

## **Internship Reflection Final Paper**

Isain Cortes, Jr.

Old Dominion University

Employer: Augusta University

Agency: CAE in Cybersecurity Community

CYSE 368/Internship

Spring 2025

04/23/2025

Table of Contents

1. Introduction ..... 3

2. Getting Started: Orientation and Organizational Background ..... 4

3. Leadership and Structure: Understanding the Management Environment ..... 6

4. Projects and Responsibilities: A Deep Dive into Internship Duties ..... 7

5. Cybersecurity Skills in Action: Applying and Expanding My Knowledge ..... 11

6. From Classroom to Real World: The ODU Curriculum in Practice ..... 12

7. Reflecting on My Objectives: Measuring Internship Success ..... 13

8. Moments of Impact: The Most Motivating Aspects ..... 15

9. When Things Got Tough: The Most Discouraging Aspects ..... 17

10. Overcoming Obstacles: The Most Challenging Parts of the Internship ..... 18

11. Advice to the Next Cohort: Recommendations for Future Interns ..... 19

12. Conclusion ..... 21

**Note:** All figures were created by the author using screenshots of live work from the team’s Google Slide presentation.

## Introduction

This Spring 2025 semester, I had the pleasure of interning at Augusta University through the organization CAE in Cybersecurity Community. Before this, I had done two previous internships and one semester of undergraduate research, dating back to my time at Germanna Community College, carrying on into my time at Old Dominion University (ODU). When I finished my internship at Amazon Web Services (AWS) and undergraduate research with COVA CCI in the second half of last year (2024), my goal was to land one more internship in the Spring 2025 semester. The reasoning for this is because I wanted to have one more internship on my resume before graduating and finishing up my bachelor's degree here at ODU. I felt with the experience that I already had doing cybersecurity and IT work, one more experience would be the perfect catapult for me to be able to finish my college career strong as I plan to venture out for full-time work upon graduating. On top of that I was made aware that I needed to have an internship accredited by the CYSE 368 course as a requirement for my degree, so I knew I had to go out of my way to land something.

I decided to apply to VIVID Cohort 6 after an email was sent by an advisor at ODU, listing details of work pertaining to cybersecurity, which is what I've been studying for the past four years and something I'm highly passionate about. The internship was going to be remote, and I was interested in the fact that I could be doing work potentially at four different universities including Augusta, Arizona, Alabama in Huntsville, and Florida International University. I knew I was probably going to be working with people outside Virginia, something I haven't experienced. I saw it as a chance to collaborate with people from different regions, backgrounds, and perspectives who all were working towards the same goals I myself am doing within the cybersecurity field.

When I landed the internship, I was pretty stoked. I've interned in cybersecurity in the past, but never for a university, so it intrigued me to see how those policies would be handled within the educational system. One of my objectives was to strengthen my understanding of how cybersecurity principles are applied in an academic setting, especially when dealing with multiple institutions. I also wanted to see how cybersecurity frameworks and policies were managed and implemented across university systems, which I knew could give me a different perspective compared to private sector. Lastly, I hoped to further sharpen my technical skills by getting involved with practical projects that challenged me to think critically and apply what I've learned in the classroom to real-world scenarios.

In this paper, I will reflect on my internship experience with Augusta University through CAE in Cybersecurity Community. I will detail the structure of the organization, the projects I contributed to, technical and professional skills I developed, and the lessons I learned along the way. This reflection will also examine how the internship aligned with my learning objectives, how it connected to my coursework at ODU, and how it influenced both my academic growth and future career aspirations in the field of cybersecurity.

### **Getting Started: Orientation and Organizational Background**

The organization I ended up interning with was Augusta University, contracting through CAE in Cybersecurity Community. Centers of Academic Excellence (CAE) in Cybersecurity is a nationwide initiative supported by the National Security Agency (NSA) and the Department of Homeland Security (DHS) to promote higher education and research in the field of cybersecurity. Augusta is one of the four designated institutions that participate in cybersecurity education and workforce development initiatives, with a particular emphasis on advancing national security through academic collaboration and innovation.

The internship was remote, which meant all orientation and training were conducted virtually. At the start, we were introduced to the project we'd be contributing to, given some background on the previous intern cohort (VIVID Cohort 5), and shown how our efforts would be building upon the work that was already done. The initial few days were spent familiarizing ourselves with the tools we would be using, the expectations of the internship, and the structure of the project we were assigned to. We were granted access to resources like the previous cohort's GitHub repository and documentation, which provided a foundation for understanding the direction of our work.

