Name: Brandon Harris

Company: Leidos

Date 10/21/2024

CYSE 368: Cybersecurity Internship

Term: Fall 2024

Old Dominion University

Table of contents

Introduction

This semester I was able to secure an internship as a cybersecurity engineer at Leidos, a leading provider of technology and solutions in sectors such as aviation, defense, and cybersecurity Leidos has a focus on supporting our nation's national security and government missions. Leidos also works with a wide range of government agencies and bodies to secure our critical infrastructure and to improve and support our nation's defense capabilities. Leidos' mission in supporting our nation's national security which is an area I am deeply passionate about is what drove me to apply to work for the company. Leidos provided a platform where I could contribute to safeguarding the critical information systems that protect our nation. Being able to give back to the country through work that makes a real impact is something I strongly believe in. I come from a long line of public servants—both of my parents served in the military, and my siblings work for the federal government in different capacities and this background has instilled in me a deep sense of responsibility and pride in serving others and giving back to my nation. The learning and growth opportunities that can come from working at Leidos was something that was also highly appealing to me as I have met some of the smartest and most talented people working here and Leido's emphasis on empowering employees to do meaningful work aligns with my personal beliefs as it allows me to use the skills I have learned to be a part of a mission that matters.

Learning Outcomes

During my internship at Leidos, I had three primary learning objectives that I decided were crucial for my professional development, as they would allow me to apply and expand upon the skills I had learned in the classroom. These objectives not only aligned with what I was interested in but also pushed me to develop both my technical and interpersonal skills in a real-world environment. Achieving these goals would provide me with practical experience in cybersecurity and help solidify my understanding of concepts that are fundamental to my field of study. The first objective I set out to achieve was gaining a deeper understanding of how enterprise networks are administered and defended from cyber threats. While I had studied network security in the classroom, I wanted hands-on experience in securing large-scale, sensitive systems like those within the Department of Defense. My goal was to learn how to protect these networks from advanced threats through active monitoring and defense strategies. The second objective I pursued was developing both my technical and soft skills for supporting end users. In addition to sharpening my technical expertise, I recognized the importance of effectively communicating with end users, many of whom may not have a technical background. In a large organization like Leidos, cybersecurity teams need to collaborate across various departments and with different stakeholders, including those who may not be well-versed in technical jargon. The final objective I set was to learn more about system analysis and engineering support. I wanted to build on my foundational knowledge of system analysis to better understand how large systems are managed, maintained, and optimized for security. This objective was important to me because it would enable me to develop a full view of system architecture and the complexities involved in securing enterprise networks. By understanding the system design, I wanted to improve my ability to identify and mitigate potential risks, which would ultimately prepare me for more advanced roles in cybersecurity. I chose these learning objectives to ensure that I could not only strengthen my technical skills but also expand my understanding of the broader cybersecurity landscape which would equip me with the knowledge and tools necessary to thrive in the field.

History

Leidos has a long history of technological innovation and solving complex challenges. Leidos was originally founded in 1969 but was known as Science Applications International Corporation (SAIC), the company began with a focus on research and development in the defense and intelligence sectors. Over time, Leidos expanded its capabilities to include advanced engineering, cybersecurity, and technology across multiple industries. In 2013, Leidos separated from SAIC to become an independent organization, positioning itself as a leader in delivering unique solutions to support national security, public safety, and critical infrastructure protection. Leidos' core services include providing defense technologies, cybersecurity solutions, and systems engineering support for government agencies, particularly those involved in intelligence, and homeland security. The company also serves customers in the healthcare and civil infrastructure sectors helping them solve complex technological and security challenges. Leidos' clients include major government bodies such as the Department of Defense, Department of Homeland Security, and various intelligence agencies such as the NSA and the CIA. The company also works with commercial organizations and international organizations to enhance their security and operational efficiency. Leidos is widely recognized for its innovative approach, research, and data analytics to address the ever-evolving threats faced by its customers.

