Final Paper

Student: Natalie Hardwicke

Company: Hillenbrand Inc.

Supervisors: Andrew Wilder and Kenneth Vanderpool

Course: CYSE 368

Term: Spring 2023

Table of Contents

Introduction

When considering where to intern, there were several important factors that influenced my decision. First and foremost, the location of the company and my work environment were paramount. I wanted to work somewhere within a reasonable distance, preferably within a thirty-minute drive, or have the flexibility to work remotely. This would help me prioritize my studies while still allowing me to gain valuable experience in the field of cybersecurity. The second factor that weighed heavily on my decision was the size and type of company. It was essential to me that I gain hands-on experience working with incidents, users, and other team members. This would provide me with valuable insight into the cybersecurity industry and help me understand the practical application of the skills I was learning in school. Therefore, I focused on finding an internship with a large enough company that could offer me these opportunities. Lastly, I was looking for a company culture that aligned with my values. It was important to me that the company promoted a healthy work-life balance and a positive working culture, while also emphasizing community involvement and giving back. Finding a company that met these criteria was essential, and I was fortunate enough to find Hillenbrand, which ticked all my boxes, and they offered a great pay rate. Accepting the offer for the Cybersecurity Intern position at Hillenbrand Inc was an easy decision.

In my first week of the cybersecurity internship, I created a list of goals that I wanted to accomplish and discussed them with my supervisor. As a new intern in the field, my primary objective was to gain hands-on experience in Security Operations. I wanted to learn how to use various platforms and SIEM tools to detect and respond to alerts. This goal aligned with my interests and future career goals, as many new graduates and entry-level professionals start in a Security Operations Center or Helpdesk. My second goal was to explore the different career paths available in cybersecurity. Although I had studied the fundamentals in school, I was eager to learn more about how these skills were applied in the real world and what career paths were available to me. By achieving this objective, I hoped to better understand the practical application of cybersecurity. Finally, I wanted to continue educating myself by attending webinars, reading the latest cybersecurity blogs and posts, and participating in demonstrations. I understood that as a cybersecurity professional, it was essential to keep up with the latest developments and have a genuine interest in the field. Fortunately, Hillenbrand provided me with the opportunity to achieve my learning objectives, gain valuable experience, and learn about different cybersecurity career paths. I am grateful for the support and guidance of my supervisor and the cybersecurity team, which helped me develop my skills and become a more effective cybersecurity professional.

Beginning of Internship and Description of Hillenbrand

Hillenbrand Inc. is a global industrial company that started its main operations in 1906 when John A. Hillenbrand bought the Batesville Coffin Company and renamed it Batesville Casket Company. Over the years, the company expanded its operations, acquired new subsidiaries, and grew in size. Initially, Hillenbrand was primarily a manufacturing company, but in recent years, it has shifted its focus to the industrial sector. This shift is evident in the sale and planned divestiture of Batesville Casket Company in February 2023 and the acquisition of several industrial subsidiaries. Currently, Hillenbrand Inc. has two main focus segments: Advanced Process Solutions and Molding Technology Solutions. The former includes Rotex, Herbold, Shaffer, Shick Esteve, Diosna, Coperion, Gabler, Unifiller, VMI, and Bakon, which provide advanced process solutions for various industries. Most of these companies are new acquisitions that have allowed Hillenbrand to expand its presence in the industrial sector. The latter includes DME, Milacron, and Mold Masters, which focus on molding technology solutions. Hillenbrand operates globally, with employees and customers in various countries. With such a huge global presence and so many subsidiaries, the cybersecurity team is important to keep these companies, sites, and machines up and running.

Prior to beginning my internship at Hillenbrand, I was fortunate to have received ample guidance from someone in the Human Resources (HR) department. They skillfully walked me through the necessary paperwork, the drug-testing process, and answered any questions I had. Hillenbrand ensured that I had all the necessary equipment, including a work computer and accessories. My supervisor, Andrew Wilder, shared important standard operating procedures and policies for me to review before my first day. On the first day, HR held an informative onboarding session to brief me on the essentials, although I had not heard from the Cybersecurity team yet. However, I did see that I had a Daily Standup call scheduled on my Microsoft Teams calendar. I inquired of Andrew if I should attend, and he replied telling me that I should. During this call, I was introduced to my colleagues, and listened to what was discussed. The meeting served as a springboard for further training, with Andrew requesting that Sagar and Yusra, the Security Operations employees, set-up Knowledge Transfer Sessions in the afternoons to train me on Operations. These hour-long sessions lasted a week and a half, providing me with valuable training. I received no other training during my onboarding, but Andrew directed me to set up meetings with everyone on the team and with specific technology sector managers in the company.

