Cybersecurity Internship Final Paper

Jonathan Roeseler

Old Dominion University

CYSE 368: Cybersecurity Internship

Xylem Tree Experts

December 7, 2025

Table of Contents

Introduction

My internship with Xylem Tree was primarily because I was job searching (I had this job for several months before this class), and they made a great employment offer. There were many learning and growth opportunities available from my position as an IT Helpdesk Technician. I hoped to understand how IT works in a large organization, understand the systems that enable our company, and seek growth opportunities by trying to learn and understand every system or tool I could get my hands on. As the name implies, Xylem Tree is a vegetation management company; however, it started to expand to construction as well over the course of the internship, and it comprised various other utility companies as well. Xylem Tree is a subsidiary of XKIG, which includes numerous utility companies (our IT was for all companies in this suite, not just Xylem). XKIG has several thousand employees, with the “big three” within the XKIG portfolio being Xylem Tree Experts, Kendall Vegetation Services, and River City Construction. Our company responds to storms, such as hurricanes, as the equipment used on tree line maintenance and other vegetation services is very effective in clearing roads and getting electrical lines cleared and backup and ready quickly. XKIG is a US-based company and stretches coast to coast. There are many main offices; however, the biggest is here in Norfolk.

I was told during the interview that “IT is backed up and a mess,” and they would need someone who can get on their feet quickly and get going. At the time, they were going through acquisitions, which resulted in IT being clogged and backed up in work, as new equipment had to go out, emails migrated and created, etc. Per the job description, I saw they used Hexnode, a Mobile Device Management [MDM] tool, and I quickly glanced at the tool before my interview, and it gave me a good understanding of how they provision and troubleshoot equipment, which was also part of my role. My first day, it was exactly as they stated.. A mess. I had a desk, a laptop, monitors, cables everywhere where I was to sit. My first task was to make it work. So, after I got everything plugged in, our systems administrator and one of the systems engineers showed how they set up laptops (interestingly, we used two MDMs, one for laptops/computers (Intune) and the other for phones and tablets (Hexnode)). I was having to write a lot down as the laptops required a lot of setup tasks, in addition to other tasks I was to be responsible for. All of this to say, I had to adapt quickly here, and I enjoyed the challenge. Working here, with my amazing coworkers, allowed me to develop a lot of skills and confidence in my abilities. I am excited to share my experience at XKIG with Old Dominion.

Management

As we were coast-to-coast, IT also had employees and management in other places besides Norfolk. Helpdesk technicians, system engineers, and system administrators reported to our Director of IT, who reports to the Vice President of IT, who reports to our CEO. There was no dedicated cyber team; however, we had a systems engineer who was also going to Old Dominion for cybersecurity, but he was doing the Master's program. We would both work together on multiple projects and were the “unofficial” cyber team for XKIG. I learned a lot of skills from our systems engineer and administrator in the Norfolk office; however, I was also able to catch on really quickly because I was allowed to not be on a call 24/7 or do tickets to learn more about our environment. This was due to our Director of IT, who is also in the Norfolk office. At first, as this was my first IT job/internship, I felt slightly overwhelmed, but I knew I could complete what was required of me. In the first month or two, I was just trying to get used to and develop the basic skills needed for my job - answering phone calls, troubleshooting, building equipment, and so on. However, as I progressed, I quickly found that I was very good at the functions of my job, and I was able to start finding time to learn about some of our other systems. My superior would be hands-off with me and let me find work, solutions, and learn when I can - I was especially encouraged to learn and develop more advanced skills, though not particularly related to my current title. I believe this approach allowed me to grow out of my role fairly quickly and started to get me experience as a security engineer or architect.