Interns were expected to work about 20 hours per week, with group meetings held every Monday and Friday alongside our supervisor. These meetings would give us the opportunity to provide updates on our progress, clarify goals, and ask questions about the next steps in development. It was made clear that we interns were supposed to host our own independent work sessions outside of those standing meetings to collaborate.

My first impression of the internship was honestly mixed. While I understood and respected the broader mission tied to national security priorities and Augusta University, the actual work we were being tasked with didn't feel clearly defined in the beginning. It wasn't immediately clear whether this would be a cybersecurity-focused internship or something more rooted in software engineering, an area I wasn't strong or experienced in. The uncertainty made it a little frustrating early on, especially since us interns were a mix of cybersecurity and computer science majors.

## **Leadership and Structure: Understanding the Management Environment**

The management structure was one of the more unique aspects of the experience. From the beginning, it was clear that this wouldn't be a rigidly controlled environment. Instead, the internship was structured to empower us as interns to work independently, collaborate regularly, and learn how to manage a project in a way that mimicked a real-world team dynamic. Our supervisor made it known early on that while he was available for support, much of the momentum and responsibility would be on us.

We were expected to take ownership of our tasks and progress. Twice a week, we had scheduled check-ins with our supervisor on Mondays and Fridays. Monday meetings typically served as a way to set the tone for the week, establish deliverables, and give everyone a chance to outline what they planned to work on. Friday meetings were more reflective as we would go over what was accomplished, what obstacles we encountered, and how the work aligned with our overall goals. These meetings were essential in keeping our group on track, with our supervisor also being open to helping us troubleshoot or walk us through issues without being left stuck too long on anything.

One thing that stood out was how much ownership we were expected to take. From the jump, we were told that we would need to host our own work sessions outside of the Monday and Friday check-ins. That meant scheduling time with the other interns, getting together to work on different parts of our project, and communicating regularly throughout the week. It wasn't like a typical internship where you just wait to be told what to do, we had to take initiative and keep each other on track.

One of the most unique and beneficial aspects of the internship structure was the rotating project manager role among the interns. Each week a different intern would step into the project manager position, which included setting meeting times, tracking progress, and ensuring tasks were being completed. This rotating leadership structure was a valuable part of the internship because it pushed each of us to get comfortable with taking initiative, organizing tasks, and speaking up. It was a great equalizer as no intern had a permanent leadership position, so we all had to support each other and communicate effectively regardless of who was leading that week.

Overall, I think the management approach worked well for the type of internship this was. It kept us focused, gave us room to grow, and created a team environment where we all played a part in making things run smoothly.

### **Projects and Responsibilities: A Deep Dive into Internship Duties**

Throughout the internship, our work was centered around the development and improvement of a tool that converts PDF documents into multiple-choice questions using a local LLM (large language model). This process required collaboration on both the frontend and backend, allowing us to develop a full-stack solution with practical cybersecurity and educational implications. Our primary task was to create a tool that would take PDF files from a local directory, extract their contents, chunk the text appropriately, and send these chunks to a locally hosted AI model that would generate multiple-choice questions in return.

Initially, we began with Google Gemini AI, but due to concerns regarding efficiency and accessibility over HTTP traffic, we transitioned to an open-source platform called Ollama, to run language models locally. After extensive testing, we settled on the Llama3 model for its performance-friendly nature, especially for devices with moderate RAM. This shift to Llama3

allowed us to better control local resources, address privacy concerns, and improve reliability when processing large documents.

My responsibilities involved contributing to this transition, helping redesign parts of the backend to integrate with Ollama's framework. This included setting up the multithreading process that would allow for efficient chunking and prompt generation to the model. Using Python through VSCode as seen in Figure 1, we implemented threading to ensure that requests to the LLM could happen simultaneously without overloading the system. We were able to process lengthy PDFs in sections, optimize the prompt formatting, and capture responses in a format that allowed for easy JSON conversion, which is an essential step for any future frontend integration or database storage.

