**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:** 06/08/23  Record the date of the journal entry. | **Entry:1**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Documenting a cybersecurity incident | | |
| Tool(s) used | None | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? (external threat , organized group of unethical hackers ) * **What** happened? ( Deployed a ransomware attack using phishing ) * **When** did the incident occur? ( this morning at 9 am ) * **Where** did the incident happen? ( A health care company ) * **Why** did the incident happen? ( an employee clicked a link that had malicious code in it ) | | |
| Additional notes | We need to provide the proper training so that employees dont provide malicious actors with an easy way to compromise our systems | | |

| **Date:** 06/09/23  Record the date of the journal entry. | **Entry:2**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Investigating a suspicious file hash | | |
| Tool(s) used | virustotal | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? ( a malicious hacker) * **What** happened? ( an employee at the company opened an email sent by a hacker and once the employee opened the file using the password provided in the email. A malicious payload was downloaded to their computer ) * **When** did the incident occur? ( 1:11 pm) * **Where** did the incident happen? ( A finacial company) * **Why** did the incident happen? ( Because an employee accessed a suspicious file which then downloaded malware on the computer) | | |
| Additional notes | We need to provide more coaching on how employees can limit their risk of being an unintentional internal threat. We can also limit the amount of threats by blocking known hash values that are associated with this malware. | | |

| **Date:** 06/09/23  Record the date of the journal entry. | **Entry:3**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Using a playbook to respond to a phishing attack | | |
| 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? (Malicious hacker ) * **What** happened? ( employee clicked on a file with a hash value that is known as malicious * **When** did the incident occur? ( 07/20/23) * **Where** did the incident happen? ( at a finance company) * **Why** did the incident happen? ( employee clicked on a link in a phishing email | | |
| Additional notes | Include any additional thoughts, questions, or findings. | | |

| **Date:** 06/10/23  Record the date of the journal entry. | **Entry:4**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Performing a query with chronicle | | |
| Tool(s) used | Chronicle | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? ( malicous hacker ) * **What** happened? ( two employees potentially clicked on phishing emails. ) * **When** did the incident occur? (once on january 1st 2023) * **Where** did the incident happen? ( At an e-commerce company) * **Why** did the incident happen? ( employee clicked on a suspicious email that based on the research i did on virus total and google chronicle i was able to see that the threat intellegence on this device suspects it to be a site that should be dropped as it collects site logs or login credentials. And we need to act now because i was able to look at the timeline in chronicle and is shows a couple of post notifications in the raw log data. This means that the phishing attacks may have already happened. | | |
| Additional notes | Chronicle has a nice free software to use with a really great gui dashboard. | | |

| **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.  Were there any specific activities that were challenging for you? Why or why not?  The ids activities were difficult because there was so much information to unpack and retain.  -Has your understanding of incident detection and response changed since taking this course?  Definitely before this course i had never had hands on experience with ids platforms or even knew that companies use playbooks. before but after getting that experience i definitely have a better understanding of incident detection and response  -Was there a specific tool or concept that you enjoyed the most? Why?    I had a blast using chronicle . i love the layout . It allows you to see so many important pieces of data with a couple clicks and i think its very easy to use. |
| --- |
|  |