Reflection on Project Pisces and Cross-Training Experiences

Capstone

COMP 4799

Angelica Shelman

Table of Contents

Introduction

My Cybersecurity program Capstone will discuss my experiences working with Project Pisces as a Tier 1 analyst and my cross-training experience shadowing and gaining hands-on experience at the organization I work at. Both experiences have shaped me to become an exceptional cybersecurity analyst in the future. The hands-on skills and training I had with these experiences are invaluable, and I hope that after this program is completed, employers see that I have the necessary educational background and experience to be a successful security analyst.

Project Pisces

I joined Project PISCES in October 2023. It offers training and practical opportunities to prepare students to start their careers as beginner-level cybersecurity analysts. Metropolitan State College of Denver (MSU Denver) and the National Cybersecurity Center (NCC) collaborated to create Project PISCES (Public Infrastructure Security Cyber Education System).

What makes Project PISCES special is that it partners with local organizations that may not have the bandwidth to support themselves in the cybersecurity landscape and allows students the opportunity to volunteer their time and skills to monitor alerts and create tickets so the organizations can be aware of any potential cyber threats. "Project PISCES in Colorado currently serves 12 community partners with an IDS network monitoring service for free, providing a public benefit to over 500,000 residents of Colorado across cities, counties, school districts, and special districts. The student analysts that monitor these networks are all trained by the team from MSU Denver Cybersecurity Center and perform their work remotely from across the state (https://cyber-center.org/national-cybersecurity-center-hosts-project-pisces-training-and-onboarding)."

The orientation was at the Cybersecurity Center on the MSU-Denver campus and included a meet and greet of the members of Project Pisces who help run the program. We received a brief overview of how the program is run and the expectations of the students as we embark on the analyst role. We were trained on how to access and use the Kibana SIEM (Security Information Event Manager) to seek out alerts from the various organizations we would be monitoring. We learned how to create tickets by including the time, date, alert ID, source and destination IPs, and source and destination port numbers. We learned how to investigate the alert and what important details and screenshots to include. We also learned how to suggest recommendations properly.

As a part of Project Pisces, as student analysts, we are required to generate at least 4 tickets a month. Just starting out, Project Pisces analysts are required to work the "easier" alert and then we can work our way up to more challenging alerts. The easier alerts we were instructed to work on initially are called "Poor Reputation" tickets. These alerts from the SIEM are generated because the source IP that is making the connection to the destination IP may be considered malicious. We were to analyze the source IP to determine how malicious the IP is, and depending on the investigation into the source IP, we are to recommend the organization with the destination IP to block or temporarily block the IP. When we recommended an IP to be temporarily blocked meant the IP address was associated with a cloud service which means

the cloud service often switches IP addresses. Temporarily blocking the IP is a good recommendation because that IP will likely be switched and may no longer have to be blocked. Malicious IP addresses that are not associated with a cloud service are recommended to be permanently blocked to prevent any malicious activity on the network. We had to prove why we came to that conclusion by utilizing trusted public IP lookups such as VirusTotal, AbuseIPDB, AlienVault, and Cisco Talos. These are trusted websites that many vendors utilize to check the reputation of an IP address. Checking various sources for the IP's reputation will provide the organization with enough evidence to support why we think they should block or temporarily block an IP address. Additionally, we find the domain and hostnames from these IP addresses. Using terminal command line commands such as nslookup or dig can help determine the domain. Nslookup and dig are valuable tools used to explore issues related to domain names and DNS records. These commands offer insights into DNS configurations and are used for obtaining detailed information about domain names and IP addresses. In the Ethical Hacking course, I had several hands-on labs and exercises, where I used nslookup and dig to simulate real-world scenarios. I perform DNS lookups, analyze DNS query responses, and interpret the results to uncover potential security issues. This practical experience helped me and prepared me to develop the skills needed to inquire about a network environment throughout my Project Pisces experience. Additionally, the Computer Networking and Network Security course helped prepare me for the Poor Reputation tickets in Project Pisces because, in class, I learned about how IP addresses can be associated with malicious activities and how IP reputation databases can be used to identify and block suspicious traffic. These courses covered a range of topics, including IP addressing, subnetting, network protocols, and security mechanisms like as firewalls and intrusion detection systems. This theoretical knowledge directly translated into practical skills during my time with Project Pisces.