After the meeting, Andrew instructed me to start requesting access, but did not specify which platforms or how to do so. I eventually found a Standard Operating Procedure (SOP) for access requests in the IT Security Teams folder and followed those instructions. Although I had little access, work, or meetings in the first week, I busied myself with reviewing various SOPs, attending webinars, and meeting with my team members. Initially, I found Hillenbrand to be a warm and welcoming place with plenty of skilled professionals. However, I wondered if they were fully equipped for another intern as I had little instruction and training during my first week. Furthermore, the other intern was on vacation when I began, and she proved to be a great help throughout my internship. As the weeks progressed, I realized that my internship would be more challenging than I had anticipated, but I was determined to take on the challenge and work hard for what I wanted.

Management Environment

During my time at Hillenbrand, I had the opportunity to work closely with Andrew Wilder, the Chief Information Security Officer, who served as my main supervisor. While he oversaw the entire team, he always made sure to provide extra assistance or support when necessary. The Information Security Team held daily calls that lasted around thirty minutes, during which we would discuss updates, plans, questions, and any obstacles we were facing. This approach allowed for open communication across the team, enabling Andrew or our project manager to identify areas where we needed additional support. Additionally, we held weekly Cybersecurity Team meetings, which were smaller and more focused, allowing us to review documentation, discuss current cyber news, and collaborate on any ongoing issues or projects. These meetings provided valuable insights into each team member's work, allowing for more productive and meaningful discussions.

Furthermore, I had a weekly one-on-one meeting with Andrew, during which we reviewed my workload, progress, development plans, and any other topics that needed to be addressed. These meetings were extremely beneficial, as they allowed Andrew to mentor me, without micromanaging, and gave me an opportunity to bring up any concerns or questions I had. Ken Vanderpool, our project manager, was also available to meet with me on an ad-hoc basis, providing an outlet for any issues, questions, or concerns I had. Although I was not closely supervised, this approach provided me with the independence to manage my workload, be proactive, and develop my time management skills. While it would have been helpful to have more supervision at times, this management structure gave me a realistic view of what a full-time job would entail, making my internship very effective. Overall, this experience taught me to take responsibility and accountability for my work and use my time effectively, skills that will be invaluable in my future career.

Work Duties and Responsibilities

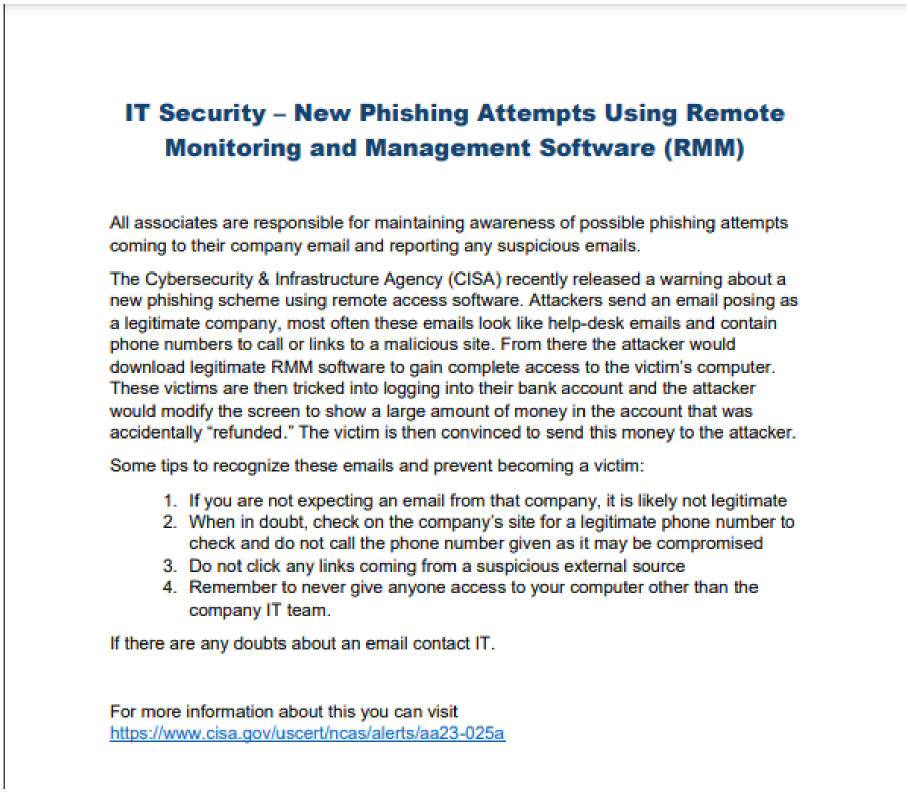
During my internship at Hillenbrand, I was given a diverse range of duties and responsibilities to fulfill over a period of three months. One of my primary responsibilities was to handle Security Operations in the afternoons. This entailed monitoring various platforms, which cannot be disclosed for security and privacy reasons, and handling any security alerts, user issues with the platforms, and tickets assigned to the Security team. I dedicated anywhere from two to four hours to this task every day. During slow periods, I would use the time to work on other projects or personal development.

