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: October 3rd 2023.	**Entry:** 1
Description	A small U.S. health care clinic experienced a security incident on Tuesday at 9:00 a.m. which severely disrupted their business operations. I will be analyzing the incident and provide additional details.
Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. ● **Who**? An organized group of unethical hackers. ● **What** happened? Ransomware was deployed encrypting the organization's computer files. ● **When**? On Tuesday at 9:00 a.m. ● **Where**? A small U.S. health care clinic specializing in delivering primary-care services ● **Why**? A malicious attachment in a phishing email was opened.
Additional notes	The company should be more careful next time they receive a suspicious email or use additional tools to prevent it from happening again.

Date: October 3rd 2023.	**Entry:** 2
Description	A ticket was sent to me about a potential malicious file installed in an employee's computer. I will be analyzing whether the file is indeed malicious, and change the status of the ticket accordingly.
Tool(s) used	VirusTotal.
The 5 W's	Capture the 5 W's of an incident. ● **Who?** The threat actor Blacktech. ● **What** happened? A trojan virus was installed in an employee's computer. ● **When**? A few minutes ago. ● **Where**? The employee's computer ● **Why**? The employee downloaded a malicious file.
Additional notes	The employee got tricked into downloading a malicious file from an email, which turned out to be a trojan virus. The severity of this issue should be considered as medium, so I am escalating the ticket and notifying a level-two SOC analyst.

Date: October 3rd 2023.	**Entry:** 3
Description	An incident's final report was just sent to me. I will be analyzing this report and provide my thoughts on it.
Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. ● **Who**? The sender's identity is unknown. ● **What** happened? An employee received an email from an external email address stating that they successfully stole customer data, and demanded a 25000$ cryptocurrency payment for not releasing it. A week later, the same employee received another email including a sample of the stolen data, and demanding 50000$ now. ● **When**? Initially, at approximately 3:13 p.m., PT, on December 22, 2022. ● **Where**? The employee's mailbox. ● **Why**? Because of a vulnerability in the e-commerce web application.
Additional notes	The company ended up discovering the log source that caused the attack and its consequences. They disclosed the data breach to their costumers and offered free identity protection services to them.

Date: October 3rd 2023.	**Entry:** 4
Description	Using the SIEM tool Chronicle to investigate the suspicious domain name signin.office365x24.com An employee received a phishing email associated to this domain, so I will evaluate whether other employees also received phishing emails.
Tool(s) used	Chronicle
The 5 W's	Capture the 5 W's of an incident. ● **Who**? The account associated with the domain name signin.office365x24.com ● **What** happened? An employee received a phishing email. ● **When**? Earlier today. ● **Where**? The employee's mailbox. ● **Why**? Potential PII leak.
Additional notes	The investigation confirmed that the suspicious domain has been involved in phishing campaigns. Multiple assets might have been impacted as logs showed that login information was submitted to the suspicious domain via POST requests. Lastly, another domain "signin.accounts-gooqle.com" was found, which could give us more information about this attacker.

Reflections/Notes: Record additional notes.

1. The exercises from the last section were the most challenging, since those were the ones that needed apply the knowledge acquired during the rest of the course.
2. Thanks to this course, I learned to use several tools to analyze incidents and use log data to research the details of the 5 W's.
3. I really enjoyed practicing with SIEM tools, since they are very practical and give a lot of information once getting used to them.