

Noah Salafranca
Professor Duvall
CYSE 368
2/15/2025

Reflection #1

My internship with the City of Virginia Beach Department of Information Technology has given me valuable hands-on experience in cybersecurity. This opportunity has allowed me to apply my academic knowledge in a practical environment while strengthening my technical and professional skills. During my first week, I learned about the structure of the cybersecurity team. The team is split into two parts: the Security Operations Center (SOC) team, responsible for triage and incident response, and the Governance, Risk, and Compliance (GRC) team, which focuses on compliance with cybersecurity frameworks. As an intern for the SOC team, I report to Bob, the Chief Information Security Officer (CISO), and Kris, the team manager, while working under Tatum, a cybersecurity analyst. The entire team has taught me so much about investigating threats.

My main responsibilities include investigating low-level alerts, risky user sign-in attempts, and phishing and spam emails reported by city employees. I work in Microsoft Azure to investigate risky login attempts and suspicious behavior. I work in Microsoft Defender to analyze alerts and emails. From this work, I've expanded my understanding of incident response and threat assessment. Furthermore, I was introduced to various open-source intelligence (OSINT) tools that help me analyze IP addresses, domains, and URLs to identify potential threats. These OSINT tools include VirusTotal, AbuseIPDB, Scamalytics, URLScan, urlquery, and ANY.RUN.

Along with my responsibilities, I have been doing a lot of self-study with the applications that the SOC team introduced to me. I have started learning about Splunk, a cloud service the department uses to consolidate security information. I am getting familiar with its scripting language so that I can perform queries in the future. Kris and Tatum have also given me lots of advice for professional development, like suggesting the best cybersecurity certifications that support my career direction.

Overall, this internship has expanded my understanding of cybersecurity operations. Although the sheer volume of information was a challenge, especially in the beginning, I am learning more and adapting to the work environment. I am excited to keep learning and gaining experience.