Carmen Taylor

CYSE 368

Professor G

6/27/24

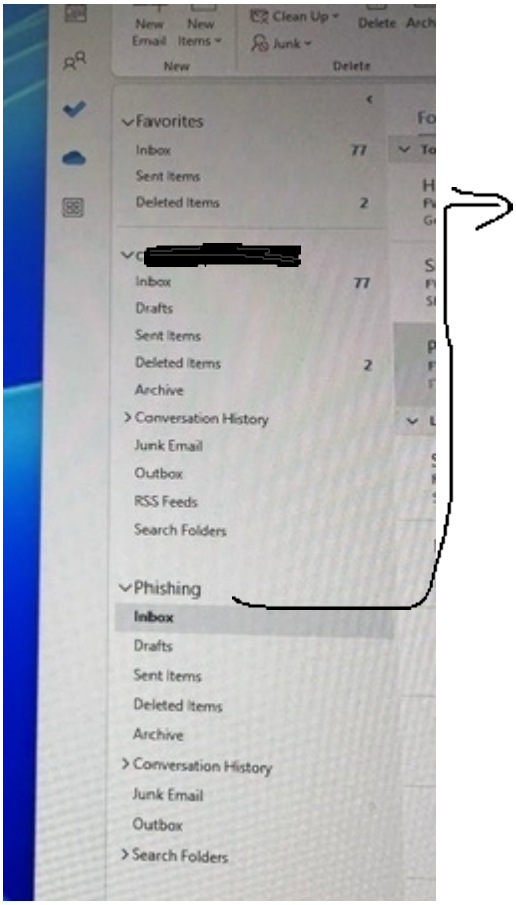
Journal 2:

Topic: Discuss the second 50 hours of the internship position:

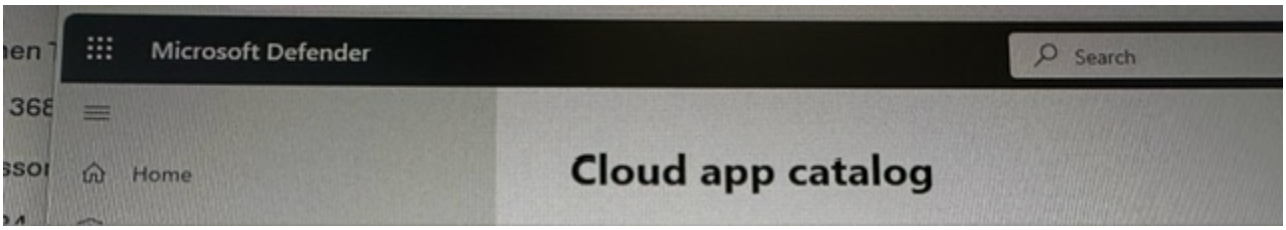
The start of my second 50 hours began on June 11, 2023, and these next two weeks were extremely thrilling. I was assigned my first ongoing projects where I was working inside of their security applications to protect against phishing schemes and sanction and unsanctioned apps that come in conflict with the company's privacy policy. The Microsoft defender cloud apps app and function played a key role when I was determining which apps should or shouldn't be sanctioned. When trying to make my decision I investigated each apps risk level, and when working on defender the lower the number for the risk level, the higher the severity of the app. This score is based off legality, security, compliance, and their general data. The app's general data is its headquarters and data center location, date of founding, its domain, privacy policy, and terms of service documents. The security category is where it lists what features the app has, like multi-factor authentication, the remember password feature, and encryption protocols. Compliance is based off the apps ability to meet certain standards that allow it to be safe. This category features certificates like ISO 27001, and other framework guidelines like ISO 27018, and GAAP. The legality feature includes information about data ownership, GDPR standards, data retention policies, and DMCA. After I investigated each of those factors, I also investigated the usage, and if an app had a critical risk score, and a low number of users, I deemed it as unsanctioned for my report. When it came to my assigned project for phishing, I was passed down the entire email thread where the employees send their emails, they believe were phishing and I had to determine if they were really phishing emails or not. With this project I strengthened my decision-making skills, and my attention to details. I used something called Barracuda to be able to further investigate emails, and see using the senders IP address, where the emails were being sent. I manage this email account everyday and check each, to see if any repeat places occur. I learned some keyways to point out phishing scams with of course small apostrophes, or weird and long emails, and if an email was sent to multiple users at the same time. I also have been refreshed on how important it is to never open pdf files, or click certain links, especially if the sender is suspicious, because malware is able to be in pdfs and links, compromising computers in an instance. In my last journal I didn't include any of what the process was like regarding the first day. I had to get a badge made to have access into the department

room, as an added security layer, along with creating a pin to enter my work area. These added layers of security show how important restricted access is when dealing with such sensitive information. It shows a perfect way to track who is coming in and out of the work area, if anything goes down from inside or outside of the department.

