Incident handler's journal

Date: 03/04/24	**Entry:** 1
Description	Documenting a cybersecurity incident.
Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? The incident was caused by a group of unethical hackers. • **What** happened? The group of hackers sent emails to several employees, once downloaded, the ransomware encrypted the organization's computer files, causing the company to shut down the computer systems. • **When** did the incident occur? The incident occurred Tuesday morning, at approximately 9:00 a.m. • **Where** did the incident happen? The incident happened at a health care company. • **Why** did the incident happen? The incident happened because one employee clicked the file attachment that the malicious actor sent via the email. Thus, the incident forced the organization to shut down the system.
Additional notes	Should the company pay the ransom to retrieve the decryption key?

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: 02/06/24	**Entry:** 3
Description	Investigating the email attachment file.
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An malicious actor. • **What** happened?

	An email that contains one malicious file attachment was sent to one employee. • **When** did the incident occur? The incident occurred Wednesday, July 20, 2022 09:30:14 AM. • **Where** did the incident happen? The incident has happened at a financial services company. • **Why** did the incident happen? The incident has happened because one employee accessed the file received via email.
Additional notes	Considering all of the above, those are clear signs of a malicious attempt. The incident was resolved using a Phishing incident response playbook.

Date: 02/06/24	**Entry:** 4
Description	Investigating the incident where an attacker gained access to PIIs using forced browsing technique.
Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? The incident was caused by an individual. • **What** happened? The attacker was able to perform forced browsing to access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page.

	• **When** did the incident occur? The incident occurred on December 22, 2022 at 3:13 p.m. • **Where** did the incident happen? The incident took place at a mid-sized retail company. • **Why** did the incident happen? The root cause of the incident was identified as a vulnerability in the e-commerce web application. This vulnerability allowed the attacker to perform a forced browsing attack.

Additional notes	The organization collaborated with the public relations department to disclose the data breach to its customers. Additionally, the organization offered free identity protection services to customers affected by the incident.
	
	And to prevent future recurrences, the next recommendations were taken:
	
	• Perform routine vulnerability scans and penetration testing.
	• Implement the following access control mechanisms:
	  ○ Implement allowlisting to allow access to a specified set of URLs and automatically block all requests outside of this URL range.
	  ○ Ensure that only authenticated users are authorized access to content.

Date: 02/07/24	**Entry:** 5
Description	Identifying security issues with the mail server.

Tool(s) used	Splunk
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An user. • **What** happened? An user tried to login from multiple accounts. • **When** did the incident occur? The incident occurred on Thu Feb 27 2023 01:39:51. • **Where** did the incident happen? The incident happened at the e-commerce store Buttercup Games.
Additional notes	

Date: 02/07/24	**Entry:** 6
Description	Perform a domain search for the domain contained in the phishing email.
Tool(s) used	Chronicle.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? The incident was caused by: ashton-davidson-pc, bruce-monroe-pc, coral-alvarez-pc, emil-palmer-pc, jude-reyes-pc, roger-spence-pc. • **What** happened? I received an alert that an employee received a phishing email in their inbox. Verifying the domain `signin.office365x24.com`

	I discovered that multiple employees received the email from this domain. • **When** did the incident occur? The incident occurred on 2024-02-5 at 14:40:40. • **Where** did the incident happen? The incident happened at a financial services company. • **Why** did the incident happen? The incident happened when employees received phishing emails and accessed it.
Additional notes	Following the Chronicle I discovered 6 POST requests to the /login.php page. POST also suggests a possible successful phish. Checking the IP address `40.100.174.34`, I also found 3 POST requests made to the /login.php page. After viewing the assets, I also discovered two more entries: amir-david-pc, warren-morris-pc. I also discovered a new Domain for this IP address: `signin.accounts-gooqle.com`

Date:	**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.