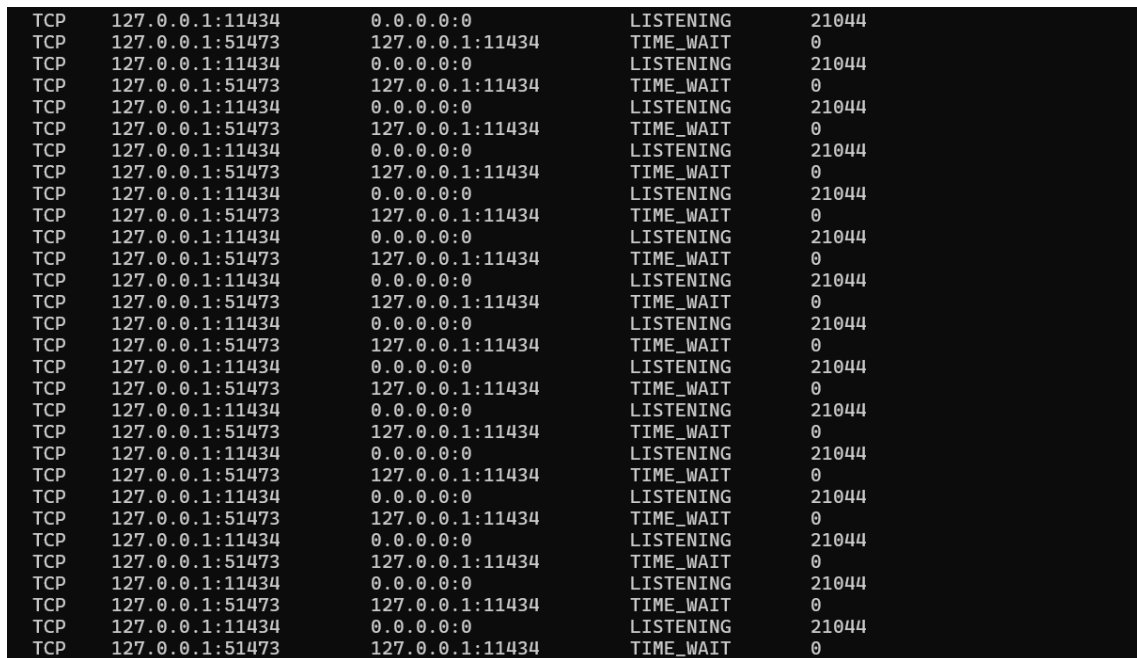
```
{ } quiz_data_20250307_160533.json > { } 0 > { } choices
1  {
2      {
3          "question": "What is the primary source of spyware?",
4          "choices": {
5              "a": "Official app stores",
6              "b": "Obscure third-party stores promoting unofficial apps",
7              "c": "Email attachments from friends or acquaintances",
8              "d": "Security software scans"
9          },
10         "answer": "b) Obscure third-party stores promoting unofficial apps"
11     },
12     {
13         "question": "What is one common way to detect malware?",
14         "choices": {
15             "a": "Installing a new operating system",
16             "b": "Scanning the computer for malicious files or programs",
17             "c": "Updating all software on your computer",
18             "d": "Unplugging your computer from the internet"
19         },
20         "answer": "b) Scanning the computer for malicious files or programs"
21     },
22     {
23         "question": "What is the primary purpose of Adware malware?",
24         "choices": {
25             "a": "To encrypt files and demand ransom",
26             "b": "To secretly create a backdoor into an infected computer system",
27             "c": "To track a user's browser and download history to display targeted advertisements",
28             "d": "To spread by infecting other programs or files"
29         },
30         "answer": "c) To track a user's browser and download history to display targeted advertisements"
31     },
32     {
33         "question": "How can malware infections occur?",
34         "choices": {
35             "a": "Malware authors only use virtual means to spread malware.",
36             "b": "Removable drives are not a common way for malware infections to happen.",
37             "c": "Malware authors use a variety of physical and virtual means, including removable drives.",
38             "d": "Physical means include only using email attachments."
39         },
40         "answer": "c) Malware authors use a variety of physical and virtual means, including removable drives."
41     },
42     {
43         "question": "What type of malware requires user interaction to function?",
44         "choices": {
45             "a": "Viruses",
46             "b": "Worms",
```

Figure 1: Screenshot from VSCode showing multithreading implementation in Python used to process PDF input and send concurrent requests to the LLM via Ollama. Created by VIVID Cohort 6, April 2025.



Another key part of the project involved text extraction from PDFs. We developed a function that filtered out non-relevant characters or formatting errors, ensuring the input sent to the model was as clean and clear as possible. This greatly improved the quality of questions being returned. Additionally, I worked on scripting diagnostic tools to evaluate model performance and stability, such as using the *netstat -ano* command, to verify whether local models were maintaining full local integrity and not making external connections.

One of the models I tested was DeepSeek. My initiative to test the DeepSeek model came from performance issues some of us were experiencing with the Llama models. I wanted to see if DeepSeek offered quicker response times and more comprehensive output, but due to the model's Chinese origins and the potential privacy implications, we were cautious. To mitigate any concerns, I downloaded the model locally via Ollama and conducted safety checks as seen in Figure 2. While it proved to be safe for local use, we ultimately kept Llama3 as our default due to its open documentation and broader trust within the community.



