**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.  12/12/2023 | **Entry:**  Record the journal entry number.  **#1** |
| Description | Provide a brief description about the journal entry.   * 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 | 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?  1. An organized group of unethical hackers. 2. They left a ransom note stating that the company's files were encrypted and demanded money in exchange for the decryption key. 3. The clinic experienced a security incident on Tuesday at 9:00 a.m. which severely disrupted their business operations. 4. A small U.S. health care clinic experienced the security incident. 5. The attackers were able to gain access into the company's network by using targeted phishing emails, which were sent to several employees of the company. The phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded. |
| Additional notes | Include any additional thoughts, questions, or findings.  A plan must be done once the control is back, sanitize the systems to remove the malware from all the affected computers, and improve the security posture against phishing. |

|  |  |
| --- | --- |
| **Date:** 26/12/2023 | **Entry: #2** |
| Description | Received an alert about a suspicious file being downloaded on an employee's computer at a financial services company. |
| Tool(s) used | The **sha256sum** function is used to create a digest from the malicious file.  Then, with the hash file, we identify additional IoCs associated with the malicious file using **VirusTotal**. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   An email containing an attachment. The attachment was a password-protected spreadsheet file. The spreadsheet's password was provided in the email.   * **What** happened?   Multiple unauthorized executable files are created on the employee's computer. An intrusion detection system detects the executable files and sends out an alert to the SOC.   * **When** did the incident occur?   An employee receives an email containing a file attachment at 1:11 p.m.   * **Where** did the incident happen?   When the employee opened the file, a malicious payload was then executed on their computer.   * **Why** did the incident happen?   The employee downloaded the file, then entered the password to open the file. |
| Additional notes | After using the hash 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b on VirusTotal, it is confirmed that the malicious file is a trojan that creates a backdoor on the computer. |

|  |  |
| --- | --- |
| **Date:**  26/12/2023 | **Entry:**  #3 |
| Description | Phishing attempt possible download of malware. |
| Tool(s) used | Phishing Incident Response Playbook. |
| The 5 W's | Here are the 5 W’s:   * Who: the email with the attached malicious file caused the incident. * What: after opening the attached file, the trojan was installed in the computer, compromising the security of the organization. * When: the incident occurred when the email was received. * Where: the incident occurred in the computer of the employee. * Why: it happened because the file attached was opened. |
| Additional notes | Here are the comments after following the Phishing Incident Response Playbook:   * Evaluating the alert as “Medium”, this incident may require escalation. * Sender details: the sender’s email address is 76tguyhh6tgftrt7tg.su, and the IP address is 114.114.114.114. * Message: the email has the indicators of a phishing attempt. The subject line and body contain grammatical errors. * Attachments: the email has an attachment that is protected by a password (paradise10789) to probably avoid being initially detected by any antivirus. The file is an executable (bfsvc.exe). * After investigating the suspicious file attached in the email, it’s confirmed that it’s a malicious file.   Since the file received is confirmed to be malicious, and it was opened, this ticket status will be changed to “Escalated” according to step 3.2 of the Phishing Incident Response Playbook. |

|  |  |
| --- | --- |
| **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. |

|  |  |
| --- | --- |
| **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. |