Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: 11/2/23	**Entry:** #1
Description	Ransomware cybersecurity incident at a small healthcare clinic This incident investigation took place in the analysis phase of the NIST Incident Response Lifecycle.
Tool(s) used	None
The 5 W's	● **Who** - A group of unethical hackers ● **What** - Ransomware locked the computer files and software ● **When** - Tuesday 9:00 a.m. ● **Where** - The healthcare clinic ● **Why** - Employees of the clinic fell victim to email phishing, which allowed the hackers to exploit the company for financial gain. Once the hackers gained access to the network, they installed ransomware. This resulted in their critical files being encrypted and a ransom note was left asking for money in return for the decryption key.
Additional notes	MGM just had a problem with this where they lost millions trying to fix it without paying the ransom. Should we pay the ransom? Also, I want to know the specific email that led to this so we can analyze and learn from it.

Date: 11/4/23	**Entry:** #2
Description	An employee fell victim to a phishing email and malicious software was downloaded on his computer. This incident investigation took place in the analysis phase of the NIST Incident Response Lifecycle.
Tool(s) used	VirusTotal
The 5 W's	● **Who** - An unethical hacker (email: 76tguyhh6tgftrt7tg.su) ● **What** - Malicious software was downloaded on the employee's computer ● **When** - 7/20/23 at 9:30 a.m. ● **Where** - At the office of the financial service company. ● **Why** - The HR employee received an email about a person interested in working at the company, When he downloaded the file it did not open a resume and he alerted the cybersecurity team. We analyzed the attachment and determined it to be a Trojan horse. The hacker did this with the intention to gain access to our network.
Additional notes	The cybersecurity team used VirusTotal to analyze the file quickly and deemed it malware. The threat actor stated that he was interested in working at our company and said he sent his resume, but really it was an executable file. There is an inconsistency between the sender’s email address “76tguy6hh6tgftrt7tg.su”” the name used in the email body “Clyde West,” and the sender’s name, “Def Communications.” This alert was escalated to a level-two SOC analyst to take further action.

Date: 11/7/23	**Entry:** #3
Description	Using Chronicle SIEM Tool to investigate a phishing event. This incident investigation took place in the analysis phase of the NIST Incident Response Lifecycle.
Tool(s) used	Chronicle (Google's cloud SIEM tool)
The 5 W's	● **Who** - An unethical hacker sent a phishing email to an employee ● **What** - They tried to sign into their account using the link in the email ● **When** - 11/7/23 ● **Where** - The financial services company ● **Why** - Employees were not suspicious enough of an email with a sign-in link.
Additional notes	There are 12 assets that have accessed the domain, and they all have similar names with interchanged last names. All of these assets were first and last accessed on the same day. Also, two users (emil-palmer-pc and ashton-davis-pc) posted to the /login.php, suggesting successful phishing attempts. When checking the IP address for other domain names, it results in a Google sign-in page alongside an office sign-in page, which is a strong indicator that this is a malicious link attempting to steal login information through phishing.

Reflections/Notes: I found the VirusTotal and Chronical activities to be very positive for my learning by getting hands-on experience with those tools. I am not yet a master, but I feel comfortable enough to complete tasks at a high level. My understanding of incident response and the NIST lifecycle is greatly improved after this course. I enjoyed using Chronicle the most because it was cool to see how a SIEM tool aggregates all of the logs in one place for analysis.