report came in from SentialOne for detection because it involved me working with Luke as we went through all the data from the computer to determine if this was a false positive or not. I felt motivated while working with the team and attending meetings because I enjoyed the work that they were doing and when we ran into an issue we would stop everyone else's report and deep dive into finding solutions for this problem. Overall I was very motivated to work with the team and I enjoyed working through every problem we faced. However, there were some things that I could say were a little discouraging in my internship. I came into the internship with no certification and to get a full-time position they did require you to have at least a Security Plus certification. This limited my knowledge and some of the work that I could do as an intern and during that first couple of weeks I felt a little bored from just doing the report it mailbox but when they started me on Detections and verifying them and then finally reporting them that issue was gone and I felt that I learned a lot from diving deeper into more responsibilities but I can understand why they wanted me to start slow and work my way up. If I had any recommendations for anyone who wants to work here for an internship I believe that having a form of certification will be helpful. I would say to at least have an A+ certification if you can't get a Security Plus or a Network Plus Certification. I also recommend trying to learn about data manipulation as well as some general process that a hacker could hijack because when we initially started looking at system resources and application processes I got confused about some of the system resources being used.

I had a great time working for Digital Wave. Luke is an awesome mentor and boss and he helped me a lot with my work and was honest about what I needed to improve on and what knowledge I needed to learn to improve at my job and in my professional career. Looking back on my time at Digital Wave I have learned a lot and I now have my foot in the door for my professional experience and I can use what I have learned in my future work. Everyone at Digital Wave was friendly and encouraged a working and learning atmosphere. I believe that after my first two weeks there I excelled in work and came to a better appreciation for the work that I do and I believe that I made the correct career choice. Being exposed to real-world scenarios has improved my knowledge as it allows me to draw upon some of the knowledge that I gained from college but it also allows me to draw upon working knowledge and allows me to see patterns in detections and phishing emails. For the rest of my college time, I want to further study cyber security and learn more about Endpoint security as well as penetration testing and working with companies to test Endpoint detection and response systems. I hopefully only have one semester left until I graduate so I want to take that time to focus on taking more cyber security classes as well as trying to get some certifications for my professional career. For my professional career during my search for an internship, I also asked my brother if he knew anyone who could assist me in finding an internship and he contacted a friend of his He offered me a job however it does require a security clearance but they are willing to sponsor me to get that job. Unfortunately for me and my wallet, I could not get that job in time for this class as the security clearance is going to take time to process. However, for my professional career, I will be starting as Junior Developer at Trilogy Incorporated and I can't wait to take some of the professional knowledge that I gained at this internship into my new job. This internship has shown me a lot of options in terms of jobs that I can do with my degree and hopefully, I can decide on what role I want to be in the future company that I will be working for. In conclusion, I have enjoyed my time at Digital Wave and I am glad I got the opportunity to work with Luke and the rest of the team. I have learned a lot of important professional knowledge that I will take with me for the rest of my academic career as well as my professional career.

Appendices

Figure 1



Verify Your Identity

You've received a secure file

56.1KB

To receive and download this PDF file, please enter specific professional email credentials that this document was sent to.

Works Cited

Pernet, Cedric. “Microsoft Phishing Page.” *Tech Republic*, 13 June 2023, www.techrepublic.com/article/microsoft-news-business-email-compromise-attacks-phishing/.