

Final Internship Paper

Mohammad Saleh

Old Dominion University

CYSE 368 – Internship

Summer 2026

Employer: Leidos

Company/Agency: Leidos – Supporting the United States Navy

Internship Supervisor: Steve Griffin

Instructor: Professor Duvall / Jade Hines

Date: August 2026

Table of Contents

1. Introduction	1
2. Management Environment	3
3. Major Work Duties, Assignments, and Projects	4
4. Use of Cybersecurity Skills and Knowledge	6
5. Connection to the ODU Curriculum	8
6. Internship Learning Outcomes and Objectives	10
7. Most Motivating and Exciting Aspects	12
8. Most Discouraging Aspects	13

9. Most Challenging Aspects	14
10. Recommendations for Future Interns	15
11. Conclusion	17
Works Cited	19

1. Introduction

My internship with Leidos during the Summer 2026 semester was one of the most important professional experiences I have had during my time as a cybersecurity student at Old Dominion University. I decided to pursue an internship because I wanted experience that went beyond what could be learned in a classroom. Cybersecurity is an extremely technical field, and although coursework provides an important foundation, I believed that working in a real enterprise environment would help me understand how cybersecurity is actually performed on a daily basis. I especially wanted an opportunity in which I could work with experienced cybersecurity professionals, see enterprise security tools, participate in real projects, and learn how government cybersecurity operations function.

Leidos was particularly interesting to me because of the type of work the company performs. Leidos is a major technology company headquartered in Reston, Virginia that provides technology and mission services to government and commercial customers. Its areas of work include defense, intelligence, cybersecurity, digital modernization, health, aviation, and other technology-focused missions. Leidos reported approximately \$17.2 billion in revenue for fiscal year 2025 and employs tens of thousands of people around the world. The company works with

customers that include the U.S. Department of Defense and other federal agencies, making it an especially valuable environment for a cybersecurity student interested in government and national-security technology.

My internship involved supporting work related to the United States Navy. Because of the environment in which I worked, security, compliance, documentation, accountability, and reliability were extremely important. During the internship, I was exposed to enterprise cybersecurity tools and processes that I had previously only studied at a high level. I also learned that cybersecurity in a major organization involves much more than simply preventing hackers from accessing a network. It includes vulnerability management, endpoint security, system configuration, automation, policy enforcement, documentation, ticketing, collaboration, testing, and continuous monitoring.

At the beginning of the internship, I went through orientation and training that introduced me to the organization, my team, the work environment, security expectations, and the technologies that I would encounter. Like many interns entering a large organization, I initially had to become familiar with a large number of acronyms, systems, tools, and procedures. I encountered technologies related to endpoint management, security monitoring, vulnerability assessment, configuration management, automation, and enterprise administration.

One of my first impressions was that enterprise cybersecurity is significantly more complex than a classroom lab. In a school assignment, the student usually knows the exact objective and is working inside a controlled environment. In an enterprise environment, a security change can potentially affect many users and systems. Before changes are implemented, employees must consider security requirements, operational requirements, testing, documentation, approvals,

dependencies, and possible unintended effects. This helped me understand why cybersecurity professionals must be both technically capable and careful.

My initial learning objectives were based on the goals established for my internship. The first objective was to learn how cybersecurity professionals manage and operate enterprise endpoint and security tools. I wanted to understand how tools such as endpoint protection, configuration management, vulnerability management, and monitoring technologies are used on a larger scale.

My second objective was to develop a better understanding of cybersecurity operations in an environment supporting the U.S. Navy. I wanted to see how cybersecurity teams manage systems, respond to security requirements, document work, and maintain compliance in an environment where cybersecurity has real operational importance.

My third objective was to improve my knowledge of cybersecurity automation. I was especially interested in understanding how repetitive cybersecurity and system administration tasks could be automated using technologies such as Ansible and scripting. I wanted to move beyond simply understanding what automation was and actually participate in creating automated solutions.

A fourth personal objective that developed during the internship was improving my professional communication. I wanted to become more comfortable communicating with engineers, managers, other interns, and leadership. By the end of the internship, this objective became especially important because I had opportunities to explain and present work I had completed.

Overall, I began the internship hoping to gain technical experience. I finished the internship with technical experience as well as a much stronger understanding of teamwork, communication,

problem solving, documentation, automation, professional responsibility, and the overall structure of cybersecurity operations.

