**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:** 6/8/2023 | **Entry:1**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Health care clinic Ransomware attack through phishing email | | |
| Tool(s) used | none | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * Hackers/employees * **What** happened? * The computer's files were encrypted by the ransomware * **When** did the incident occur? * Tuesday 9:00 a.m * **Where** did the incident happen? * In the health care clinic * **Why** did the incident happen? * Because the employees were not trained in identifying phishing emails. An employee opened a malicious attachment that installed ransomware on the employees computers that encrypted their files in exchange for a large sum of money. | | |
| Additional notes | Include any additional thoughts, questions, or findings. | | |

| **Date:**  8/8/2023 | **Entry:2**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Gmail Phishing attack through malicious payload file attachment | | |
| Tool(s) used | SHA256sum and VirusTotal website | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * An employee * **What** happened? * A employee opened a malicious file * **When** did the incident occur? * 1:11 p.m * **Where** did the incident happen? * At a financial service company * **Why** did the incident happen? * An employee received a phishing email containing a malicious attachment. * The attachment was a password-protected spreadsheet file. The spreadsheet’s password was provided in the email. * The employee downloaded the file, then entered the password to open the file when the employee opened the file, a malicious payload was then executed on their computer | | |
| Additional notes | Include any additional thoughts, questions, or findings.  The extracted SHA256 file **hash:** 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b  VirusTotal had 57 security vendors and 2 sandboxed flagg the file as malicious | | |

| **Date:**  9/8/2023 | **Entry:3**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Alert Ticket-SERVER-MAIL Phishing attempt possible download of malware | | |
| 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? * HR employee at Inergy * **What** happened? * A phishing email was send to a Hr employee containing malware * **When** did the incident occur? * Wednesday, July 20, 2022 09:30:14 AM * **Where** did the incident happen? * At the Inergy company * **Why** did the incident happen? * An employee received a phishing email containing a malicious attachment. * The attachment was a password-protected spreadsheet file. The spreadsheet’s password was provided in the email. * The employee downloaded the file, then entered the password to open the file when the employee opened the file, a malicious payload was then executed on their computer   The phishing alert is not legitimate because it is coming from a strange email address and it is full with grammatical errors  Also the file send is not a resume cover letter as the email states it is in fact an executable file. | | |
| Additional notes | * **Alert severity**   + **Medium: May require escalation** * **Receiver Details**   + The receiver’s email address     - [hr@inergy.com](mailto:hr@inergy.com)   + The receiver’s Ip address     - 176.157.125.93 * **Sender details**   + The sender’s email address     - 76tguyhh6tgftrt7tg.su   + The sender’s Ip address     - 114.114.114.114 * **Subject Line**   + Re: Infrastructure Egnieer role * **Message body**   + Dear HR at Ingergy,  I am writing for to express my interest in the engineer role posted from the website.  There is attached my resume and cover letter. For privacy, the file is password protected. Use the password paradise10789 to open.   Thank you,  Clyde West * **Attachment or links**   + Attachment: filename="bfsvc.exe" | | |

| **Date:**  10/8/2023 | **Entry:4**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Review of closed incident - Unauthorized access to customers PII and financial information | | |
| 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? * The email sender * **What** happened? * Sender is demanding $50.000 in crypto for not leaking stolen customer data * **When** did the incident occur? * on December 28, 2022, at 7:20 p.m., PT, * **Where** did the incident happen? * At a retail company * **Why** did the incident happen? * Vulnerability in the e-commerce web application. The threat actor accessed 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:**  12/8/2023 | **Entry:5**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Identifying possible security issues / failed ssh login attempts on the root account | | |
| Tool(s) used | Splunk | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * Multiple failed logins * **What** happened? * Multiple failed ssh login attempts * **When** did the incident occur? * 02/27/2023 to 03/06/2023 * **Where** did the incident happen? * On the buttercup games mail server * **Why** did the incident happen? * Because multiple people tried to unsuccessfully login | | |
| Additional notes | Include any additional thoughts, questions, or findings. | | |

| **Date:**  12/8/2023 | **Entry:6**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Phishing emails containing *signin.office365x24.com domain* | | |
| Tool(s) used | Google chronicle | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * Threat actor * **What** happened? * Phishing email was received containing *signin.office365x24.com domain* * **When** did the incident occur? * Not specified * **Where** did the incident happen? * Not specified * **Why** did the incident happen? * Email was sent by a Threat actor | | |
| Additional notes | *Signin.office365x24.com* Only 1/88 vendors flagged the domain as malicious on virustotal  [Office365x24.com](https://www.virustotal.com/gui/search/office365x24.com) 5/88 had flagged the domain as malicious and sophos had flagged it for malware  ET Intelligence Rep List has category of Drop site for logs or stolen credentials  Assets  Ashton-davidson-pc  Jude-reyes-pc  Coral-alvarez-pc  Emil-palmer-pc  Ashton-davidson-pc made a sucsessful Post request to /login.php | | |

### 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. |
| --- |