**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 January 24 | **Entry:**  1 | | |
| --- | --- | --- | --- |
| Description | Documenting a cybersecurity incident  This incident occurred in two of the NIST Incident Response Lifecyle:  **Detection and Analysis:** employees were unable to access files and a ransom note was displayed on their screens. The organization then reached out to other organizations for technical assistance.  **Containment, Eradication, and Recovery:** The organization shut down its computer systems. | | |
| Tool(s) used | N/A | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: An organized group of unethical hackers * **What**: A ransomware security incident that severely disrupted business operations * **When**: Tuesday at 9:00am * **Where**: A small US health care clinic * **Why**: Unethical hackers were able to access the clinic’s systems via a phishing email that contained a malicious attachment. Ransomware was deployed encrypting the organization’s computer files and a ransom note was left demanding money for the key to decrypt the information. | | |
| Additional notes | Employees should be educated on the latest social engineering tactics to minimize the risk of this same kind of threat from happening again.  Should the clinic pay the ransom for the decryption key to access their files? | | |