2. Management Environment

The management environment during my internship was structured but also provided opportunities for independence. Because Leidos is a large organization and the work involved government systems and customers, there were clear processes and responsibilities. Employees were expected to understand their assignments, communicate progress, document work, and follow established procedures.

My direct supervisors and more experienced members of the team were important resources throughout my internship. Rather than expecting me to already understand every technology, they provided explanations and helped me understand how individual systems connected to the larger cybersecurity mission. At the same time, I was encouraged to investigate problems and develop solutions independently instead of relying on someone else for every answer.

This balance was extremely helpful for my development. If an intern is given no independence, it becomes difficult to develop confidence. On the other hand, giving an inexperienced intern complete responsibility for important systems would not be appropriate. My internship provided a middle ground where I was able to learn from experienced professionals while gradually becoming more independent.

The internship also exposed me to an Agile working environment. Work was organized around tasks, projects, meetings, priorities, and progress updates. I learned that technical ability is only one part of successfully completing cybersecurity work. A team must determine priorities, track

progress, communicate obstacles, coordinate responsibilities, and make sure work contributes to organizational goals.

I also noticed that employees with different technical specialties frequently had to communicate with each other. A cybersecurity issue may involve a security engineer, system administrator, endpoint management team, automation engineer, project manager, and customer. This demonstrated why communication is so important in cybersecurity.

I considered the management environment effective because I was given meaningful work while still having access to guidance. The fact that I was trusted with increasingly significant projects throughout the summer demonstrated that the internship was designed to provide actual professional development instead of simply giving interns administrative tasks.

3. Major Work Duties, Assignments, and Projects

My internship included several different responsibilities, but one of the major themes of my summer was cybersecurity automation. One of the most important areas in which I worked involved Security Technical Implementation Guides, commonly known as STIGs.

STIGs contain security configuration requirements that help organizations configure systems securely. In a large environment, manually reviewing and remediating every configuration can require significant time. One of the projects I worked on involved helping automate STIG remediation tasks.

I learned how automation could be used to apply configuration changes in a repeatable and consistent way. I worked with Red Hat Ansible and Ansible Automation Platform, commonly

referred to as AAP. Earlier in the internship I was still learning the basics of Ansible, playbooks, packages, Linux commands, and system configuration. By the end of the internship, I had become much more comfortable using Ansible and understanding how automation workflows could be structured.

One of my major accomplishments was completing an automation playbook. Completing the playbook was especially meaningful because it represented progress from initially learning the technology to actually using it to build something useful. Automation is valuable to the organization because repetitive manual work can require a considerable amount of employee time. Automation can improve consistency, reduce repetitive effort, and allow cybersecurity professionals to focus on problems that require human analysis.

Another project involved automating the creation of HPSM tickets. Ticketing systems are an important part of enterprise IT because they allow work to be documented, assigned, tracked, and reviewed. Tasks that happen repeatedly can become inefficient if an employee has to manually enter the same types of information every time. I developed automation that helped generate tickets automatically.

That assignment helped me understand that cybersecurity automation does not have to involve only highly advanced security operations. Improving a routine process can provide significant value. Saving a few minutes on a task may seem small, but when the process is repeated many times by multiple employees, those savings become meaningful.

I was also exposed to Microsoft Endpoint Configuration Manager, or MECM. MECM helped me understand how large organizations centrally manage systems rather than treating every

computer as an independent device. I learned more about software deployment, configuration, administration, and enterprise endpoint management.

Another technology I became familiar with was DCMS and related system-management processes. Working with several management and cybersecurity tools allowed me to see how different parts of enterprise cybersecurity connect. Endpoint management, vulnerability remediation, security policies, configuration management, ticketing, monitoring, and automation are not completely separate areas. They frequently interact with one another.

During the internship, I was also exposed to tools and concepts involving endpoint protection, vulnerability scanning, monitoring, data-loss prevention, policies, and system administration. My goal was not simply to memorize what each acronym meant. Instead, I gradually tried to understand the purpose each technology served within the environment.

I also spent time learning Linux and Red Hat-related administration. Commands and concepts involving RPM, DNF, packages, files, permissions, and configuration became more meaningful because I was using them as part of actual technical tasks rather than simply practicing commands for an assignment.

