# 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:**<br>2024/04/18 | **Entry:**<br>1 |
|---|---|
| Description | This entry is about a ransomware attack that occurred to a small U.S. health care clinic. The business operations were down because employees were unable to access the files and software needed to do their job. |
| Tool(s) used | NA |
| The 5 W's | Capture the 5 W's of an incident.<br>• **Who:** Organised group of unethical hackers<br>• **What:** Ransomware attack<br>• **When:** Approximately 9:00 a.m.<br>• **Where:** A small U.S. health care clinic<br>• **Why:** The attackers sent several phishing emails to the company's employees. The phishing emails contained a malicious attachment that installed malware on the employee's computer once downloaded. Once the attacker gained access, they deployed their ransomware, encrypting critical files. The motive is likely financial due to them asking for a large sum of money to decrypt the files. |
| Additional notes | What security controls are in place to deal with phishing emails? |

| | |
|---|---|
| | What security training have the employees been trained on? |

---

| **Date:**<br>2024/04/22 | **Entry:**<br>2 |
|---|---|
| Description | This entry is about a trojan horse attack that occurred on an employee's computer of a financial services company. |
| Tool(s) used | TotalVirus |
| The 5 W's | Capture the 5 W's of an incident.<br>• **Who**: Threat actor BlackTech<br>• **What**: Trojan horse<br>• **When**: 1:11 p.m.<br>• **Where**: A financial services company<br>• **Why**: The attacker sent an employee of the company an email containing a password protected attachment and the password. The employee downloaded the file, then entered the password to open the file. A malicious payload was then executed on their computer. Due to the malware having input capture, it is likely it is designed to obtain credentials. |
| Additional notes | • The malware is a trojan under the name Flagpro commonly used by threat actor BlackTech<br>• What is the best way to prevent similar attack in the future |

---

| | |
|---|---|
| **Date:**<br>Record the date of the journal entry. | **Entry:**<br>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.<br>• **Who** caused the incident?<br>• **What** happened?<br>• **When** did the incident occur?<br>• **Where** did the incident happen?<br>• **Why** did the incident happen? |
| Additional notes | Include any additional thoughts, questions, or findings. |

---

| | |
|---|---|
| **Date:**<br>Record the date of the journal entry. | **Entry:**<br>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.<br>• **Who** caused the incident?<br>• **What** happened?<br>• **When** did the incident occur?<br>• **Where** did the incident happen?<br>• **Why** did the incident happen? |
| Additional notes | Include any additional thoughts, questions, or findings. |

---

| | |
|---|---|
| **Date:**<br>Record the date of the journal entry. | **Entry:**<br>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.<br>• **Who** caused the incident?<br>• **What** happened?<br>• **When** did the incident occur?<br>• **Where** did the incident happen?<br>• **Why** did the incident happen? |
| Additional notes | Include any additional thoughts, questions, or findings. |

| | |
|---|---|
| **Date:**<br>Record the date of the journal entry. | **Entry:**<br>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.<br>• **Who** caused the incident?<br>• **What** happened?<br>• **When** did the incident occur?<br>• **Where** did the incident happen?<br>• **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. |