Asia Hobson
Employer: Kumaran Guargan
Company: Sentara Health
CYSE 368- Spring
4/22/25

Table of Contents

Introduction

This semester, I had the incredible opportunity to work remotely as an intern with Sentara Health, where I supported the Identity and Access Management (IAM) team. From my home office, I regularly worked through ticket requests using ServiceNow, gaining hands-on experience in real-time access provisioning, account management, and troubleshooting user access issues—critical components in any healthcare IT environment. This wasn't just a random internship for me, I specifically sought out this opportunity because of my long-term goal to combine my passion for both healthcare and cybersecurity. As a junior majoring in cybersecurity with a minor in data science, I'm deeply committed to driving secure, data-informed innovation within the healthcare industry.

My journey to this internship started through a program called WIN (Women's Initiative Network), where I was fortunate to meet a mentor who helped guide and support me in my professional development. Through that connection, I was introduced to Ann Jones, the Director of Sentara's IAM division. Her openness to mentoring emerging talent and her belief in the value of student potential played a huge role in me securing this internship. What started as a summer opportunity has since extended into an ongoing role with the company, allowing me to build strong relationships and deepen my experience across multiple semesters.

Being able to list this internship on my resume has opened doors to other opportunities as well—most recently, it helped me secure another internship at Sentara for Summer 2024, this time in a different department where I can continue growing and exploring new areas of the organization. In this reflection, I'll share some of the challenges I encountered early on, the areas where I realized I needed to grow, and the academic and professional insights I gained throughout the experience. I'll also discuss three key learning outcomes from this internship: learning hands-on in a real enterprise environment, advocating for myself to grow professionally, and gaining a clearer understanding of compliance in healthcare IT.

First Impressions

Being the only online intern for my department at the start was a little intimidating, but I saw it as an opportunity to challenge myself and stand out. Like many other new hires at Sentara including nurses, pharmacists, and fellow interns I attended my orientation via Zoom. It was incredibly eye-opening. As someone passionate about healthcare, I appreciated seeing just how many moving parts work together behind the scenes to keep the organization running smoothly. We reviewed key information like timesheets, benefits, company policies, and internal systems, all of which set a professional tone from the beginning. What stood out most, though, was the warmth, professionalism, and organization of the staff it left a lasting first impression and made me feel welcome, even from behind a screen.

After orientation, we were instructed to check in with our respective supervisors. I wasn't entirely sure who mine was at first, so I took the initiative to reach out to the recruiter who initially contacted me for clarity. Once connected, my manager informed me that I needed to complete some preliminary training before officially starting my role. The modules covered essential workplace topics like customer and colleague interaction, HIPAA and PII compliance, ticketing system usage, and general safety protocols. While much of the material, particularly the cybersecurity-related content, was already familiar to me with my coursework, it served as a valuable refresher and a great way to align myself with organizational standards.

What really impressed me as I began working with the Identity and Access Management team was the intelligence, diversity, and precision of the professionals around me. The team came from a range of technical and cultural backgrounds, which made collaboration insightful and refreshing. Everyone was not only knowledgeable in their specific domain but also demonstrated a strong attention to detail, especially when dealing with access requests, policy enforcement, and compliance. Their thoughtful approach to problem-solving and their ability to communicate complex tasks clearly inspired me to hold myself to a higher standard and learn as much as I could from every interaction.

Management Environment

From what I've observed during my time at Sentara, every well-structured IT department typically consists of an IT Analyst, Cybersecurity Architect, Infrastructure Architect, Infrastructure Engineer, Business Analyst, Senior IT Specialists, an IT Manager, and a director. Each plays a unique and essential role, especially within the Identity and Access Management (IAM) team, where collaboration and precision are key to maintaining security and operational efficiency.

The IT Analyst often serves as the first line of support managing ticket flow, analyzing access requests, and ensuring data accuracy across systems. Cybersecurity Architects focus on designing and refining access control frameworks to ensure they align with security best practices and compliance standards such as HIPAA and NIST. Infrastructure Architects take a high-level approach, ensuring that the IAM systems are scalable, well-integrated with existing infrastructure, and future proofed. Infrastructure Engineers are hands-on, maintaining the IAM tools, automating provisioning tasks, and supporting day-to-day system performance.

The Business Analyst bridges the gap between technical solutions and business needs by gathering access requirements, aligning them with role-based access control policies, and

working to streamline approval processes. Senior IT Specialists typically mentor junior staff, oversee complex access scenarios, and manage privileged access reviews. The IT Manager oversees the team's performance, coordinates cross-departmental projects, and ensures timelines and compliance metrics are met. At the top, the Director sets the strategic vision for access governance, evaluates risk management practices, and ensures that IAM initiatives support the organization's overall cybersecurity posture.