One particularly interesting part of my internship was the use of artificial intelligence to assist with automation and development. I used Claude AI as one resource while developing and improving automation. This showed me how AI can support cybersecurity professionals by helping them understand code, troubleshoot issues, generate ideas, and work more efficiently.

However, the experience also taught me that AI-generated information cannot simply be accepted without review. In cybersecurity, an incorrect configuration or command could create

problems. Anything produced with AI assistance still requires technical understanding, testing, and validation by the person using it.

Near the end of the internship, I prepared to present the work I had completed during the summer to leadership, including an opportunity to present in Reston. Preparing for this presentation required me to think differently about my projects. Instead of focusing only on whether the technology worked, I had to explain the problem, what I created, why it was useful, what I learned, and how the work benefited the organization.

This reinforced the idea that technical professionals must be able to communicate the value of their work.

4. Use of Cybersecurity Skills and Knowledge

Before beginning my internship, I already had a foundation in cybersecurity from my studies at Old Dominion University and from studying for industry certifications. I understood concepts including the confidentiality, integrity, and availability triad, authentication and authorization, access control, networking, security policies, vulnerabilities, endpoint security, operating systems, and general cybersecurity principles.

I also understood the theoretical importance of system hardening. Before the internship, I knew that unnecessary services should be disabled, configurations should follow security standards, software should remain updated, and organizations should minimize attack surfaces.

The internship changed my understanding by showing me how these principles are implemented on a larger scale.

For example, it is easy to say that an organization should securely configure every computer. The challenge is determining how an organization can efficiently configure and verify hundreds or thousands of systems while maintaining consistency and minimizing disruption. This is where technologies such as centralized configuration management, STIGs, automation, endpoint tools, and vulnerability scanners become important.

My work with STIG remediation strengthened my understanding of security hardening. Instead of thinking of system hardening as a general recommendation, I began understanding it as a structured process involving specific controls, technical settings, validation, documentation, and remediation.

Automation was probably the technical area in which I experienced the most growth. Before my internship, I understood programming and scripting concepts, but I had limited experience applying automation to an enterprise cybersecurity workflow.

Learning Ansible helped connect programming logic to system administration and cybersecurity. A playbook could define desired system states and execute tasks across systems consistently. This introduced me to the idea of infrastructure and security configuration being managed through reusable code rather than only through manual administration.

My experience also improved my troubleshooting skills. When automation does not work, simply knowing cybersecurity terminology is not enough. I had to examine errors, understand what a command was attempting to accomplish, review syntax, identify dependencies, research unfamiliar behavior, make changes, and test again.

That process taught me that troubleshooting is one of the most important skills a cybersecurity professional can develop.

I also gained experience thinking about cybersecurity from an operational perspective.

Cybersecurity decisions exist within a larger mission. A security control must protect systems, but systems must also remain functional for authorized users. Security professionals therefore have to consider both protection and availability.

My understanding of cybersecurity became much broader during the internship. I entered with the idea that cybersecurity was primarily about protecting networks, detecting threats, preventing attacks, and securing systems. Those areas are important, but I now understand more clearly that enterprise cybersecurity also depends on automation, configuration management, asset management, documentation, ticketing, policies, communication, testing, administration, and continuous improvement.

5. Connection to the ODU Curriculum

My coursework at Old Dominion University provided an important foundation for my internship, although the internship also introduced technologies and situations that are difficult to recreate completely inside a classroom.

The biggest benefit of my ODU education was that I already understood cybersecurity terminology and fundamental principles. Concepts involving networking, operating systems, vulnerabilities, authentication, access controls, security policies, and cybersecurity risk were familiar to me.

Programming coursework was also valuable. Even when I was not writing the same programming language I had used in a class, programming courses taught me how to think logically. Programming teaches students to divide a larger problem into smaller steps, understand conditions, identify errors, and develop structured solutions.

Those skills transferred directly to automation.

Courses involving Linux and command-line environments were also helpful. Working with Red Hat systems became easier because I already understood basic operating-system concepts, directories, permissions, packages, processes, and command-line operations.

The internship reinforced many cybersecurity principles I had learned in school. One example was least privilege. In the classroom, least privilege may appear as a definition on an exam. In a professional environment, access has to be controlled because users should only have the permissions required to complete their responsibilities.

