



Incident handler's journalInstructions

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: Record the date of the journal entry.	Entry: Tuesday, 09/04/2024 0900,
Description	An unethical hacker group used ransomware to shut down a medical records system. They employed phishing emails to send malicious attachments to employees, facilitating the installation of malware and unauthorized access to the system.
Tool(s) used	Ransomware, Phishing, malware,
The 5 W's	<ul style="list-style-type: none">• Who: Unethical hacker group• What: Ransomware attack• When: 09:00, Tuesday• Where: A small U.S. health care clinic• Why: The incident occurred due to the exploitation of vulnerabilities in the clinic's system via phishing emails and subsequent deployment of ransomware.•
Additional notes	<ul style="list-style-type: none">• Business operations were severely disrupted due to the encryption of critical files.• Immediate technical assistance and reporting to relevant organizations were sought.• Strategies for data recovery and enhancing cybersecurity measures should be prioritized to prevent future incidents.

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.

Reflections/Notes: Record additional notes.