4/19/2026

Final Internship Paper

CYSE 368 / Internship

Old Dominion University – Spring 2026

Student Name: Daniel Akpovi

Instructor Name: Professor Teresa Duvall / T.A. Joshual Russel

Employer: Leidos Inc.

Company or Agency: McDonald Army Health Center - Defense Health Agency

Table of Contents

Final Internship Paper

1. Introduction

I completed my internship through my current position as a Leidos contractor at the McDonald Army Health Center (MCAHC), where my daily work provided a practical environment to study cybersecurity more focused. MCAHC is a military treatment facility (MTF) whose mission is to provide healthcare to active-duty military members and their families in the Tidewater community (McDonald Army Health Center, 2026). As for Leidos, it is a technology company that works with both government and commercial clients in areas like cybersecurity, health, and defense (Leidos, 2025). Thus, I felt that this internship would be meaningful to me and allowed me to view my routine work with a new mindset. Since the beginning of the internship, I remained in the same workplace but began to see my daily work as relating to cybersecurity, something that is new to me compared to my routine network support work.

My goals for the internship were to use the basics of cybersecurity within my normal work. Also, I wanted to learn the different tools and processes used in an actual organization, and to improve my skills in incident response, vulnerability work, and technical communication. My supervisor helped me to outline and understand these goals early in the internship. He ensured I had access to tools like SolarWinds, Siphon, and the Palo Alto firewall, enabling me to fulfill these goals. As the internship moved forward, I also began to become more aware of the importance of access control, segmentation, documentation, and the link they have with risks. The rest of my experience was guided by that early focus.

My internship took place in an environment shaped by a long history of service to the military community. MCAHC's history began with the establishment of a station hospital at Fort Eustis in 1941 and continues today as a facility that provides healthcare to over 27,000 active-duty military members and their dependents in the area (McDonald Army Health Center, 2016). As for Leidos, it traces its history to 1969 and has grown to become a Fortune 500 company with tens of thousands of employees (Wikipedia Contributors, 2025). Although I was not entering a brand-new workplace, during my initial orientation, I became more familiar with some aspects of the organization, its mission, and its history. Furthermore, I learned about the tasks that I would be performing as an intern, as well as the importance of each of these tasks. Thus, the initial period for the internship gave an overview that the task I will be performing is mission-focused and more important than it might seem from the outside.

2. Management Environment

The management environment of the Army Health Center was very structured and mission-driven. As a contractor, I did not fall within one chain of command. Instead, my reports were to two different organizational hierarchies. I reported to the network manager for the hospital, whose reports were to the Chief Information Manager (CIO). Also, I reported to the program manager for Leidos, the contractor firm, whose reports were to the higher management

at the corporate level. Thus, the management structure had an impact upon me and the way that I executed my tasks. Overall, the management of the facility was structured in a way that indicated the importance of accountability and appropriate permissions for each individual within the facility. Each individual had access to only those areas of the facility associated with their role within the hospital. Any changes to that role require approval from the appropriate authorities within the facility.

My immediate supervisor was Richard Trabbold, the lead network engineer at the hospital. He took an active role in reviewing the work that I was to accomplish during the internship and provided me with the knowledge necessary to understand each task. He was very involved in my internship and required me to think about the tasks that I was to perform and why I was to perform those tasks. His level of involvement in my internship forced me to be more intentional in the work that I performed.

Another strong point of the management environment was that each task had a purpose. Each device, process, firewall access, and setting was for a specific reason and purpose within the MTF. Thus, the management structure was a good learning environment for me as an intern.

The management structure within the facility was effective due to the division of tasks between technicians and engineers. Because I was limited in what I was allowed to do on the network infrastructure, I was somewhat frustrated. However, those limits were set to protect the MTF's environment and ensure that any modifications are made with the appropriate level of control.

3. Major Work Duties, Assignments, and Projects

My duties consisted of monitoring the network, reviewing firewall entries requests, performing segmentation checks, documentation duties, and when I am off work, working with my home lab. I had administrator access to SolarWinds, submitter access to Siphon, as well as read-only access to the Palo Alto firewall. Each tool helped me see how cybersecurity supports typical network operations in a live production environment.

My first major duty was monitoring the network with SolarWinds. By keeping track of all the devices in the network, I could make sure that they were working as they were intended to. Over time, I was able to learn how to distinguish between false alerts and normal network function. This was essential in recognizing when there was an issue with a device without having to react to each alert. Furthermore, I learned how to ensure that my work was presented in a way that other network technicians could understand and utilize to complete their own tasks.

