Incident handler's journal

Date: May 31, 2024	**Entry:** #1
Description	Documenting a cybersecurity incident. Investigation occurred in the Detection and Analysis phase of the NIST Incident Response Lifecycle, but actions did move into the Containment, Eradication, and Recovery phase as well. This is because the security team was not informed until after the incident took place.
Tool(s) used	N/A
The 5 W's	• **Who:** An organized group of unethical hackers well-known to healthcare and transportation organizations • **What:** A ransomware security incident • **When:** Tuesday, 9:00 a.m. • **Where:** On-premises of a small U.S. health care clinic • **Why:** Phishing emails with malicious attachments were sent to employees that deployed the ransomware upon download, encrypting critical files. Motivation seems to be financial because they left a ransom note demanding a large sum of money in exchange for the decryption key.
Additional notes	1. This incident should prompt employee training regarding phishing emails and malicious attachments. 2. Should they pay the ransom to get the key?

Date: June 3, 2024	**Entry:** #2
Description	Documenting a cybersecurity incident and VirusTotal lookup. Investigation occurred in the Detection and Analysis phase of the NIST Incident Response Lifecycle, but actions

	did move into the Containment, Eradication, and Recovery phase as well. This is because the security team was not alerted until the executables started being deployed.
Tool(s) used	VirusTotal
The 5 W's	• **Who:** Unknown threat actor • **What:** Trojan x phishing security incident • **When:** 1:11 p.m. – 1:20 p.m. • **Where:** Financial services company • **Why:** Phishing email with malicious attachment received by employee. Email contained password-protected spreadsheet with password in email body. Employee downloaded the spreadsheet and entered the password, which when opened, deployed and executed the malicious payload. Multiple unauthorized executable files were created on the employee's computer. Motivation seems to be about gaining control as the malware was a trojan backdoor, known as Flagpro, commonly used by advanced threat actor BlackTech.
Additional notes	1. How to prevent this in the future? – Training 2. VirusTotal revealed the names associated with this; should the company be worried about future threats from this actor or others?

Date: June 3, 2024	**Entry:** #3
Description	Documenting a ticket investigation. Follow-up using ticketing system to Entry #2's incident. Falls into NIST Containment, Eradication, and Recovery phase.
Tool(s) used	Ticketing System & Playbook
The 5 W's	• **Who:** "Def Communications" <114.114.114.114> • **What:** Phishing attempt prompting alert and ticket • **When:** Wednesday, July 20, 2022 09:30:14 AM

	• **Where:** Inergy, Financial Services company • **Why:** Phishing email, pretending to be applying for a job, caused a trojan deployment on employee computer, which resulted in an alert and ticket creation. File attachment was determined to be malicious.
Additional notes	Upon investigation and following playbook, it was determined that the file was indeed a known malicious file, and therefore required ticket escalation. Escalated and informed Level 2 Analyst.

Date: June 5, 2024	**Entry:** #4
Description	Investigating failed SSH attempts using Splunk. Part of the Post-Incident Activity or Preparation phases of NIST Incident Response Lifecycle.
Tool(s) used	Splunk Cloud
The 5 W's	• **Who:** I investigated log data using Splunk • **What:** I queried for failed SSH attempts to login as root on a mail server • **When:** Daily at 1:39:51 AM from 2/27/23 till 3/6/23 • **Where:** From multiple different IP addresses and port numbers • **Why:** It is suspected that a malicious actor was trying to gain root access to the mail server, as there are an average of 40+ failed attempts from different IPs every day that all occur at the same exact second.
Additional notes	This malicious actor knows what they're doing since they have multiple different IP addresses that they're using to make these SSH attempts, which makes it harder to prevent these attempts. Perhaps consider changing the root password and making it even stronger or putting up additional layers of security around it.

Reflections/Notes:

1. **Were there any specific activities that were challenging for you? Why or why not?**

None of these activities were challenging for me, as I have had exposure to a lot of these tools or concepts before. Also I am a quick learner so any new topics covered I was able to quickly pick up on. The newest too that I had the least experience with were Splunk and Chronicle, but those weren't hard to navigate.

2. **Has your understanding of incident detection and response changed since taking this course?**

Yes it has, as before this I didn't know the types of tools used by security analysts to detect and respond to incidents, nor all of the frameworks involved in this area. Now I am more comfortable stepping into this field and utilizing my knowledge and skills to accomplish security goals.

3. **Was there a specific tool or concept that you enjoyed the most? Why?**

I enjoyed learning and using Splunk and Chronicle, as these SIEM tools I had not had the chance to use befor Now that I have been able to become as least somewhat familiar with them, I see the value that they bring to security systems and security analysts, and I'm excited to use them in the future.