Throughout my internship, I worked closely with both the IT Analyst and the Cybersecurity Architect. This gave me the chance to understand both the operational and architectural sides of IAM.

Work Duties

My primary responsibilities during the internship revolved around managing a high-volume ticketing queue within the Identity and Access Management (IAM) team. I was responsible for processing access requests through ServiceNow, which included adding and removing users from Active Directory (AD) groups in accordance with Sentara's internal policies and compliance standards. Before executing any group modifications, I verified managerial approval from the group owner or designated authority, ensuring that all changes were properly authorized and auditable.

In addition to routine access requests, I frequently handled tickets involving the creation of new AD groups. This process required careful attention to naming conventions, group scopes, and hierarchical placement within the AD structure, ensuring full alignment with organizational standards and security policies. A critical part of my role also involved provisioning Privileged (PB) accounts for users who required elevated access. These accounts come with stricter controls and are subject to additional security protocols, so precision and compliance were essential.

Beyond technical, I regularly engaged in proactive communication with requestors and department managers to confirm access needs, troubleshoot any issues, and ensure timely resolution of requests. This often involved determining which AD groups were necessary to restore or grant appropriate access based on role or department. In doing so, I developed a deeper understanding of access governance, user lifecycle management, and the importance of cross-functional collaboration in maintaining system integrity.

Skills/ Knowledge

Throughout my internship, I gained a solid foundation in both technical and professional skill sets that will benefit me long-term in my cybersecurity career. On the technical side, I became highly proficient in using ServiceNow for ticket management and workflow tracking, and I deepened my hands-on experience with Active Directory, particularly in user group administration, account provisioning, and understanding group policy structure. I also gained exposure to Privileged Access Management (PAM) and learned how to securely provision and monitor privileged accounts, which are critical components in any enterprise security framework. Working within a real-world IT infrastructure helped reinforce the importance of access control, the principle of least privilege, and compliance with regulatory standards like HIPAA and PII protection.

On the professional side, I developed strong communication skills by regularly collaborating with end users, managers, and cross-functional IT staff to clarify requirements and resolve access issues. I learned the importance of attention to detail and accountability, especially when handling sensitive information and privileged accounts. Additionally, I became more confident in managing multiple tasks under deadlines, which significantly improved my time management and organizational skills.

One of the more personal lessons I took from this experience was how vital it is to remain open-minded and curious. There were many moments where I encountered unfamiliar systems, terminology, or procedures, but my willingness to ask questions, research independently, and learn on the fly allowed me to keep up and even get ahead. My academic background in cybersecurity gave me a solid foundation, but it was my curiosity and ability to draw on outside knowledge—from coursework, independent research, and even online communities—that helped me understand new technologies and adapt to changing tasks more quickly. I also learned that being open to feedback and flexible in unfamiliar situations is what helps turn good team members into great ones.

Ultimately, this internship taught me that technical knowledge alone isn’t enough—it’s a mix of skills, attitude, and adaptability that allows you to thrive in a professional IT setting**.**

ODU Curriculum

ODU's curriculum gave me a solid foundation that helped me step into my internship with confidence, especially when it came to understanding the laws, regulations, and policies that govern cybersecurity in professional environments. Courses like my Windows 280 class introduced me to the basics of Active Directory through lab simulations, which made concepts like user provisioning and group management feel familiar during the internship. It was exciting to see how the theory translated into real-world applications.

That said, the internship offered an entirely new level of hands-on experience that the classroom can't fully replicate. At Sentara, I worked in a live enterprise environment, where I had to navigate real ticketing systems, interact with actual users, and troubleshoot access issues in real time. I also learned how to communicate professionally across departments, follow strict change management protocols, and ensure compliance with internal policies—skills that aren't always emphasized in academic labs.

One of the biggest technical skills I gained during the internship that I hadn't learned in school was privileged access provisioning and understanding the nuances of role-based access control (RBAC) in a healthcare setting. I also gained a deeper understanding of how tools like ServiceNow integrate with Active Directory for request automation, which is something we didn't cover in coursework. Overall, the experience bridged the gap between theory and practice and gave me a clearer view of what it's like to work in an enterprise-level cybersecurity role.

Internship Fulfillment

One of my primary goals going into the internship was to gain experience working in a real-world ticketing queue. This goal was fully met. I spent most of my time managing and completing access requests through ServiceNow, where I processed tickets involving the creation of Active Directory groups, added and removed users from those groups, and ensured appropriate manager approvals were documented. This hands-on experience not only strengthened my technical skills but also gave me a clearer understanding of how structured workflows operate within an enterprise environment.