Work Duties

I was hired as a Helpdesk technician. My primary responsibilities were to answer user calls to troubleshoot issues, monitor our ticketing system for issues, and provide equipment for our users, such as phones, laptops, and tablets. Without the equipment, our employees could not charge their time (and their crews) properly, estimate costs for a project, etc. For our in-office personnel, those who are not “in the field” (those working on bidding a project or clearing trees, etc), they usually just need a laptop. All of this entails many steps, such as, in order to get assigned a laptop or device, you need an email created. When I first started, we had to add users manually to our Microsoft tenant, which, when tickets came in of new users needing emails or equipment, could be time-consuming. Luckily, we eventually hired a workflow company that would automatically do this part for us. I had to learn a lot about how to set up our devices, which familiarized me with Android and Windows a lot, as well as Office products, as users had many issues with them from time to time. I learned how

our MDM tool, Hexnode, works, to be able to properly assign devices to the proper user, and to troubleshoot issues, which were commonly connectivity issues for users in the field. By assisting users in the field, I was keeping/enabling their productivity. Without equipment or connectivity, our company may eventually lose a contract for failure to meet requirements in time. As I understood the Office suite and some of our common issues across other apps and devices, I began to transition into more security tools. I would first get into our email security solution, Mimecast, and begin troubleshooting email deliverability issues. In doing so, I learned a lot about how email really works and I gained tremendous experience in configuring very important security features for our organization. At a similar time, I was also given access to KnowBe4, which is a phishing training solution for organizations and their user base. I would eventually come to respond to phishing incidents by utilizing these two tools. When users report phishing in our organization, the IT team is notified - users were trained to use a Phish Alert button, developed by KnowBe4. Once that was done, I would remediate the attempt and determine how it got in, who clicked or interacted with it, and then deliver a report to my superiors (Vice President of IT and Director of IT) alongside our systems engineer. After some of these incidents, our leadership tasked the systems engineer and me with implementing DMARC for our organization. DMARC, or Domain-based Message Authentication, Reporting, and Conformance, is a vital email security feature that protects an organization's reputation by preventing spoofing of its domain(s). We used Mimecast's DMARC analyzer to help complete this task. I had to learn a lot about DNS, SPF, DKIM, in addition to DMARC to complete this project successfully. I successfully got our domains, at least a majority of them, to "completion", which means it is set to reject emails not conforming to ur SPF and DKIM records. This project took several months, and I was still working on it up until my departure from the company. As I was working on this project, I was being brought into more meetings as well. I was further tasked with implementing/evaluating Data Security Posture Management [DSPM] and Data Loss Prevention [DLP] tools. I worked alongside our systems engineer in the Norfolk office on these projects as well. As I was learning more on these tools, I was also implementing global changes to our Microsoft environment to better secure it. I was using Microsoft's Intune, Defender, Purview, as well as the other various Microsoft admin centers like SharePoint, to tighten controls in our tenant. I implemented numerous changes, such as restricting what permissions users are allowed to give apps without admin approval, turning on web content filtering in Defender, implementing some Conditional Access policies in Entra, limiting guest access in SharePoint, editing connectors to lockdown email flow in Exchange, and so on. I was also invited to collaborate on evaluating new Endpoint Security solutions/ SOC partners. Our current provider was very troublesome for numerous reasons. As a result, our systems engineer in Norfolk and I evaluated some tools that we may move to, such as CrowdStrike or

SentinelOne, with any other SOC provider. In one of my meetings with my manager, I noted users were struggling with some of our platforms and had questions because they were never trained on them… (Somewhat like me!) Our onboarding was pretty much non-existent. So, I agreed to help train some of our folks in the field on basic tablet maintenance, identifying phishing, in addition to answering some of their questions. This was a meeting I led, and it was very nerve-racking at first, but as I grew my confidence in our tools and how our environment operated, I found it somewhat easy, and even a little fun. I was happy to educate some of our users on how to better use their tools to be more productive and ensure they are promoting a positive cyber environment. All of this responsibility did not come at once; it grew over time, which allowed me ample time to understand each tool or project I was getting introduced to, so I could perform well. After so many tickets and calls, I knew I wanted to learn how our environment really worked, so I made a tremendous effort to understand the systems I would be a potential engineer or subject matter expert in. All of these security tools I learned can make or break an organization. An organization with lax permissions or configuration may open the door to attackers, and lead to catastrophic loss, such as loss of PII or proprietary company information.