Figure 1.0

Observations:
Alert name: ET CINS (Emerging Threats Community Intrusion Detection System) Active Threat Intelligence Poor Reputation IP group 46
Threat: Poor Reputation
Time: Nov 26, 2023 @ 17:23:13.735
Source IP: 45.83.89.150
Source Port: 37345
Destination IP: 192.168.XX.X
Destination Port: 8080
Domain: m247.com
Investigation Notes:
On Nov 26, 2023 @ 17:23:13.735 system time IP 45.83.89[.]150 resolving from a domain m247.com, communicated with XXXXXX IP 192.168.XX.X. When ran through multiple reputation checks, IP 45.83.89.150 returned malicious. 4 security vendors on VirusTotal has flagged this IP as malicious. On AbuseIPDB this IP has a 100% confidence of abuse. According to AlienVault, this IP has historical OXT (Open Threat Exchange) telemetry as well as being associated with botnets, and overall being labeled a malicious IP. OPX is a crowd-sourced computer-security

platform where threat intelligence collaborates can work together to find threats (https://cybersecurity.att.com/documentation/resources/pdf/otx-user-guide.pdf).

Recommendations:

We recommend further investigation of this traffic. If communication with IP 45.83.89.150 is not needed for business, then we recommend blocking it for 90 days.

Figure 1.0 is an example of a Bad Reputation ticket I generated for an organization. For privacy reasons, I obfuscated the organization's name and part of its IP address.

After working hard to complete more than four tickets each month, I became Analyst of the Month in November 2023 and January 2024. Then, in January 2024, I was officially promoted to Tier 1 analyst, which meant I had proven myself and shown dedication to Project Pisces. I was seen as a reliable analyst who could tackle more complex alerts, other than the poor reputation alerts.

I was encouraged to investigate various kinds of alerts, and since this was still a learning opportunity, we would continue to receive feedback on how to improve the tickets. By working on different alerts, such as suspicious login attempts, malware installation, injection attacks, privilege escalation, etc., I was able to branch out and broaden my knowledge and understanding of the cyber threat landscape.

Figure 2.0

Observations:

Alert name: ET (Emerging Threat) EXPLOIT LB-Link Command Injection Attempt (CVE-2023-26801)
Threat: ET EXPLOIT LB-Link Command Injection Attempt (CVE-2023-26801)
Time: Mar 22, 2024 @ 11:49:39.514
Source IP: 46.40.115[.]166
Source Port: 34857
Destination IP: 192.168.XX.X
Destination Port: 8080
Domain: bulsat[.]com

Investigation Notes:

On Mar 22, 2024 @ 11:49:39.514 MST, IP 46.40.115[.]166 resolving from a domain bulsat[.]com, which is a cloud service provider, communicated with XXXXX's IP 192.168.XX.X After using the nslookup command, the hostname resolved to: 46-40-115-166.dbr.ddns.bulsat.com. When ran through multiple reputation checks, IP 46.40.115[.]166 returned malicious. On AbuseIPDB this IP has a 50% confidence of abuse. According to Cisco's Talo website, this IP has a poor reputation. The alert indicates that the alert is related to an attempt to exploit a command injection vulnerability in LB-Link networking devices. This alert specifically notifies about an attempt to exploit the CVE-2023-26801 vulnerability, which involves command injection in LB-Link networking devices. According to Akamai.com, CVE-2023-26801 is a vulnerability that stems from inadequate scrutiny of the "mac" parameter, enabling

unauthorized individuals to run commands of their choosing on impacted devices. In other words, exploiting this weakness may result in unauthorized entry, compromising the device, and allowing movement laterally within the system. The security flaw is being used to disseminate the Mirai botnet malware across specific firmware versions such as: LB-LINK BL-AC1900_2.0 V1.0.1, BL-WR9000 V2.4.9, BL-X26 V1.2.5, and BL-LTE300 V1.0.8.