Another of my major duties was the review of firewall requests. Because I did not have write access to the Palo Alto firewall, I was only able to review the requests that were to be submitted to the firewall. These requests were reviewed through Siphon to ensure that they were appropriate for the network. This task was necessary to ensure that no systems within the network were threatened by the rules that were created on the firewall. Furthermore, it allowed

me to get used to the firewall and understand the impact that each request could have on the network.

Segmentation was another of my major duties. This task included reviewing the settings of the VLANs, the names of each VLAN, and the access rules for each network segment. I also reviewed the settings of each switch within the network during this phase of the internship. These tasks ensured that the systems within the network were contained in the segments to which they were to be restricted. Documentation is also a consistent task throughout the internship. I documented all ticket related notes and summaries, including investigation results, and records of all changes and rationale. Documented activities reduce time spent on subsequent activities while assisting with troubleshooting by providing a basis for other technicians to follow my actions and to refer back to when necessary.

The largest of my projects was the building of a home lab. This lab used pfSense and Tenable Nessus Essentials. I created this home lab because I did not have all the access to the firewall in the hospital, and I did not have access to ACAS either. Within my home lab, I set and tested firewall rules, configured NAT, performed port forwarding rules, examined logs and packet captures, ran vulnerability tests, and evaluated segmentation decision-making. This lab provided me with hands-on experience, which enhanced my judgment when working in the production environment. The hands-on experience made me become more cautious when evaluating new requests for access and more thoughtful of how slight modifications can affect the overall security posture of a network.

4. Specific Use of Cybersecurity Skills and Knowledge

Prior to this internship, I had some background in cybersecurity, both from my classes and in my job working as a network specialist I had a bit of background in cybersecurity before this internship, from both my coursework and my work as a network specialist. For example, I took both CS 462 (Cybersecurity Fundamentals) and CYSE 301 (Cybersecurity Techniques and Operations), which provided me with an understanding of topics like traffic analysis, vulnerability identification, countermeasures, firewalls and specifically pfSense firewall work, the Internet, common attacks, authentication, VPNs, access control, segmentation, monitoring, and vulnerability reduction. I therefore entered this internship knowing that I had not had the opportunity to explore a real-world production setting.

During the first phase of the internship, I was able to start using some of those earlier technical skills in a more serious way. My supervisor walked me through identity and access control and helped me develop an appreciation for the process of permission approval and how excessive permission can lead to increased risk. Also, I began to view segmentation differently than before. I used to look at VLANs, ACLs, and Routing only as components of network design. Through my internship experience, I came to realize that they are security boundaries limiting potential movement if something goes wrong. I spent a lot of time reviewing configurations on switches, I learned how to harden them, and learned good practices about

checking log, following up on alert and documentation. This has enabled me to convert class concepts into daily practices.

I developed some skills as the internship progressed and I completed tasks. A major one of these skills included learning how to use SolarWinds, network, system monitoring and management tools. At the beginning, I was overwhelmed by all the metrics and alerts that it was throwing at me. Eventually, with time, working directly with it, I developed the ability to determine if there were any unusual spikes or dips in activity compared to a typical baseline, as well as identify trends across multiple machines prior to making any conclusions. In addition to developing technical abilities, I also realized that creating useful notes requires as much discipline as performing the technical aspects of the task. I had to learn how to write my notes in a way that allowed other technicians to understand the issues I was working on and the reasoning behind the solution that I provided. Such a documentation skill became more important than I had originally thought; good notes can save lots of time when troubleshooting an issue.

Firewall review was another skill in which I gained knowledge. I was only able to review the firewall entries requests through Siphon, as I did not have the full access to directly make changes to the Palo Alto firewall. Every entry request was reviewed to ensure it met the need of the operation and remained within a defined scope. This task taught me the importance of patience, paying attention to details, and being disciplined in the tasks that I perform. In the context of approving firewall rules in a live production environment one misstep will create potential exposure for much longer than the time it takes to approve or reject a request.