TCP	127.0.0.1:11434	0.0.0.0:0	LISTENING	21044
TCP	127.0.0.1:51473	127.0.0.1:11434	TIME_WAIT	0
TCP	127.0.0.1:11434	0.0.0.0:0	LISTENING	21044
TCP	127.0.0.1:51473	127.0.0.1:11434	TIME_WAIT	0
TCP	127.0.0.1:11434	0.0.0.0:0	LISTENING	21044
TCP	127.0.0.1:51473	127.0.0.1:11434	TIME_WAIT	0
TCP	127.0.0.1:11434	0.0.0.0:0	LISTENING	21044
TCP	127.0.0.1:51473	127.0.0.1:11434	TIME_WAIT	0
TCP	127.0.0.1:11434	0.0.0.0:0	LISTENING	21044
TCP	127.0.0.1:51473	127.0.0.1:11434	TIME_WAIT	0
TCP	127.0.0.1:11434	0.0.0.0:0	LISTENING	21044
TCP	127.0.0.1:51473	127.0.0.1:11434	TIME_WAIT	0
TCP	127.0.0.1:11434	0.0.0.0:0	LISTENING	21044
TCP	127.0.0.1:51473	127.0.0.1:11434	TIME_WAIT	0
TCP	127.0.0.1:11434	0.0.0.0:0	LISTENING	21044
TCP	127.0.0.1:51473	127.0.0.1:11434	TIME_WAIT	0
TCP	127.0.0.1:11434	0.0.0.0:0	LISTENING	21044
TCP	127.0.0.1:51473	127.0.0.1:11434	TIME_WAIT	0
TCP	127.0.0.1:11434	0.0.0.0:0	LISTENING	21044
TCP	127.0.0.1:51473	127.0.0.1:11434	TIME_WAIT	0
TCP	127.0.0.1:11434	0.0.0.0:0	LISTENING	21044
TCP	127.0.0.1:51473	127.0.0.1:11434	TIME_WAIT	0
TCP	127.0.0.1:11434	0.0.0.0:0	LISTENING	21044
TCP	127.0.0.1:51473	127.0.0.1:11434	TIME_WAIT	0
TCP	127.0.0.1:11434	0.0.0.0:0	LISTENING	21044
TCP	127.0.0.1:51473	127.0.0.1:11434	TIME_WAIT	0
TCP	127.0.0.1:11434	0.0.0.0:0	LISTENING	21044
TCP	127.0.0.1:51473	127.0.0.1:11434	TIME_WAIT	0

Figure 2: Local deployment of the DeepSeek model in Ollama, with listed network connections confirming no external communication. Created by VIVID Cohort 6, April 2025.

To further improve accuracy and reduce hallucinations, we explored retrieval-augmented generation (RAG) techniques. This involved filtering prompts and structuring the context more effectively, ensuring that the model's questions stayed grounded in the source text. Once questions were generated, we formatted the results into JSON for consistency and to enable future integration with frontend interfaces, databases, or learning management systems.

We also experimented with integrating a third-party web user interface called WebUI through Docker to make testing more accessible. As seen below in Figure 3, WebUI provided a simplified, visual interface for sending requests to the model and receiving responses, making it easier to track model behavior and improve the overall user experience. This integration allowed us to test models more interactively, mimicking how the final product might function in a real-world educational or cybersecurity setting.

