



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: October 20	Entry: 1
Description	Documenting a cybersecurity incident
Tool(s) used	None
The 5 W's	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none">• Who caused the incident? An organized group of unethical hackers• What happened? They deployed ransomware on a small health care clinic• When did the incident occur? Tuesday at 9:00 AM• Where did the incident happen? At a health care clinic• Why did the incident happen? The incident happened because the group got access through a phishing attack. After gaining access, ransomware was deployed
Additional notes	<ol style="list-style-type: none">1. How can this be prevented from happening again?2. How much money was asked for? How do we know they won't try 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	<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.

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.

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.

<p>Reflections/Notes: Record additional notes.</p>
--