

Mohammad Saleh

Course: Cybersecurity Internship

Term: Summer 2026

Instructor Name: Professor Duvall

TA Name: Jade Hines

Company/Organization Name: Leidos

Reflection #4

Internship Reflection

During the most recent part of my internship, I continued learning more about how cybersecurity and information technology are used in a real work environment. One of the main things I continued doing was using Claude AI to help complete different tasks. Earlier in my internship, I started learning how artificial intelligence could help automate certain processes, and during these hours I became more comfortable using it as a tool. I used Claude to help me understand technical information, organize ideas, improve scripts, and think through different problems related to the work environment.

Using Claude has shown me that artificial intelligence can be very useful when it is used correctly. It can help save time, explain complicated information, and assist with repetitive tasks. However, I am also learning that AI is not something that should be trusted without checking its work. I still have to review the information, make sure it is correct, and follow the security requirements of the organization. This experience has helped me understand that AI should be used as an assistant instead of something that completely replaces human decision-making.

I have also been learning about AI beyond just using it to complete tasks. Through my internship, I am seeing how AI is being used in real organizations and how it is affecting

employees, cybersecurity teams, businesses, and everyday work. AI can improve productivity and help people complete work faster, but it can also create new security risks. Cybersecurity professionals have to think about how attackers may use AI, how sensitive information is protected, and how employees use AI tools inside a secure work environment.

Learning about these issues has made me more interested in the connection between cybersecurity and artificial intelligence. Before this internship, most of my knowledge about AI came from school, online tools, and personal projects. Now I am seeing how it is used in an actual professional environment. I am learning that organizations have to create rules and policies for AI use because employees may accidentally enter sensitive information into an AI system or depend on incorrect results. This has helped me understand why cybersecurity professionals must be involved when organizations introduce new technology.

Another major task I completed was patching multiple SQL servers. I was first taught the correct process by members of my team. They showed me how to remotely connect to the servers using Remote Desktop Connection, also known as RDC. I learned how to identify the correct server, log in securely, review the system, and complete the required patching steps. I also learned the importance of following instructions carefully because servers can support important systems and applications.

After I was shown the process, I was able to patch several SQL servers. This gave me more hands-on experience with server administration and system maintenance. Patching is important because updates can fix security vulnerabilities, improve stability, and protect systems from attacks. Even though patching may seem like a basic task, I learned that it requires attention to detail. A mistake could cause a system to stop working correctly or affect users who depend on the server.

This task also helped me understand the importance of preparation and documentation. Before making changes to a server, I had to make sure I was working on the correct system and following the approved process. After completing the work, it was important to confirm that the server was still operating correctly. Being trusted to work on several servers helped increase my confidence and showed me that I am becoming more capable of completing technical tasks in a professional environment.

I also continued working with DCM exceptions. These exceptions are needed when users require approval to connect devices such as disks, external hard drives, or other removable storage devices to their computers. Because removable media can create security risks, users cannot always connect these devices without permission. I helped with the process of allowing approved users to use these devices when there was a valid business need.

Working with DCM exceptions taught me more about access control and security policies. The purpose of the process is not to make work difficult for users. It is meant to protect the organization from malware, unauthorized data transfers, and other security threats. At the same time, employees may need removable media to complete their jobs, so cybersecurity teams must balance security with business needs. This showed me that cybersecurity often involves reviewing requests, following policies, and making sure access is only provided when it is necessary and approved.

Throughout these internship hours, I continued improving my technical and professional skills. I am becoming more comfortable asking questions, following procedures, communicating with team members, and completing tasks independently. I have also learned that working in cybersecurity involves much more than using security tools. It includes maintaining systems, supporting users, documenting work, reviewing approvals, solving problems, and understanding how new technologies affect the organization.

Overall, this part of my internship was another valuable learning experience. I continued building my knowledge of artificial intelligence while also gaining practical experience with servers and security exceptions. I feel that I am becoming more confident and more prepared for a future career in cybersecurity. I still have a lot to learn, but each task gives me a better understanding of how a real cybersecurity environment operates. This internship has helped me improve my technical skills, understand professional expectations, and see the importance of continuing to learn as technology changes.