Another connection involved defense in depth. During the internship, I encountered many different technologies that contributed to security. Endpoint protection, vulnerability management, configuration standards, monitoring, access control, policies, and automation all contribute different layers of protection.

At the same time, the internship revealed areas where classroom education cannot completely prepare a student for the workplace.

The scale of enterprise environments was one major difference. A classroom environment may contain a few virtual machines. A major organization may be responsible for enormous numbers of endpoints, users, applications, services, and dependencies. A change that would be simple on

one computer can become a significant project when it must be performed consistently throughout an enterprise environment.

I was also introduced to technologies that I had not previously used extensively in school, including MECM, Ansible Automation Platform, HPSM-related processes, enterprise endpoint tools, and specific government cybersecurity procedures.

Another difference was documentation. In school, the goal is usually to demonstrate that an assignment works and submit it to an instructor. In a professional environment, documentation may need to allow another employee to understand what was changed, why it was changed, who approved it, and what happened afterward.

The internship therefore did not demonstrate that the ODU curriculum was inadequate. Instead, it demonstrated the difference between education and experience. ODU gave me the foundation needed to understand the environment. The internship gave me the opportunity to apply that foundation to real systems and processes.

6. Internship Learning Outcomes and Objectives

The first major objective I established was to learn how cybersecurity professionals manage and operate endpoint security tools.

I believe the internship successfully fulfilled this objective. Through my exposure to MECM and other endpoint-related technologies, I gained a better understanding of centralized system management. I learned that endpoint security requires coordination between configuration, software, security policies, monitoring, updates, and user requirements.

My second objective was to understand cybersecurity operations while supporting the U.S. Navy.

This objective was also fulfilled. I gained experience in an environment where cybersecurity requirements were connected to an important mission. I saw the emphasis placed on procedures, documentation, configuration requirements, security standards, and accountability.

I also learned that government cybersecurity environments have requirements that may be more structured than environments students experience in school. Changes cannot simply be implemented because someone thinks they are a good idea. Work must align with security requirements, operational requirements, organizational policies, and established procedures.

My third major objective was learning cybersecurity automation.

This was probably the objective that was fulfilled most strongly. At the beginning of the summer, automation was an area I wanted to understand. By the end, I had worked with Ansible Automation Platform, developed automation playbooks, worked on STIG remediation automation, and automated elements of ticket creation.

The progression was important to me because I could clearly measure my improvement. I went from learning terminology and asking questions about how the technologies worked to being able to complete an automation project.

Another objective was improving my understanding of daily cybersecurity work. Before the internship, my perception of a cybersecurity job came primarily from coursework, certifications, research, and job descriptions.

After several hundred hours in the internship, I developed a much more realistic picture.

Cybersecurity professionals spend time researching issues, testing solutions, attending meetings, communicating with other teams, reviewing requirements, writing documentation, troubleshooting errors, developing automation, and continuously learning new technologies.

My final personal objective was professional development. I wanted to become more confident working in a professional environment.

The internship fulfilled this objective in ways I did not initially expect. Being trusted with projects increased my confidence. Presenting my work required me to explain technical concepts clearly. Working with professionals also helped me understand workplace expectations regarding communication, responsibility, time management, and professionalism.

Perhaps the strongest indication that I had grown professionally was being invited to continue working part-time while attending school. That opportunity made me feel that my contributions during the internship had value beyond simply completing required internship hours.

7. Most Motivating and Exciting Aspects of the Internship

The most motivating part of the internship was completing work that could provide actual value to the organization.

In a classroom, an assignment usually exists primarily to demonstrate that a student understands a concept. Once the assignment is graded, it may never be used again. During my internship, I could work on automation and processes that addressed actual problems.

Automation was especially motivating for me because the results were easy to understand. If a process previously required repetitive manual effort and I could find a way to automate portions of it, I could see the value immediately.

Completing my automation playbook was one of my favorite accomplishments. There were times when I had to troubleshoot problems, research unfamiliar concepts, and make corrections, but completing it demonstrated how much progress I had made.

Another motivating aspect was receiving positive feedback from managers and team members. Knowing that experienced professionals considered my work useful increased my confidence.

Preparing to present my work to leadership was also exciting. Being given an opportunity to demonstrate what I had accomplished made me feel that the internship was not simply a requirement for college credit. I was contributing to a professional team.