The Beginning

My internship started with an orientation at Leidos' headquarters in Reston, Virginia. During orientation, I had the opportunity to learn about the company's history, culture, and core values, and where I learned that Leidos places a strong emphasis on collaboration, innovation, and empowering its employees to do things that matter. I also had the chance to network with other new hires, which helped build a sense of community and connection within the organization. During this time, I was given access to my employee account, which provided the necessary resources to begin my work. I was also given some company swag which included a shirt I could wear to the gym a customized water bottle, a notebook, and a pen. Following the orientation at headquarters, I traveled to a facility near my worksite called a Sensitive Compartmented Information Facility (SCIF) to complete a required process for gaining access to the location where I would primarily be working. Because of the sensitive nature of the contract I was assigned to, my worksite was located at the customer's site, and part of my onboarding process involved being "read into" the specific program I would be working on. This program briefing introduced me to the contractual obligations, security protocols, and the specific tasks I would be handling during my internship. These initial days were filled with excitement as I began to see how my role would fit into Leidos' larger mission of supporting national security efforts. My first impressions of Leidos were positive. The company showed a strong interest in its employees and provided them with the tools and resources necessary to succeed and the focus on national security made me eager to get to the work site and start contributing to something bigger than myself. The structured onboarding process, from orientation to gaining access to the work site, made for a smooth transition into my internship.

Management Structure

The management structure at my internship was a hierarchy that placed importance on guidance and flexibility, providing a foundation for both mentorship and autonomy. I had a direct supervisor who was responsible for overseeing my daily progress and ensuring that I was meeting the goals set for the internship. My supervisor reported to the program director, who was responsible for the contract’s overall objectives and aligning our team’s work with the expectations of the agency we were working under. This agency, the ultimate authority in our contract, sets the security and operational standards, requiring our team to execute our roles with a high degree of accuracy and confidentiality. Along with my direct supervisor and the program director, I also had a manager who provided daily tasks and instructions for both our short-term goals and the contract's long-term mission. A unique aspect of this management structure was the high degree of trust my managers placed in me. From early on, I was told by my managers that they trusted my skills and judgment enough to assign me larger projects that would contribute meaningfully to our team’s objectives. This level of trust allowed me to work independently on tasks and projects, making decisions based on the knowledge and skills I had developed. My managers also encouraged me to explore my own interests within the scope of our work, allowing me to pursue aspects of cybersecurity and security operations that I was passionate about. This management approach created a supportive environment that balanced oversight with autonomy and allowed me to develop my technical and problem-solving skills within a framework that was still guided by experienced professionals.

Work Duties

Due to the classified nature of my work, I am restricted from sharing specific details of my assignments and projects but in general terms, my role involved several key responsibilities that were necessary to the success of our contract and our client’s mission. One of my primary duties was analyzing system logs to detect potential security incidents. This involved reviewing large amounts of data to identify anomalies that could indicate cybersecurity threats, Another significant responsibility was conducting vulnerability scans to identify and address any security weaknesses within the network and these scans were essential for ensuring that systems remained secure from attackers trying to break into our network. Another task I had was creating custom dashboards and alerts that enhanced our security monitoring capabilities. The dashboards I created allowed our team to monitor critical security events in real time and respond to any threats. I also worked on conducting risk assessments and examining network configurations to ensure compliance with the client’s and the federal government's security policies. Through these responsibilities, I was able to contribute directly to Leidos’ mission of providing cybersecurity solutions that protect our clients’ sensitive information and support national security. Each of my duties played a part in ensuring the reliability and security of the systems we were contracted to protect, This hands-on experience allowed me to see firsthand how cybersecurity theory translates into practice and gave me a sense of ownership over projects that directly impacted our team’s success.

The Skills I Used

During my internship at Leidos, I used the skills and knowledge gained from my studies at Old Dominion University (ODU) and prior experiences such as Cyber Patriot. Before starting, I had a foundation in network security protocols, threat detection, and Python programming for automating security tasks. My hands-on experience with Python, gained through ODU's Basic Cybersecurity Programming and Networking course, was useful, as it enabled me to automate routine checks and analyze data efficiently. I also had familiarity with threat detection frameworks, having practiced with Splunk through the Collegiate Cyber Defense Competition (CCDC), Where I defended a fictional corporate environment against penetration testers for the public and private sectors. On the job, I was able to improve my skills as I took on more complex tasks, such as analyzing large-scale network logs and customizing security alerts. Working within a high-security environment required me to understand network protocols like DNS, DHCP, and SSH on a larger scale, which deepened my understanding of their role when trying to monitor and defend enterprise networks. while I had used SIEMs for basic detection tasks, my internship introduced me to advanced functions like setting up custom dashboards and real-time alerts, which allowed our team to maintain constant visibility into a wide range of network activities. This hands-on experience has fundamentally transformed my understanding of cybersecurity, moving it from a theoretical field of study to a dynamic, real-world application that requires continuous learning and adaptability.