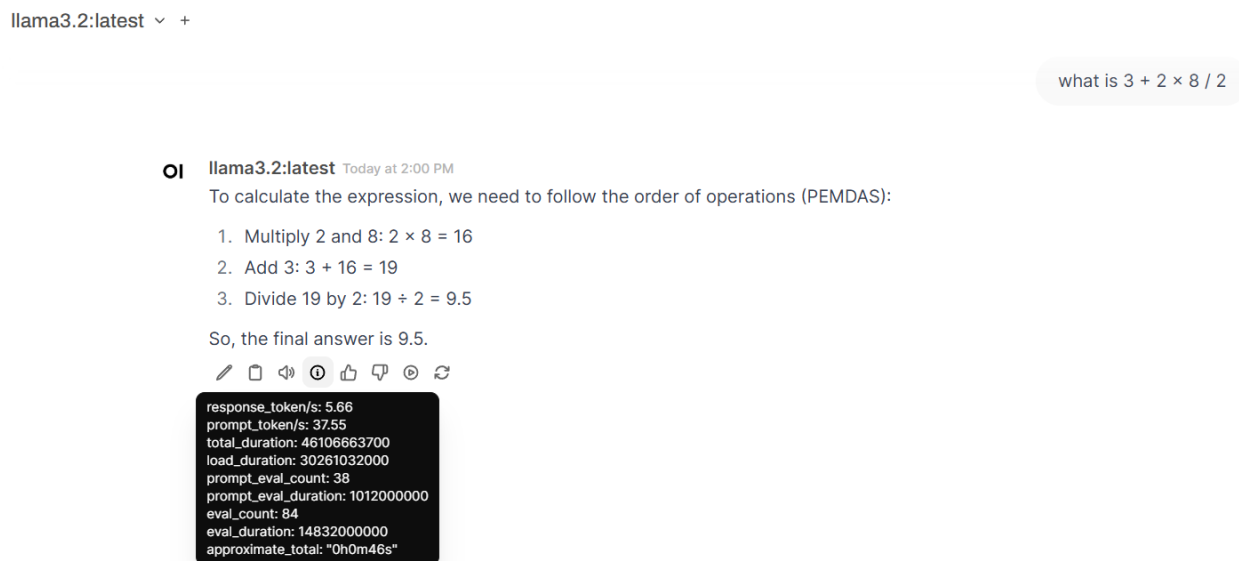


Figure 3: Docker-deployed WebUI interface, enabling interactive testing of LLM responses and providing a visual framework to simulate real-world user interactions. Created by VIVID Cohort 6, April 2025.

Our team presented the project during our final internship presentation to faculty at Augusta University, as well as to contractors from Booz Allen Hamilton and the Department of

Defense. I specifically walked the audience through the architecture of our tool and explained the technical decisions that went into choosing models and building the pipeline. This project was necessary not only to fulfill the internship objectives but also to demonstrate a real-world application of cybersecurity principles, ethical model use, and the balance between innovation and safety when using AI systems. The tool we built can be used as a foundation for further educational tools or even assessment platforms that prioritize data security by running completely offline.

### **Cybersecurity Skills in Action: Applying and Expanding My Knowledge**

Before the start of the internship, my skillset was more aligned with the responsibilities of a cybersecurity analyst, particularly within a blue team role. I had a stronger foundation in areas such as network monitoring, vulnerability management, and threat detection. However, once the internship began, it became clear that the responsibilities would lean more toward cybersecurity engineering and software development. Because of this shift, I had to quickly revisit and refine my programming skills, especially in Python, to gain a functional understanding of the existing codebase and contribute meaningfully to both frontend and backend development tasks. One of the most immediate challenges I faced was working with backend scripts that handled LLM communication and JSON generation. While I had a general understanding of the scripting prior to the internship, I had never worked in a full-stack environment that required multithreading or integration with third-party tools like Docker and Ollama. This meant I had to learn how to work with threads to manage prompt generation in parallel, troubleshoot dependency conflicts during Docker container builds, and understand the logic flow of how data moved from a PDF document, through an LLM, and back as a structured multiple-choice output.

From a cybersecurity perspective, one of the most significant takeaways was how deeply privacy and security concerns influence architectural decisions. For example, the switch from cloud-based AI services to locally hosted LLMs was primarily driven by national security concerns and privacy implications. Being part of the discussions around these decisions gave me a new insight into how software and tools are vetted for use in sensitive environments, and how even the origin of a tool (ex. DeepSeek's ties to China) can become a critical consideration in its implementation.

This experience broadened my understanding of cybersecurity. It's not just about detecting or defending against threats, but also about designing secure systems from the ground up. Selecting the right tools, protecting user data, and ensuring that the technology stack aligns with security policies and mission-critical requirements. The hands-on exposure to software engineering in a security-focused context gave me a much more holistic view of what it means to work in cybersecurity.

### **From Classroom to Real World: The ODU Curriculum in Practice**

ODU's curriculum prepared me for this internship more from the policy, ethical, and criminology aspects of cybersecurity rather than the hands-on, technical side. My coursework at ODU gave me a solid foundation understanding of the implications of cybersecurity decisions, such as the importance of data privacy, ethical AI use, and the legal frameworks surrounding digital systems. These themes were surprisingly relevant during the internship, particularly when we evaluated the use of cloud-based vs. local LLMs. The decision to switch from Gemini to a locally hosted model like Llama3 through Ollama stemmed directly from concerns over privacy and national security, which echoed many of the ethical and policy-focused discussions from my classes at ODU.

However, when it comes to practical, hands-on components, much of that knowledge came from outside ODU. I gained those skills through previous internships, self-study with my certifications, and previous courses at Germanna Community College, where the curriculum was more lab-based and technical in nature. Germanna exposed me to the fundamentals of networking, system hardening, and basic scripting, all of which were useful during this internship.

So, while ODU helped me grasp why cybersecurity is important and how to think critically about its broader implications, this internship gave me the technical context and real-world scenarios to put that knowledge into action. The experience made it clear how both perspectives of technical and theoretical sides are necessary to succeed in the field.

