

Internship Reflection #2

Zachary Six

Old Dominion University

CYSE 368

Professor Duvall

July 7th, 2025

Even through the second set of 50 hours, this internship has proven to be extremely beneficial to my career as a person in the land of Cyber Security. After I got through my first couple of weeks getting to know the team and the different software used by the company, I was assigned my first task as an intern. This task was essentially to come up with an idea for a “universal filter” for our system logs. Currently the company uses a software known as Cribl for a log manager to ingest, manipulate, and output logs to wherever they were needed. This task was assigned because the end goal is to be able to automate the onboarding of new log sources as they are added to the network. This would use the famous Ansible automation tool to utilize playbooks to make the appropriate API calls to the Cribl server. I started this task by looking around the software to determine any changes that were being made to *all* logs. This helped determine the changes that need to happen first in the filter and then make log-specific changes based on the source of the log. To make sure that I have the required skillset to perform this task, I had to teach myself a programming language, the structure of JSON formatted files, and the structure of YAML formatted files. Thankfully, JSON and YAML are very similar in that they both use ‘key:value’ pairs to store values for specific variables. Learning this file format proves to be very useful when creating API calls and testing them with a software known as Postman. Learning Python was a very exciting task because I took an existing program I wrote in C++ and converted it to Python with even more features. I decided to teach myself this programming language and develop AI prompt engineering skills at the same time by utilizing my company’s CoPilot license to ask the AI questions about Python and interpret this information in a way that best suits me. In between the time I work on this task, I have been instructed to “learn something of interest in Cyber” and took off to develop deeper knowledge of my Network+ certification. I have noticed that this learning has also helped me understand the processes that make our

network work as well as it does. Alongside completing the task that has been assigned to me, I have gotten to know the world of endless meetings quite well. Every Monday and Thursday we have Security Scrum meetings to go over the team's tasks and accomplishments for the week and anything standing in the way of finishing a task. At first, I questioned the purpose of these meetings but quickly realized that the Scrum meetings help me understand all that is happening in the cyber department of Floor and Décor. Each team member from a different department has a different task, no matter how tedious or simple, and I can start to see how these different tasks fit into the every-day development that gets done by the team. Recently, in one of the cycles of endless meetings, there was a *very* interesting conversation regarding a new application being implemented into the company. This meeting taught me that nothing goes perfectly in the IT space and innovative solutions must be made on the fly. It was found that the process to implement this application would be extremely time consuming (taking about 3 months to finish) and very expensive. Several revelations about this app came to light including an incompatibility with the app in the way that we were originally planning and a whole redesign of the implementation architecture must be made to accommodate for this incompatibility. I have also had several meetings with different members of the IT team to give an overview of that particular area of the IT department and how they benefit the company. So far, I have had meetings with the "Governance, Risk, and Compliance" area, Data loss prevention, and the Incident Response team. Although these are not the areas that I would particularly like to specialize in, they definitely shed some light to the processes of the IT team. I believe that the meeting about the Incident Response Plan was potentially one of the most important meetings I had since the start of my internship. I believe this is the case because the worst possible scenario for an IT team is a data breach and a threat actor having access to our systems. Knowing what to

do when “the poop hits the real fan – my boss” makes sure that the team can effectively mitigate the issue in as little time as necessary. So far in the internship I have been able to hit all of the learning objectives with the exception of the AI incident response. This is still a topic being researched by the team to find potential use-cases of AI in our incident response plan to potentially mitigate threats even faster and more efficient.