Recommendations:
We recommend further investigation of this traffic. If communication with IP 46.40.115[.]166 is not needed for business, then we recommend temporarily blocking it for 90 days. Additionally, we recommend mitigating the vulnerability related to CVE-2023-26801. According to Akamai, there are 6 ways in which to mitigate this vulnerability. You may find this information at the following secure website: https://www.akamai.com/blog/security-research/cve-2023-26801-exploited-spreading-mirai-botnet#mitigations. The mitigations include the following:
1. Stay updated with firmware: Keep an eye on the vendor's website for firmware updates tailored to the impacted models (LB-LINK BL-AC1900_2.0, BL-WR9000, BL-X26, and BL-LTE300), both globally and in China.
2. Swiftly install updates: Once the updated firmware becomes available, promptly download, and install it to fix the vulnerability.
3. Limit network access: To enhance security, avoid direct internet accessibility to LB-LINK routers. Apply firewall rules or segment the network to restrict access to these devices.
4. Strengthen authentication: To minimize unauthorized entry, employ robust, unique passwords for router administration. If supported, consider implementing multi-factor authentication.
5. Regularly update security measures: Stay vigilant for security advisories and firmware releases concerning LB-LINK routers. Check the vendor's website periodically for updates specific to your device model.
6. Monitor network activity: Employ network monitoring tools to detect and analyze any suspicious activity, aiding in the early identification of potential exploits.

Figure 2.0 is an example of a ticket I wrote on a more complex alert.

The Secure Software Engineering course helped me with more complex alerts, like in Figure 2.0, because I learned about the Common Vulnerability Scoring System (CVSS) which is a standardized method for assessing and rating the severity of software vulnerabilities based on factors such as exploitability, impact, and ease of remediation. I also learned about Common Weakness Enumeration (CWE) and Common Vulnerabilities and Exposures (CVE), which provide a structured framework for understanding and categorizing software vulnerabilities. This knowledge was helpful when the alert detected a software vulnerability so I could understand where to find the details of the vulnerability and what specifically caused the vulnerability. NIST NVD, which is the National Institute of Standards and Technology's National Vulnerability Database, was an essential resource when investigating vulnerabilities (https://nvd.nist.gov/).

I am currently active in Project Pisces as a Tier 1 analyst. After 6 months as a Tier 1 analyst, I could officially be promoted to a Tier 2 Analyst while receiving a salary and officially working for

Project Pisces. I am going to continue working hard because this experience could lead to a full-time cybersecurity analyst position, and it would be great for my resume and to discuss in future interviews.

Cross-Training Experience in the Information Security Office

I had the great experience and pleasure of having the opportunity to cross-train in the cybersecurity department at my organization. The organization I work at and cross-trained with will not be mentioned in this capstone paper to protect the organization since I am going into detail about specific alerts and incidents and processes and procedures I learned.

The way I was able to gain this invaluable experience to be able to sit with a full-time cyber security analyst was because I reached out to the department manager to ask if they had any available internships. Unfortunately, this department did not have any internship opportunities available, but the manager suggested that I could cross-train and sit with a full-time analyst and members of the team to gain some hands-on experience and to see the work a security analyst does for the organization. I was thrilled for the opportunity and had the pleasure to work with this team twice a week for 6 months from September 2023 to February 2024.

The cybersecurity team at my organization is called the Information Security Office (ISO). I was shown all the cybersecurity tools used daily which included two Security Information Event Managers (SIEM), which takes in logs, threat intel, vulnerability feeds, and then outputs alerts from highest priority to lowest priority. Another cybersecurity tool used is called CyberArk/Password Vault, which is an identity security and access management tool. Other tools included an inventory management tool, a Microsoft Azure tool called Entra ID, which is essentially the active directory of the cloud, and Microsoft Defender, which is the antivirus tool for Microsoft Office 365. There are additional tools mentioned as I discuss my experiences in this capstone.

After spending 6 months with the ISO team and their cybersecurity analysts, I was shown many different alerts from the SIEMs and other notification methods. I learned a decent amount of the alerts were false positives and a decent amount were genuine concerns that needed further investigation. What I enjoyed most about this experience was that even if an issue was prevented early or it wasn't as it seemed, the analyst still took the time to show me a "what-if" had the experience been much worse, so I learned how to handle situations even if I didn't get a chance to see it.

