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 31, 2023 Tuesday @ 9:00 am.	**Entry: 1**
Description	Rasnsomware attack on small health clinic
Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. • A group of unethical hackers executed a ransomware attack • The hackers managed to encrypt medical records of the patients while denying its access to the employees which interrupted the daily operations of the clinic. They also displayed notes on employees' computers' screens demanding ransom in exchange for the encryption key • The incident took place on the Tuesday morning at 9:00 AM • The attack happened at a small local clinic • The attackers targetted the employees with phishing emails and they were able to install a malicious software on the employee's computer which gave them access to the system which allowed them to deploy ransomware which encrypted the clinic's medical files.
Additional notes	The unethical hackers belong to a known group who target health and

	transportation industries. Several of the employees fell for the phishing attack indicating lack of security controls or policies.

Date: November 8, 2023 7:00 PM	**Entry:** 2
Description	Investigate a suspicious file hash
Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. ● Employee downloaded a suspicious file which sent alert ● Employee received a password protected spreadsheet file in an email with password. Employee downloaded the suspicious file and executed it. After opening the file the malicious payload was executed on the computer. ● The incident took place during business hours ● The incident took place on company's computer ● Phising email was the cause of the accident
Additional notes	The employee was unable to identify and report suspicious email which suggests more rigid training regarding spotting phishing/suspicious emails is required

---

Date:	**Entry:** 3

July 20, 2023 Wednesday @ 9:35 AM	
Description	Evaluate the ticket alert
Tool(s) used	Company's Playbook
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? - A HR employee ● **What** happened? - The employee received a suspicious email with an attachment and executed it. ● **When** did the incident occur? - Wednesday, July 20, 2023 @ 9:30 AM ● **Where** did the incident happen? - HR department ● **Why** did the incident happen? - The employee failed to identify the signs of a phishing email
Additional notes	Employee failed to identify and report the phishing email. There were clear signs present in the email such as grammatical mistakes, impersonation of trusted entity, email and username mismatch and an executable attachment which indicates that it was a phishing email. Employee has been assigned for retraining on how to spot phishing attempts.

Date: November 11, 2023	**Entry:** 4

Description	Reviewing the final report
Tool(s) used	NA
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? - A malicious actor ● **What** happened? - The attacker stole a large amount of customers' transactions data ● **When** did the incident occur? - December 22, 2022 at 7:20 PM ● **Where** did the incident happen? - The incident happened on the company's web application ● **Why** did the incident happen? - The attacker was able to exploit a vulnerability in company's web applicationvia forced browsing by modifying the order number available in the URL string
Additional notes	Security team recommended to implement allowlisting to allow specified set of URLs to prevent similar attacks in future.

Date: November 15, 2023 Wednesday @ 2:45 PM	**Entry:** 5
Description	Investigating the threat intelligence data

Tool(s) used	Chronicle
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? - A email from a suspicous domain ● **What** happened? - An employee received a phishing email from a suspicious domain which triggered the alert. After investigation, the team determined that upto 6 devices visited the suspicious domain. The devices involved in the accident were: ashton-davidson-pc, bruce-monroe-pc, coral-alvarez-pc, emil-palmer-pc, jude-reyes-pc, and roger-spence-pc. ● **When** did the incident occur? - November 15, 2023 @ 2:45 PM ● **Where** did the incident happen? - Email server ● **Why** did the incident happen? - Due to the lack of email filters
Additional notes	After investigating domain signin.office365x24.com on Chronicle, the domain was labelled malicious by security vendors on VirusTotal.Investigation also reveled that two of the six devices i.e., ashton-davidson-pc and emil-palmer-pc sent data to the suspicious domain on six different occasions. The domain is also categorized as Drop site for logs or stolen credentials by ET Intelligence Rep List. After analyzing the unresolved IP address, I noted that there was an additional device that made POST request to another suspicious domain which indicates successful phishing attempt. The device involved was warren-morris-pc which made a POST request to signin.accounts-gooqle.com/login.php which suggest that the device sent data to the suspicious domain.

Date: November 15, 2023	**Entry:** 6
Description	Reflection Entry
Tool(s) used	NA
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? - NA ● **What** happened? - NA ● **When** did the incident occur? - NA ● **Where** did the incident happen? - NA ● **Why** did the incident happen? - NA
Additional notes	1. Were there any specific activities that were challenging for you? Why or why not? - I found log analysis a bit challenging than any other topic in the program so far. The reason for this is that I'm still learning or familiarizing myself to all the components to thelog analysis. 2. Has your understanding of incident detection and response changed since taking this course? - Before taking this course, my understanding of incident detection and response was very limited to theoretical approach. I haven't had used any of the SIEM tools and incident journal entry. After using incident journal entry and

	SIEM tools, I feel more confident as I get to actually practice something. 3. Was there a specific tool or concept that you enjoyed the most? Why? - I really liked using Chronicle due to its simplicity. I found it easier to analyze log alerts via Chronicle than Splunk as I feel it is easier to get a detailed analysis.