A Comprehensive Overview of My Internship Experience

Caleb R. Judy

Robert C. Branch

School of Cybersecurity, Old Dominion University

CYSE 368: Cybersecurity Internship

City of Virginia Beach

Fall 2025

December 1, 2025

Virginia Beach was established in 1906 and is home to 459, 470 Virginians. The actual city government of Virginia Beach has about 7,500 employees across 35 departments. Each and every one of these employees has their personal data, like cell phone numbers, bank details, social security numbers, etc, stored on databases that bad actors continuously attempt to gain access to. At the City, it is our duty to safeguard the personal data of the 7,500 city government employees while keeping city systems, networks, and devices operational and accessible for twenty-four hours and day and seven days a week. In addition to this, we also strive to keep the data of Virginia Beach citizens safe and secure in the same manner as we do with the employees.

My orientation to the city was nothing special admittedly, they didn't do anything special like roll out a red carpet for me as I walked in or put on a ceremony or show. I had applied around April or May of this year and I was interviewed around the same time. My first day on the job was around late August or early September and my first day was pretty uneventful, I was shown some stuff but not much as I was getting onboarded, and I had not finished being onboarded even by the time I had left. I met the members of our SOC (Security Operations Center) team, which included our level 1 analysts Tatum, Noah, and Harshul, as well as Sam and Elliot, who work in Governance, Risk and Compliance (GRC), and our other intern, Faith.

Prior to starting my internship, I had tried to come up with some learning objectives or goals for myself while I progressed through the internship. Admittedly, some of the objectives listed below I had made up as I went along (which I will touch on later). The three learning outcomes I had when I decided to take on this internship were as follows:

1. Learn what cybersecurity is like in a professional work environment
2. See what prior skills can be applied at my internship
3. Learn how to operate and conduct myself in a professional career-based environment

Management

Management at my internship is fairly simple and was easy to follow. Our office was comprised of two different teams, the SOC (Security Operations Center) team and the GRC (Governance, Risk and Compliance) team. Both teams are fairly small, with the SOC team having a total of five members including two interns, while the GRC team is even smaller, with only one team member and one contractor. Because both teams are so small, the SOC team and GRC team are led by 1 person, who is technically just the SOC manager, but

he also guides the GRC team if they need anything. The SOC manager then answers to our CISO.

I am primarily supervised by one of our level I analysts, Tatum, and we have two other analysts that have showed me some stuff, Noah and Harshul. Tatum has been very good at teaching me and showing me the many functions of being an analyst when she can. I say when she can because she is generally very busy, because as I said this is a small team so there is a large part of this internship where I am left to sort of teach myself some of the things. But regardless of that Noah and Harshul also show me some stuff but not as much primarily because they have both started their careers around the same time I started my internship, and they both are still learning similar to me.

I think the effectiveness of this supervision and management can be both good and bad depending on how you look at it. On one hand if I were to be constantly monitored and observed working, like how I probably would be if I went to work for any other organization or company, I think it would be good in the sense that there would be less room for error and I wouldn't cause issues or create problems as much, but that is the fundamental issue with that approach. It doesn't allow for error or the opportunity to fail or learn from my mistakes. Then on the other hand, If I'm not under constant supervision and I'm free to look around and toggle with anything I want (which is not entirely accurate to what I have experienced but it is close), this allows me to really dive into everything and learn every part and bit of all of the systems and applications that they provide me with, and overall this approach has really helped me to teach myself, which is a great life skill just in general. I actually wasn't a fan initially of the limited supervision I had because I generally am not great in environments where I have to teach myself the skills, but now that I'm almost completed with the internship, I wouldn't want it any other way. Of course, there is a lot more opportunity for error and things to go wrong, and while I haven't caused any major problems the door is always technically open for that. But overall, I think that this approach to supervising me has in fact been effective.

