- Kyle Sershon
- CYSE368_24518
- Spring - 2026
- Teresa Duvall
- Joshua Russell
- The Global Electronics Association
- Reflection #2

Internship Reflection Journal 2

Over the past few weeks, I have participated in several tasks related to information technology and cybersecurity. I have participated in backing up several of our Development environment servers to ensure the integrity and availability of our Data. This involved a deeper understanding of “Cold”, “Warm”, and “Hot” back-ups. Additionally, I have reviewed and resolved issues using CrowdStrike ATP monitoring on each device in our tenant. This involved monitoring and resolving detections as they appeared in the Endpoint Detection portal.

Backup infrastructure is extremely important in any environment to ensure data integrity and availability. Integrity and Availability are 2 of the pillars in the CIA triangle. I worked on creating monthly “Warm” backups. We pulled these backups for approximately 10 development environment Drupal servers and placed them on a drive on an AWS backup server. We keep a year's worth of Warm backups for each Drupal server. Each month, 1 Full Backup is taken, and subsequent incremental backups are performed between full backups. The reason for this structure is to allow critical servers to be easily

restored in the event of corruption or improperly executed code that requires a rollback. Incremental backups let us be space-conscious and capture only daily changes. We also store 7 years' worth of cold backups in an AWS S3 bucket; the cloud storage is cheaper, but data retrieval takes much longer. This way, we always have our data duplicated and eliminate any single point of failure. It was valuable for me to learn the balance among data storage costs, retention policies, and the feasibility of backup infrastructure. In the event a server needs to be restored, we can use Veeam to restore our data from the backup needed. One of the challenges I faced was the pace at which I was transferring each backup from one server to another. Though duplicating backups from our hot repository to the warm repository was a straightforward manual process, I faced a challenge with the time required to transfer each backup. With my PowerShell experience, I can automate and schedule this process. This will also help by saving the organization's man-hours and eliminating the possibility of human error, such as missing a manual server transfer. Engaging in this process taught me the importance of having a well-balanced backup structure and how that revolves around a Business Continuity Plan as well as our Disaster Recovery plan. This way, in the event of a failure, our leaders can anticipate and plan accordingly around downtime.

Regarding CrowdStrike's endpoint protection, I have been tasked with reviewing daily any new alerts. This required careful monitoring and inspection. I learned that it is important to maintain our internal systems and protect them from threats. A majority of the alerts were labeled as “informational.” We only had 1 detection that required significant attention. When reviewing this threat, I used the CrowdStrike portal to identify the device

and the user associated with the device. The .dat file was detected, and shortly after, a PowerShell session. I spoke directly with the user and asked if there had been any potentially malicious activity. I did not want to accuse the employee of wrongdoing, but I did want to verify whether a malicious file had been downloaded or an email opened. I decided to keep the file in quarantine, even though the user did not mention anything suspicious. Proper communication was key here. I did not want the laptop user to become defensive; I was trying to find clues, not accuse the person. I approached this case with context as well. I reviewed the user's position in marketing and determined that their access to other higher-priority systems was minimal.

In conclusion, I was able to reflect on the importance of structuring data integrity and availability, and how this was critical to business operations. It taught me how IT and well-planned infrastructure are important at the Global Electronics Association. Our website and training portal, all developed in Drupal, are under constant change, and having a consistent, well-maintained backup plan ensures minimal downtime. Using CrowdStrike to detect immediate threats through real-time scanning helped me reflect on how to balance active threat detection with a proper, tactful approach to investigating the matter. It is much like any investigation; I felt that if I approached the user from an accusatory standpoint, I would not get any help in identifying the potential issue, which could have led to a risk going undetected or a safe file being quarantined for no reason. In the age of AI, we can use machine learning to detect potential threats, but human interaction to investigate them remains important.

Detections in CrowdStrike.