Reflection #1

I gained hands-on experience in cybersecurity operations, incident response, and security monitoring throughout the first fifty hours of my internship as an IT security analyst intern. My main duties included installing IBM QRadar on an Ubuntu server, managing phishing alerts using PagerDuty, and looking into DMCA copyright notices by examining Palo Alto firewall logs.

Examining DMCA copyright notices was one of the most interesting assignments. I was able to find possible copyright breaches, track down the origin of traffic that was detected, and determine if the incidents were false positives or actual violations by looking at firewall logs. I now have a better understanding of how crucial the visibility of networks and enforcement of rules is to maintaining compliance. Additionally, using PagerDuty to handle phishing warnings was a crucial learning experience. I looked at URLs, examined email headers, and compared questionable activities to threat intelligence sources. This strengthened the need of prompt incident response and enabled me to create a methodical approach to detecting and blocking phishing attacks. Upgrading IBM QRadar on an Ubuntu machine was another important effort. This necessitated adhering to a planned upgrade procedure, resolving compatibility problems, and making sure the SIEM operated at its best after the upgrade. I gained more knowledge of security information and event management (SIEM) systems and improved my technical troubleshooting abilities as a result of this experience.

Overall, these first 50 hours have significantly expanded my knowledge of cybersecurity operations, strengthened my analytical and technical skills, and provided me with a real-world understanding of security monitoring and compliance. I look forward to building upon these experiences and further refining my expertise in IT security throughout the remainder of my internship.