Finally, being invited to return and work part-time during the school year was extremely motivating. It showed me that the effort I put into learning, asking questions, completing projects, and helping the team had been noticed.

8. Most Discouraging Aspects of the Internship

Although the internship was an extremely positive experience, there were also discouraging moments.

The biggest discouraging factor was the learning curve. During the first few weeks, there were many technologies, acronyms, procedures, and systems that I did not understand.

In school, students usually focus on a limited number of topics during each course. In the workplace, many technologies exist simultaneously. One conversation could involve endpoint security, another configuration management, another ticketing, and another automation.

At first, this could make me feel behind compared with employees who had worked with the systems for years.

However, I eventually realized that no one enters the cybersecurity field knowing every technology. Even experienced cybersecurity professionals constantly encounter new systems and problems.

Another discouraging experience occurred when automation or technical solutions did not work as expected. It can be frustrating to spend a significant amount of time troubleshooting something that appears like it should be simple.

These experiences ultimately became valuable lessons. They taught me to be patient, review errors carefully, research problems, ask questions when appropriate, and continue testing.

Some restrictions within the environment could also occasionally make tasks take longer than expected. However, I learned that these restrictions exist for legitimate security and operational reasons. A highly controlled environment is supposed to require careful processes.

9. Most Challenging Aspects of the Internship

The most challenging aspect of my internship was adapting from academic cybersecurity to enterprise cybersecurity.

The technical environment was significantly larger and more complicated than the systems I had worked with before. I had to learn not only individual technologies but also how they interacted.

Automation was another major challenge. Writing a playbook requires more than understanding what result is desired. I needed to understand the systems being modified, the commands or modules required, the correct syntax, dependencies, possible errors, and how the result should be validated.

Troubleshooting automation sometimes required repeated attempts. An error might be caused by incorrect syntax, a missing package, permissions, a variable, a dependency, or a difference between environments. Learning how to identify the actual source of a failure was difficult but extremely valuable.

Communication also became a challenge in a positive way. As my responsibilities increased, I had to become better at explaining my work.

It is one thing to understand a project personally. It is another to explain it to an experienced engineer, manager, or executive. Preparing to present my work forced me to identify the most important information and explain technical subjects without unnecessary complexity.

Time management was another challenge. I was learning new technologies while also completing assignments and projects. Sometimes I had to decide whether I should continue researching independently or ask another employee for assistance.

Over time, I learned that a good cybersecurity professional must balance independence with collaboration. Attempting to solve problems independently is valuable, but spending hours stuck on something that a team member could explain in a few minutes is not always efficient.

10. Recommendations for Future Interns

My first recommendation for future cybersecurity interns is to become comfortable with Linux before beginning the internship. They do not need to be Linux experts, but understanding navigation, files, permissions, package management, processes, and common terminal commands would make the transition easier.

My second recommendation is to learn basic scripting or programming. Python would be useful, but the most important skill is understanding programming logic. Variables, loops, conditions, functions, input and output, and debugging are valuable skills even when working with automation tools rather than traditional applications.

I would also recommend learning the basics of Ansible. A student who understands inventories, playbooks, YAML syntax, modules, variables, and automation concepts would have an advantage.

Future interns should also review networking fundamentals. They should understand IP addresses, DNS, ports, protocols, firewalls, servers, clients, and common network-security concepts.

Understanding basic cybersecurity frameworks and system-hardening principles would also help. Students should know why organizations patch vulnerabilities, apply secure configurations, restrict privileges, monitor systems, and document changes.

My most important nontechnical recommendation is to ask questions.

There were many times during my internship when I encountered unfamiliar acronyms or tools. Future interns should not pretend to understand something they do not know. It is better to write down the term, research it, and ask an informed question.

At the same time, interns should attempt to solve problems independently before immediately asking someone else. A good approach is to research the issue, try reasonable solutions, document what happened, and then ask for assistance while explaining what has already been attempted.

I also recommend keeping detailed notes. There may be dozens of new tools, commands, systems, and acronyms introduced during the first few weeks. Remembering everything without notes is extremely difficult.

Interns should also document their accomplishments throughout the summer. By the time they need to prepare a final report, resume update, or presentation, they may forget smaller projects completed several months earlier.

