**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:** April 23,2025 | **Entry:**  #1 |
| Description | A phishing email with a malicious spreadsheet was opened by an employee. I retrieved the file, created a SHA256 hash, and confirmed through VirusTotal that it was malware. Related URLs and domains were flagged for further review. |
| Tool(s) used | SHA256 hashing tool, VirusTotal |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? A threat actor who sent a phishing email containing a malicious spreadsheet attachment. * **What** happened? The employee downloaded and opened a malicious spreadsheet, triggering a payload on their device. * **When** did the incident occur? The email was received and the file opened earlier today, April 23, 2025. * **Where** did the incident happen? The incident occurred on an employee’s workstation within the financial services company. * **Why** did the incident happen? The phishing email successfully tricked the employee into opening the malicious file by including the password and making it appear trustworthy. |
| Additional notes | Include any additional thoughts, questions, or findings. |