In addition to Security Operations, I was assigned the task of managing company assets and aiding in the implementation of a new platform to help the Security team in asset management. Given the company's vast size and global presence, there were thousands of assets to keep track of, with varying classifications and locations. My daily routine involved monitoring how many company assets were appearing on different platforms and keeping track of how many assets the new platform received from the client. During the implementation phase, we encountered issues with pushing the client to certain systems, and we resorted to using a shell script to target these assets.

Although asset management may seem dull, it is critical to the business to ensure that assets are properly protected, accounted for, and not lost or stolen.

The most tedious but significant responsibility I had during my internship was to update and write Standard Operating Procedures (SOPs), policies, playbooks, and other essential documentation. I invested a considerable amount of time drafting and revising the Asset Management Standard, which was an eleven-page document that referenced other policies and standards. Despite the fact it was a challenging task, I was able to complete it in approximately two weeks, after several rounds of revisions, and finally got it approved. In addition, I successfully composed three specific incident response playbooks for User Fraud, Data Breach, and Third-Party Compromise, respectively. I also wrote two SOPs for the new platforms the company adopted and updated six other SOPs that the company already had in place. Since these documents contain sensitive information, I am unable to provide evidence of my work. However, I have included some IT Security Memos that I wrote in the appendices A and B below. I would write these memos and have the CISO review them before being sent out to all Hillenbrand employees. The importance of documentation cannot be overstated, as it facilitates new hires to understand proper procedures, helps current employees to refer to the documentation for specific situations, and ensures compliance with regulatory requirements.

Apart from these duties, I also assisted with vulnerability management, website scanning, project management, user issues, and other tasks assigned to me.



IT Security – New Phishing Attempts Using Remote Monitoring and Management Software (RMM)

All associates are responsible for maintaining awareness of possible phishing attempts coming to their company email and reporting any suspicious emails.

The Cybersecurity & Infrastructure Agency (CISA) recently released a warning about a new phishing scheme using remote access software. Attackers send an email posing as a legitimate company, most often these emails look like help-desk emails and contain phone numbers to call or links to a malicious site. From there the attacker would download legitimate RMM software to gain complete access to the victim's computer. These victims are then tricked into logging into their bank account and the attacker would modify the screen to show a large amount of money in the account that was accidentally "refunded." The victim is then convinced to send this money to the attacker.