Professional communication is equally important. Interns should arrive on time, respond to messages, participate in meetings, provide updates, and communicate when they encounter obstacles.

Finally, future interns should be willing to accept challenging assignments. Some of the projects that initially seemed the most difficult became the experiences from which I learned the most.

An internship is one of the safest times in a person's career to encounter technologies they do not understand because they are surrounded by professionals who expect them to be learning.

11. Conclusion

My Summer 2026 internship with Leidos significantly changed my understanding of cybersecurity and my expectations for my future career.

At the beginning of the internship, my primary objective was to gain technical experience. I wanted to see how cybersecurity worked outside the classroom, learn enterprise tools, and strengthen my resume.

I accomplished those goals, but the experience gave me considerably more.

My main takeaway is that cybersecurity is a field in which continuous learning is necessary. No college course or certification can teach every system an employee will encounter. Technology changes too quickly, and organizations use different combinations of technologies.

The most valuable skill is therefore the ability to learn.

The internship strengthened my technical abilities in areas such as automation, endpoint management, Linux administration, system hardening, STIG remediation, configuration management, and enterprise cybersecurity processes. It also strengthened skills that are harder to measure, including troubleshooting, communication, teamwork, documentation, adaptability, and professional confidence.

One of the biggest changes in my perspective involved automation. Before this internship, I viewed automation as an additional technical skill. After working with automation in a professional environment, I now view it as an important part of the future of cybersecurity.

Cybersecurity teams are responsible for increasingly large environments and enormous amounts of information. It is unrealistic to expect every repetitive task to continue being completed manually. Professionals who understand cybersecurity while also knowing how to automate tasks can potentially make organizations more efficient and consistent.

My internship has therefore influenced what I want to study during the remainder of my time at Old Dominion University. I plan to continue strengthening my Linux, networking, programming, cloud, automation, and cybersecurity knowledge.

Instead of studying concepts simply because they may appear on an exam, I now have examples of how those concepts are used professionally. When I learn about access control, system hardening, vulnerability management, automation, networking, or operating systems, I can connect those subjects to situations I experienced during my internship.

The internship also increased my interest in pursuing additional industry certifications and technical projects. Certifications can help verify knowledge, while projects demonstrate the ability to apply that knowledge.

Professionally, this internship confirmed that cybersecurity is a career field I want to continue pursuing.

Working in an environment supporting the United States Navy gave additional meaning to the technical work. Cybersecurity was not simply about protecting theoretical systems in a laboratory. The technologies and procedures I worked around supported a larger mission.

I also discovered that I enjoy automation and solving problems that improve existing technical processes. In the future, I would like to continue developing skills that combine cybersecurity, system administration, cloud technology, artificial intelligence, and automation.

Another major takeaway was the importance of taking initiative. Some of the best opportunities I received during my internship happened because I showed interest in learning more, attempted difficult tasks, and continued improving my work.

Being invited to present the work I had completed and being offered an opportunity to continue working part-time during the school year were especially meaningful outcomes of my internship. They demonstrated that an internship can become more than a temporary summer position when an intern treats the opportunity seriously.

When I began the internship, I was a cybersecurity student attempting to understand what working in the industry would actually be like. By the end of the experience, I felt significantly more comfortable operating in a professional technical environment.

I still have a great deal to learn, but that is another lesson this internship taught me.

Cybersecurity professionals never reach a point where there is nothing new to learn.

Overall, my internship with Leidos was one of the most valuable parts of my education at Old Dominion University. It allowed me to apply classroom knowledge, gain experience with professional cybersecurity technologies, improve my communication skills, understand enterprise operations, and determine areas in which I want to continue developing.

The experience has given me greater confidence entering the remainder of my college career and eventually beginning my full-time cybersecurity career.

I entered the internship wanting professional experience.

I finished it with professional experience, new technical skills, stronger career goals, greater confidence, and a much clearer understanding of what it means to work as a cybersecurity professional.

Works Cited

Leidos. "Company." *Leidos*, 2026.

Leidos. "Who We Are." *Leidos*, 2026.

Leidos. "Leidos Delivers Strong Q4 Results to Cap an Outstanding 2025." *Leidos*, 17 February 2026.

Leidos. "About Us." *Leidos Careers*, 2026.

Leidos Holdings, Inc. Company filings and corporate information, 2025–2026.