Incident handler's journal

Date: 11/2/2023	**Entry:** #1
Description	Ransomware Incident
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. • **Who**: An organized group of unethical hackers known for targeting organizations in healthcare and transportation industries • **What**: a ransomware attack that disrupted business operations by encrypting medical records • **When**: Tuesday at 9:00 a.m. • **Where**: At the small U.S. health care clinic • **Why**: to hold get money from the company
Additional notes	The attackers gained access via targeted phishing emails sent to several employees. These emails contained a malicious attachment that installed malware onto employee computers, encrypting medical files. A ransom note was displayed on employee computers. 1. The company should work to prevent these attacks from happening again. 2. The company should consider paying the ransom.

Date: 11/4/2023	**Entry:** #2
Description	I received a phishing alert about a suspicious file being downloaded on an employee's computer. After investigating the email attachment file's hash, the attachment has already been verified to be malicious.
Tool(s) used	List any cybersecurity tools that were used. • VirusTotal

The 5 W's	Capture the 5 W's of an incident.
	• **Who** caused the incident?
	  ○ An employee opening an email
	• **What** happened?
	  ○ The employee opened the email that contained a known malicious file
	• **When** did the incident occur?
	  ○ Wednesday, July 20, 2022 09:30:14 AM
	• **Where** did the incident happen?
	  ○ On the employees computer
	• **Why** did the incident happen?
	  ○ The employee was not aware that the email contained a malicious file.

Additional notes	Include any additional thoughts, questions, or findings.

Date: 11/7/2023	**Entry:** #3

Description	Analyzing a packet capture file
Tool(s) used	For a section in the course, I used Wireshark to analyze a packet capture file. Wireshark is a network protocol analyzer that uses a graphical user interface (GUI). Wireshark allows security analysts to capture and analyze network traffic, aiding in detections and investigations of malicious cyber activity.
The 5 W's	• **Who**: N/A • **What**: N/A • **Where**: N/A • **When**: N/A • **Why**: N/A
Additional notes	The interface has a lot of filtering and colorization options. It is a powerful asset for analyzing network traffic.

Date: 11/8/2023	**Entry:** #4
Description	As a security analyst working at the e-commerce store Buttercup Games, I've been tasked with identifying whether there are any possible security issues with the mail server. To do so, I must explore any failed SSH logins for the root account.
Tool(s) used	List any cybersecurity tools that were used. • Splunk
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? ○ N/A • **What** happened?

	○ N/A ● **When** did the incident occur? ○ N/A ● **Where** did the incident happen? ○ N/A ● **Why** did the incident happen? ○ N/A
Additional notes	SIEM tools such as Splunk are powerful tools to monitor networks and find suspicious activity.

Date: 11/11/23	**Entry:** #5
Description	I'm a level one security operations center (SOC) analyst at a financial services company and have received an alert about a suspicious file being downloaded on an employee's computer. I discovered that the employee received an email containing an attachment, which was a password-protected spreadsheet file. The spreadsheet's password was provided in the email. The employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer. I create a SHA256 hash of the file to use on VirusTotal to find IoCs.
Tool(s) used	List any cybersecurity tools that were used. ● Pyramid of Pain

	• VirusTotal website • SHA256 file hash

The 5 W's	Capture the 5 W's of an incident.
	• **Who** caused the incident?
	  ○ A threat actor sending an email to an employee
	• **What** happened?
	  ○ The employee received an email with an attachment that was password protected and downloaded the attachment, which contained malware.
	• **When** did the incident occur?
	  ○ 1:11 p.m.: An employee receives an email containing a file attachment.
	  ○ 1:13 p.m.: The employee successfully downloads and opens the file.
	  ○ 1:15 p.m.: Multiple unauthorized executable files are created on the employee's computer.
	  ○ 1:20 p.m.: An intrusion detection system detects the executable files and sends out an alert to the SOC.
	• **Where** did the incident happen?
	  ○ At the office on the employees computer
	• **Why** did the incident happen?
	  ○ The employee was not informed on phishing tactics and safe practices for emails.

Additional notes	We need to train all employees on phishing attacks so that they are aware of the signs of a malware attack.

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.