How ODU Prepared Me

The ODU curriculum provided me with a great foundation that equipped me with many of the skills I needed for my internship. For example, the Introduction to Cybersecurity and Cybersecurity Techniques and Operations classes covered topics that directly applied to the technical demands of my role. Introduction to Cybersecurity introduced me to threat detection and response, through exposure to intrusion detection and prevention systems (IDS/IPS), endpoint detection and response (EDR), and SIEM tools like Splunk and Security Onion. This coursework provided foundational knowledge of risk assessments, network security, and security frameworks such as NIST, ISO 27001, and MITRE ATT&CK, which I referenced often at Leidos to evaluate systems for vulnerabilities and how to respond to security incidents. Cybersecurity Techniques and Operations gave me knowledge of threat response and defense-in-depth strategies. By working with tools such as Splunk and Security Onion in a classroom setting, I was prepared for log analysis, incident detection, and vulnerability management. This class gave me practical exposure to risk management techniques, which I applied in my role when analyzing system security and recommending improvements to safeguard against vulnerabilities. Another Class that prepared me for my internship was Introduction to Information Systems this class provided an overview of information systems and IT fundamentals and helped with my understanding of hardware and software components, programming basics, and information security concepts, all of which were valuable for understanding system workflows and security implications in real-world applications. These classes offered me a solid technical foundation, and the hands-on experience from my internship allowed me to further apply and expand this knowledge. The ODU curriculum prepared me well for the fundamental aspects of cybersecurity, while my internship reinforced and broadened these skills.

Evaluating Internship Outcomes

The several key learning objectives I introduced earlier in my paper were meant to guide my experience and ensure my professional development is aligned with my aspirations. These objectives included understanding how networks are administered and defended from threats, improving both technical and soft skills to support end users effectively, and gaining hands-on experience with system analysis and engineering support. The first objective, to understand how networks are administered and defended from threats, was rooted in my desire to gain practical, hands-on experience with enterprise network defense. I am glad to say that this objective was fulfilled through my work analyzing network logs, identifying potential vulnerabilities, and observing how enterprise security policies and procedures are implemented. I gained a much deeper understanding of network defense, including the importance of continuous monitoring and the use of advanced tools to detect and respond to threats. While I had some prior knowledge of how to respond to security incidents I was able to apply these skills to real systems and this allowed me to understand their practical importance in securing networks against adversaries.

The second objective, improving my technical and soft skills to support end users, focused on developing my ability to work effectively with others in a professional setting. Cybersecurity is not solely a technical field; it often involves collaboration, clear communication, and the ability to provide solutions that address both technical and user-centered concerns. Throughout the internship, I had opportunities to interact with end users such as different unit leaders and even some military commanders to answer their questions and resolve technical challenges that I was faced with. These interactions taught me the importance of tailoring my communication style to any audience whether I was working with technical colleagues or non-technical users. I also improved my ability to explain complex concepts in simpler terms and gained confidence in collaborating with teams to troubleshoot and resolve issues. These experiences not only strengthened my technical abilities but also helped to train my interpersonal skills, both of which are needed for success in the cybersecurity field.

The final objective, gaining experience with system analysis and engineering support, was to deepen my understanding of how systems are managed and optimized in a high-security environment. This goal was largely met through my exposure to system risk assessments, vulnerability analysis, and the identification of outdated devices in need of replacement or updates. I was also involved in creating custom dashboards and alerts to improve monitoring and security posture of the system and the network. These tasks not only expanded my technical expertise but also showed me the importance of proactive measures in maintaining system health and security. Through these experiences, I developed a better understanding of the challenges and responsibilities associated with system analysis and engineering in a critical and highly regulated environment. Overall, my internship at Leidos fulfilled the majority of the objectives I set for myself, It provided me with a well-rounded experience that built on my existing skills while introducing me to new concepts and practices. Each goal was designed to enhance my professional growth and better prepare me for a career in cybersecurity. By achieving these objectives, I gained invaluable insights into the field, solidified my technical expertise, and developed a greater appreciation for the people who work every day to protect your nation and the professionals who take cybersecurity seriously because they know and understand the risk of having unsecured systems on a network. The combination of technical challenges and problem-solving has made me even more passionate about cybersecurity and has strengthened my resolve to continue to contribute to our nation's national security through the skills I am learning.