Cybersecurity Skills

I utilized many cyber skills across the course of my internship. I would like to mention that I have always wanted to be in cybersecurity, and with my Security+ and some ODU cyber classes, I was confident I could handle anything thrown at me. I knew phishing and/or social engineering were the easiest way into an organization for initial access. Phishing is by far the most likely reason for an organization to be compromised completely; there are numerous reports and studies proving this. Luckily for me, the first two “cyber” systems I had access to aimed to tackle this challenge. KnowBe4 attacked the human element by aiming to educate our users, and Mimecast, our email security gateway, to block (or attempt to) phishing attempts. I knew some basic incident response tactics through Security+, such as containing the incident, documenting it, etc. However, what all the classes and certs do not teach you is how to use various tools to effectively respond to an incident. That is something you need to learn on the job. With my knack for trying to understand every system I touch in depth, I quickly found out how to utilize both tools. Document and help documents are by far the easiest way to understand a new tool. Both KnowBe4 and Mimecast have tremendous support articles, and I am very grateful for that, as it allowed me to develop a quick expertise in their solution(s).

I am going to share an incident that proves how on-the-job experience helped me develop a deep understanding of email, particularly email security. One incident I found was that there were emails in quarantine in Microsoft Defender threat protection. I investigated the email for maliciousness, and using some of Microsoft's tools in Defender as well as other free online tools, such as any.run, and Cloudflare's URL scanner, I found these emails to be malicious. There were many others like it in quarantine, too, all with a subject line like “A caller left VM..” I wanted to understand why this was held up by Microsoft’s Defender for email and not Mimecast, where our emails are supposed to be routed through first. Interestingly, when I went to look these emails up in Mimecast, they were not there. I was confused. Our MX records, which tell other users on the internet where to send emails, point to Mimecast. My conclusion was that, somehow, these hit Microsoft first, not Mimecast. I did not know how this was possible. So, I reached out to our support at Mimecast, and they hit me back with an explanation and an article. At the time, I did not know, but the malicious actor was abusing Microsoft’s Direct Send feature. The article I received from Mimecast was to lock down our connectors in Exchange by essentially telling Exchange (Microsoft's email service) that it is only to accept mail from Mimecast’s servers. Also, with their answer and some investigation of my own via Google and some AI chatbots, I understood they were bypassing our MX records. How? Because every tenant on Exchange gets their “own” email server. So, let's say Mimecast was not our primary email security solution and Exchange was, our MX would be xkig-com.mail.protection.outlook.com. As Mimecast forwards email from the outside to Exchange, and vice versa, that never goes away. So, before I implemented their solution, I tried to mimic the attacker. I got an AI tool to make me a script and found that our Mimecast to Exchange was not locked down, and our MX records were able to be bypassed. I was able to directly send to our Exchange server. After talking with my counterparts (systems engineer, VP of IT, and Director of IT), we made the decision to move forward to lock down our connector. We wanted to ensure our users would still get their mail, so this was high-stakes. It worked out; I quickly determined the mail flow was as expected. Then, I reran my script, and BOOM! That message was blocked as it's not from Mimecast. Our exchange/tenant was now locked down and more secure. Maybe a month or so later, I came across an article from Varonis, “Ongoing Campaign Abuses M365’s Direct Send to Deliver Phishing Emails.” It was exactly what we experienced. Furthermore, I reran the script the attackers likely used, per the article, and found we were not vulnerable there as well - it was blocked as it was not originating from a Mimecast server. This, one of many of my experiences of a security incident, gave me a lot of confidence that I can work in this field. I utilized various tools, engaged partners and my team, and remediated essentially a “zero-day.” This incident, alongside other phishing and account incidents, and leading a DMARC project, made me very familiar with email security practices (as well as DNS!) across different

platforms. I am very sure I can adapt to any email security gateway and ensure it's locked down effectively while ensuring users are not having their workflow(s) disrupted.