Credential Compromise

My organization's ISO Team is subscribed to the HaveIBeenPwned service that will notify the team if any employees' accounts have been found in password dumps. Compromise of credentials can occur when a user enters passwords into phishing sites, exposes passwords in plaintext documents, accidentally pastes a password into social media, shares passwords with other employees, or when re-using passwords stolen from other sites. Attackers use various

methods to steal or guess passwords. Additionally, cybercriminals steal passwords and databases and sell them to other criminals.

On Monday, following a weekend, I began cross-training with the ISO team, and we began reviewing the alerts from the SIEM from over the weekend; I observed the security analyst reviewing alerts showing a user logging in at unusual times and from unusual locations. The alert showed the user logging in at 4 am on Saturday morning in the Florida area. This became a red flag because our company's organization only resides in Denver, Colorado, and the type of work the user does, does not require them to need access on the weekend- let alone in the state of Florida. The analyst proceeded to further investigate the alerts. The analyst created a chat with the entire ISO team through Microsoft Teams to make the team aware and to discuss the investigation efforts. The analyst then proceeded to reach out by phone and call the user directly to confirm if the user did log in on the date and time. After speaking with the user, they were, in fact, out of town, working remotely in Florida. They had received approval from their manager to work overtime on the weekend and they confirmed their login time. The alert we received was at 4 am MST but it was 6 am EST. The analyst also confirmed with the user's manager to ensure the accuracy of what the user told the analyst.

Fortunately, this alert was cleared, allowing the analyst to move on to other tasks. However, the analyst wanted to demonstrate what actions would be necessary if the user had indicated they did not sign in. If the employee confirmed their password was stolen or exposed, the analyst would immediately work with our ITCS team to reset the password to prevent unauthorized access and protect the employee's account. If the employee was unavailable to reset their password, the analyst would have to block sign-ins for the account in the Office 365 Admin Center and sign out of all sessions using Active Directory - Users and Computers, accessible through Password Vault/Cyber Ark. This step ensures that the compromised account is secured and prevents further misuse.

The analyst would then check Microsoft Office 365 for any email forwarding rules or changes to the user's profile to identify any signs of account tampering. This is important because unauthorized forwarding rules or profile changes can indicate that an attacker is redirecting communications or altering account settings for malicious purposes. Additionally, the employee would be required to check ADP for any unauthorized changes to their direct deposit, bank account, or contact information, as these changes could indicate fraudulent activities aimed at financial gain. Monitoring ADP is crucial because it is the organization's software for managing payroll, timekeeping, and timecards, making it a critical area to monitor for potential security breaches. Ensuring the integrity of ADP helps protect employees' financial information and prevents unauthorized access to payroll data.

If unauthorized access was suspected, the analyst would narrow down the date of the first compromise by analyzing logs for remote logins, unusual login times, and logins to unfamiliar systems. This helps to understand the scope of the breach and identify how long the account has been compromised, which is crucial for assessing the potential impact.

Next, the analyst would investigate for persistence and backdoors by examining local accounts, new Active Directory accounts, remote access methods such as VNC, Netcat, Metasploit, and scheduled tasks for remote shells or data transfers. Identifying and removing these threats is essential to prevent future unauthorized access and ensure the system's integrity. The analyst would create a timeline of the intruder's activity and search logs to

determine when the behavior began and was last observed, providing a clear picture of the attack's duration and progression.

Additionally, identifying the method of entrance is crucial, which could include vulnerable network software, improperly secured service accounts, open services with vendor or guest access, compromised employee credentials, or even a cloned badge. Understanding how the attacker gained access helps to address security weaknesses and prevent similar incidents in the future.

The following steps involve containment, eradication, and recovery. If the intruder's session is still active, the analyst would terminate the connection to stop ongoing unauthorized access. For endpoints capable of Windows Defender quarantine, the analyst would trigger the quarantine action, disconnecting the compromised system from the network, shutting down the vulnerable service, and disabling the compromised account or service password. This isolates the threat and prevents it from spreading.

Subsequently, the analyst would monitor for additional authentication attempts to Microsoft Office 365, ADP, and cloud servers, blocking IP addresses or malicious domains as necessary. This helps to prevent further attacks and secures the environment against ongoing threats. The user would be advised to change passwords for any other accounts where they reuse their credentials, particularly for banks, personal email, retirement accounts, or credit card companies, to prevent potential identity theft and financial fraud. Additional training to enhance password protection would be provided to the user, ensuring they understand best practices for maintaining account security.