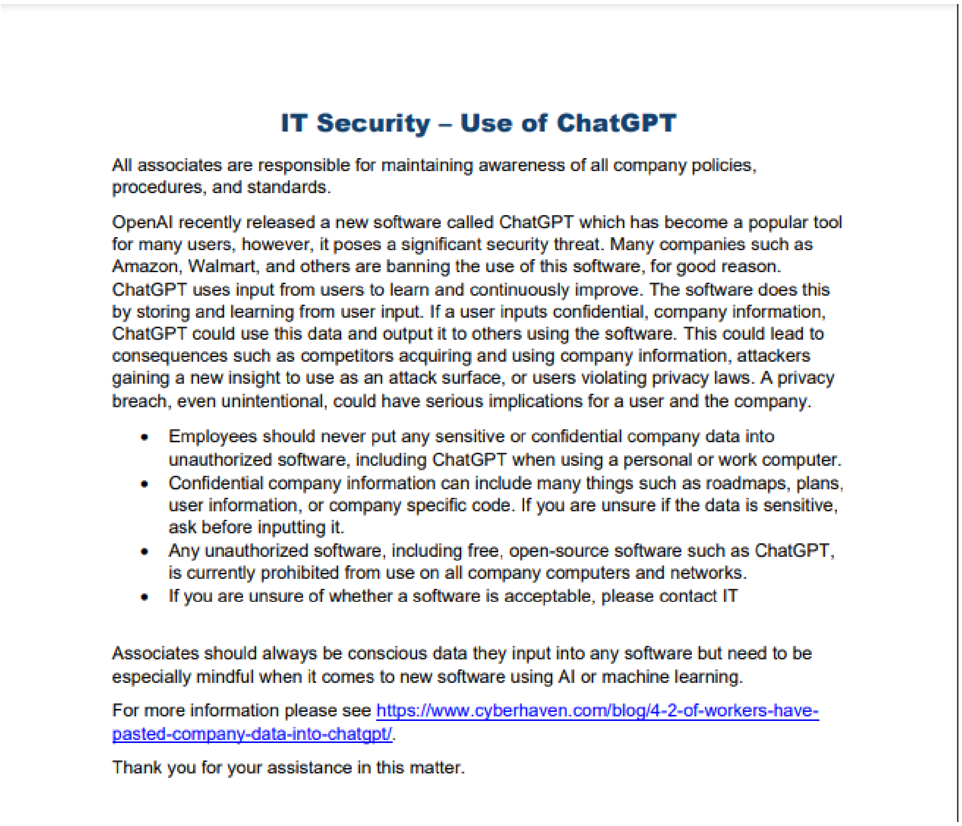
Some tips to recognize these emails and prevent becoming a victim:

1. If you are not expecting an email from that company, it is likely not legitimate
2. When in doubt, check on the company's site for a legitimate phone number to check and do not call the phone number given as it may be compromised
3. Do not click any links coming from a suspicious external source
4. Remember to never give anyone access to your computer other than the company IT team.

If there are any doubts about an email contact IT.

For more information about this you can visit
https://www.cisa.gov/uscert/ncas/alerts/aa23-025a

Appendix A: IT Security Memo – New Phishing Attempts



IT Security – Use of ChatGPT

All associates are responsible for maintaining awareness of all company policies, procedures, and standards.

OpenAI recently released a new software called ChatGPT which has become a popular tool for many users, however, it poses a significant security threat. Many companies such as Amazon, Walmart, and others are banning the use of this software, for good reason. ChatGPT uses input from users to learn and continuously improve. The software does this by storing and learning from user input. If a user inputs confidential, company information, ChatGPT could use this data and output it to others using the software. This could lead to consequences such as competitors acquiring and using company information, attackers gaining a new insight to use as an attack surface, or users violating privacy laws. A privacy breach, even unintentional, could have serious implications for a user and the company.

- Employees should never put any sensitive or confidential company data into unauthorized software, including ChatGPT when using a personal or work computer.
- Confidential company information can include many things such as roadmaps, plans, user information, or company specific code. If you are unsure if the data is sensitive, ask before inputting it.
- Any unauthorized software, including free, open-source software such as ChatGPT, is currently prohibited from use on all company computers and networks.
- If you are unsure of whether a software is acceptable, please contact IT

Associates should always be conscious data they input into any software but need to be especially mindful when it comes to new software using AI or machine learning.

For more information please see https://www.cyberhaven.com/blog/4-2-of-workers-have-pasted-company-data-into-chatgpt/.

Thank you for your assistance in this matter.

Appendix B: IT Security Memo on the Use of ChatGPT

Use of Skills and Knowledge

During my internship, I was able to leverage some of my existing cybersecurity and professional skills, but I also had to learn a lot of new skills on the job in order to work efficiently. Coming from a serving background and having completed coursework in cybersecurity, my communication skills were strong, which proved useful in collaborating and communicating with various teams and personnel within and outside the company. However, the internship allowed me to further develop my communication skills by learning corporate language and terminology, as well as how to communicate effectively with personnel despite language barriers, and how to speak and write in a more professional manner. Additionally, my prior experience in vulnerability scanning using Tenable Nessus was beneficial, and I was able to expand on this skill by utilizing Tenable.io to scan for vulnerabilities and websites within the company.

Beyond these skills, I learned several new technical skills that were invaluable to my development as a cybersecurity professional. For example, I learned how to use SIEM platforms to monitor alerts from various endpoints, users, and systems. I became proficient in investigating alerts, contacting users to gather more information, and connecting to hosts to perform in-depth investigations. Another important skill I acquired was using ticketing platforms to submit and solve tickets sent to us by users, which taught me how to investigate issues and effectively communicate with others if I was unsure about what I was seeing. I also gained experience with Active Directory, which I had no prior experience with, and was able to utilize it to look up users, identify unauthorized access, and understand how the organization's domains were structured.

