# Incident Handler's Journal

## Instructions

Use this template throughout the course to record findings after activities, take notes on specific tools or concepts, and capture key takeaways from the cybersecurity topics you study.

| **Date:**<br>September 1, 2026 | **Entry:**<br>1 |
|---|---|
| Description | Logging what's currently known about a ransomware incident affecting a small primary-care clinic in the U.S.- operations ground to a halt after a phishing email opened the door for attackers. |
| Tool(s) used | No tools applied at this stage - this is a first-pass summary from incident reports. Going forward, I'd expect endpoint detection software, a SIEM platform, and network monitoring to come into play. |
| The 5 W's | Capture the 5 W's of an incident.<br>● **Who** caused the incident? A cybercrime ring with a history of hitting healthcare and transportation targets.<br>● **What** happened? Staff computers locked up and patient files became inaccessible after ransomware was quietly installed through a phishing email.<br>● **When** did the incident occur? Staff first noticed problems around 9 a.m. on a Tuesday, right as the clinic day was getting underway.<br>● **Where** did the incident happen? Inside the clinic's own IT environment - the malware spread across internal systems that staff rely on daily, cutting off access to patient records. |

| | |
|---|---|
| | ● **Why** did the incident happen? A staff member unknowingly triggered the attack by opening an attachment from a deceptive email, which handed the attackers a way in. From there, the motive looks purely financial, given the demand for payment in the ransom note. |
| Additional notes | It's striking that one employee clicking the wrong attachment was enough to bring the whole clinic to a stop. This makes me want to know more about the clinic's security awareness training before the attack, and whether paying cybercriminals ever actually guarantees the files come back safely. |

---

| | |
|---|---|
| **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. |

| | |
|---|---|
| **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. |