**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:**  2025-09-12 | **Entry:**  1 |
| Description | A phishing email attack was conducted against a small health care clinic. The attack deployed ransomware to computers on the network via an email attachment. A ransom note was displayed on computers that are infected. |
| Tool(s) used | **None** |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? Company employees * **What** happened? A phishing attack targeted employees to open an attachment that deployed ransomware on the organizations computers. * **When** did the incident occur? 2025-09-12 * **Where** did the incident happen? unknown * **Why** did the incident happen? Users opened an attachment that was sent by an outside email. |
| Additional notes | Include any additional thoughts, questions, or findings.  1. Was the email address a known bad actor email that has done this type of attack in the past?  2. Does the email server\or device scan for known ransomware attachments coming into the company.  3. Are there computer policies that disable running executable directly from the document\attachment? |

|  |  |
| --- | --- |
| **Date:**  9/16/2025 | **Entry:**  2 |
| Description | Phishing email received by the HR mailbox. |
| Tool(s) used | Used VirusTotal to determine if the hash of the attached file matched any threats. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? Email sent from Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114> * **What** happened? Email contained trojan attachment * **When** did the incident occur? Wednesday, July 20, 2022 09:30:14 AM * **Where** did the incident happen? HR inbox * **Why** did the incident happen? User may have opened the attachment |
| Additional notes | Include any additional thoughts, questions, or findings.  Attached file name bfsvc.exe, file looks to be malicious. Following phishing incident response playbook and esscalating to level 2.  Senders email address and IP were suspect. <76tguyhh6tgftrt7tg.su> <114.114.114.114>  Spelling mistakes in the email and poor grammer. |

|  |  |
| --- | --- |
| **Date:**  9/16/2025 | **Entry:**  3 |
| Description | Use Suricata to generate logs using pcap sample file |
| Tool(s) used | Suricata |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? NA * **What** happened? Used sudo suricata -r sample.pcap -S custom.rules -k none to generate suricata logs * Viewed json logs with jq . /var/log/suricata/eve.json | less * **When** did the incident occur? NA * **Where** did the incident happen? NA * **Why** did the incident happen? NA |
| Additional notes | Running Suricata generated a number of log files as part of the exercise the fast.log and eve.json log files were used as part of the investigation of logs generated by the tool. |

|  |  |
| --- | --- |
| **Date:**  9/16/2025 | **Entry:**  **4** |
| Description | Imported log data into splunk Cloud |
| Tool(s) used | Splunk Cloud |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? NA * **What** happened? Imported 8 log files to Splunk to run queues against. For a simulated Splunk event data. * **When** did the incident occur? NA * **Where** did the incident happen? NA * **Why** did the incident happen?NA |
| Additional notes | Ran some initial queues on the data to view the various log files  example: source="tutorialdata.zip:\*" host=vendor\_sales |

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

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