

Mohammad Saleh

Course: Cybersecurity Internship

Term: Summer 2026

Instructor Name: Professor Duvall

TA Name: Jade Hines

Company/Organization Name: Leidos

Date: July 27, 2026

During this stage of my internship, I continued to expand my technical knowledge while also becoming more confident in my ability to contribute to a professional cybersecurity and information technology environment. This period was especially meaningful because I learned how to develop a standard operating procedure, improved my ability to use Ansible Automation Platform, and received opportunities that demonstrated how much I have grown throughout the summer.

One of the main tasks I completed was developing a standard operating procedure, or SOP, for securely burning information onto a disk. Creating the SOP required me to carefully document each step of the process so that another employee could follow the instructions correctly and consistently. I had to make sure the procedure was organized, easy to understand, and aligned with the security requirements of the work environment. This experience showed me that technical knowledge alone is not enough. Cybersecurity professionals must also be able to clearly communicate procedures, especially when those procedures involve sensitive information, removable media, and organizational security policies.

Writing the SOP helped me better understand the importance of documentation in the workplace. A well-written SOP reduces confusion, prevents mistakes, and ensures that tasks are completed according to the same standards each time. It also provides employees with a reliable reference when they need to perform a task they may not complete regularly. This assignment improved my technical-writing skills and taught me to consider the perspective of the person who will eventually use the document.

I also spent a significant amount of time improving my skills with Ansible Automation Platform, commonly referred to as AAP. Earlier in my internship, I was introduced to automation and learned how it could be used to support cybersecurity tasks. During this period, I became much more comfortable using the platform and understanding how its different components work together. I learned how to use AAP to automate multiple repetitive tasks within the work environment instead of completing each task manually.

Working with Ansible helped me recognize the major benefits of automation. Manual processes can take a large amount of time and may lead to inconsistent results or human error. Automation allows the same process to be performed efficiently and consistently across multiple systems. It also gives employees more time to focus on complex responsibilities that require analysis and decision-making. As I practiced creating and managing automated workflows, I developed a better understanding of how organizations can use automation to improve productivity, strengthen security, and standardize their operations.

This experience also connected directly to what I have learned in my cybersecurity and computer science courses. Programming teaches students how to break a large

problem into smaller steps, while cybersecurity emphasizes consistency, access control, documentation, and risk reduction. Using Ansible required me to apply these ideas in a real workplace environment. I had to understand the goal of a task, determine how it could be automated, test the process, and make sure the results were accurate. I am no longer only learning about automation as a concept. I am now gaining practical experience using it to solve real organizational problems.

One of the most exciting developments was being invited to Reston to present my summer work to a vice president at Leidos and other members of the organization. This opportunity means a great deal to me because it shows that the work I completed during my internship was noticed and valued. Presenting to senior leadership will allow me to demonstrate the projects I worked on, explain how I used automation, and show the progress I made throughout the summer. It will also help me improve my public-speaking and professional-communication skills.

Preparing for this presentation has encouraged me to reflect on everything I accomplished during the internship. At the beginning of the experience, I was still learning about the environment, the tools, and the different responsibilities of the team. Over time, I became more involved in technical assignments, including automation, STIG remediation, system patching, documentation, and other cybersecurity processes. Being selected to present this work has increased my confidence and motivated me to continue developing my skills.

Another major accomplishment was receiving an invitation to return and work part time while I attend school. I am extremely excited and grateful for this opportunity. Being

invited back demonstrates that my supervisors recognized my effort, willingness to learn, and ability to contribute to the team. It will allow me to continue gaining real-world experience while completing my cybersecurity degree. I will also be able to keep improving my skills with automation, cybersecurity tools, system administration, and professional collaboration.

Overall, this period of my internship was one of the most rewarding so far. I improved my ability to create professional documentation, became more experienced with Ansible Automation Platform, and learned how automation can support multiple tasks within a secure workplace. The invitation to present my work in Reston and the opportunity to return part time have made me feel that my hard work throughout the summer has paid off. These experiences have strengthened my interest in cybersecurity and automation and have made me more confident about pursuing a long-term career in the field.