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: 10.15.25	**Entry:** 1
Description	Documenting a ransomware incident affecting a small U.S. health clinic.
Tool(s) used	None used – analysis based on scenario review only
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ Unauthorized hacker group targeting health care and transportation industries ● **What** happened? ○ The group gained access to the company's network using targeted phishing emails containing malicious attachments that installed malware to several employees. Once access was gained, the hackers deployed a ransomware demanding a high sum of money. ● **When** did the incident occur? ○ The incident occurred on Tuesday 10/14/25 at 9am as first reported by employees. ● **Where** did the incident happen?

	○ The incident occurred at a small health care clinic specializing in primary care services. ● **Why** did the incident happen? ○ The incident happened because employees were targeted with phishing emails containing corrupt attachments. The group requested a large ransom payment in exchange for the decryption key.
Additional notes	1. Employees were unable to access patients' medical files potentially causing issues with HIPPA 2. No tools were mentioned or email filtering the organization may have in place. 3. Recommend implementing phishing awareness training and email filtering to reduce risk of future incidents.

Date: 10.30.25	**Entry:** 2
Description	Investigating a suspicious file hash associated with a potential security incident involving a malicious attachment.
Tool(s) used	VirusTotal report
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ The responsible party for this incident is unknown ● **What** happened?

	○ An alert was triggered after an employee received an email containing a password protected attachment. Once downloaded and opened with the password provided in the email, a malicious payload was executed on the employee's computer. The attacker used a Trojan backdoor delivered via a Win32 EXE to gain persistent access. The file connected to multiple IP addresses some lacking ASN information and reached out to suspicious domains. The activity aligned with common backdoor behavior likely for remote command and control operations. ● **When** did the incident occur? ○ The incident has a scan timestamp of 9/14/2020 and detected through a system alert. ● **Where** did the incident happen? ○ On an employee workstation at a financial services company ● **Why** did the incident happen? ○ An employee was targeted with a phishing email containing a malicious password protected attachment, which they opened.
Additional notes	1. No information was provided on the impact that this incident had on the company. 2. Recommend implementing phishing awareness training for all employees to reduce future incidents. 3. The file contacted over 400 IP addresses suggesting scanning behavior.

Date: 11/4/25	**Entry:** 3
Description	Responding to phishing incident using alert A-2703
Tool(s) used	Phishing Playbook
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ A malicious actor carried out a phishing attempt by impersonating a job applicant and targeting an internal HR. email. ● **What** happened? ○ An employee received an email containing a password protected EXE file that was claimed to be a resume. The attacker included the password in the email body to encourage opening the attachment, which was later confirmed to be malicious. ● **When** did the incident occur? ○ The phishing email was received on Wednesday, July 20, 2022, at 9:30 AM, and a detection alert was triggered shortly after. ● **Where** did the incident happen? ○ The incident occurred at a financial service company, specifically involving an employee's workstation. ● **Why** did the incident happen? ○ The employee opened a password protected attachment from a suspicious email, falling victim to a social engineer tactic designed to bypass email filters and gain initial access.
Additional notes	• Recommend phishing awareness training for all employees to reinforce email safety and reduce human error. • Ticket was escalated due to a verified malicious attachment.

Date: 11/7/25	**Entry:** 4
Description	Final Report Review
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ An external attacker exploited a vulnerability in the company's e-commerce application. ● **What** happened? ○ An attacker exploited a vulnerability in the e-commerce application to perform a forced browsing attack. By modifying order numbers in purchase confirmation page URLs, they gained unauthorized access to approximately 50,000 customer records containing PII and financial information. The attacker initially demanded a $25k crypto ransom, later increasing it to $50k. The breach resulted in an estimated $100k in direct cost and lost revenue. The company disclosed the breach and provided affected customer with free identity protection. ● **When** did the incident occur? ○ The incident began on December 22, 2022 when an external ransom email was received at 3:13 PM (PST). The attacker sent a follow-up email on December 28, 2022 with sample stolen data. The breach was confirmed and investigated the same day at approximately 7:20PM (PST).