The most motivating or exciting aspects of the internship

My internship at Leidos provided numerous opportunities to learn, grow, and contribute to meaningful work, but several aspects motivated me to come to work every day. The chance to work on projects that directly supported national security, the trust given to me by my supervisors, and the opportunity to collaborate with and learn from highly skilled professionals all made this experience rewarding. The most motivating aspect of my internship was the knowledge that my work directly contributed to national security and critical missions. Leidos' focus on supporting government agencies and safeguarding critical infrastructure gave every task I performed a sense of purpose and importance. Knowing that the logs I analyzed, the vulnerabilities I identified, and the risk assessments I conducted played a role in protecting sensitive systems and information was incredibly fulfilling. This sense of responsibility was a constant source of motivation, driving me to approach each project with care and dedication. It was inspiring to be part of a mission so closely aligned with my values and to feel that I was making a tangible difference, even as an intern. Another exciting part of the internship was the trust and responsibility my managers and supervisors placed in me. From the beginning, I was encouraged to explore my interests and take on challenging projects that pushed me to grow. My managers not only assigned me meaningful tasks but also trusted me to take ownership of these assignments and see them through to completion. This autonomy was both empowering and motivating, as it allowed me to demonstrate my capabilities and build confidence in my skills. Whether I was developing tools for system monitoring, troubleshooting issues, or collaborating with cross-functional teams, I was given the freedom to approach problems creatively and learn through hands-on experience. This trust showed me that my contributions were valued, which made me feel like a true member of the team.

Another motivation was the opportunity to collaborate with and learn from highly skilled professionals. The team I was working with at Leidos consisted of individuals with extensive expertise in cybersecurity and related fields, and their willingness to share their knowledge was invaluable. Through conversations, mentorship, and hands-on experience, I learned the practical applications of cybersecurity concepts and learned new techniques for addressing challenges. This environment made the internship not only educational but also enjoyable. Being surrounded by such talented individuals inspired me to aim higher, continuously improve my skills, and stay curious about new developments in the field. The dynamic nature of cybersecurity also added to the excitement of the internship. No two days were the same, as new challenges and tasks constantly arose. Whether analyzing network traffic for potential threats, conducting vulnerability scans, or assisting in incident response efforts, I was consistently engaged in problem-solving and critical thinking. This kept the work interesting and encouraged me to remain adaptable and resourceful. It also showed me the importance of staying up-to-date with industry trends and tools, as cybersecurity is a field that evolves rapidly in response to threats.

The most motivating and exciting aspects of my internship came from the combination of meaningful work, professional growth opportunities, and a supportive environment that encouraged my exploration and learning. Contributing to national security efforts, gaining the trust of my supervisors, and working alongside talented professionals all made this experience impactful. This internship confirmed my belief that meaningful work and personal growth go hand in hand, and it has motivated me to strive for excellence in my future career.

The most discouraging aspects of the internship
While my internship at Leidos was largely a positive experience, certain aspects proved to be discouraging. These challenges provided valuable lessons but also had areas where I felt limited or where the experience fell short of my expectations. The most discouraging aspects included the lack of hands-on analytical work, the long commute, and the rigid nature of certain tasks that limited creativity and innovation. One of the most significant sources of discouragement was the limited opportunity to engage in hands-on analytical tasks, which was one of the primary objectives I had set for the internship. My passion lies in analyzing logs, investigating potential threats, and exploring root causes of security incidents, and I had hoped to delve deeply into these areas during my time at Leidos. While I gained valuable experience in network defense and system monitoring, the nature of my assigned tasks often leaned more toward operational maintenance rather than detailed, investigative analysis. This disconnect between my expectations and the reality of the role left me feeling somewhat unfulfilled, as I could not fully explore the aspects of cybersecurity that excite me most. Another challenging aspect of the internship was the lengthy commute to the worksite. Traveling an hour and forty-five minutes each way significantly impacted my daily routine, leaving less time for personal development, rest, and other commitments. The long commute often added stress to my day, especially during periods of heavy traffic or bad weather. This made it difficult to maintain a work-life balance and occasionally diminished my overall enthusiasm for the role, despite the importance of the work I was doing.

