



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: 2024/04/18	Entry: 1
Description	This entry is about a ransomware attack that occurred to a small U.S. health care clinic. The business operations were down because employees were unable to access the files and software needed to do their job.
Tool(s) used	NA
The 5 W's	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none">• Who: Organised group of unethical hackers• What: Ransomware attack• When: Approximately 9:00 a.m.• Where: A small U.S. health care clinic• Why: The attackers sent several phishing emails to the company's employees. The phishing emails contained a malicious attachment that installed malware on the employee's computer once downloaded. Once the attacker gained access, they deployed their ransomware, encrypting critical files. The motive is likely financial due to them asking for a large sum of money to decrypt the files.
Additional notes	What security controls are in place to deal with phishing emails?

	What security training have the employees been trained on?
--	--

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	Entry: Record the journal entry number.
---------------------------------	---

of the journal entry.	
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.