Finally, I was able to develop strong writing skills through creating policies, standard operating procedures, and other documentation required for the company. Although I had some experience with writing prior to the internship, this opportunity allowed me to hone my skills and gain experience with writing documentation that was essential for both the company and me. Overall, the internship provided me with invaluable experiences and skill development that will be useful as I continue to pursue a career in cybersecurity.

Internship Versus Schooling

During my internship at Hillenbrand, I realized that the curriculum at ODU had not fully prepared me for the demands of my job. Although the program provided some practical coursework such as the CYSE 270 Introduction to Linux class, most of the other courses focused on the fundamentals of cybersecurity and basic terminology. The program did not adequately explore the various career paths available in cybersecurity and the breadth of the field. While the curriculum covered topics such as penetration testing, cybersecurity risk management, and ethical hacking, it did not offer guidance on other jobs that most students will inevitably start in such as a security operations personnel or analyst. I also felt that there should have been more on how to remediate attacks or provide instruction and exposure on critical tools such as SIEM platforms that are crucial in any cybersecurity position.

Despite these shortcomings, the ODU curriculum did equip me with some essential foundational knowledge and transferable skills that proved useful during my internship. For instance, the program helped me to improve my writing skills, which proved invaluable when I had to write policies, standards, and other documentation. Although the cybersecurity policies course I took focused primarily on the structure of policies and their interrelation, it did offer exposure to cybersecurity policies, which was beneficial when I started writing policies for the company and team. Additionally, the ODU curriculum instilled in me the importance of time management skills since most of the courses were offered online, requiring self-motivation and effective time management. Finally, the curriculum exposed me to various operating systems such as Windows, Linux, and Ubuntu, which proved advantageous when looking at vulnerabilities or investigating issues for specific systems. All of these skills allowed me to begin the position with some knowledge beforehand and join conversations without being completely lost on the topics.

In summary, while I believe that the ODU cybersecurity curriculum provided a strong foundation of theoretical knowledge, it did not equip me with all the necessary skills to succeed in my internship without prior experience. However, I did acquire some fundamental skills and knowledge that helped me adapt to the internship's demands and overcome some of the knowledge gaps that existed.

Accomplishment of Goals

During my three-month internship at Hillenbrand, I set out to achieve three main goals: gain hands-on experience in security operations, learn about the various career paths available in the cybersecurity field, and further develop myself both professionally and educationally. I am proud to say that I successfully accomplished all three objectives. Throughout my internship, I received thorough training from experienced analysts who taught me how to use various software and platforms. This training enabled me to analyze alerts, communicate effectively with users, and conduct investigations. These skills will undoubtedly prepare me for a future career as a cybersecurity analyst if I choose to go down that path.

In addition to gaining valuable experience, I also had the opportunity to learn about the numerous career paths that exist in the cybersecurity field. I had the pleasure of meeting with members of the cybersecurity and IT teams, who shared their day-to-day experiences and insights into the industry. I was pleasantly surprised to learn about the many diverse options available, such as vulnerability management, data loss prevention, access management, asset management, cloud security, email security, cyber project management, and more. This exposure has given me a better understanding of the cybersecurity landscape and the opportunities available to me. If there is one job I do not enjoy, I know there are many more to try out.

Finally, I was able to develop myself both professionally and educationally. Hillenbrand provided me with various opportunities to improve my resume and LinkedIn profile, receive feedback, and network with professionals. Additionally, I was granted time to study and prepare for the AWS Certified Cloud Practitioner certification, which I passed with flying colors. I also attended webinars, kept up with cybersecurity news, and participated in meetings and trainings. Overall, my internship at Hillenbrand was a resounding success. I accomplished my goals and gained a wealth of experience and knowledge. I am grateful for the opportunity and look forward to taking what I learned and applying it in my future career.

Aspects of the Internship

Before starting my internship, I was thrilled just to have landed the opportunity and received the job offer. As someone who had never interned or interviewed for a professional/corporate role outside of the service industry, the entire process was new and exhilarating, providing me with valuable lessons for the future. Once I began the internship, the most exciting part was being able to gain hands-on experience in security operations and tackle new projects. As a team player, I was eager to contribute my skills and make a difference. The most motivating aspect of the internship was to demonstrate my worth to the team, proving to them that I was a quick learner capable of adding value, rather than just a clueless intern constantly bombarding them with questions. I am proud to say that I was able to prove my value, take on multiple projects, and assist the team tremendously in areas that were unfamiliar to me initially.

