

Reflection Journal #3

Zachary Six

Old Dominion University

CYSE 368: Cyber Security Internship

Professor Duvall

August 1st, 2025

The last set of 50 hours at Floor and Décor have been more active than the previous 50-hour segments combined. During this segment of 50-hours, I completed my task in Cribl, assigned a new task in Cribl, and given old production code written by a former intern to modify and add features. For the first initial task involving Cribl, I was told to create a universal filter for our syslog ingestion that would allow for an automation to be built for onboarding new sources of syslogs. To start this process, I began by examining the routes we had in-place already to perform any custom-handling on the log before sending to the database for storage. I found that we only had two log sources that required custom changes to be made, and the other syslogs were having one or two common changes among them. One of these common changes was adding an index to the log specifying where the log came from. To implement this as a common change, I created a pipeline that would filter anything coming off of our syslog server with the source name starting with 'syslog: ...' and continues with the name of the application. Being that all of these syslog sources were originating from the same server and containing the same pattern in their source name, I was able to come up with a custom JavaScript regex to extract the name of the application out of the source name. This was required because I didn't want all the filler material in the name and want to isolate just the name of the application. Another change I added dealt with severity levels of the syslog messages themselves. A stream of syslogs can contain a number of different *types* of syslog including 'info' and 'debug' denoted as a number for the "severity" attribute within a log. These types of syslogs generally come with quite a bit of traffic that can drown out the more important events, therefore we would like to drop them the second they are seen. This was possible through a super simple expression that filters anything with that severity level or containing the names 'info' or 'debug'. The last universal change made was a timestamp to ensure all the logs, whether they came from a west coast store or east coast store,

have the same time stamp in relation to the data center. Following these universal changes, I am able to add the few custom changes for specific log sources by adding a filter depending on the log source. This allows the pipeline to be segmented per application and easier to read and modify in the future.

Following this I was given an older Python program written by a former intern at the company that automated the process of sending an email to the managers of employees who failed the most recent phishing campaign. My task for this program was to implement a feature that would allow the user to select the number of months to analyze in a report pulled from another application. Our updated policies on phishing campaigns changed the length of time from six months to twelve months to count the failures of an employee. The dates of each campaign and failure are put into a CSV file for each employee and manually chosen by the user after running the program. I am also implementing new verbiage sent in the email to the managers to comply with our updated policies of the phishing campaigns. When attempting to test the program and analyze a sample email sent by the program, I encountered an issue when attempting to connect to the SMTP server. There can be multiple reasons for this kind of situation and different solutions to resolve this are currently being evaluated.

Overall, the last 50 hours of the internship have given me the best possible view into the processes and methods used by professionals in an IT department. I have been able to accomplish my own work, experience issues, and resolve those issues with the help of my fellow members of the IT department and Security Operations Center. I have learned valuable information I will use in the pursuit of my career as a Cyber Security professional and will use this information to benefit myself in my last semester at ODU. Learning about retail security has given me insight into the security and protection of thousands of devices and users. Talking

about finances and how the IT department shows just how this department acts like any other requiring proper funding to operate efficiently. My experience in network security have shown me real-world applications to the secure methods and protocols that govern the modern web beyond what I have been shown in the classroom. This experience combined with my determination makes me excited for my future in Cyber Security and graduating from ODU in December 2025.