



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: | Entry: |
| July 23, 2024 | #1 |
| Description | Documenting a cybersecurity incident |
| Tool(s) used | None |
| The 5 W's | <ul style="list-style-type: none">• Who: An organized group of unethical hackers• What: A ransomware security incident• Where: At a health care company• When: Tuesday, 9:00 a.m.• Why: The incident occurred because unethical hackers gained access to the company's systems through a phishing attack. Once inside, the attackers deployed ransomware, encrypting critical files. The motivation appears to be financial, as the ransom note demanded a large sum in exchange for the decryption key. |
| Additional notes | <ol style="list-style-type: none">1. How could the health care company prevent a similar incident in the future?2. Should the company pay the ransom to recover the encrypted data? |