The last part of the internship had the most impact upon me. I set up a home lab environment using pfSense and Tenable Nessus Essentials to supplement the access limitations I have at my internship place. With the home lab, I was able to create rules, test traffic flows, practice NAT and port-forwarding, examined logs, and perform vulnerability scans after each time I made a rule or configuration change. The experience on the home lab has given me insight into how each decision made at a firewall level directly affects an organization's security posture. Before this internship, I saw cybersecurity as a set of topics and tools. After this experience, I see it as disciplined daily work built on evidence, careful review, documentation, and restraint.

5. How the ODU Curriculum Prepared Me

The ODU curriculum prepared me for my internship in some respects, but in others left some gaps. The ODU curriculum provided me with a solid foundation in networking, security, and problem-solving. Through my classes, I understood how devices communicate on a network, what access control is trying to protect, and why segmentation and monitoring are important to a network. These concepts allowed me to fully understand the systems in place at MCAHC. I did not go into the internship without a fundamental understanding of the language and concepts that I would encounter. I could relate many of the systems that I saw to the concepts that I learned in my classes.

One of the main connections between my education and my internship is the understanding of cause and effect through my coursework. In my classes, we learned that certain rules, permissions, misconfigurations, and services can lead to certain outcomes. At MCAHC, for instance, a broad firewall request could expose the network to external threats. If there were an exception in the network's segmentation, there would be movement throughout the network. If the documentation was poor within a process, it would slow the troubleshooting process of common issues. Furthermore, my education provided me with the troubleshooting skills necessary for both network monitoring and my home lab work.

Despite the benefits that my education provided me with, my internship showed me aspects of the job that my classroom education did not provide for me. I had not experienced the process of requesting approvals, creating tickets, following a privilege system, or documenting changes to networks. Furthermore, I had not experienced how vital effective communication is within the workplace. In my education, if I provided the correct answer to a question, the process would be over. In my internship, if I answered the question correctly but did not adequately document my answer or explanation, I could still have caused problems for the team. This is one of the main differences between my classroom and internship experience.

Beyond the skills and routines I learned during my internship, ODU prepared me for the role of a network and information security professional. While the internship allowed me to gain experience with new methods and software, university education equipped me with the knowledge of how to perform these tasks. For example, while I had learned about least privilege and defense in depth within my coursework, seeing how this security concept applied to my current department was eye-opening. In many ways, my education at ODU helped to reinforce what I was learning during my internship, but in other ways, my internship helped to correct what I had learned at school. While my education helped to prepare me for the role I will play in securing the network, my internship helped to connect the education I received to my role within the organization. For instance, during my coursework, I was presented with opportunities to learn about the relationship between networking and information security. Though these were separate coursework assignments, they often went hand in hand when I performed network tasks. This relationship between networking and information security was presented to me during my education at ODU, and it was very helpful during my internship. Also, my internship showed me the added pressure that comes with a live environment. While performing a lab task in the classroom can be challenging, there are fewer consequences to performing that task incorrectly. However, when performing the same task in my internship, there was additional pressure to complete that task correctly and ensure that the network is running smoothly for the organization. Though this presented challenges for me due to my lack of experience, it helped me to grow overall.

6. Fulfillment of Learning Outcomes and Objectives

For the internship, I wanted to accomplish three main objectives. Among others, apply the knowledge of cybersecurity that I had learned in my education to the internship place, gain experience with the tools and processes of an actual organization, and develop a sense of judgment in the workplace regarding communication, documentation, and security, especially. Right from the start, I can say that all three of these objectives have been fulfilled by the internship.

The first objective was fully met as I monitored the network for several weeks, reviewed the firewall configuration, evaluated users' access to resources based upon their need-to-know requirements, implemented and enforced segmentation of resources within the network, and reviewed the configurations of routers and switches. I observed firsthand how concepts such as least privilege, logging, containment, and controlled change relate to the real environment of networking, beyond what I learned about them in class. Although I did not have the responsibility of initiating any direct changes to the network infrastructure, especially the firewall, I was still given the task of determining the scope, potential risks, and purposes prior to approving or recommending any type of action. My home lab environment contributed significantly to achieving this objective as well, since I could design, implement, and test various types of controls similar to those that I was evaluating in the production environment of my internship place.

My second objective was also realized as I acquired hands-on experience with SolarWinds, Siphon, and the Palo Alto review process. In addition to gaining practical experience with these tools, I also understood where they fit into an overall workflow. Equally important, I began to understand how organizations use processes to manage risk. This was another aspect of practical learning. Practical experience consisted not only of using click-through software but also understanding approval processes, reviewing standards, and why some types of changes can be made by no one other than specified employees.