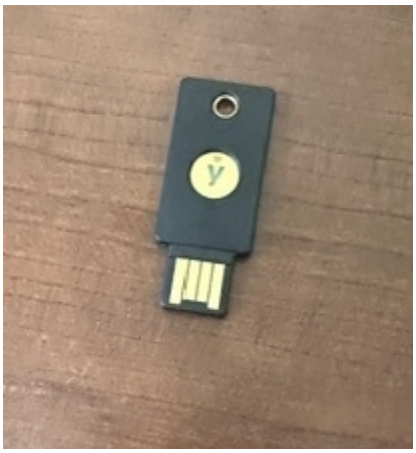
Some pictures from the following weeks:



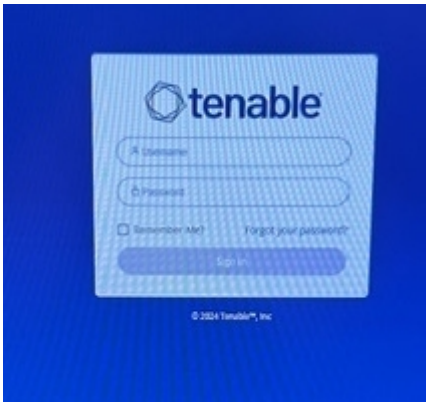
Where I manage the phishing email threads, to begin addressing them properly, and the proper research when looking into them. I also blacked out my email to ensure no one uses my email for phishing schemes.



Utilizing the cloud apps catalog when determining which ones to sanction and not



Exploring more about the use of Fido security keys vs. the use of Multi Factor Authenticator apps. As well as researching if MFA could be mandated or not.



I'm unable to directly show any dashboards discussed in the tenable app, but this is how I log into this amazing app.

Some of the security layers the COS uses to successfully restrict access to the data, Pin pad, Badge

I had to black out info on my badge to protect from any attempts to recreate it

COS IPS Info Sheet

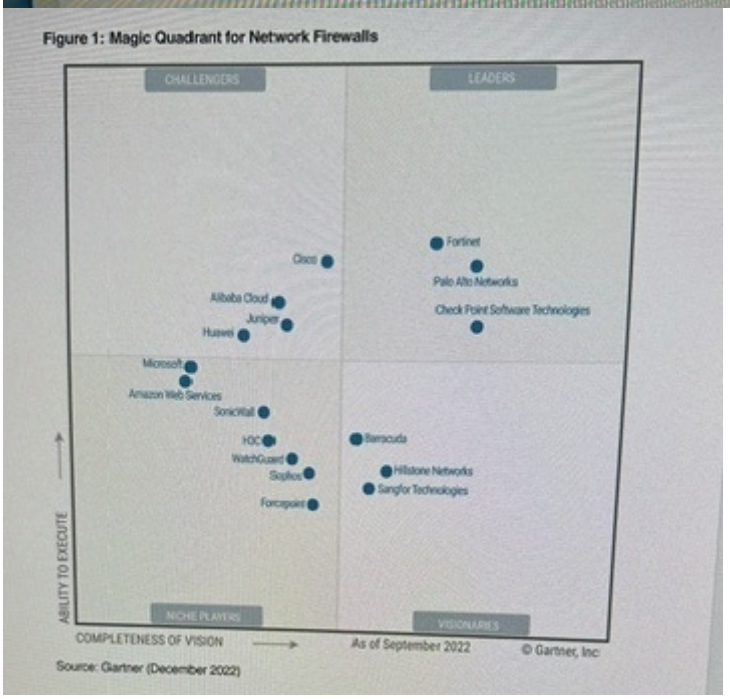
Top 5 IPS:

1. **Check Point IPS**
   Quantum Intrusion Prevention System (IPS) - Check Point Software
   a. Low false positive rates
   b. Check Point IPS protects you with the detection and prevention of:
      i. Specific known exploits, such as specific CVEs
      ii. Known and unknown vulnerabilities
      iii. DNS tunneling attempts indicating data leakage or evasion
      iv. Generic attack types without any pre-defined signatures
      v. Protocol misuse which may indicate malicious activity
   c. Thousands of signatures and preemptive behavioral protections.
   d. Security gateway users have a reduced cost, with the added IPS
      i. This feature allows for the IPS to play off the infrastructure.
         1. Detect-only mode: All protection devices will detect vulnerabilities, and not block the traffic.
         2. With antivirus, anti-bot, and Sandblast enabled the firewall will better protect against zero-day protection.
   e. Updates every 2 hours: regarding virtual patching upon the check point management server and security gateways.
   f. Integrates Smart Event, which uses Check Point enforcement points data logs, to identify suspicious activity, trend tracking, and investigate events. Easy interface with easy personalization for the best usage.
      i. Allowing for:
         1. Full Threat Visibility
         2. Real Time Forensic and Threat Investigation (allowing for easy drilling)
         3. Schedule reports and Integrated Threat Management
   g. Flag new protections to follow-up maintenance changes of the IPS policies.
   h. Up to 1TB per second of IPS throughput
   i. **RANKED #1 in MICROSOFT THREAT COVERAGE**

I recommend looking into the **Enterprise** or the **Industrial Control System Security Gateway** categories.

This link will show some of the NGFW I compared with IPS:

Comparison Preview - Check Point Software



This is a direct picture from my report and finding when discussing IDS and IPS systems. I included an example of the 2023 Magic Gartner Quadrant, I learned about. After doing the research in some of the software options, I put bullet points about the benefits of each one and created my own recommendations for which IPS would be best for our use from each company, and inserted a link for my supervisor to do an easy comparison himself to see which one's he thought would be best.