### **Reflecting on My Objectives: Measuring Internship Success**

One of my objectives was to strengthen my understanding of how cybersecurity principles are applied in an academic setting, particularly when dealing with multiple institutions. While I didn't have the opportunity to work across multiple universities as I had thought from when I applied, working within a single university (Augusta) still gave me valuable insights into the specific challenges and security needs of an academic environment. I was able to see firsthand how cybersecurity policies and frameworks are tailored to fit the unique needs of university systems, and this perspective gave me a better understanding of how to address security within a large, decentralized environment. With working on researching and drafting AI-related policies, this experience deepened my understanding of how institutions are beginning to address the risks and responsibilities that come with integrating AI into academic systems, and how policy needs to evolve alongside the technology to ensure security, compliance, and trust.

Another key objective was to observe and assist with the implementation of frameworks and policies within university systems. This goal was met through my exposure to the collaborative nature of policy development, where multiple departments had to align on technical, ethical, and legal standards. I was included in discussions and review sessions that emphasized how cybersecurity decisions are made not in isolation, but with a broad, interdisciplinary approach. Even though the scope was limited to one institution, I gained a much clearer view of the policy lifecycle from how frameworks are developed, reviewed, and implemented in response to emerging threats and technologies.

Lastly, I aimed to further sharpen my technical skills by working on practical projects that would challenge me to apply what I've learned through my studies to real-world situations. This objective was mostly fulfilled as I was able to contribute to the frontend and backend development for internal tools that supported cybersecurity policy work, hands-on tasks like conducting policy audits, reviewing system documentation, and researching cybersecurity best practices. While I didn't get to work directly with SIEM tools as I had hoped, I gained valuable experience working with other security technologies such as network monitoring tools and vulnerability scanning software. These tasks pushed me to think critically about how technical design and functionality intersect in cybersecurity principles.

This internship was highly valuable in fulfilling my objectives, even if some aspects didn't align exactly with what I had originally anticipated. While I didn't spend my days tracking down threats and providing incident response, the experience provided a well-rounded view of cybersecurity in an academic environment and how to develop something from the ground up to grow both technically and professionally.

### **Moments of Impact: The Most Motivating Aspects**

One of the most motivating and exciting aspects of this internship was the chance to work on something that felt truly relevant and timely. Policy development around artificial intelligence in higher education. As someone deeply interested in the intersection between cybersecurity and ethics, the opportunity to help shape AI policy during a period of major technological transformation was both exciting and energizing. It was clear from the start that this wasn't just a side project, it was a priority. The work we were doing had the potential to influence how institutions can navigate AI adoption responsibly and securely. Knowing that my research and input would directly feed into Augusta's broader strategy around AI made the work feel meaningful and impactful. It gave me a sense of real ownership and I took pride in being able to contribute to a conversation that's becoming increasingly central to the future of cybersecurity.

The hands-on nature of the work made the experience so engaging. While I originally anticipated that I'd be doing more observation than action, I was quickly brought into the fold and trusted with tasks that required critical thinking, technical knowledge, and strategic analysis. I contributed to both the frontend and backend development of tools that supported our policy infrastructure, and I was involved in mapping out processes that could help streamline AI documentation, usage tracking, and compliance monitoring. These were not just simple assignments; they were complex challenges that demanded I combine technical problem-solving with a deep understanding of cybersecurity principles. I found myself more engaged because the work wasn't just technical for the sake of being technical. It had a purpose tied directly to policy outcomes.

Working in an academic setting also added to the motivation, particularly because of the unique dynamics at play within a university system as opposed to private sector. Higher

education institutions often have to balance open access to information with the need for robust security, and that tension creates interesting policy and infrastructure challenges. Being in a space where those issues were constantly being negotiated provided a level of insight I hadn't experienced before. It gave me a new appreciation for how cybersecurity frameworks must remain adaptable, especially in environments where the priorities of various departments may sometimes clash.

What made the experience even more fulfilling was the opportunity to work alongside other interns from across the East Coast. Although the five of us never met in person due to the remote nature of the internship, we built a strong bond through our consistent collaboration and support. We communicated often outside of our scheduled meetings to share ideas, troubleshoot roadblocks, and review each other's work. That peer-driven teamwork made the whole process more enjoyable and helped create that sense of community that's often missing in remote internships. Having a group of like-minded individuals to lean on, learn from, and grow with added a whole new layer of motivation and made the challenges more manageable.

The internship was exciting not just because of the content of work, but because of the way I was treated as a contributor. The blend of technical exposure, policy relevance, mentorship, peer collaboration, and inclusion in big-picture conversations made the experience stand out. It solidified my interest in cybersecurity policy and gave me new clarity about the type of work I could pursue after graduation.



