

CYSE 368 – Reflection Paper #1

Sotiris Economos

Old Dominion University

CYSE 368: Internship in Cybersecurity

Internship Organization: Captivize LLC

Reflection #1

Date: February 7, 2026

After completing my first fifty hours of my internship, I have gained a clearer understanding of how cybersecurity principles apply in real-world business and technical environments. Going into this experience, I expected cybersecurity work to primarily involve technical security tools or defensive systems. Instead, I have learned that cybersecurity is deeply connected to system reliability, secure automation, troubleshooting, and decision-making, especially in organizations that rely heavily on technology and AI-driven workflows.

During my initial hours, much of my work involved becoming familiar with the company's existing automation processes and internal tools. I reviewed current AI-driven workflows to understand how tasks were being automated, what data was being processed, and where failures or inefficiencies occurred. This onboarding process helped me recognize how even small misconfigurations or poorly documented processes could introduce security and reliability risks. For example, I observed how automation workflows that lack proper validation or error handling could unintentionally expose sensitive data or create system failures that impact client operations.

A significant portion of my first fifty hours was spent assisting with troubleshooting technical issues related to automation and system performance. When workflows did not behave as expected, I worked to identify root causes rather than applying quick fixes. This included reviewing logs, retracing steps in automation sequences, and testing changes in a controlled manner before implementation. Through this process, I learned the importance of maintaining system integrity and avoiding changes that could introduce new vulnerabilities. This experience reinforced cybersecurity concepts such as minimizing attack surfaces, preventing misconfigurations, and ensuring systems behave predictably.

I also contributed to discussions surrounding optimization and system improvements. In several instances, I was asked to provide input on whether proposed changes would improve efficiency without compromising reliability or security. These discussions emphasized the balance between performance and risk. For example, while faster automation can improve productivity, it may also increase the likelihood of errors or reduce oversight if not properly designed. Being included in these conversations helped me understand how cybersecurity professionals must evaluate both technical benefits and potential risks before implementing solutions.

Another important area of growth during my first fifty hours was documentation and communication. I assisted in documenting troubleshooting steps and workflow behaviors so that issues could be more easily identified in the future. This documentation not only improves operational efficiency but also supports security by ensuring consistency and reducing reliance on undocumented knowledge. Additionally, working in a remote environment required me to communicate technical findings clearly to team members with varying levels of technical expertise. This experience strengthened my ability to explain risks, solutions, and technical concepts in a professional and understandable manner.

Overall, the first fifty hours of my internship have shown me how cybersecurity thinking applies beyond traditional security roles. I have learned that secure system design, careful troubleshooting, and thoughtful decision-making are essential to protecting both data and operations. This experience has helped me better understand how cybersecurity integrates with AI, automation, and business processes. As I continue my internship, I look forward to expanding my technical responsibilities while continuing to apply cybersecurity principles to real-world challenges.