**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:**  Record the date of the journal entry. | **Entry:**  01 | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry.  This is on a security incident for a healthcare service where targeted phishing emails lead to a ransomware attack disrupting business operations by holding clients health data | | |
| Tool(s) used | List any cybersecurity tools that were used.  Hackers used encryption  Hackers used phishing emails | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   Unethical hackers   * **What** happened?   Hackers sent targeted phishing emails to employees at a health clinic which contained a malicious attachment when installed it encrypts all the client medical records impairing business operations   * **When** did the incident occur?   Tuesday morning approximately 9:00 am   * **Where** did the incident happen?   In a health care clinic   * **Why** did the incident happen?   Result of employees downloading a malicious attachment through a phishing email | | |
| Additional notes | Who were the phishing emails claiming to be ? | | |

| **Date:**  Record the date of the journal entry. | **Entry:**  02 | | |
| --- | --- | --- | --- |
| Description | This is investigating a possible malicious hash with virustotal after a employee received an email with a malicious attachment which executed a payload when a password was provided | | |
| Tool(s) used | virustotal | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   Employee of the company   * **What** happened?   They received an email with an attachment and then entered a password to open the attachment which executed the malware   * **When** did the incident occur?   Wednesday, July 20, 2022 09:30:14 AM   * **Where** did the incident happen?   It happened onsite at the company on a work computer   * **Why** did the incident happen?   The employee did not verify integrity of email attachment or check with someone before executing it | | |
| Additional notes | The sending email does not appear legitimate, it is just random letters and numbers. There are also several spelling mistakes/broken english in the email indicating it may not be legitimate. | | |

| **Date:**  Record the date of the journal entry. | **Entry:**  03 | | |
| --- | --- | --- | --- |
| Description | Identifying possible security issues for an e-commerce stores mail server | | |
| Tool(s) used | Splunk | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   Hacker ?   * **What** happened?   Unsuccessful root login attempts   * **When** did the incident occur?   06/03/2023   * **Where** did the incident happen?   Was happening from a variety of IP addresses   * **Why** did the incident happen?   Attempt to gain a high privilege account | | |
| Additional notes | All failed login attempts for root user | | |

| **Date:**  Record the date of the journal entry. | **Entry:**  04 | | |
| --- | --- | --- | --- |
| Description | Determine if employees have received phishing emails by identifying a suspicious domain name in the emails body. | | |
| Tool(s) used | Chronicle | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   Hacker using domain name signin.office365x24.com domain in email   * **What** happened?   Assets accessed a domain and submitted login information   * **When** did the incident occur?   2023-01-31   * **Where** did the incident happen?   On site at the financial service company   * **Why** did the incident happen?   Hacker is trying to gain access to an employees account through phishing | | |
| Additional notes | Several POST requests found from different employees | | |

| **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. |
| --- |