Finally, the analyst would complete a formal report detailing the timeline, evidence collected, actions taken, and lessons learned. This report is important for documenting the incident, providing insights for future prevention, and ensuring accountability and transparency in the incident response process.

From this experience, I learned the importance of proactive measures in cybersecurity. The idea that compromised credentials can lead to significant security breaches was reinforced. It also highlighted the prevalence of credential leaks and the necessity of constant vigilance and timely response. Fortunately, this alert did not turn into anything malicious, or the analyst would have had to do a lot more work to investigate further, contain, eradicate, and recover. The analyst was relieved this incident was not malicious but was prepared had it been. I am grateful to the analyst for sharing with me the “what-ifs” of the alert because I learned there are a lot of different scenarios that call for different ways of handling certain situations. One surprising aspect was the volume of alerts generated and the varying degrees of severity associated with each alert. Initially, I expected credential exposure incidents to be relatively rare because my organization puts forth a lot of effort to educate all employees on the importance of preventing credential compromise, but the frequency of alerts like this and other similar alerts indicated otherwise. This emphasized the reality of organizations' constant threats and the need for vigorous monitoring efforts even when employees are constantly trained. The Ethical Hacking course taught by Dr. Nate Evans provided me with invaluable insights into how attackers think and operate, specifically regarding unethically obtaining a user’s credentials. I learned cybercriminals' methods and techniques, such as credential stuffing, social engineering, phishing, man-in-the-middle attacks, and exploiting vulnerabilities using tools like Metasploit. Understanding what an attacker does and how an attacker works helps cybersecurity

professionals better anticipate and better defend against potential threats related to user information being compromised.

Malware Installation

Malware may include rootkits, backdoors, keyloggers, wipers, DDOS components, command and control services, crypto miners, ransomware, spyware, banking trojans, and other unauthorized software. Malware can be installed through a physical attack, a credentials compromise, a phishing attack, a supply-chain compromise of trusted software, or an employee installing unauthorized software. Malware may open outbound remote interactive sessions from employee laptops or servers and enable additional targeted compromise deeper into the network of servers and workstations. The process of investigating potential malware on an employee's device is crucial in cybersecurity to ensure the integrity of the network and the safety of organizational assets. Understanding how to respond to malware threats is essential for maintaining a secure environment and minimizing the impact of potential breaches.

While cross-training with the security analyst, we received a notification from an employee/user who had been complaining of strange behavior and performance issues and had suspected malware only because their computer at home had become infected with malware and their work laptop was having similar symptoms. Potential malware issues are often brought to the ISO team for this very reason as well as suspicious folders, cleared logs or TEMP folders, files getting encrypted or deleted, applications starting up or shutting down, advertisements or “upgrade” pop-ups on screen, changes in network setting, new task scheduler or cron jobs, or new Startup scripts or files that show up in unexpected locations with unusual names.

To further investigate the issue, the analyst created a chat with the entire ISO team through Microsoft Teams to make the team aware and to discuss the investigation efforts. The analysts communicated with the user to determine if they had remembered clicking on a phishing email/link or recently downloading or upgrading anything on their device. The user denied doing anything but just thought it would be worth looking into since the user had a similar situation at home. The analyst advised that the organization uses Tenable Nessus for daily endpoint malware activity and wanted to check the report to see if this device showed any activity. The device did not have any reports of any malware activity. The analyst ran another malware scan on the endpoint to make sure and the results showed no malware was on the device. The analyst checked Window’s Event Viewer logs to see if there were any security or system log failures that could help with troubleshooting the device. There were no questionable logs that needed attention. The analyst also checked Task Manager and Device Manager to see if there were any software or hardware issues that could be causing performance issues on the device. It turns out there was a missing driver that needed to be installed. The security analyst advised that the Help Desk could update the driver on the device and look further into the performance issues. Luckily, there was no malware installed on the user’s device, but the analyst told me the steps that would have to been followed if there had been.