Duties, Assignments, Projects

The first main assignment I had while working with the City of Virgina Beach was reviewing email reports in Microsoft Defender. Any time a city employee reports an email, whether it be for the reasons of spam, phishing, or not junk, they all end up in a centralized system within defender, called "Email Submissions". I would have to click on a submission and review the contents of the email, including reading the actual plaintext of the email, and interacting with attachments to determine if there was any foul play. I wasn't able to

open any links or attachments within Defender for obvious reasons, so I would have to download the email from defender and upload it as a file through a service known as AnyRun. AnyRun is a sandbox tool used to view the contents of links, files, etc. It can even detect foul play happening in the background, far from what they eye can see. Based on my observations in AnyRun, I would make a determination on if a reported email were to be categorized as spam, phishing, or no threats found. If an email did come back as malicious, it is standard to take note of the IP address the email was sent from and block the email address from sending any more emails in defender. I would let the other analysts take care of blocking the email address, as I did not have the necessary permissions to do so.

Another assignment/duty they had me take care of was looking into potentially compromised user accounts. In Azure, there is a page called “risky users” and within that page was a list of users whose accounts were potentially compromised/in danger. You can filter the users by risk level from low, medium, and high. When looking into a risky user, I usually have two tabs open: one showing the risky sign in that they were flagged for, and another showing all of their sign in logs from the past 24hrs (I like to keep a sperate tab open with all their sign in logs because it helps in determining context). From there I would look at the risky sign in that was detected, copy the IP address of that sign in to the clipboard, and run it through open-source intelligence (OSINT) tools. I primarily use tools like Scamalytics, AbuseIPDB, VirusTotal, etc. The main one I use however is Scamalytics, because unlike the other two, Scamalytics can actually detect if an IP address is using a VPN, which is particularly helpful for this task, because it explains why some users log in from a consistent location and then login from across the world within 30 seconds. However, a VPN can’t always explain risky sign ins, and you have to be careful about it. Sometimes an IP address will come back with VPN enabled, but have a high fraud score, which is how Scamalytics in particular determines the risk factor of certain IPs. A lot of it depends on context and making careful choices. But once I can make a safe determination, there are a couple of options to choose from on the risky users page, Confirm User Safe, Confirm User Compromised, and Dismiss Risk User. I never really use either of the “Confirm…” buttons, because confirming a user safe essentially ignores any future risky sign ins from a user, and confirming a user compromised will automatically lock them out of their account and revoke their multi-factor authentication (MFA). If I feel that a user’s account is safe and not in danger, I always hit “Dismiss Risk User” because if their account ever has another risky sign in, it will always appear back on the risky user page. Now if I find a user who I believe to be in danger, I will leave the alert on the page and contact the user in question either by email or phone and make a determination based on my interaction with the user. I usually ask them if they logged in between a certain time

period, like from 10:00am to 11:00am because people often don't know the exact time that they logged in, then I ask if it was on xxx date to access an application, like Office365, with their device, such as Windows10 (which I know isn't technically a device but that is how it appears under the "device" tab on the alert, other examples include Mozilla, mobile safari IOS xxx, etc).

While working at the City of Virginia Beach I had the opportunity to work on something I consider to be pretty big, which is something that is being actively used by the SOC team. It's known as a Standard Operating Procedure (SOP) and it is essentially an instruction manual on how to perform certain tasks, how to respond in the case of events, etc. The SOP I worked on focused on Autopsy Forensic Investigation, which is an application that analyzes compromised devices and recovers evidence, analyzes things like user data, web artifacts, and registry information to find the root cause of an incident and identify threats. In my SOP, I had to include instructions on how to upload a case to Autopsy, which included how to disable BitLocker, how to use FTK imager (FTK imager creates the file format needed to upload a case to autopsy), and then how to set up the case once it is uploaded into autopsy. To create the SOP, I relied on Tatum to show me how to disable the BitLocker, as I did not have permissions to do it due to my intern status.