I grew the most from the third objective. Documentation turned out to be more important than I realized. I learned that taking clear notes is part of security because it allows for continuity and accountability. I became better at explaining what I did and why, without unnecessary details. I learned to slow down, justify my actions, and think about whether any given step was what the situation truly called for. One area of the internship that I fell short of was related to the direct access I had to some component of the live environment. But I filled that shortcoming by building a home lab. I have learned more in the process than I would have if I only relied on the level of access I had at work. In general, the internship experience met all the objectives that I set, and it gave me a true perspective on what is required in the computer security field. It also met a minor but personal goal that emerged during the experience itself. I wanted to feel more confident in my ability to learn and grow in this field. Through the second and third parts of the internship I was able to accomplish this goal. I was using security tools with more confidence. I

was documenting my activities with more sense of purpose. I was asking better questions to improve myself. I did not gain that confidence because I felt like I knew everything. Instead, it is the opposite. I did it because I was eager to learn, and especially I was learning how to think in a more professional way. During this internship, I found a connection between cybersecurity work and a higher purpose, because my technical work is highly connected to the health of people. These goals I set for this internship made me realize that they were well thought of as they contributed to providing a trusted service within an organization where technological issues can impact patient care and operational flow. The internship experience also met my goal of becoming more intentional in thinking about ethical responsibility as part of this kind of work. Working with the systems with such high levels of privilege, I became more deliberate in the way in which I thought about my access to the systems, my scope of work, and the importance of maintaining accurate records of the work that I performed.

7. Most Motivating and Exciting Aspects.

What motivated me the most during the internship was seeing my daily work in a different light. Since my internship took place in the same environment I already work in as a network specialist, the workplace did not pose a significant challenge for me. However, my mindset changed, especially after several of the talks with my supervisor that outlined some of the aspects of cybersecurity that I should be focusing on while I perform my normal work. He encouraged me to focus on the security aspects of my daily work of network management, the tools and processes used in the organization, incident response routines and skills, network vulnerabilities, technical communication, and work ethics. All these gave my daily tasks a new purpose and meaning instead of moving through my workday on autopilot as I used to do before.

Another motivation for me included the shift from observing others in the security department to actually doing their work. In the second part of the internship, I had more time to work with the security tools of the organization, especially SolarWinds. At first, it was challenging to read the information it was displaying. However, with more time working within the software, I was able to read the trends within the network. I could compare each device in the network and write down my observations and findings. Additionally, creating documentation for each network device also gave me a sense of usefulness because others would be able to quickly troubleshoot any issues within the network using my notes.

Another factor that inspired me was that the work had practical implications. My firewall tasks were to review and validate requests since I had limited access to the Palo Alto firewall. Nevertheless, despite that limit, the work was still important. I could use Siphon to examine source and destination information, ports, business purpose, and requested-access scope. In case a request appeared to be too wide or unneeded, I recorded the concern and re-forwarded it via the appropriate channel. That made me realize that even a minor exception can cause a risk that will extend way beyond the duration of the change. This was the same with the segmentation work. The way I have been thinking of VLANs and ACLs as security boundaries caused me to have a

second thought regarding what occurs once an exception has been placed in the wrong place or when an over-permissioned account has been created. The feeling of consequence had kept me occupied since the work was evidently important.

The most invigorating part of the internship was during the last fifty hours, when I built a home lab with pfSense and Tenable Nessus Essentials to engage more with firewall and vulnerability work than my workplace access allowed. The lab changed everything for me. I implemented rules, tested traffic, scanned networks, inspected logs, set NAT and port forwarding, and even troubleshot failed connections. I also used the lab to think more thoroughly about segmentation and least privilege. I found this part of my internship the most. I could test my judgment and see the outcome in real-time. The end result was that I became more attached to firewall operations, more deliberate in my reasoning, and more inspired to continue growing in this area.

8. Most Discouraging Aspects

The most discouraging aspect of the internship was the limit on my direct access to the Palo Alto firewall. Due to that, I could not do some of the work that I most desired. I could only log into the firewall to review logs, requests, source and destination addresses, and ports. However, I could not go through to the ultimate implementation step. This was frustrating because at first, I was hoping to move past the review aspect of the job and be able to configure firewalls directly within the production network. Such a limitation caused my development to be sluggish compared to the wider exposure I could have had.