If Tenable Nessus indicated that malware was installed on a device, the analyst would quarantine the device in Defender APT and disconnect it from the network. This step is crucial to prevent the malware from spreading across the network. The analyst would then check for potential spread to adjacent systems like servers by examining the network traffic between the endpoint and any other connected devices such as USB devices, SMB and RDP connections, Microsoft Office 365 cloud synchronization, Dropbox, or scheduled backups. This thorough check ensures that the malware has not propagated to other critical systems. If the malware was found to be spreading, the analyst would quarantine domain controllers and keep the infected device shut off. This containment measure is essential to stop the malware from affecting the broader network infrastructure. The analyst would attempt to obtain a copy of the malware and run it through an online sandbox, such as Joe Sandbox, only if it is not sensitive. This helps in understanding the behavior and capabilities of the malware in a controlled environment. If more data is required to determine the infection's potential scope, the analyst might test the attachment or link in a sandbox environment. Next, the analyst would identify the attack methods, the source, and the vector of spread to determine the best steps to contain and eradicate the malware. This investigation is vital for understanding how the attack occurred and preventing future incidents. Additionally, the analyst would ensure that future protections are installed or configured to prevent the attack from being successful again. Implementing these protections strengthens the organization’s security posture. Once malware is no longer detected, and/or the Operating System is reinstalled, and the systems are put back into production, the ISO team would monitor for a month to watch for command and control or anomalous behaviors. This monitoring, facilitated through SIEM or Windows Defender, helps detect any remaining threats and ensures the malware has been fully eradicated. Finally, a formal report of the incident would be documented with the timeline of events, the evidence collected, actions taken, and lessons learned. This documentation is important for providing insights for future prevention, ensuring accountability, and maintaining a record of the incident response process. Although this situation did not yield anything malicious, it was an excellent experience to see what steps were taken to confirm if malware had been installed and what steps would have been taken to remove the malware and recover the system.

This experience taught me how to properly approach and investigate potential malware incidents using tools such as Tenable Nessus for malware activity reports, Windows Event Viewer logs for identifying security or system log failures, and Task Manager and Device Manager for troubleshooting performance issues. I also observed how important communication and collaboration are within the team to ensure security incidents are responded to properly. One surprising aspect was discovering that the performance issues were due to a missing driver rather than malware, highlighting the importance of a thorough investigation and not jumping to conclusions based on initial symptoms. Furthermore, it was interesting to me to see the similarities between personal and work devices, where similar symptoms can lead to different root causes because while the user's suspicion of malware was incredibly valid, further investigation revealed that the work laptop's performance issues were caused by a missing driver, emphasizing the importance of thorough troubleshooting and analysis. Additionally, this experience stressed the importance of cybersecurity professionals having an open mind and considering a range of possibilities beyond the obvious. Courses like Operating Systems, Network Security, and Digital Forensics are courses where I could have

applied what I learned had this been a malware incident. In the Operating Systems course, I learned about the intricacies of file systems and their importance in identifying potential malware. Understanding how file systems operate is crucial for detecting suspicious changes and behaviors. Knowledge of file structures helps in investigating abnormalities that could indicate malware presence. This understanding is critical for conducting detailed investigations and identifying malicious activity within an operating system. The Network Security course helped me understand the importance of firewalls and how to configure them, as well as network traffic analysis, in detecting and preventing malicious activities. Implementing a firewall and learning to configure it to accept or block specific IP addresses and traffic types based on data criteria is a practical skill and this knowledge is directly applicable to real-world scenarios like the one I observed in cross-training where network security is vital in defending against cyber threats. In the Digital Forensics course, I gained an understanding of how to investigate cyber incidents and trace malware involvement. Learning to collect and analyze digital evidence, trace the source of malware infections, and understand the broader impact of these infections was invaluable. Using log files and maintaining a meticulous record of the investigation process, such as through a CrowdStrike template, were essential skills I gained that will be carried with me and useful as a cybersecurity analyst.

Lost or Stolen Device

While cross-training with the ISO team, we received a notification from a user who stated their car was stolen and their company laptop was in the stolen vehicle. This could be a potentially dangerous situation because depending on who stole the car, if they have access to the user's credentials, the thief could then have access to the organization's environment. However, the analyst advised me that all company devices should use BitLocker with a TPM chip to help encrypt the data on the device. A TPM chip prevents attackers from taking the drive out of the device or booting the device off a flash drive to try and read the data. The TPM holds the master key and will only decrypt the volume when the operating system is launched in its original configuration and is then up to the application to prevent access to the data.