Old Dominion

I made several connections to the course material over the various projects and incidents I came across. For example, I had to run numerous VMs, write several PowerShell and Python scripts over the duration of the internship. A reason I was confident in running such commands was a result of having done it so many times across multiple cybersecurity classes I have taken at Old Dominion. In CYSE 250, I got comfortable with Python; in CYSE 270, I made multiple Linux VMs and got comfortable with its command line; in CYSE 280, I was very comfortable with operating an Active Directory environment, and I was able to find and understand Windows tools a lot better. There are various other classes that contributed to my success in this role. CYSE 450 and another class utilized nslookup commands, which were essential in the DMARC project I was responsible for. I ran that command daily and knew its syntax very well. I would use commands like nslookup -type=txt xkig.com or nslookup -type=txt -dmarc.xkig.com across our domains to verify correct DNS settings. In Old Dominion's Networked Systems Security and Cybersecurity Fundamentals courses (CS 464 and CS462, respectively), I was taught DNS a fair amount, which aided in my ability to get this project up and running smoothly. I haven't come across a class offered at Old Dominion specifically for email security, but I think there should be a course dedicated to it, especially after all I experienced. Email is the primary way of communication on the Internet, and the leading cause of breaches in organizations, costing hundreds of billions, if not trillions, in damages globally. Such a class would be able to dive into a lot of the stuff I learned and showcase attacks and defenses relatively easily. With that being said, Old Dominion did prepare a structure for me to grow from. I know that for my title as a helpdesk, the courses here are very helpful. Although I took a Windows System Management and Security class, our environment was entirely cloud-based; thus, no Active Directory or group policy. So I had to slightly adapt what I learned to a cloud-based environment. So instead of GPOs that define what a user may do to their computer, I define something within Intune. I lot of what I learned came from just trying to understand how a tool works. For example, when evaluating some DLP tools, although discussed through several courses, there was not a lot of depth. So when I first came across a dashboard for it, it was pretty overwhelming. However, as you work through the tool and read its documentation, you can understand pretty quickly its uses and value to the organization. Old Dominion offers a very good foundation for being able to

excel at work in cybersecurity. I am taking CYSE 420 - Applied Machine Learning in Cybersecurity. This course has helped me understand how some of these DLP and email security companies use models to filter out spam or phishing emails and enforce compliance. Although I am not done with the course yet, it has opened my eyes tremendously. Email security can get complex very quickly, especially as attackers are increasingly sophisticated.

Internship Outcomes

I believe I fulfilled all the goals I set for myself in the internship. I utilized various tools in my work that allowed me to understand how IT works in a large organization. I understood our environment very well, and I took every opportunity that came my way, as my goal was to learn. Towards the end of my internship, a lot of the larger issues in our environment I was increasingly able to resolve with ease. I closed complex tickets and aided in numerous other issues. I became very familiar with Microsoft administration, and I am very confident I would be able to pass their 365 Admin exam (MS102). I had some experience with Azure as well, so I am also confident I could pass their Azure Admin exam (AZ104). I wish I had taken a day to go out and certify in these; however, I never got around to it.

I learned so many cybersecurity tools that I am 100% sure I will be working with them at another organization. In fact, the new place I am at uses the same learning platform, KnowBe4, and is a Microsoft-based environment. A lot of Microsoft's tools I have experience with, and I have spent a lot of my time trying to understand them. Before the end of my internship, I was looking at implementing some of Purview's features to better classify our data in and out of our environment. I really wish I had grabbed some certifications at XKIG, especially since they would pay for training.

I also exceeded some of my own expectations in this role. Leading a meeting of dozens of employees at a time is something I never thought I would be able to do. However, once I got through the first one, I knew I could not only do it, but do it well. I found that because the meeting was related to something I love, I was not really nervous to talk about it for half an hour or answer questions about it, because I know IT and cybersecurity. Additionally, I had the support of either the VP or Director of IT in the meeting as well to answer some questions that may be considered "above" me/before my time. I am incredibly grateful for this opportunity; it taught me so much about cybersecurity, people, and myself.

Internship Aspects

The most motivating thing for me was learning new, challenging tools. I wanted to know how our environment really worked and find security gaps in the process. Learning about so many tools and how they are integrated was very exciting. By the end of the internship, I had experience across a diverse set of security appliances, from identity-based to email security, and so on. I enjoyed the challenge of having to learn things in-depth as well. As an example, the DMARC project I was tasked with required me to do tremendous research on SPF, DKIM records as well. In the process of the project, I learned how to analyze mail headers, troubleshoot mail flow, and change records in the DNS to move the project forward. I also challenged myself by taking on leading meetings for employees to help them understand IT's role in the organization and how to best use our tools/equipment.

I would say the most discouraging part of the internship is the minimal downtime. There is always something to do, which over time can start being stressful. Our environment was constantly being backed up, a lot to do with my additional workload and projects; however, it was mainly a result of repeated acquisitions, which doubled the company size over the course of the internship. Acquisitions take tremendous time away from projects and other tickets. In many cases, when these acquisitions came along, I was building hundreds of tablets a day to meet just their equipment needs. It was very time-consuming and repetitive, which gets uninteresting very quickly. One thing about the acquisitions I liked, however, was that they all came from differing environments, so moving their mail over and editing the DNS to point to ours was a fun challenge. Furthermore, there would be some more challenging tickets that would come in, which were fun to troubleshoot and remediate.