The nature of some tasks and processes sometimes felt limiting. In the field of cybersecurity, creativity, and innovation are crucial for addressing complex and evolving threats but the highly structured environment of a government-contracted role left little room for experimentation or the exploration of unconventional solutions. While I understand that I have to follow protocols to maintain security and compliance and that some of these limitations were due to the structure of the program and the specific needs of the organization which I was contracted under, the lack of flexibility occasionally makes the work feel boring. This also restricted my ability to apply some of the problem-solving skills I had developed in school and through personal projects. Lastly, there were moments when the scope of my responsibilities felt repetitive, especially when dealing with routine tasks such as system updates or log ingestion. While these tasks are necessary for maintaining secure and functional systems, they sometimes felt disconnected from the broader mission I was passionate about. The lack of variety in some aspects of my work left me wanting more challenging and impactful projects that aligned with my interests and long-term career goals. Despite these discouraging aspects, I recognize that they were valuable learning experiences. They helped me understand the realities of working in a high-stakes, structured environment and the importance of balancing expectations with practical limitations. These challenges showed me what roles I should seek that would align more closely with my passions and professional aspirations, such as positions that do more analytical work and investigation rather than working to configure tools all day. while the most discouraging aspects of my internship at Leidos occasionally dampened my enthusiasm, they also provided a view into the nature of the cybersecurity field and the importance of finding the right fit in a professional role. These experiences have motivated me to pursue opportunities that offer a balance between structure and creativity, ensuring that my work remains both meaningful and engaging.

The most challenging aspects of the internship
This internship at Leidos presented a range of challenges that pushed me to grow both personally and professionally. The challenges I faced during the internship were primarily tied to the technical complexity of the work, the expectations of the role, and the need to consistently perform in a high-stakes environment. These challenges tested my resilience and adaptability, shaping me into a more capable professional. One of the most difficult aspects was managing the technical demands of the position. Even though I entered the role with foundational knowledge from my academic coursework, the nature of the projects I was assigned required a depth of understanding that I had to quickly develop. This included analyzing unfamiliar systems, identifying vulnerabilities, and applying security measures that demanded critical thinking and precision. Tackling these tasks often involved problem-solving and learning on the job, which was demanding but rewarding.

The level of accountability expected in my role was another significant challenge. Operating in a field as sensitive as cybersecurity, where even small errors can have serious consequences, required me to maintain attention to detail at all times. The need to ensure accuracy in my work, especially in a classified environment, pushed me to develop a greater sense of discipline. Meeting these standards meant consistently double-checking my work, managing my time effectively to avoid rushed errors, and maintaining a calm and focused approach even when under pressure. Balancing my responsibilities with the structure of a government-contracted program was also a challenge. Adapting to a workplace where tasks and priorities could shift based on directives from multiple levels of management required flexibility and communication skills. Understanding where my work fits into the larger framework and ensuring that I met expectations without overstepping the bounds of my role was a constant learning process. This demanded that I be proactive in seeking clarity and asking questions while maintaining focus on my core responsibilities.

Another significant challenge was adapting to the fast-paced nature of the work environment. The constantly evolving priorities and tight deadlines required me to shift focus and manage multiple tasks simultaneously quickly. This level of demand was unlike anything I had encountered before, pushing me to enhance my organizational skills and to remain calm under pressure. While this challenge was taxing at times, it taught me how to manage priorities and deliver high-quality work within limited time frames. The ability to navigate such a demanding environment has improved my ability to think on my feet and produce consistent results. Lastly, the learning curve associated with the highly specialized nature of the work proved challenging. Diving into real-world projects required me to familiarize myself with unique protocols and industry-specific processes that were not covered in my coursework. This challenge meant I had to do a lot of self-learning and collaboration with team members to ensure I could meet the expectations of the role

The internship's challenges were demanding, but they provided me with an opportunity to develop critical professional skills such as adaptability, accountability, and problem-solving. These experiences taught me how to navigate complex technical environments, handle high expectations, and thrive in a structured and mission-driven workplace. While the challenges were significant, they strengthened my abilities and prepared me for the future demands of a career in cybersecurity.

Recommendations for future interns in this internship

If someone were to intern at Leidos they should approach the experience with a proactive mindset, as the internship offers a lot of growth opportunities but requires adaptability, strong organizational skills, and a willingness to take initiative. The technical nature of the work means that while foundational cybersecurity knowledge is important, many tasks involve specialized applications or unique protocols that extend beyond what we are learning in the classroom. It is crucial to ask thoughtful questions and invest time in researching and understanding concepts independently. They should get used to continuous learning as that will not only help them succeed in an internship at Leidos but also prepare them for the nature of the cybersecurity field.