Because of the Autopsy SOP, I also had to create my own case in Autopsy in order to help me better understand the platform and write clear and concise instructions for it. Unfortunately, at this time my case in autopsy has not been fully uploaded yet and I cannot see all the details at this point in time. We created the case around the end of September, and the data is still being uploaded into the case. This is because there is an extremely large quantity of data that is being both uploaded and analyzed. This is pretty universal among Autopsy cases. It took about two weeks just for everything to be uploaded and Autopsy has been analyzing the data ever since.

I also gained access to a specialized security incident and event management (SIEM) software program known as Cortex XSIAM (eXtended Security Incident and Automation Management). Prior to the XSIAM, we responded to tickets primarily through a platform known as ServiceNow as well as Microsoft Defender. What makes the XISAM special is that both of these services are integrated into it. In fact, it integrates several services including but not limited to Office365, CISCO, VMware CarbonBlack, VMware NSX, etc. The XISAM can be tailored to fit an organization's needs and display the information that the organization wants to see. For example, we have several dashboards that can be pulled up, like the SOC dashboard. The SOC dashboard displays a variety of information, including total logins and the total failed/interrupted logins. Going back to the tickets, they seem easy to respond to and resolve. I say they seem because I cannot

actually resolve tickets within XIASM, because I only have read permissions due to my intern status. I have however looked over the platform and have a pretty good understanding of how everything works. When you click on a ticket, it displays a variety of information related to the case. The overview section will show the issue itself and the source of the issue, as well as a general view of the key assets and the artifacts. Key assets and artifacts also has its own section next to the overview, and that section goes into detail of the source of the issue and the user associated with the issue. Clicking on a user within this section displays even more information, including a timeline of the user's activities, other cases (or tickets) related to the user, a graph of their usual activity hours, login attempts, authentication attempts, and Software-As-A-Service (SAAS) logs. There is even an artificial intelligence (AI) chatbot integrated into XSIAM, which can help with resolving cases and issues, creating quires, etc.

Use of Cybersecurity Skills/Knowledge

I have gained many skills and attained much knowledge prior to this internship, ranging from technical skills to more mental skills. The first big bit of knowledge used for this internship was my critical thinking ability. This is not only a life skill, but it is also extremely important in the world of cybersecurity. This job requires that you think outside the box and to think critically, because you can't take anything at face value. A lot of this job is thinking like a bad actor and what they might do and thinking about their decisions and behaviors. Prior to attending ODU and pursuing my degree, I think my critical thinking skills were lacking a bit but because of the many papers I've had to write throughout the many courses I've taken and the many labs I've also had to do, these experiences have helped me think harder and outside the box a little bit.

Additionally, I have also earned by CompTIA Security+ Industry Certification (Sec+) prior to starting my internship, passing my exam about a week or two before my internship started. Sec+ goes over a variety of cybersecurity topics, including attacks, vulnerabilities, architecture and design, implementation, operation and incident response, and governance, risk & compliance. I was able to apply all of these aspects to my internship, but I was able to apply operation and incident response the most. We had a few incidents throughout my time there, including an account that was breached about a week ago. Since I am an intern, I really only attended the Microsoft Teams meetings which essentially covered how to handle the situation and what our next steps should be. This reminded me of what I learned throughout my sec+ training, where the incident response process involves the phases of detection & analysis, containment, eradication, recovery, and post-

incident analysis. This is generally how the incident response at the City of Virginia Beach is modeled, and this is what the SOC team followed when addressing the compromised user.

Role of ODU Curriculum

The difference in the ODU cybersecurity curriculum and the skills needed and used at my internship is admittedly a bit jarring. The Curriculum places a heavy emphasis on learning Linux, which is an operating system I have taken three classes on and the first of which I started when I was a sophomore, most of which are required on my degree, and I never opened a Linux terminal or even used the operating system for that matter while I was working there. All of the tools that we used to operate and do our jobs was on web-based Windows applications, and from my experience there are almost no courses in the cybersecurity program that focus on Windows or Windows applications; I actually recall taking one windows course total throughout my time at ODU.

