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: Tuesday, 9:00 a.m.	**Entry:** #1
Description	Small US healthcare company was the victim of a ransomware attack on Tuesday at 9:00a.m. The incident was caused by a phishing email containing a malicious attachment. The threat actors demanded money in exchange for the decryption key for their data.
Tool(s) used	None

The 5 W's	Capture the 5 W's of an incident.
	• **Who** caused the incident?
	  ○ An organized group of unethical hackers caused the incident.
	• **What** happened?
	  ○ The group of threat actors sent a phishing email to employees containing a malicious attachment. Once downloaded, ransomware was deployed, encrypting the organization's computer files. The group left a ransom note and demanded money in exchange for the decryption key.
	• **When** did the incident occur?
	  ○ Tuesday at 9:00 a.m.

	• **Where** did the incident happen?
	  ○ The incident occurred in a small U.S. health care clinic.
	• **Why** did the incident happen?
	  ○ The incident occurred as a byproduct of the threat actor's motivation to profit off of the desperation of the small U.S. health care clinic for the return of their data. This was indicated by the ransomware note that the group of unethical hackers left.

Additional notes	The U.S health care clinic must implement employee training on phishing and social engineering attacks. The clinic should not pay the ransom to the group of unethical hackers.

Date: 1:20 pm	**Entry:** # 2
Description	A financial services company was the victim of a trojan attack at 1:20pm. The incident was caused by an employee opening a file attachment from an email containing a malicious payload.
Tool(s) used	None

The 5 W's	Capture the 5 W's of an incident.
	• **Who** caused the incident?
	  ○ The ATP Blacktech caused the incident.
	• **What** happened?
	  ○ Trojan malware was attached to a phishing email. The malicious payload was executed on the receiving computer when it was opened.

	• **When** did the incident occur?
	  ○ 1:20 pm
	• **Where** did the incident happen?
	  ○ The incident occurred at a financial services company.
	• **Why** did the incident happen?
	  ○ An employee received an email with a file attachment. When they opened the attachment, a malicious payload was executed on their computer.

Additional notes	This financial services company must implement better employee training to raise awareness about these types of attacks and how to avoid phishing attacks.

Date: 12/28/22 7:20 p.m.	**Entry:** # 3
Description	Reviewed the final report for a security breach.
Tool(s) used	None

5 W's	Capture the 5 W's of an incident.
	• **Who** caused the incident?
	  ○ A malicious threat actor.
	• **What** happened?
	  ○ an individual performed a ransomware attack. They stole customer data and threatened to release it to public forums if they were not compensated with $25,000. They later increased it to $50,000.

	• **When** did the incident occur?
	  ○ December 28, 2022, at 7:20 p.m., PT
	• **Where** did the incident happen?
	  ○ The incident occurred at a mid-sized retail company.
	• **Why** did the incident happen?
	  ○ the individual used a vulnerability on the e-commerce web application to perform a forced browsing attack. This gave them access to customer transaction data. They then sent the ransomware email to an employee who ignored it. They then sent a second one with higher demands.

Additional Notes	This mid-sized retail company must patch this vulnerability on the e-commerce website to ensure that an attack like this does not occur again. They should also implement better training to prepare employees for potential future attacks and how to respond better.

Date: N/A	**Entry:** # 4
Description	Performed a query with Splunk.
Tool(s) used	Splunk

Notes	• Hosts
	  ○ vendor_sales
	  ○ www1
	  ○ www3
	  ○ www2

	○ mailsv ● sourcetype ○ secure-2 ○ access_combined_wcookie ○ vendor_sales ● Number of events in the main index = 109.864

Date: N/A	**Entry:** # 5
Description	Exploring the signin.office365x24.com domain using Chronicle.
Tool(s) used	Chronicle
Notes	● Assets: ○ 6 assets in total ○ Asset names: ■ ashton-davidson-pc ■ bruce-monroe-pc ■ coral-alvarez-pc ■ emil-palmer-pc ■ jude-reyes-pc ■ roger-spence-pc ● POST requests for /login.php ○ ashton-davidson-pc

	■ Port: [Unknown], ashton-davidson-pc, 14:40:45 ■ Port: [Unknown], ashton-davidson-pc, 5:02:47 ■ Port: [Unknown], ashton-davidson-pc, 5:02:44 ○ emil-palmer-pc ■ Port: [Unknown], emil-palmer-pc, 14:42:45 ■ Port: [Unknown], emil-palmer-pc, 5:04:47 ■ Port: [Unknown], emil-palmer-pc, 5:04:44

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.

Reflections/Notes:

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

   Using the cybersecurity tools Splunk and Chronicle were challenging for me. I had no prior experience with using these tools and everything was new to me. It was very fun and challenging to navigate and figure out how they work.

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

My understanding of incident detection nad response has grown tremendously since taking this course. I have learned a great deal and am grateful for the opportunity.

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

   I enjoyed using Splunk and Chronicle for the challenge and their usefulness in the field. I will be using these tools in my career and it was great to be able to get practice with them in an environment that encouraged curiosity.