Building effective communication skills is something I would recommend as interns must navigate, a government-controlled environment where clear communication with supervisors, program directors, and other team members is used to ensure alignment on tasks and expectations. Be sure to ask for clarification when needed and provide updates on your progress. Building relationships with colleagues is also important. Networking with coworkers, seeking mentorship opportunities, and engaging in projects can open doors to potential career opportunities within the organization or beyond. Strong time management skills are also critical, as interns will frequently balance multiple tasks and tight deadlines. Use organizational tools such as calendars, and to-do lists, to stay on top of your responsibilities. The ability to manage your workload will help you meet deadlines and will also help you to maintain a high standard of work under pressure. If you are interning at Leidos you should be prepared to work in a classified environment if that is what job you choose to take. Making sure you follow the protocols, procedures, and expectations tied to your role, as well as security policies is of utmost importance. While this aspect of the internship may seem odd to begin with it will provide invaluable experience in handling sensitive information and working within highly regulated settings.

One of the most rewarding aspects of the Leidos internship is the organization’s trust in its interns to take on meaningful work. At Leidos you are encouraged to explore projects that align with your professional interests and career, so taking the initiative to engage with such opportunities can show your enthusiasm and commitment. While this trust or freedom is nice to have, it also comes with a lot of responsibility but not every task or project will go smoothly, and setbacks should be viewed as opportunities to learn and grow. Seek feedback from supervisors, reflect on your experiences, and look for ways to improve your skills and performance. I think interns at Leidos should also prioritize their self-care. The intensity of the internship, combined with demanding tasks and potentially long commutes, can be physically and mentally taxing. strategies to manage stress, maintain focus, and recharge outside of work are important to have. Make sure you establish a routine with regular exercise, healthy eating, and sufficient sleep as it can help you sustain your energy and productivity. Engaging in hobbies or activities outside of work can also provide a much-needed mental reset, which will allow you to return to your tasks with a new focus and motivation.

Future interns at Leidos can maximize their learning and professional development, contribute meaningfully to the organization’s mission, and take significant steps forward in their cybersecurity careers. This internship can be a unique opportunity to gain real-world experience, make meaningful contributions, and build a strong foundation for a future in cybersecurity if you put the time and effort into it.

Conclusion

My internship at Leidos has been a transformative experience that has significantly shaped both my professional abilities and my personal growth. It offered me a unique opportunity to bridge the gap between my academic learning and the real world by allowing me to develop a deeper understanding of the cybersecurity industry and its critical role in safeguarding our national security. This experience has not only broadened my technical skills but helped me develop my ability to adapt to fast-paced environments, solve complex problems, and thrive in high-pressure situations.

Throughout the internship, I was challenged to rise above my comfort zone and address tasks that demanded a high level of technical expertise. These challenges taught me lessons about the importance of resilience, continuous learning, and collaboration. Working in a classified environment has required me to maintain professionalism and grow significantly in my ability to handle sensitive responsibilities that have a large impact on the world around me but has also helped me develop soft skills, such as effective communication and time management, which are just as important as technical knowledge in cybersecurity. Leidos' mission-driven environment deeply resonated with me, confirming my passion for contributing to the protection of critical systems and national infrastructure. Being entrusted with significant responsibilities and receiving encouragement to explore my interests instilled in me a sense of purpose and confidence in my capabilities. This empowerment allowed me to approach challenges not as obstacles but as opportunities to learn and grow. Working alongside experienced professionals and being part of a team that values meaningful contributions made the experience all the more enriching.

My coursework at Old Dominion University provided a strong foundation that prepared me to excel in this role, particularly in understanding cybersecurity frameworks, network protocols, and security operations. The hands-on nature of the internship introduced me to new methodologies and practices that could only be learned through direct experience. As I reflect on this journey, I am immensely grateful for the opportunity to intern at an organization like Leidos. It has solidified my career goals in cybersecurity and provided me with the tools, knowledge, and confidence to pursue more advanced roles in the industry. The skills and insights I gained during this internship will serve as a strong foundation as I continue to grow both academically and professionally.

This internship was more than just a stepping stone; it was a pivotal moment in my development as a cybersecurity professional. It not only prepared me for the challenges and complexities of the field but also inspired me to approach my career with a sense of purpose and determination. I am excited to carry forward the lessons learned and to continue making meaningful contributions to the cybersecurity industry, driven by the values of excellence, and service that I have learned during my time at Leidos.