

Mohammad Saleh

Course: Cybersecurity Internship

Term: Summer 2026

Instructor Name: Professor Duvall

TA Name: Jade Hines

Company/Organization Name: Leidos

Reflection #2

During my second 50 hours at my internship with Leidos, I have been able to move beyond only observing and have started becoming more involved in actual tasks and projects. Compared to my first reflection period, I feel like I have gained more confidence in understanding the environment, asking questions, and applying what I am learning. The first 50 hours were mostly about taking in information, learning the tools, and understanding how the team operates. During this second 50 hours, I have started to connect those observations to real work, especially through automation, system support, and ticketing processes.

One of the biggest areas of growth for me during this period has been learning more about automation tools and how they are used to complete cybersecurity and IT tasks more efficiently. I started using automation tools to work on tasks and better understand how repetitive processes can be improved. This was important because I was able to see how automation is not just a technical skill, but also a way to save time, reduce errors, and support the team's overall mission. In cybersecurity and systems administration, many tasks require accuracy and consistency, so automation can make a major difference in how work gets completed.

A major accomplishment for me during this reflection period was creating an automation tool that automatically makes tickets in HPSM. This was one of the first times during the internship where I felt like I was not only learning, but also contributing something useful. The tool helped

connect automation with the ticketing process, which is important because ticketing systems are how many issues, requests, and tasks are documented and tracked. Being able to create something that supported that process made me feel proud of my progress. It also impressed some of my managers, which encouraged me and showed me that the hard work I have been putting in is being noticed.

I also learned more about systems and tools such as DCMS and MECM. Learning about these tools helped me better understand how organizations manage devices, allow users to access systems, and support operations across a larger environment. MECM especially showed me how important centralized management is when working with many systems. Instead of handling every device separately, tools like MECM help teams manage software, updates, configurations, and system information more efficiently. This connects closely to endpoint management, which has been one of the main themes of my internship so far.

During this second 50 hours, I also helped with work related to allowing people to use systems. This helped me see that cybersecurity is not only about blocking threats or securing machines. It is also about making sure the right people have the right access to the right systems. Access and system availability are important because employees need to be able to do their jobs, but that access still has to be managed carefully and securely. This gave me a better understanding of the balance between security and usability. A system can be very secure, but if users cannot access what they need, operations can slow down. At the same time, access cannot be given without proper control and documentation.

The work I am performing relates strongly to the curriculum I have studied in cybersecurity. In my classes, I have learned about security principles such as confidentiality, integrity, and availability, as well as concepts like access control, endpoint security, system administration, and risk management. During the internship, I am seeing how those concepts apply in a real

workplace. For example, when learning about endpoint tools, MECM, and system access, I can connect that to what I have studied about securing devices and managing users. When working with automation and ticketing, I can connect that to operational processes, documentation, and incident or request management. This experience is helping me understand that the topics I learn in class are not just theory. They are used every day in real cybersecurity environments.

I do see this as a field I can grow in. Cybersecurity is a field where there is always something new to learn, and I have already seen that during my internship. Even people who have worked in the field for many years still continue learning new tools, systems, and processes. That motivates me because it shows that growth in this field does not stop after earning a degree or getting a job. There are many directions I can take, including endpoint security, automation, systems administration, compliance, and cyber operations. This internship has helped me see that I enjoy learning how systems work and how cybersecurity tools support a larger mission.

Professionally, I believe I bring several important attributes to my role. I bring curiosity, because I am always trying to understand why a tool or process is used, not just what it does. I also bring a strong work ethic, because I have been working hard to absorb new information and contribute whenever I can. Another attribute I bring is adaptability. During the internship, I have had to learn many new terms, tools, and processes in a short amount of time, and I have had to adjust quickly. I also try to bring a positive attitude and willingness to ask questions, which helps me learn from the people around me.

I find the work rewarding and meaningful because I can see that it supports real operations and helps people do their jobs more effectively. Creating the automation tool for HPSM was especially rewarding because it gave me a chance to solve a real problem and create something useful. It felt meaningful because I was not just completing a practice assignment or classroom lab. I was working on something connected to an actual workplace process. Knowing

that my work can help save time, improve organization, or support the team makes me more motivated to keep improving.

A challenge I faced during this second 50 hours was trying to keep up with the amount of new information while also starting to perform more hands-on tasks. Since I am still learning, there are moments where I have to slow down and make sure I fully understand what I am doing. I have learned that it is better to ask questions and do the task correctly than to rush and make mistakes. This has helped me become more careful and more confident. I am learning that in cybersecurity, attention to detail is extremely important because small mistakes can affect systems, users, or processes.

Overall, my second 50 hours at Leidos have shown real growth from my first reflection. I have gone from mostly observing tools and meetings to starting to use automation, learning about DCMS and MECM, helping with system access, and creating a tool that automatically makes tickets in HPSM. I feel that I am making strong progress toward my learning objectives, especially in understanding endpoint tools, cyber operations, and day-to-day tasks. This experience has also helped me see how my cybersecurity curriculum connects to real work. Moving forward, I want to continue improving my technical skills, learn more about automation and endpoint management, and keep finding ways to contribute to the team in a meaningful way.