Another aspect of the training that I felt was somewhat discouraging was the pace at which I had to learn the various aspects of SolarWinds. At the beginning of my training, there were seemingly endless alerts, metrics, and changes to the status of various devices that are monitored by the software. I often did not know which of the alerts were important versus those that were simply part of the normal operation of the network. Over time, however, I did learn how to recognize which of the alerts were important and which of them were normal, but it was slow, repetitive, and somewhat discouraging at the outset of the internship. Many hours were spent performing the same tasks to learn how to properly complete each task or to learn the reasons that some tasks may have to be performed over time.

Another of the more discouraging aspects of the internship was the pressure to ensure that I did not create any problems within the healthcare network. As I learned early in the internship, creating an exception to a request to the firewall, providing over-permissioned access to a system or a user, or creating a bad rule within the firewall could create problems for the network that can go beyond the system to which that rule applied. Therefore, every request for a rule change required careful consideration and thought before acting upon the request to ensure that I did not create a problem for the organization.

Even though these aspects of the internship were seen as discouraging, overall, I found the experience to be still very useful to me. For instance, I have become more patient in the face of technical problems; I have become more self-controlled in my approach to fulfilling the tasks that have been assigned to me, and I understood how much thought goes into any of the work that is performed within the cybersecurity field.

9. Most Challenging Aspects

The hardest part of the experience was learning to think more deeply about the job, an environment where small decisions carry real weight. Since my internship is at the same place as my full-time job, much of the work that I performed was somewhat familiar. However, the challenge was the shift in mindset that I had to make between my everyday tasks of network specialist and the security-related decisions associated with each task. My supervisor told me to focus on identity and access control, network segmentation, systems hardening and monitoring, and ethics within the job. These gave me a sense of direction but also increased the standard by which I had to evaluate even the most basic tasks that I performed.

Another of the major challenges within the internship was gaining a thorough understanding of the tools. For example, SolarWinds had a lot of alerts and information at the same time when I first started using it. I often did not know what information was important, which was normal for the systems, and which one to ignore. However, by focusing and observing the systems over time, I began to understand what information was important to consider, what normal metrics meant, and what spikes or drops in those metrics meant, as well as how to document the information for later retrieval by another technician who needed such information.

The firewall aspect of the internship presented a whole different kind of challenge. As I did not have full access to the Palo Alto firewall itself, I had to learn through observation as opposed to a direct configuration. I used Siphon to investigate requests to add entries to the firewall, verify source and destination information, check ports and purpose, and ensure that the access was appropriately narrowed. For the most part, there was more judgment required than I thought there would be. One rule or a few access decisions could become issues further down the road for the network if not reviewed properly before being implemented. Thus, that was a challenge for me for having to slow down and think more about least privilege concepts rather than quickest access.

Beyond the above challenges, segmentation and documentation also tested me. When reviewing the network and security settings, I had to ensure that no exception would allow one of the networked systems to access another system without proper permission. Similarly, documenting the work that was performed was also challenging as I had to ensure that my notes were clear, brief, and described the topic in a way that was easy to understand for those of different experience levels with the network. Thus, I had to ensure that I understood the topic well enough to describe both the steps that I performed and why those steps were taken.

The last of the major challenges for me came from my lack of access to certain tools. Since I did not have access to ACAS or the firewall fully, I had to create my own home lab utilizing pfSense and Tenable Nessus Essentials. I had to configure my networking hardware to appropriately allow and block traffic through the pfSense firewall. Additionally, I learned how to use Tenable Nessus Essentials to scan my home lab network for vulnerabilities. This presented more of a challenge for me than some of the other aspects of the firewall at the workplace. Nonetheless, I walked away from the firewall portion of the internship with an understanding of the challenges of network segmentation, appropriate documentation, and how to appropriately configure and secure a network using available tools. I came out with more carefulness, more patience, and more awareness of how much thought good security work requires.

10. Recommendations for Future Interns

My main recommendation for future interns in this role would be to have a solid understanding of networking and be open to learning things outside of their coursework's scope. As the name suggests it, a position in network security is in the intersection between computer networking and security; therefore, having a solid understanding of topics like IP addressing, ports, VLANs, access controls, routing and firewalls would be beneficial for future interns. Understanding these concepts will allow interns to better understand the access to systems and the impact that each of their actions could have on the network. It would also be beneficial for them to learn about least privilege, network segmentation, logs, and documentation prior to this internship. These topics came up during my internship and were followed throughout the entirety of my experience.

