

Mohammad Saleh

Course: Cybersecurity Internship

Term: Summer 2026

Instructor Name: Professor Duvall

TA Name: Jade Hines

Company/Organization Name: Leidos

Reflection #1

During my first 50 hours at my internship with Leidos, I have been introduced to a professional cybersecurity environment that has already taught me a lot about how day-to-day cyber operations work in a real organization. Coming into the internship, I knew that I would be learning about cybersecurity tools, endpoint operations, and how teams support larger missions, but actually being inside the building and observing the work has helped me understand how much coordination, communication, and continuous learning is involved.

One of the biggest things I have observed so far is the number of different tools and systems that are used in the Leidos environment. I have been exposed to tools and technologies such as SEP, SDCS, RHEL, and other cybersecurity endpoint tools. At first, hearing all of these terms and seeing how many systems are involved felt overwhelming. There is a lot of information to take in, especially because each tool has its own purpose, process, and role in supporting cybersecurity operations. However, I have started to understand that these tools are not separate pieces working alone. They are part of a larger system that helps protect, monitor, and manage endpoints and the organization's cyber environment.

This connects directly to one of my learning objectives, which is learning how to manage and operate endpoint tools. So far, I have mostly been observing and asking questions, but even that has helped me build a stronger foundation. I have learned that endpoint security is not just about installing software or checking alerts. It involves understanding how tools interact, how policies are applied, how systems are monitored, and how issues are identified and handled. Seeing professionals use these tools in real time has helped me understand how important accuracy and attention to detail are in cybersecurity work.

Another major part of my first 50 hours has been learning how the daily operations work when employees come into the building. I have observed how people get started for the day, how they check their systems, how they communicate with each other, and how they organize their tasks. This has helped me understand that cybersecurity is not only technical, but also very structured. The work depends on routines, procedures, teamwork, and making sure everyone understands what needs to be done. Watching this process has helped me see what a normal day in a cyber environment looks like, which supports my learning objective of understanding day-to-day cyber tasks.

I have also observed the daily stand-up meetings, where the team discusses company goals, current tasks, and what different workers are focusing on. These meetings have shown me how important communication is in a cybersecurity workplace. Even when people are working on different tools or different parts of a project, everyone still needs to understand the bigger picture. The stand-up meetings help the team stay aligned, share updates, and identify any problems or blockers. I noticed that these meetings are not just about reporting what someone did. They are also about making sure the whole team understands priorities and can support each other when needed.

One thing that stood out to me during these first 50 hours is how much information I have had to absorb. Every day, I am learning something new, whether it is a new acronym, a new tool, a new process, or a new way of thinking about cybersecurity operations. At times, it has felt like a lot, especially because many of the tools and procedures are new to me. However, I have also realized that feeling this way is part of the learning process. I am still early in my internship, so I do not expect to understand everything immediately. Instead, I am trying to stay patient, take notes, ask questions, and connect what I am seeing to what I have learned in school.

Something that encouraged me was hearing from people who have worked there for over 20 years that they still learn new things every day. That showed me that cybersecurity is a field where learning never really stops. Even experienced professionals continue to adapt because tools, threats, systems, and procedures are always changing. This made me feel more comfortable with not knowing everything yet. It also reminded me that one of the most important skills in cybersecurity is being willing to keep learning.

A challenge I have faced so far is trying to understand all of the terminology and how each tool fits into the larger mission. Since there are many acronyms and technical systems, it can be difficult to remember everything at once. To handle this challenge, I have been trying to write down new terms and ask for clarification when I need it. I am also trying to review what I learn after each day so that the information becomes more familiar. I know that if I keep doing this consistently, the tools and processes will start to make more sense over time.

This internship has also helped me better understand what it means to support the United States Navy through cybersecurity work. Even though I am still learning, I can see that the work being done has a larger purpose. The tools, meetings, procedures, and daily tasks all connect to

protecting systems and helping operations run smoothly. This has made the internship feel meaningful because I can see that cybersecurity work has real responsibilities attached to it.

Overall, my first 50 hours at Leidos have been a valuable introduction to the professional cybersecurity field. I have observed endpoint tools, learned about daily operations, attended stand-up meetings, and started to understand how much teamwork and communication are involved. I still have a lot to learn, but I feel that I am making progress toward my learning objectives. Moving forward, I want to continue building my understanding of the tools used in the environment, ask more questions, and become more confident in explaining the processes I observe. This first reflection period has shown me that cybersecurity is a field that requires patience, curiosity, and constant learning, and I am excited to keep growing throughout the internship.