The analyst logged into Microsoft Intune Admin Center and searched for the device. Once the device was located, the analyst verified that encryption was enabled. Encryption is essential because it transforms readable data into an unreadable format using algorithms and keys, which ensures that an attacker or anyone who is unauthorized cannot access the information. The importance of encryption cannot be overstated, as it safeguards data at rest, in transit, and in use. The analyst informed me that the organization uses full disk encryption. For full disk encryption, symmetric key encryption algorithms are typically used. AES (Advanced Encryption Standard) is the most common algorithm due to its strong security and efficiency. Implementing encryption on company devices guarantees that even if the physical device is compromised, the data remains inaccessible without the proper decryption key.

While logged into Intune, there is an option to “Locate Device”. When the device checks in this will give an approximate location of the device. The analyst proceeded to “Wipe” the device. Wiping the device removes all components of the organization from the laptop, so if the adversary tried to access data or information, the device would be empty. The process of remotely wiping the stolen laptop is crucial in mitigating potential security risks by removing all sensitive information and access credentials, preventing unauthorized access to the organization’s environment. This emphasizes the importance of implementing security measures such as BitLocker with a TPM chip to protect data on company devices, especially in situations where physical theft can lead to data breaches.

The remote wipe feature enables the organization to command the stolen laptop to erase all stored data. Microsoft Intune, a mobile device management (MDM) solution, provides centralized management where administrators or, in this case, a cybersecurity analyst, have the option to issue commands to wipe a stolen device remotely.

I found this experience interesting because the remote wipe feature has limitations. For example, it is only effective when the stolen device connects to the internet. So, if the thief were to quickly disconnect the device from the internet, the remote wipe command may not be executed, which would leave the organization at high risk. Additionally, this experience of dealing with a stolen laptop emphasizes the important role that encryption has in securing data. Encryption ensures that even if a laptop or device is physically compromised, the data remains protected, which reduces the risk of unauthorized access. I find that this experience highlights the importance of being proactive and having a defense-in-depth approach to help safeguard against threats.

Social Engineering

Social Engineering includes Phishing, Vishing, and Tailgating as common methods of getting a victim to do something that profits the attacker. My organization has two primary ways to detect Social Engineering attempts or successful attacks. The ISO Team has a contract with Mimecast to provide a first-tier Phishing response. The ISO Team members review Mimecast reports after they analyze emails to confirm phishing emails.

During my cross-training experience, the analyst had to manually respond to a phishing attempt because someone within the organization had reported a phishing email through Outlook mail. The phishing email was reported to the ISO team because it asked for the employee to enter their username and password by clicking a link. The email sender stated they needed access to billing to pay a bill. Because the organization is big on employee education regarding social engineering, the employee spotted the attempt and automatically reported it. After receiving the report, the analyst checked the content in the message and links. The analyst opened the link in a sandbox to analyze further. The analyst determined that the URL link was a landing spot for a malware download. The analyst proceeded to reach out to the user to confirm whether the user clicked on the link. The user confirmed they did not click on the link. The analyst then had to create a Microsoft Teams chat to coordinate the response to the investigation and to notify the appropriate employees, such as the Manager of IT security. The analyst then had to determine the scope of the phishing email by searching Mimecast for the sender and to identify further if other employees received the same email. Thankfully, no

other employees were sent this email. The analyst proceeded to block attachments and URLs immediately using Mimecast. Additionally, the analyst blocked URLs in the VPN as well.

Had the phishing email been sent to multiple employees or if an employee had clicked the URL, there would have been additional, essential tasks to complete. The analyst explained that in a more severe situation, it would be necessary to follow the notification matrix and incident response plan to inform all users of the situation. The analyst would be required to speak to all targeted employees to determine if they clicked the link and entered their user credentials, such as their username and/or password. Those targeted employees would have to reset their passwords in Active Directory and disconnect their session tokens. Additionally, if any user had opened the link and downloaded malware, the analyst would check Microsoft Defender for alerts and run antivirus/malware scans using Tenable Nessus. If there were evidence of malware infection, the user's endpoint would be quarantined and disconnected from the network. Further investigation would be required to determine if any sensitive information was stolen or if there was potential for blackmail or extortion. A formal report would then be created with a timeline of events, evidence collected, actions taken, and lessons learned. Fortunately, none of the events or alerts during my cross-training led to an incident or breach, so the analyst did not have to conduct any further investigation.