The most challenging part of this internship was dealing with a constant workload. As I progressed through my role, I got more and more responsibility, but I never really got to move away from the initial tier one items, so I was constantly in and out between projects, building equipment, and taking calls. I liked how the workload kept me busy; however, I was also trying to have some time to really work on projects or learn a new tool or skill. Another challenge would be learning complex topics quickly. At first, I knew very little about DMARC. However, I had to find the time to really dive into it, so I could meet our organization's directives. I would say the tier one calls are the easiest part of the job after you get a little familiar with the environment you are working in. Most of

the time, tickets in the queue or those calling in are experiencing an already documented issue.

Preparing for Xylem

Read the job description! If you spend just a few minutes learning about each bullet point on the job application for any interview, nine times out of ten, you will be chosen over someone who may have better qualifications but lacks the initiative. The goal of an internship, at least for me, is to learn. Find out how others work, and change it as needed so it works for you. Take notes! This shows initiative, too, and others will respect that you are paying attention. Furthermore, if you write it down, I have always found that I am more likely to remember it a bit quicker. A huge way I learned here is to just “click around”. By getting comfortable with the tools needed for your job and by clicking around, you will learn a lot about the tool, and you will be much more confident when you have to go in there to grab information and/or make a change. During times when tickets or calls are slow to come in, try to bring up a knowledge article, or see how others' tickets have been solved. This will tremendously contribute to your success. Be confident in your abilities and your ability to learn challenging things.

Being in IT, you also must be quick to adapt, so don’t become ultra-reliant on a tool; understand how it works and why something is done a certain way. This will help you adapt to complex, changing systems. Another piece of advice is to treat every task, whether it be a phone call or a complex project, as a chance to improve. Not every day may you build knowledge of a tool; however, if you are able to build relationships and soft skills, you are improving just as much as if you were diving into knowledge articles. As you grow into the role, try to think about the processes you are doing: why is this done a certain way? Do not be afraid to ask questions; sometimes you will come across something that needs to be improved. Another thing I would do to prevent burnout is automate and script when you can. I had written a PowerShell script to automate 90% of our laptop preparation, and it saved massive amounts of time. Automation is your best friend in an IT or cybersecurity position. By staying curious, documenting what you do, and automating when possible, you will be tremendously successful in this role and others.

Conclusion

My main takeaway is that I know I can handle complex projects and tools. I have built tremendous experience and relationships with Xylem, and I will carry what I have learned with me whenever I go. As I take higher-level classes, I am starting to see how the tools I work with function. For example, with my Applied Machine Learning class, I am seeing how they may train and use models that are then used to identify potential attacks. Furthermore, my experience helps me a lot in discussions, papers, and labs. A lot of what I did at Xylem, I do at Old Dominion and vice versa. A majority of my skills came from the constant repetition of work at Old Dominion and Xylem. For example, running Python and PowerShell effectively, or using Windows' command prompt for various reasons.

My experience with Xylem showed that I am able to be a skilled cybersecurity engineer in the future. I am very certain that I will use similar tools elsewhere and make a similar impact. The various tools I consider myself at least an intermediate in are in demand everywhere: Entra, Mimecast, Intune, Defender, KnowBe4, Purview, DLP/DSPM tools, etc. Diving into each of their respective documentation, I learned so much and was able to help the organization thrive. I always thought I wanted to be a red team operator or ethical hacker; however, I found that the blue team may be just as fun. Investigating how and why an incident occurred is very important - and a skill many organizations lack.

I set all my goals for this internship, and I feel I got more out than I expected. I demonstrated tremendous initiative and leadership. I feel confident I could have passed many of our vendors' certifications, essentially becoming a subject matter expert for many of the platforms in our organization. I know I belong in this field, not only because I know I can do the work, but I always like to learn new things, which is an essential part of cybersecurity and IT. As I move forward and continue my career, I will use lessons learned and my experience to make significant contributions wherever I am able.