

CYSE 368 – Reflection Paper #2

Sotiris Economos

Old Dominion University

CYSE 368: Internship in Cybersecurity

Internship Organization: Captivize LLC

Reflection #2

Date: March 2026

After completing one hundred hours of my internship with Captivize LLC, I have gained a much clearer understanding of how AI-driven automation systems are built, maintained, and improved in a real-world business environment. While my first fifty hours focused mainly on learning the company's systems and observing workflows, the second fifty hours allowed me to take a more active role in troubleshooting issues, improving automation processes, and contributing to technical discussions about system performance and reliability.

One of the primary areas I worked on during this period was analyzing automation workflows that support client operations. These workflows are designed to automate repetitive tasks and allow the system to process large amounts of information without manual intervention. As I became more familiar with these systems, I began assisting in reviewing how these workflows were structured and identifying areas where improvements could be made. In several cases, I helped trace how data moved through the automation pipeline in order to identify where errors or delays were occurring. This required carefully reviewing configuration settings, observing system behavior, and comparing expected outputs with actual results.

During this process, I encountered situations where workflows were failing due to small configuration errors or unexpected input data. When this occurred, I assisted in troubleshooting the issue by reviewing system logs and retracing the steps that the automation system followed during execution. This helped me understand how important logging and monitoring systems are when diagnosing technical problems. Rather than immediately changing the system, we focused on identifying the root cause of the issue and testing potential fixes in a controlled way before implementing them. This experience reinforced the importance of careful troubleshooting and change management, which are critical practices in both system administration and cybersecurity.

Another responsibility I became more involved in was evaluating potential improvements to existing automation processes. As the company continues to expand its AI-driven tools, small adjustments can significantly impact overall performance and reliability. During team discussions, we often evaluated whether proposed changes would improve efficiency without introducing new technical risks. For example, some automation tasks could be executed faster by reducing validation steps, but removing these safeguards could also increase the chance of incorrect outputs or data processing errors. Being part of these discussions helped me better understand how technical decisions must balance performance with reliability and security considerations.

Throughout the second half of my internship hours so far, I also gained additional experience documenting system behaviors and troubleshooting procedures. When issues were identified and resolved, I helped record the steps taken to diagnose and correct the problem. This documentation allows future issues to be resolved more efficiently and helps maintain consistency across the team. From a cybersecurity perspective, documentation also helps reduce the risk of misconfigurations and ensures that system knowledge is not dependent on a single individual.

Working in this environment has also helped me improve my ability to communicate technical information clearly. Because the team includes individuals with different technical backgrounds, it is important to explain problems and solutions in a way that is easy for others to understand. When discussing troubleshooting results or proposed workflow adjustments, I practiced summarizing technical findings and explaining how certain changes might affect system behavior. Developing this skill is important because cybersecurity professionals often need to communicate risks and technical concepts to both technical and non-technical audiences.

One of the most important lessons I have learned during this portion of my internship is how closely cybersecurity principles are connected to system reliability and automation design. Many cybersecurity risks arise not from direct attacks, but from system misconfigurations, poor validation processes, or insufficient monitoring. By helping review automation workflows and troubleshooting system behavior, I was able to see how proactive system design and careful testing can prevent operational issues and reduce potential vulnerabilities.

Overall, completing one hundred hours of this internship has allowed me to gain meaningful hands-on experience with AI-driven automation systems and real-world technical problem solving. I have become more comfortable analyzing system behavior, diagnosing workflow issues, and contributing to discussions about system improvements. These experiences have strengthened both my technical skills and my understanding of how cybersecurity concepts apply in modern technology environments. As I continue progressing through my internship, I look forward to expanding my technical responsibilities and further developing the skills necessary for a career in cybersecurity.