While there were several exciting and motivating aspects of my internship, there were also some discouraging ones. One of these was the lack of training. I had anticipated more guidance and training than the few hours I received upon starting the internship. Although it encouraged me to be resourceful, it was challenging to figure out some aspects of security operations and other tasks by myself, particularly when there were few resources to consult. Another discouraging aspect was feeling like some of my work lacked significance. While some of my assignments were meaningful and made me feel like I was truly contributing, others felt inconsequential, like writing pieces that would just gather dust in a folder. Despite these challenges, I remained committed to enjoying my work and making the most of my time at Hillenbrand.

The most difficult part of the internship was having to research, rely on my resources, and find solutions independently. As previously mentioned, I received little to no training or support for most of the projects and writing assignments I was given, which compelled me to leverage my knowledge and external resources to resolve issues. When I encountered difficulties, I would seek help from my team until I received the necessary assistance.

Overall, my internship at Hillenbrand was a valuable experience that allowed me to achieve my goals of gaining experience in security operations, learning about different career paths in the cybersecurity field, and developing myself professionally and educationally. While there were some discouraging aspects, such as the lack of training and feeling like some of my work had no meaning, overall, I was able to enjoy my job and make the most of my time at Hillenbrand. The most challenging aspect of the internship was having to research and figure things out on my own, but it also allowed me to be resourceful and learn how to use my knowledge and outside resources to solve problems.

Recommendations for Future Interns

For those embarking on an internship in ODU’s School of Cybersecurity or considering this path for their future career, there are a few things you can do to prepare and make the most of your experience. Firstly, it is crucial to update your resume, LinkedIn profile, and conduct some research on the job paths that are available for someone with a cybersecurity degree. This will help you identify the classes that will be most valuable to your career goals. Additionally, creating a vision board to hang up and see daily will be helpful. This can provide motivation and remind you of your purpose while navigating the difficult demands of school, work, and a social life.

During your internship, it is important to make connections and seek out a mentor. Having a network of professional relationships and recommendations can greatly enhance your job prospects. Furthermore, seeking out additional work or projects beyond your assigned tasks can demonstrate your initiative and help you develop new skills. Continuing to learn and grow is also essential in the cybersecurity field. Setting aside time each week to participate in webinars, read the latest news, study for certifications, or engage in other career-enhancing activities will work out in your favor in the long run. Additionally, it is important to not be afraid to ask questions or seek guidance. Your coworkers and supervisors understand that you are new to the industry and are there to help you succeed. In the end, the only person responsible for your success is yourself. By being open to new opportunities, staying curious, and advocating for your own growth and development, you can make the most of your internship and set yourself up for a successful career in cybersecurity.

Conclusion

Reflecting on my time at Hillenbrand, I am grateful for the opportunities and experiences that I gained during my short three-month internship. This internship has not only allowed me to explore various career paths in the cybersecurity field but also helped me develop a clear understanding of what I want to pursue in the future. Before starting the internship, I had limited knowledge of the field and only knew about a few cybersecurity roles. However, through various conversations and meetings with experienced cybersecurity professionals, I learned about the diverse opportunities that exist within the industry, such as vulnerability management, data loss prevention, access management, asset management, cloud security, email security, and more.

Furthermore, I was able to gain hands-on experience in security operations, analyzing alerts, investigating incidents, and communicating with different stakeholders. This experience has helped me develop critical thinking and problem-solving skills, which are essential in the cybersecurity field. In addition, working in a corporate environment has helped me understand how businesses operate, how departments collaborate, and how professionals communicate and work towards common goals. This internship has given me exposure to the job application process and taught me valuable interview skills. Before this internship, I had no experience in the corporate world, and I was not confident about my interviewing skills. However, after attending mock interviews and learning from experienced professionals, I became more comfortable and confident in the job application process. This internship has helped me prepare for future job interviews and has equipped me with the skills to market myself effectively.

Lastly, this internship has allowed me to gain experience in the cybersecurity field, which I believe will set me apart from other new graduates looking for a job. The skills and knowledge I have gained at Hillenbrand have prepared me for a career in the cybersecurity field, and I feel confident that I will be able to contribute effectively in any role that I take on. My internship experience at Hillenbrand has been incredibly beneficial and valuable. I am grateful for the opportunities and experiences that I gained during my short time there, and I am excited to take the next steps in my career with the knowledge and skills I have developed.