### **When Things Got Tough: The Most Discouraging Aspects**

One of the most discouraging aspects of the internship was the noticeable gap between the job description and the actual work we were assigned. When I applied, I expected a role that leaned more towards a cybersecurity analyst. Something that would allow me to focus on identifying threats, interpreting logs, understanding attack vectors, and working with defensive tools. However, much of the role ended up heavily leaning into cybersecurity engineering and software development. While it wasn't entirely outside of my skillset, it didn't align with the expectations I had set or the kind of experience I was hoping to gain in preparation for a cybersecurity analyst role.

We ended up getting handed a large and complex codebase from the previous cohort (Cohort 5) in GitHub with little to no background information or guidance on what we were looking at. Those first couple weeks were especially tough as we were expected to make progress on a system we barely understood. Eventually, we managed to speak with a former intern from Cohort 5 and it helped big time as it allowed us to start to make sense of the code and figure out how to move forward. That initial period felt like a major blocker that could have been avoided with even minimal documentation.

There were times during our scheduled meetings when I found myself having to bring the conversation back to cybersecurity principles, reminding our supervisor and the team that our work needed to be grounded in more than just functional design. It needed to reflect security policy, threat modeling, and risk mitigation. It sometimes felt like cybersecurity took a backseat to software development, and that shift in focus made it hard to feel fully connected to the core goals I had entering the internship.

Another letdown was the lack of career development or progression built into the experience. Aside from the technical tasks and collaborative check-ins, there was not much structured feedback, mentorship, or insight into how our work could translate into future career paths. While our supervisor did a great job supporting us and staying engaged with the team, it became clear that his responses were limited when we asked about career pathways or how this internship could lead to further opportunities, especially in my case where I'll be looking for full-time work after everything concluded. It often felt like the main goal was just to complete the work, wrap it up, and move on. While the experience was still valuable, it left me wanting more in terms of guidance and intentional professional growth. Something I consider essential in any strong internship program.

### **Overcoming Obstacles: The Most Challenging Parts of the Internship**

The most challenging aspect of the internship was, without a doubt, reteaching myself how to program and effectively read through code. While I've always felt confident in my cybersecurity knowledge, stepping into a space that leaned more toward software development was a real test. Early on, I realized I was going to need to relearn quite a bit of Python just to keep up with the expectations. I spent a lot of time outside of meetings and working hours going back over old programming concepts, watching tutorials, and practicing my own just to close the gap. It was intimidating, especially knowing that three of the five interns were computer science majors, but they were extremely helpful and supportive. They never made me feel behind and were more than willing to walk me through logic, syntax, and structural choices when I had questions. That collaborative spirit kept me going, and I'm genuinely proud of the fact that I eventually became comfortable enough to contribute significantly to backend development. I

even helped edit and refine the backend logic to ensure it worked smoothly with Ollama, which was a huge step for me.

Another touch challenge was coordinating outside collaboration with all five interns. While we were a solid group overall, trying to get everyone together beyond our scheduled meetings proved difficult. I understood that we all had school and other responsibilities to juggle, but sometimes it felt like not everyone was making an equal effort to prioritize progress on the project. A few of us constantly tried to carve out extra time to troubleshoot, brainstorm, or just review the codebase, while others were harder to pin down. This uneven availability sometimes slowed down our momentum and forced us to make decisions without full team input. That said, the people who did show up consistently really helped carry the weight, and together we still managed to push the project forward.

Through these challenges, I developed a stronger sense of resilience and adaptability. Being thrown into unfamiliar territory forced me to think critically and independently, which ended up accelerating my growth more than I expected. I gained not only technical confidence, but also a deeper understanding of what it means to contribute meaningfully to a team.

### **Advice to the Next Cohort: Recommendations for Future Interns**

For future interns stepping into this internship, preparation is key to making the most of this internship experience. First and foremost, come in with a flexible mindset. The position may be labeled as cybersecurity-focused, but a good portion of the work falls under software engineering and development, meaning you are more of a cybersecurity engineer, not a cybersecurity analyst or any other blue team position, so being ready to adapt is crucial. I'd strongly recommend brushing up on Python before the internship begins, especially if you don't

have a strong programming background. You'll likely need to spend a good deal of time reading, editing, and writing frontend and backend code to support tools like Ollama or integrating other AI models. None of which will make sense unless you're confident in your scripting and debugging capabilities. Understanding the basics of Flask, APIs, and general software architecture can also be a huge help.