Having said that, I do think that the Curriculum has prepared me for the amount of critical outside thinking that is required for this job, to an extent. I say to an extent because it is a certain type of critical thinking, that being “thinking outside the box”. The labs I’ve had to perform in my coursework have occasionally required some outside thinking and I think my experiences with that have helped some. A lot of the outside thinking involved at my internship revolves around the idea of thinking like a bad actor and their motivations, which wasn’t necessarily what I was doing within my lab environments, but I do believe that the lab environments strengthened these critical thinking skills.

I must also mention that I did take a class for the CompTIA Security+ certification prior to taking the exam for it. I did a lot of solo studying, but I did start off taking a course through ODU for the exam. We used the official CompTIA Security+ course, which is essentially an online textbook that gives you access to reading lessons, videos, labs, quizzes, etc. I do think that the studying I did on my own helped me prepare myself more for the exam, but I did learn a lot in that course, and I think that it was the bulk of studying and preparation, if that makes sense. The studying I did on my own time was more so about fine-tuning a lot of the concepts I had trouble with or didn’t understand.

Learning Goal Fulfillments

In my General Introduction, I explained that the three learning goal outcomes that I had were:

1. Learn what cybersecurity is like in a professional work environment
2. See what prior skills can be applied at my internship
3. Learn how to operate and conduct myself in a professional career-based environment

I can say with confidence that each of these goals were fulfilled. To start, I learned a lot about what cybersecurity is like in a professional work environment. There is a degree of alertness and attentiveness that is not felt within a classroom setting, due to the fact that I am within a real active environment, and not a test environment like at school.

I also was able to use a lot of my prior skills that I had before my internship, as mentioned in the "Use of Cybersecurity Skills/Knowledge" section. The Security+ certification definitely came in handy as I was able to utilize my knowledge, I gained from that, and I was able to understand much of how the SOC team operated and what it does in case of events or mishaps. The critical thinking skills I have gained throughout life and from the coursework at ODU has also come in handy.

Lastly, I did learn a lot about conducting myself in a professional environment. I learned how to pace myself and put 100% effort into my work without burning myself out, and I learned how I to be as helpful as I can be in a working environment.

Motivating aspects

One of the most motivating aspects of the internship for me was the fact that it feels like I am working toward something bigger than my internship. I think If I play my cards right, I could end up staying here past my internship and potentially be hired full-time once I am out of college. I plan to discuss it sometime this week with my boss, Bob, who is our CISO. In fact, one of our analysts, Noah, followed a similar path to what I am currently trying to follow. Noah was an intern before being hired, and when his internship ended, he had a discussion with Bob about staying and landing a job as a level I analyst. The only issue was that he was still in school and couldn't work full time, so what ended up happening was that he took on a volunteer role and came in when he could to help out and gain more experience working with others. He kept this volunteer role throughout the rest of his time in school and during the summer as well and was hired as a level I analyst around the same time I was brought in as an intern, sometime in late August. I'm hoping I can follow a path similar to this and land a job as a level I analyst right after I gradate. I want to stay there because I feel I've gained a lot of insight and experience during my time there and I want to be able to continue that

To add to the feeling of working towards something bigger, I have to mention all of the experience and insight I have gained. Throughout my time there I felt like I was learning something new and gaining more knowledge about cybersecurity, for the most part. There were definitely days where it felt like I was going through the motions and performing tasks I was already comfortable with rather than learning something new, but for the most part it did consistently feel like I was learning more and more, from teaching and experiencing things myself to being guided by my coworkers. This is part of the reason that I wish to stay, because I want to continue to gain more experience and insight and use this job as a solid starting point for my career, to prepare me to move on eventually to bigger things within the industry.

