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: 24 May 2025	**Entry:** 1
Description	Documentation of cybersecurity incident
Tool(s) used	None
The 5 W's	● **Who**: Organized group of unethical hackers who are known to target organizations in healthcare and transportation industries. ● **What**: Employees were unable to access the files and software needed to do their job due to ransomware ● **When**: Tuesday morning, at approximately 9:00 a.m ● **Where**: At health care company ● **Why**: Hackers were able to gain access into the company's network by using targeted phishing emails which were sent to several employees. The phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded. Once the attackers gained access, they deployed their ransomware, which encrypted critical files. The hackers demanded a large sum of money in exchange for the decryption key, motivation seems to be for financial gain.

Additional notes	Employees required additional training to avoid phishing attacks. The company needs to decide if they should pay ransom.

Date: 25 May 2025	**Entry:** 2
Description	Investigation of phishing alert
Tool(s) used	None
The 5 W's	● **Who:** Def Communications / Clyde West ● **What:** Received phishing alert about a suspicious file being downloaded ● **When**: Wednesday, July 20, 2022 09:30:14 AM ● **Where:** HR's computer ● **Why:** Bad actor attempted to trick HR employee into downloading and opening malware into company's computer under guise of a job application
Additional notes	**Alert severity**: Medium **Sender details**: ● Email Address: 76tguyhh6tgftrt7tg.su (Lack of email domain name) ● IP Address: 114.114.114.114 **Subject line**: Re: Infrastructure Egnieer role (Contain typos) **Message body**: ● "Dear HR at Ingergy" (Typo of company name) ● "I am writing for to express my interest", "There is attached my resume and cover letter" (Grammar Error) **Attachments**: filename="bfsvc.exe" (executable file)

Date: 27 May 2025	**Entry:** 3
Description	Documentation of data theft incident
Tool(s) used	None
The 5 W's	● **Who:** Hacker ● **What:** Employee received email claiming sender had successfully stolen customer data and requested money in exchange for not releasing the data. Another email later received with a sample of the stolen customer data and an increased payment demand. ● **When**: December 22, 2022 3:13 pm & December 28, 2022 ● **Where:** At retail company's office ● **Why:** Root cause of was identified as a vulnerability in the e-commerce web application which allowed the attacker to perform forced browsing attack and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page. The attacker demanded money in exchange for not releasing the stolen customer data, leads to motivation being financial gain
Additional notes	Security team are taking following actions to prevent future recurrences: ● Perform routine vulnerability scans and penetration testing ● Implement the following access control mechanisms for URLs and authenticated users

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.

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: Record additional notes.