Name: Romelo Gilbert
Course: CYSE 368
Term: Spring 2026
Instructor: Professor Teresa Duvall
TA: Joshua Russell
Company/Organization: Watsco Inc
Reflection #: 6

This week I was involved in a go-live phase as our team transitions from a V1 backend service to a new V2 implementation for one of our business units. During this phase, the business unit executes a series of tests across various services and endpoints to validate that responses match expected behavior. As issues were discovered during testing, I was tasked with identifying and resolving problems related to incorrectly implemented endpoints. Due to the modular design of our codebase and my familiarity with its structure, I was able to quickly locate and correct the issues. This experience reinforced the importance of having a well organized and maintainable system. As it allows for faster identification and resolution of problems during critical phases such as go-live.

In addition to resolving endpoint issues, I spent time reviewing our Datadog dashboards, focusing on our Kubernetes infrastructure and other supporting services. My goal was to better understand how the different components of our system interact and how system behavior is reflected through monitoring tools. This task helped me begin developing a broader view of the system beyond just the code I write. By observing metrics and system activity, I started to recognize how performance, errors and infrastructure level behavior can provide insight into potential issues or areas of concern.

One of the more challenging tasks I encountered this week involved troubleshooting issues within my local development environment. Initially, there were multiple factors contributing to the problem, including outdated environment variable values and expired VPN credentials. After resolving those issues, I discovered that the root cause was related to IP whitelisting. The machine running our development application needed its IP address to be added to an approved list in order to communicate with the business unit's network servers. This issue

highlighted how multiple layers of configuration (local environment setup, authentication and network access controls) must all be correctly aligned for a system to function properly.

This experience made me more aware of how configuration and network level controls can impact system accessibility and behavior. Something as simple as a missing IP whitelist entry or misconfigured routing can prevent communication between services and create significant downstream issues. It also reinforced how important it is to methodically isolate variables when troubleshooting, as multiple overlapping issues can make it difficult to quickly identify the true root cause.

Through these experiences, I am beginning to see how my work connects to conducting security audits and risk assessments. While I am not formally performing audits, I am developing the ability to evaluate system behavior, identify misconfigurations and understand how different components contribute to overall system functionality. Reviewing system dashboards, troubleshooting environment issues and resolving endpoint errors all require analyzing how systems are expected to behave versus how they are actually behaving. This aligns closely with the process of assessing system health and identifying potential risks.

Overall, this week helped me gain a deeper understanding of how systems interact across different layers, including application logic, infrastructure and network access. I am beginning to recognize that risk assessment is not limited to identifying obvious vulnerabilities, but also includes understanding how misconfigurations and access controls can affect system reliability and communication. This experience is helping me build a more analytical approach to evaluating systems and identifying areas where issues may arise.