**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:**  12/02/2023 | **Entry:**  Document 1 | | |
| --- | --- | --- | --- |
| Description | * A small U.S. health care clinic experienced a security incident on Tuesday at 9:00 a.m. which severely disrupted their business operations. * The cause of the security incident was a phishing email that contained a malicious attachment. Once it was downloaded, ransomware was deployed encrypting the organization's computer files. * An organized group of unethical hackers left a ransom note stating that the company's files were encrypted and demanded money in exchange for the decryption key | | |
| Tool(s) used | NONE | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * An organized group of unethical hackers * **What** happened? * The cause of the security incident was a phishing email that contained a malicious attachment. Once it was downloaded, ransomware was deployed encrypting the organization's computer files. * **When** did the incident occur? * Tuesday at 9:00 a.m.. * **Where** did the incident happen? * A small U.S. health care clinic * **Why** did the incident happen? * phishing email that contained a malicious attachment. Once it was downloaded, ransomware was deployed encrypting the organization's computer files. | | |
| Additional notes | Unethical Hackers, Phishing Email, Ransomware, Encrypting computer files. | | |

| **Date:**  12/18/23 | **Entry:**  Number 2 | | |
| --- | --- | --- | --- |
| Description | Employee receives a phishing email that contains a malware file and might be opened the attachments or clicked the link | | |
| Tool(s) used | Playbook | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114> * **What** happened? * Employee probably opened a phishing email that contains malware. * **When** did the incident occur? * Wednesday, July 20, 2022 09:30:14 AM * **Where** did the incident happen? * Through email from hr * **Why** did the incident happen? * A malicious actor posing as a person looking for a job and sending an email that contains a malware file. | | |
| Additional notes | How can i avoid this email in future times and why does he send a phishing email to hr. | | |

| **Date:**  12/19/23 | **Entry:**  Document 3 | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry. | | |
| Tool(s) used |  | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * email sender * **What** happened? * An email sender claimed that they had successfully stolen customer personal identifiable information and financial information. * **When** did the incident occur? * On 3:13 p.m., PT, on December 22, 2022, * **Where** did the incident happen? * From the organization * **Why** did the incident happen?   -The root cause of the incident was identified as a vulnerability in the e-commerce web application. This vulnerability allowed the attacker to perform a forced browsing attack and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page. This vulnerability allowed the attacker to access customer purchase confirmation pages, exposing customer data, which the attacker then collected and  exfiltrated. | | |
| Additional notes | How are we gonna make sure our website is secured from an attacker? | | |

| **Date:**  Record the date of the journal entry. | **Entry:**  4 | | |
| --- | --- | --- | --- |
| 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. | | |

| **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. |
| --- |