From this cross-training experience, I learned the importance of a defense-in-depth approach and the role of human observance. The analyst demonstrated the importance of being thorough and precise when handling this potential threat. Additionally, this experience brought to light the importance of employee education on cybersecurity awareness because the employees recognized and reported the phishing attempts. Having employees aware of potential security threats enhances the protection and safeguarding of the organization's environment. Taking courses like Computer Networking, Networking Security, and Ethical Hacking taught me how important it is to understand how your network is set up and how to secure and monitor it. Computer Networking provided me with a comprehensive understanding of how networks are structured and operate. This knowledge is essential for identifying normal network behavior and recognizing anomalies that might indicate malicious activities. Also, understanding various protocols, and network devices and knowledge of how data flows equipped me to pinpoint potential vulnerabilities and optimize the network's performance and security. Network Security provided me with a deeper understanding of how to protect a network. Throughout this course, I learned about firewall configuration, encryption and hashing methods, and VPN implementation and usage. This knowledge is crucial to ensuring that all network components are secured against unauthorized access and potential exploits. Ethical Hacking was particularly enlightening to me because it provided an attacker's perspective on applying social engineering techniques. This course covered a broad spectrum of social engineering tactics, such as phishing, vishing, and smhing, and how these methods are used to manipulate individuals into disclosing confidential information and/or granting unauthorized access. By understanding these techniques and tactics from the attacker enables me to anticipate social engineering attempts on employees. Knowing the psychological and deceptive tactics used in phishing emails helped me educate employees on what to watch out for which will help improve the organization's overall security.

What surprised me the most about my experience was how a seemingly benign phishing email could potentially escalate into a significant security incident. The in-depth steps the

analyst would have taken if the email had reached more employees or if the link had been clicked illustrated the potential severity of the situation. This experience shows how important it is to be quick and make critical choices to prevent further spread and damage within the organization.

There were some limitations that I found while observing this experience. For example, when phishing attempts are only reliant on user's reporting them could lead to certain attacks going unnoticed. This means there should be additional mechanisms in place that can catch such events if a user were to miss them. Mimecast provides a service that does just that, so the organization is well-equipped to handle situations like this. However, it is important to note, that while Mimecast is an excellent provider of analyzing emails, it does not guarantee 100% of stopping such attacks, so certain attacks could potentially slip through. In other words, it is important to know that despite having sophisticated security systems in place, a single successful social engineering attack can bypass multiple layers of defense. This fact by itself entices me to pursue further a PhD in research involving the blending of my master's degree in psychology and its impact on cybersecurity, particularly how a single point of failure from a successful engineering attack can easily bypass multiple layers of defense and how it can potentially be changed. I find it interesting how humans are the easiest and most vulnerable when it comes to cybersecurity.

Conclusion

Overall, my experiences with Project Pisces and the cross-training within my organization have provided invaluable insights into becoming a successful cybersecurity analyst. The skills and deep understanding I have gained from these experiences have been reinforced by the education I received in the Master's program in Cybersecurity at the University of Denver. The classes, skills, tools, and languages I have learned throughout this program have prepared me for a successful career in cybersecurity. The experiences discussed in this Capstone paper further reinforce the foundation and direction of my future career.

References

National Cybersecurity Center Hosts Project Pisces Training and Onboarding
https://cyber-center.org/national-cybersecurity-center-hosts-project-pisces-training-and-onboarding/

Akamai SIRT Security Advisory: CVE-2023-26801 Exploited to Spread Mirai Malware
https://www.akamai.com/blog/security-research/cve-2023-26801-exploited-spreading-mirai-botnet#mitigations

National Vulnerability Database
https://nvd.nist.gov/

AT&T and Cybersecurity
https://cybersecurity.att.com/documentation/resources/pdf/otx-user-guide.pdf