I would also tell future interns to be patient, especially to expect a slow learning curve with some tools. Tools like SolarWinds, Siphon, and Palo Alto, in my case, became more familiar with time, not after one quick lesson on how to use them. Interns should become proficient in reading logs and writing notes on any technical issues. Good communication skills are needed beyond the technical work in this environment. People, especially non-tech-savvy personnel, need to understand what was reviewed, what looked wrong, and why a request should be narrowed or changed. Furthermore, interns should always ask questions when something does not sound or look clear to them. I learned more when I stopped trying to figure out every detail by myself and started asking experienced people about what I do not know.

My last recommendation will be to not stop at only what they are learning at their internship. They should go beyond and, for example, build a home lab to overcome any limitations they might have at their internship place. For instance, my home lab with pfSense and Tenable Nessus Essentials allowed me to practice many of what I could not do at my job, such as rule creation and vulnerability scanning. That kind of practice makes the workplace duties easier to understand and makes the intern more confident from the start.

11. Conclusion

This internship has helped me to understand the cybersecurity field in new ways. While I understand the different technical topics related to cybersecurity from my education and my current job, I did not know how they all linked to one another. During this internship, I saw how concepts like access controls, rules, logs, segmentation, firewalls, vulnerability management, and documentation connected to the security of a network. I was also surprised by how much the cybersecurity field requires quiet tasks. A task as seemingly simple as reviewing firewall entry requests, or even simple documentation, can have a significant impact on the security of the network. Lastly, I was surprised at some of the limitations of my visibility on the network. With limited access to firewalls and ACAS, I was forced to create my own lab to gain the specific experience that I desired for this internship. However, this extra task ultimately proved to be one of the most valuable experiences of my time in this internship.

The experience has influenced the remainder of my college time at ODU by allowing me to understand the areas of my degree that I need to strengthen. I now have a further understanding of the skills that I need to improve in my career, as well as the communication skills that I need to have to succeed. Furthermore, I will pay closer attention to the topics relating to organizations and their technical needs in my future courses. The internship has influenced my future professional planning, as it has confirmed my interest in the cybersecurity field, especially in networking security. It made me realize that I need to focus on network defense, firewall skills, vulnerability assessment, and security operations. However, I also want to ensure that I am looking for some mentorship and mission-driven environments.

Though this internship started in a well-known environment, it ended with a new perspective on many aspects of my job. I had previously thought of network security requiring patience, accuracy, and responsibility only during emergencies, but this internship showed me that keeping a network safe requires all that every day; a lesson that will last with me through my education and into my future career.

Appendix A. Representative Tools and Work Samples

Tool / Platform	How It Was Used	Skills Strengthened
SolarWinds	Monitored device and interface health, compared observations to baseline behavior, verified trends before escalation.	Network monitoring, anomaly review, documentation
Siphon	Submitted and tracked firewall requests, reviewed scope, ports, purpose, and least-privilege alignment.	Change review, access control, written justification
Palo Alto Firewall (read only)	Inspected request context and validated whether proposed access appeared necessary and appropriately limited.	Firewall analysis, risk awareness
VLAN and ACL review	Checked segmentation logic, naming, and boundary purpose during operations and troubleshooting.	Segmentation, containment thinking
Configuration and log review	Reviewed switch consistency, log timelines, and recorded what changed and why.	Hardening, evidence awareness, traceability
pfSense home lab	Built and tested firewall rules, segmentation, NAT, and port forwarding in a controlled setting.	Hands-on firewall practice, troubleshooting
Nessus Essentials home lab	Ran vulnerability scans after rule changes to see exposure and confirm the effect of configurations.	Vulnerability assessment, validation

References

McDonald Army Health Center. (2016). *McDonald army health center history*. Tricare.mil. https://mcdonald.tricare.mil/About-Us/McDonald-Army-Health-Center-History

McDonald Army Health Center. (2026). *Mission and vision*. Tricare.mil. https://mcdonald.tricare.mil/About-Us/Mission-Vision

Leidos. (2025). *Who we are*. Leidos. https://www.leidos.com/company/who-we-are

Wikipedia Contributors. (2025, October 27). *Leidos*. Wikipedia; Wikimedia Foundation. https://en.wikipedia.org/wiki/Leidos