	● **Where** did the incident happen? ○ The incident was identified as a vulnerability in the e-commerce web application, affecting its online operations. ● **Why** did the incident happen? ○ The application failed to restrict access to sensitive URLs allowing the attacker to manipulate URL order numbers to access customer confirmation pages and exfiltrate data.
Additional notes	• Recommend routine vulnerability scans and penetration test. • Web server logs played a critical role in identifying the attack method. • Access enhancements and authentication should be enforced.

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.

Activity Overview

In this activity, you will review the details of a security incident and document the incident using your incident handler's journal. Previously, you learned about the importance of documentation in the incident response process. You've also learned how an incident handler's journal is used to record information about security incidents as they are handled.

Throughout this course, you can apply your documentation skills using your incident handler's journal. With this journal, you can record information about the experiences you will have analyzing security incident scenarios through the course activities.

By the time you complete this course you will have multiple entries in your incident handler's journal that you can use as a helpful reference to recall concepts and tools. Later, you'll add this document to your cybersecurity portfolio, which you can share with prospective employers or recruiters. To review the importance of building a professional portfolio and options for creating your portfolio, read Create a cybersecurity portfolio.

Be sure to complete this activity and answer the questions that follow before moving on. The next course item will provide you with a completed exemplar to compare to your own work.

Note: *You can use your incident handler's journal as a personal space where you can keep track of your learning journey as you learn about incident detection and response concepts and interact with different cybersecurity tools. Feel free to include your thoughts, reflections, and any other important details or information.*

Scenario

Review the following scenario. Then complete the step-by-step instructions.

A small U.S. health care clinic specializing in delivering primary-care services experienced a security incident on a Tuesday morning, at approximately 9:00 a.m. Several employees reported that they were unable to use their computers to access files like medical records. Business operations shut down because employees were unable to access the files and software needed to do their job.

Additionally, employees also reported that a ransom note was displayed on their computers. The ransom note stated that all the company's files were encrypted by an organized group of unethical hackers who are known to target organizations in healthcare and transportation industries. In exchange for restoring access to the encrypted files, the ransom note demanded a large sum of money in exchange for the decryption key.

The attackers were able to gain access into the company's network by using targeted phishing emails, which were sent to several employees of the company. 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 company was unable to access critical patient data, causing major disruptions in their business operations. The company was forced to shut down their computer systems and contact several organizations to report the incident and receive technical assistance.

Step 1: Access the template

To use the template for this course item, click the link and select *Use Template*.

Step 2: Review the scenario

Review the details of the scenario. Consider the following key details:

- A small U.S. health care clinic experienced a security incident on Tuesday at 9:00 a.m. which severely disrupted their business operations.
- The cause of the security incident was a phishing email that contained a malicious attachment. Once it was downloaded, ransomware was deployed encrypting the organization's computer files.
- An organized group of unethical hackers left a ransom note stating that the company's files were encrypted and demanded money in exchange for the decryption key

Step 3: Record a journal entry

Use the incident handler's journal to document your first journal entry about the given scenario. Ensure that you fill in all of the fields:

1. In the **Date** section, record the date of your journal entry. This should be the actual date that you record the entry, not a fictional date.
2. In the **Entry** section, provide a journal entry number. For example, if it is your first journal entry, enter 1.
3. In the **Description** section, provide a description about the entry.
4. In the **Tool(s) used** section, if any cybersecurity tools were used, list them here.
5. In the **The 5 W's** section, record the details about the given scenario.
    a. Who caused the incident?
    b. What happened?
    c. When did the incident occur?
    d. Where did the incident happen?
    e. Why did the incident happen?
6. In the **Additional notes** row, record any thoughts or questions you have about the given scenario.

Pro Tip: Save a copy of your work

Finally, be sure to save a copy of your incident handler's journal so that you can quickly access it as you progress through the course. You can use it for your professional portfolio to demonstrate your knowledge and/or experience to potential employers.

What to Include in Your Response

Be sure to include the following elements in your completed activity:

- The journal entry date and number
- A description of the journal entry
- 1-2 sentences addressing each of the 5 W's of the scenario:
    - Who caused the incident?
    - What happened?
    - When did the incident occur?
    - Where did the incident happen?
    - Why did the incident happen?
- 1-2 sentences on any additional thoughts or questions about the scenario.