

Jonathan Roeseler

Reflection Paper 6

Date: 10/9/2025 - 10/17/2025

ODU Fall 2025

Professor Teresa Duvall

### **Internship Reflection Paper**

**300 Hours**

Working as a Helpdesk Technician for 300 hours has given me invaluable experience in resolving tickets and responding to common security incidents. I learned a lot about managing an Azure environment, troubleshooting common Microsoft and Android operating system and application issues, as well as resolving and mitigating different security incidents. During these last fifty hours, I gained a lot more experience in the management and overall security posture of our environment through Microsoft's Device Management solution, Intune, through Microsoft's Defender secure score and baseline initiatives, and through our Anti-Virus or endpoint detection and response tool [EDR], SentinelOne. I searched for some articles and resources on secure baselines as well for Azure / Entra environments, and found some very useful information that I used to better secure our systems and data. For example, I found that we had the ability for users to register any app, no admin approval needed - so using the resources I had and secure baselines, I turned it off. I obviously researched it a little more to ensure there was no negative user or workflow impact. I also gained some work experience with

Intune, Microsoft's device management/MDM tool. Another systems engineer and I were tasked with implementing and reviewing a Data Loss Prevention [DLP] tool, and it required some of our Intune knowledge to push the agent to a test group of devices. Furthermore, I found that this agent, particularly the extension, actually caused some negative impact on user systems - it essentially would not let them upload files to SharePoint online due to a bug. On an affected user's device, I was able to trace the error using the console log in Chrome to the extension. I then reached out to their team, with proper logs and screenshots, with methods to reproduce, and they fixed it in an update. In the meantime, I removed the agent from the affected systems via Intune.

The value of teamwork is the most important thing I've learned during my 300 hours. A lot of the tickets and security incidents I encountered and resolved, I had either learned from another co-worker, if not by myself, or collaborated with a co-worker to resolve them. Any large organization or information technology/cybersecurity role requires a certain level of collaboration to meet the needs of the organization effectively.

Overall, the 300 hours have been a great introduction to information technology and cybersecurity. I really enjoyed working with XKIG, I learned a lot about some of the most commonly used operating systems (Windows, Android), utilizing proper customer service skills, leading presentations and projects, and responding to security incidents. I give a lot of thanks to the leadership there for allowing me to grow from my role into more challenging topics, such as leading our DMARC project, training users, responding to incidents, and managing our training platform (KnowBe4). Unfortunately, as of October 20th, I have decided to move to a new, yet similar role at another

company; however, with the skills and working knowledge I gained here, I am very confident that I will succeed and hopefully gain a more cyber-specific role in the future.