For computer science majors, I'd recommend brushing up on foundational cybersecurity concepts before starting the internship. While much of the work can lean toward development, the project was still rooted in cybersecurity, and it's important to understand the "why" behind what you're building. Familiarize yourself with basic security principles like least privilege, secure coding practices, encryption, and access control. You should also be comfortable with discussing the frameworks like NIST or understanding how security policies tie into real-world systems, especially in an academic setting where decentralization presents unique challenges. Even though your role may involve writing or debugging code, you're still contributing to a larger cybersecurity objective, and being able to think like both a developer and security analyst will make you far more effective.

Another major recommendation is to get comfortable using both GitHub and Discord. Our team inherited a large and complicated codebase from the previous cohort with little to no documentation, which made the first few weeks extremely difficult. If you're not used to navigating repositories, understanding commits, or managing branches, you'll find yourself lost quickly. It also helps to understand version control principles and collaborative workflows because everything you work on will likely be shared and built upon others. Just as important is having an effective communication method in place and for us that was Discord. It became our go to platform for daily check-ins, quick questions, file sharing, and coordinating impromptu

meetings. Being comfortable using Discord to stay connected with your team can make a huge difference in how smoothly the collaboration flows, especially in a remote setting.

Understand that your fellow interns are likely going to be from other regions of the country. Whichever school you get assigned to through CAE in Cybersecurity Community, it's vital that you place an emphasis on communication. It's easy to fall into a routine where everyone works in isolation. You should enter this experience with realistic expectations. While this is labeled as an internship, it's very independent by nature. You will be expected to take initiative, manage your own time, and frequently solve problems on your own or collaboratively with your peers. Be the one who reaches out, schedule extra meetings when needed, and checks in with the group. Never hesitate to advocate for you and your team when something feels unclear or off-course.

Lastly, be mentally prepared to navigate a bit of ambiguity. The project scope might shift, and you might find yourself doing work outside of what you originally envisioned. Embrace that and take it as an opportunity to stretch yourself and gain experience in areas that might prove useful down the road. While the career development aspects were limited, the technical exposure and collaborative environment are what you make of them. With the right mindset, this internship can be a highly rewarding experience both personally and professionally.

## **Conclusion**

Looking back at my internship as a cybersecurity engineer at CAE in Cybersecurity Community, I can confidently say it challenged me, shaped me, and ultimately expanded my understanding of what it means to work in the cybersecurity field. My biggest takeaway is that not every experience will align perfectly with your expectations, and that's okay. In fact, the

mismatch between the role I expected and the responsibilities I was handed is what pushes me to grow the most. I entered this program expecting to sharpen my skills as a cybersecurity analyst but quickly found myself immersed in software engineering tasks. That meant stepping far outside my comfort zone. It was intimidating at first, but leaning into that discomfort is what made the experience meaningful. Growth doesn't happen when you're comfortable, it happens when you're challenged, and this internship was proof of that.

I learned the value of collaboration in a remote setting. Working with a diverse group of interns spread across the East Coast taught me the importance of strong communication, especially when there are no in-person meetings to fall back on. Tools like Discord became essential for maintaining our team dynamic, and I genuinely appreciated how we made the effort to support one another outside of our scheduled check-ins. The bond we formed virtually carried through some tough sprints, late nights troubleshooting, and navigating a confusing legacy codebase along with a new AI tool. The people I worked with made this experience more meaningful, and the camaraderie we built will stick with me.

As I wrap up my time at Old Dominion University and prepare to graduate this semester, this internship left a lasting impression on how I approach my studies and career preparation. It's made me realize that it's not just about passing courses or checking boxes, it's about building actual skills, staying adaptable, and taking ownership of your development. I now feel more intentional about the online training I want to take, the certifications I want to pursue, and the types of full-time opportunities I seek next. I'm more interested in roles that blend cybersecurity with hands-on engineering, and I'm motivated to use my remaining time at ODU to solidify that hybrid skillset.

Professionally, this internship has influenced my trajectory in a major way. It opened my eyes to how broad the cybersecurity field really is and how many roles sit at the intersection of tech disciplines. It also taught me that job titles don't always tell the full story. Because of this experience, I'm now open to pursuing roles that mix threat modeling, secure software design, DevSecOps, or even policy-driven security implementation. Most importantly, I am no longer shy away from job listings that include responsibilities I'm not fully confident in because I've proven to myself that I can learn, adapt, and succeed when it matters.

This wasn't a perfect internship, and I think that's what made it valuable. It was real and it gave me a space to struggle, to question things, to feel unsure, and still show up and contribute something meaningful. I walk away from this experience with more than just technical knowledge. I walk away with resilience, clarity, and the confidence of stepping out of my comfort zone is not something to fear, but something to lean into. The mindset shift alone will guide me for years to come, both at ODU and in my future career.