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: 04/01/2024	**Entry:** 01
Description	Cyber Security Incident (Ransomware)
Tool(s) used	-
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Organized group of unethical hackers • **What** happened? Several employees reported that they were unable to use their computers to access files like medical records • **When** did the incident occur? Tuesday morning, at approximately 9:00 a.m • **Where** did the incident happen? At U.S. health care company • **Why** did the incident happen? The breach occurred due to unethical hackers successfully infiltrating the company's systems through a phishing attack. Once inside, they initiated a ransomware attack, encrypting essential files. The attackers seem financially

	motivated, as evidenced by the ransom note requesting a significant amount in exchange for the decryption key.
Additional notes	1. Do they need to pay the ransom to get system back to normal? 2. If yes, is there any possibility the incident occurs again? 3. How to prevent this incident occurring again?

Date: 09/01/2024	**Entry:** 02
Description	Use VirusTotal to analyze file
Tool(s) used	VirusTotal (Open-source files and URLs analyzer)
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? BlackTech which is a cyber espionage group ● **What** happened? Suspicious file being downloaded on an employee's counter ● **When** did the incident occur? 1.11 pm ● **Where** did the incident happen? Financial services company ● **Why** did the incident happen? The breach occurred due to unethical hackers successfully infiltrating the company's systems by sending malicious malware. When employee opened the file, malicious payload was then executed on employee computer.
Additional notes	- How VirusTotal help uncover additional IOCs? - How Pyramid of Pain contribute to reduce attack?

Date: 09/01/2023	**Entry:** 03
Description	Alert Ticket Generated (Phishing Attempt)
Tool(s) used	-
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? Unethical hacker known as Clyde West ● **What** happened? Phishing attempt occurred by sending malicious malware ● **When** did the incident occur? Wednesday, July 20, 2022 09:30:14 AM ● **Where** did the incident happen? Inergy ● **Why** did the incident happen? The user may have opened a malicious email and opened attachments or clicked links.
Additional notes	- Apply email filtering for the organization - How to increase awareness regarding phishing

Date: 11/01/2024	**Entry:** 04
Description	Incident Final Report – Major Data Breach
Tool(s) used	-
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? Attacker that performs forced browsing attack ● **What** happened? Approximately 50,000 customer data had been stolen ● **When** did the incident occur? 3:13 p.m., PT, on December 22, 2022 ● **Where** did the incident happen? e-commerce web application for mid-sized retail company ● **Why** did the incident happen? Web application vulnerability allowed the attacker to perform a forced browsing attack and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page
Additional notes	- Need to perform routine vulnerability scans and penetration testing.

Reflections/Notes:

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

Analyzing files has been a bit tricky for me since it's my first time dealing with such tasks. Initially, it felt challenging as I had to learn the ropes and figure out the nuances of the process. However, I see it as a valuable experience that's helping me expand my skills. Slowly but surely, I'm getting the hang of it and finding it genuinely interesting. Each attempt teaches me something new, making the journey worthwhile and contributing to my overall learning in this field.

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

My understanding of incident detection and response has significantly evolved since taking this course. Previously, I had some exposure related to this during my diploma studies. The in-depth exploration of incident detection and response mechanisms has provided me with a more comprehensive understanding of the field. As a result, I now feel more confident about delving further into the realm of cybersecurity, armed with a deeper knowledge base and enhanced skills acquired through this course.

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

I enjoyed learning about network traffic analysis and using tools for it. Going through this topic a few times felt like reviewing and strengthening my basics. It was interesting to capture and examine live network traffic. Now, I'm even more curious about diving into this area and aim to improve my skills with network protocol analyzer tools.