Another objective I hoped to achieve was growing professionally, specifically learning how to advocate for myself, communicating effectively, and taking initiative in my own development. I achieved this by reaching out to my manager early in the internship to set up meetings, discuss my progress, and identify ways I could contribute more meaningfully to the team. These proactive steps helped me stay aligned with expectations and even opened doors for future opportunities. As a result of this initiative, I secured another internship for the upcoming summer within a different department at Sentara, showing that my efforts to grow and stand out professionally were successful.

Lastly, I wanted to deepen my understanding of compliance, especially within a healthcare setting. While I had learned about privacy laws like HIPAA in school, this internship brought those lessons to life. I saw firsthand how seriously compliance is taken when it comes to access management from requiring manager approvals to ensuring privileged accounts were provisioned carefully and monitored. This experience made me more aware of how cybersecurity practices must align with legal and ethical standards in the real world, especially in industries as sensitive as healthcare

Motivation

The most motivating part of my internship was the sense of accomplishment I felt knowing I had finally taken a major step forward in my career by securing an opportunity in my field. Getting my foot in the door with a respected healthcare organization like Sentara meant more than just checking a box, it signified growth, potential, and a company that believed in investing in its interns. I was fortunate to be placed in an environment that not only allowed me to learn but encouraged me to explore different areas of the organization based on my interests.

Since I've always been passionate about both people and healthcare, it felt like a privilege to gain an insider's perspective on how healthcare professionals rely on secure access to digital systems to keep patients safe. Being exposed to the back end of what supports frontline care from managing access to critical applications to understanding what systems nurses and doctors rely on made me feel like I was contributing to something meaningful. One of the most rewarding parts of the experience was engaging employees across departments, including non-technical staff, and helping explain technical concepts in a way that made sense to them. It not only improved my communication skills but helped build my confidence in representing IT as approachable and collaborative.

Another unexpected and deeply motivating aspect of the internship was my involvement in a professional development group called Women in the Field. We held monthly Zoom sessions where women across Sentara shared their experiences, supported one another, and discussed challenges faced by women in tech and corporate environments. It was inspiring to hear directly from my director about initiatives she wanted to implement to create a more inclusive, comfortable, and empowering workplace for everyone. Being a part of those conversations made me feel seen, supported, and encouraged to keep pushing forward in a male-dominated industry.

Discouragements

The most discouraging part of my internship was the initial isolation of being the only intern on my team. Unlike more structured internship programs that offer a cohort of peers and a predefined schedule, my experience was far more independent and self-directed. There wasn't a formal onboarding plan or set learning path, I was trained briefly and expected to begin working right away. While that fast-paced transition was challenging, it also pushed me to adapt quickly and take the initiative in shaping my own learning experience.

Because my team members were deeply involved in their own projects and responsibilities, it was sometimes difficult to receive in-depth training on new tools or processes. I realized early on that if I didn't speak up or actively ask for more exposure, the opportunities wouldn't just come to me. So, I made it a point to advocate for myself whether it meant scheduling check-ins with my manager, volunteering to take on more complex tickets, or asking to shadow others in different roles. Despite the hurdles, I turned the lack of structure into a growth opportunity. It taught me to be resourceful, persistent, and self-motivated with qualities I now see as some of the most valuable takeaways from this internship.

Challenges

The most challenging aspect of my internship was navigating the ambiguity that sometimes comes with being new in a complex IT environment. One of the biggest challenges was not always knowing who the right point of contact was when I encountered access issues or needed approval to perform certain tasks like creating or modifying cloud-based groups in Active Directory. As an intern, my permissions were understandably limited, so I often had to track down managers or senior staff members to gain the necessary access, which could sometimes delay the completion of tickets. Learning how to escalate requests appropriately and follow the correct chain of command became a skill I had to develop quickly.

Another major challenge was communicating technical concepts to individuals across the organization who didn't come from an IT background. Many of the users I supported were healthcare professionals, nurses, clinical staff, or administrators who understandably had little familiarity with terms like "AD groups" or "privileged access." It required a lot of patience and adaptability on my part to break down technical processes in a way that was approachable and meaningful, while still ensuring that access requests were handled accurately and securely. This experience sharpened my ability to translate complex technical information into everyday language, which I now consider one of my most valuable professional skills.

There were also moments when the workload slowed down, particularly when the ticket volume was low. Because I hadn't yet been trained in every area, I sometimes found myself without tasks I could confidently complete. Instead of waiting passively, I made it a point to reach out to my manager, request new responsibilities, and express interest in learning more advanced tasks. However, gaining access or being granted new responsibilities as an intern required additional approvals, which at times made it harder to keep a consistent workflow. Despite these limitations, I remained proactive and used downtime to review documentation, shadow team members when possible, and deepen my understanding of the IAM ecosystem at Sentara. In the end, each of these challenges pushed me to become more independent, resilient, and adaptable skills I know will serve me well in my future career.

