



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: Sep 10, 2025	Entry: # 1
Description	Documenting the Security 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? Ransomware Security Incident• When did the incident occur? Tuesday 9.00am• Where did the incident happen? A small U.S. health care clinic• Why did the incident happen? Hackers motivation is money as the ransom note demanded a large sum of money in exchange for the decryption key.
Additional notes	<ul style="list-style-type: none">• How should we prevent a similar kind of incident from the health care company in the future?• Is the company ready to pay in order to retrieve the decryption key?