

CYSE 368 – Reflection Paper #3

Sotiris Economos

Old Dominion University

CYSE 368: Internship in Cybersecurity

Internship Organization: Captivize LLC

Reflection #3

Date: April 5, 2026

After completing one hundred and fifty hours of my internship with Captivize LLC, I have developed a much better understanding of how AI-driven automation systems function in a real business setting. Earlier in my internship, I was mainly learning the company's systems and observing how workflows were built. During my final hours, I became more comfortable taking part in troubleshooting, reviewing workflow behavior, and thinking more critically about how technical decisions affect performance, reliability, and security.

One example I saw involved an automation workflow that was not producing the expected output because of a small configuration issue and unexpected input data. At first, the problem did not seem major, but after looking more closely at the workflow, it became clear that even a small mistake could affect the rest of the process. That experience showed me how important validation, logging, and careful troubleshooting are in automated systems. It also taught me that many technical problems are caused by overlooked details rather than one major system failure.

Another example involved discussions about improving workflow efficiency without removing important safeguards. In one case, reducing validation steps could have made the process faster, but it also could have increased the chance of inaccurate outputs or unnoticed errors. Seeing that tradeoff in a real work environment helped me understand that technical decisions are not only about speed. They also involve reliability, accountability, and risk. From a cybersecurity perspective, this reinforced how weak processes and poor oversight can create vulnerabilities even when no direct attack is involved.

This internship also made me think more deeply about errors in AI systems. Based on what I observed, many of those errors do not come from AI alone, but from how the systems are designed, configured, and monitored. AI is still a developing technology, so it can be

unpredictable at times, but many issues are really caused by weak validation, unclear input data, or poor workflow design. That showed me that AI can be a very powerful tool, but it still requires strong human oversight to be effective and reliable.

Professionally, I learned that one of my strengths is patience when solving problems. I prefer to understand the cause of an issue instead of rushing to a quick fix. I also strengthened my ability to adapt and communicate clearly. Because this internship involved both technical work and collaboration, I had to explain problems and solutions in a way that others could understand. That made me realize how important communication is in any cybersecurity or technical role.

This experience also helped me answer an important question about my future. I can see myself growing in this field because I enjoy work that involves problem-solving, technical analysis, and improving systems. What made this internship meaningful was seeing how even small technical decisions could affect larger operations. Overall, these one hundred and fifty hours helped me grow both technically and professionally, and they gave me a clearer understanding of how cybersecurity connects to automation, system reliability, and real-world business needs.