Recommendations

My recommendations for future interns stepping into this role would start with one simple mindset: come open-minded and ready to learn. This internship offers an incredible opportunity to grow, but only if you take initiative. Before your first day, I'd suggest watching a few videos or reading introductory material about identity and access management (IAM). Having a general overview of how IAM fits into the broader scope of cybersecurity especially in a healthcare organization, will help you understand the bigger picture and how your work directly impacts patient safety and system security.

One of the most important things to realize early is that no one is going to spoon-feed you tasks or force you to learn beyond your assigned duties. If you want to grow, you have to set your own goals and actively pursue them. Take time to identify what skills you'd like to develop, whether it's learning more about Active Directory, understanding how ServiceNow workflows operate, or gaining exposure to privileged access provisioning. Then, communicate those goals with your manager. I recommend setting up a recurring 1:1 meeting to stay connected with your manager, share your progress, and discuss new learning opportunities. IT managers have incredibly busy schedules, so it's important to be prepared. I always came to those meetings with a brief outline of what I had accomplished, what I was currently working on, and what I wanted to learn next. That level of preparation not only showed initiative but helped me make the most of the time they generously made for me.

Another important piece of advice is to build strong relationships with your team. Don't be afraid to reach out and introduce yourself. Even though my internship was remote, I made an effort to get to know the people I was working with. When you've already established that connection, asking for help feels much easier—and they'll be more likely to support you when you need guidance. Beyond your immediate team, take advantage of any networking opportunities the company offers. Attend virtual events, join professional development groups, and turn your camera on in meetings when you can. I joined a group called Women in the Field, where I connected with women across the organization, listened to their experiences, and gained insight on how to navigate the workplace as a woman in tech. These connections not only expanded my network but made me feel more grounded and supported.

Also, don't be surprised if the communication style is more casual than what you may be used to. Many employees, especially in IT, use informal and friendly language when texting or messaging on Microsoft Teams. It might feel a little odd at first, but getting comfortable with that tone will help you feel more at ease and blend more naturally into the team culture.

Lastly, be as proactive as possible when completing your assigned tasks. If you find yourself in downtime or notice a drop in ticket volume, speak up. Ask for new responsibilities or suggest areas where you think you can contribute. If you see something that could be improved, or if you have an idea for a better process, don't be afraid to voice it. Managers and team leads appreciate interns who think like professionals and come to the table with solutions—not just questions. This level of drive and curiosity is what will set you apart and open even more doors in the future.

Conclusions

Looking back on this internship experience, I can confidently say that it was a turning point in both my academic journey and professional development. Interning with Sentara Health's Identity and Access Management team not only gave me the technical exposure I needed but also allowed me to grow in ways I never fully anticipated. From mastering tools like ServiceNow and Active Directory to learning how to communicate effectively with both technical teams and non-technical stakeholders, I walked away with more than just knowledge—I walked away with confidence, clarity, and direction.

What made this experience even more meaningful was the level of trust and independence I was given. While the internship didn't follow a traditional structure, that flexibility taught me how to create my own path and take control of my learning. I learned how to advocate for myself, reach out when I needed guidance, and set goals that pushed me forward. Those efforts didn't go unnoticed—because of them, I was offered a new internship within Sentara for the upcoming summer, allowing me to continue expanding my skill set and exploring different areas within the organization.

This internship also deepened my appreciation for the importance of cybersecurity in healthcare. It's one thing to study HIPAA, PII, and access control frameworks in a classroom setting—it's another way to see them applied in real time, where a single error could compromise patient safety or delay critical care. Being part of a team that takes those responsibilities seriously was eye-opening, and it solidified my passion for using technology to protect people and data in high-stakes environments. It reminded me that cybersecurity isn't just about systems—it's about people, trust, and responsibility.

Beyond the technical and professional growth, I was especially grateful for the relationships I formed and the mentorship I received. Being a part of initiatives like Women in the Field helped me find community, support, and inspiration as a woman in tech. It showed me that there's space for compassion and collaboration in cybersecurity, and that you don't have to fit a specific mold to succeed, you just have to be willing to learn, speak up, and show up fully.

As I continue my studies at Old Dominion University and pursue future opportunities in cybersecurity and data science, I'll carry everything I've learned from this experience with me. Whether it's managing access requests, communicating across departments, or stepping into leadership roles, this internship has laid a strong foundation for the professional I hope to become. I'm excited for what comes next, and I'm incredibly thankful for this opportunity that helped me realize just how capable I am when I'm given the space to grow.