



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: 7/31/2025	Entry: 1
Description	<ul style="list-style-type: none">• A small U.S. health care clinic experienced a security incident, specifically a ransomware attack on Tuesday at 9:00 a.m. which severely disrupted their business operations.
Tool(s) used	Phishing, Malware Attack,
The 5 W's	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none">• Who: An organized group of unethical hackers• What: The hackers sent targeted phishing emails which contained a malicious file attachment that installed malware on the employee's device when downloaded. This led to employees clicking on the email and as a result reporting that they were unable to use their computers to access files like medical records. Business operations were then shut down because employees were not able to access files or software needed to complete their jobs. There were reports of ransom notes being displayed on employee's computers demanding payment in exchange for decryption keys.• When: Tuesday 9am

	<ul style="list-style-type: none"> • Where: A small health clinic • Why: Hackers wanted money by blackmailing vulnerable health employees 		
Additional notes	The phishing attacks were reported to be targeted, meaning that they were personalized for the intended receiver. The clinic may need to practice prevention measures to make sure incidents like this never happen again.		

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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none">• 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	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none"> • 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	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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.
