**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:**  9/8/24 | **Entry:**  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? A group of unethical hackers. * **What** happened? They deployed phishing software to employees’ email addresses to gain access to their server. From there, they used a ransomware attack to encrypt files and demand payment for their return. * **When** did the incident occur? Tuesday at 9:00 a.m. * **Where** did the incident happen? A small U.S. healthcare clinic * **Why** did the incident happen? An employee had clicked on an attached document that had malware on it, thus encrypting the computer and the server. | | |
| Additional notes | Include any additional thoughts, questions, or findings. | | |

| **Date:**  9/9/24 | **Entry:**  2 | | |
| --- | --- | --- | --- |
| Description | The organization experienced a security incident on December 28, 2022, at 7:20 p.m., PT, during which an individual was able to gain unauthorized access to customer personal identifiable information (PII) and financial information. Approximately 50,000 customer records were affected. The financial impact of the incident is estimated to be $100,000 in direct costs and potential loss of revenue. The incident is now closed and a thorough investigation has been conducted. | | |
| Tool(s) used | None. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? Unethical hackers * **What** happened? Ransomware attack on an employee * **When** did the incident occur? December 28, 2022 at 7:20 PM * **Where** did the incident happen? An office * **Why** did the incident happen? Vulnerability in the e-web application allowed the hacker 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. | | |
| Additional notes | Include any additional thoughts, questions, or findings. | | |

| **Date:**  9/9/24 | **Entry:**  3 | | |
| --- | --- | --- | --- |
| Description | Capturing my first packet | | |
| Tool(s) used | I used tcpdump to capture and analyze network traffic. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: N/A * **What**: N/A * **Where**: N/A * **When**: N/A * **Why**: N/A | | |
| Additional notes | I'm still new to using the command-line interface, so using it to capture and filter network traffic was a challenge. I got stuck a couple of times because I used the wrong commands. But after carefully following the instructions and redoing some steps, I was able to get through this activity and capture network traffic. | | |

| **Date:**  9/10/24 | **Entry:**  4 | | |
| --- | --- | --- | --- |
| Description | Investigate a suspicious file hash | | |
| Tool(s) used | VirusTotal | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: An unknown malicious actor * **What**: An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b * **Where**: An employee's computer at a financial services company * **When**: At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file * **Why**: An employee was able to download and execute a malicious file attachment via e-mail. | | |
| Additional notes | How can this incident be prevented in the future? Should we consider improving security awareness training so that employees are careful with what they click on? | | |

| **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. |
| --- |