Unmotivating aspects

I say with some regret that there isn't much that kept me unmotivated from working this internship. The only thing that comes to mind is the receptiveness of some of the tasks that I did. The email submissions in particular are very mundane and repetitive in my view and that was my primary task for the majority of the time that I was there. I think the process of doing the same thing over and over made me feel like I wasn't really progressing or going anywhere made it feel not as exciting, which unmotivated me to a certain extent.

Challenging aspects

The most challenging aspect of the internship by far was learning to teach myself how to utilize certain applications or how to perform certain tasks independently. It wasn't so much so that the applications or programs or tasks themselves were difficult to use or the tasks were difficult to complete, but more so the aspect of learning on my own. As I mentioned, I generally have never been great when it comes to teaching myself. I feel that I thrive when I am under the supervision of somebody else and I am being guided through tasks. I think this internship has helped me thrive in a new environment though, and I am glad that I wasn't under constant supervision, because I had to learn a new life skill by myself, which is an extremely valuable skill in the grand scheme of things.

A bit of a nitpick admittedly but working with my co-workers was also occasionally difficult and I wish it was easier to work with them sometimes. This is not due to the fact that they are difficult people, I think that they are all easy to work with and I enjoy the time that I've had working with them, the issue revolves around the fact that they are so busy. As I mentioned, our SOC team is pretty small, with only about five or six people. Because of this, there is a higher workload for everyone else and not enough time to show me stuff. We

don't have a training department or anything so it's not like I could have gone to that to find new things to do, and a lot of times what happened was I would ask in Teams if there's anything going on to let me know so that I can look into it too and watch or help with whatever situation was going on, but I guess it ended up being easier on them if they just handled it on their own without my input. I would like to restate that I don't have difficultly working with them when I have the opportunity. When they're not slammed and can show me stuff, I think that it's actually the climax of my experience working there, because I get to learn something new and interact with my coworkers while doing it. So again, a bit nitpicky, but still challenging, nonetheless.

Advice for Future ODU Interns

I highly advise that future ODU interns take notes at their internship. Throughout the first few weeks of my internship, I failed to take any notes pertaining to what I was doing, the assignments/projects I was given, etc. Taking notes during an internship can be highly beneficial because it provides clear documentation on what you've been doing and the things you have learned. Think of it as sort of a timeline of everything you've done. Note taking can also be beneficial for filling in a resume.

As for advice on what to do before taking on an internship, make sure that you have goals in mind on what you want to achieve during your time there. On my first day, the goals I had in mind were complete this internship for accreditation on my degree, and gain cybersecurity experience and that was it. The goals I had mentioned above I had honestly kind of made up as I went along in the internship. I'm glad to say that I accomplished all of my goals, but it would have felt far less chaotic coming up with goals prior rather than during.

Additionally, I cannot overstate the importance of networking with peers/professors/etc. I landed this internship a bit last minute through a family friend and my internship search prior to that was bleak to say the least. I applied to a couple of different places but couldn't land any interviews. I'm learning that when it comes to computer science or IT jobs in general, having connections really helps when trying to find an internship or even a job for that matter. I admittedly did not utilize the opportunities provided by ODU, such as the career fair, which is a great place to connect with people in the industry and classmates. I think if I had connected and networked with people I would have had more options to choose from which would have significantly reduced my stress levels when I was looking around. Take advantage of the opportunities that you have.

Conclusion

In essence, this internship has been highly beneficial to my professional development, so much so that I am currently making efforts to stay with the City of Virginia Beach and continue working there. I have gained so much knowledge and insight during my time there and hope to stay to continue gaining knowledge and insight.

This internship will influence the rest of my time at ODU because I have a better understanding of where I want to go with my career. I need to utilize school events like the career fairs we have to meet with people in the industry and build connections with people and make the most of resources like the career center at ODU, which can also help me get on track and aid in setting a path for me and my career.

This internship has influenced my professional path because I have realized in my time there that it is a good starting point for my professional development, as I've mentioned. I hope to stay there in some capacity and use this experience to learn and develop myself and then eventually move on to bigger things.