**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:**  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:** 8th of November 2021. | **Entry:**  1 | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry.  A small U.S Healthcare Clinic Ransomware security incident | | |
| Tool(s) used | List any cybersecurity tools that were used.  Phishing tools. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? The employees of the hospital * **What** happened? They opened a phishing email. * **When** did the incident occur? Tuesday 9am * **Where** did the incident happen? A small US hospital * **Why** did the incident happen? Some employees downloaded a phishing email that encrypted some important documents of the Clinic. | | |
| Additional notes | Include any additional thoughts, questions, or findings. They should employ a cybersecurity expert and dont pay the ransom because they would just ask for more | | |

| **Date:**  Record the date of the journal entry. | **Entry:2**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry. **Investigate a suspicious file hash** | | |
| Tool(s) used | List any cybersecurity tools that were used.  VirusTotal | | |
| 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: 3**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry. | | |
| Tool(s) used | List any cybersecurity tools that were used. Playbook, VirusTotal | | |
| Comments about the incident | 57 of 72 flagged the file as malicious file therefore it is unsafe to download. | | |
| 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? * **ho caused the incident;** Def Communications * **What happened:** A threat actor sent a malicious file * **When did it take place**: July 20, 2022 * **Why;** He is trying to gain access. * **Where did the incident occur; Ingergy** | | |
| Additional notes | Include any additional thoughts, questions, or findings.   * **At the end of this step, you should have 2-3 reasons on why you believe the phishing alert is or isn't legitimate.** * The first one is incorrect spelling and the second reason is that it is a forwarded email. * **Should the alert be escalated:** Yes it should be escalated because it was discovered that it was malicious software. It is malicious because 50 of 72 external vendors of VirusTotal discovered it as malicious. I chose to escalate this ticket to a level 2 SOC analyst to take further action. | | |

| **Date:**  Record the date of the journal entry. | **Entry: 4**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry.  **FINAL REPORT** | | |
| Tool(s) used | List any cybersecurity tools that were used. Vulnerability scans | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? An unauthorised user * **What** happened? He used forced browsing to gain unauthorised access to Personal Identifiable Information PII and financial information. * **When** did the incident occur? December 28, 2022, at 7;20 p.m., * **Where** did the incident happen? At a mid-sized retail company * **Why** did the incident happen? There was a vulnerability in the e-commerce web application. | | |
| Additional notes | Include any additional thoughts, questions, or findings. | | |

| **Date:**  Record the date of the journal entry. | **Entry:5**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry.  **Chronicle Search for Phishing Email** | | |
| Tool(s) used | List any cybersecurity tools that were used.  **Chronicle, VirusTotal** | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? signin.office365x24.com * **What** happened? An employee received a phishing alert * **When** did the incident occur? 2024-12-08T10:52:06.647 * **Where** did the incident happen? n/A * **Why** did the incident happen? An Attacker is trying to receive sensitive information | | |
| **POST REQUEST TO THE LOGIN/PHP** | **2023-01-31 Asset Identifier FullyQualifiedDomanainName**  [**14:40:45**](https://demo.backstory.chronicle.security/assetResults?assetIdentifier=ashton-davidson-pc&assetType=hostname&namespace=%5Buntagged%5D&referenceTime=2023-01-31T14%3A40%3A45.000Z&selectedList=AssetViewTimeline&startTime=2023-01-31T14%3A34%3A05.000Z&endTime=2023-01-31T14%3A44%3A05.000Z&selectedTab=chart&selectedDomain=signin.office365x24.com&selectedEventTimestamp=2023-01-31T14%3A40%3A45Z) **ashton-davidson-pc signin.office365x24.com**  [**14:42:45**](https://demo.backstory.chronicle.security/assetResults?assetIdentifier=emil-palmer-pc&assetType=hostname&namespace=%5Buntagged%5D&referenceTime=2023-01-31T14%3A42%3A45.000Z&selectedList=AssetViewTimeline&startTime=2023-01-31T14%3A36%3A05.000Z&endTime=2023-01-31T14%3A46%3A05.000Z&selectedTab=chart&selectedDomain=signin.office365x24.com&selectedEventTimestamp=2023-01-31T14%3A42%3A45Z) **emil-palmer-pc signin.office365x24.com** | | |
| **ASSESTS AFFECTED BY OFFICE364X24** | **ashton-davidson-pc**  **First accessed: January 31, 2023**  **Last accessed: July 09, 2023**  **.bruce-monroe-pc**  **First accessed: January 31, 2023**  **Last accessed: July 09, 2023**  **coral-alvarez-pc**  **First accessed: January 31, 2023**  **Last accessed: July 09, 2023**  **emil-palmer-pc**  **First accessed: January 31, 2023**  **Last accessed: July 09, 2023**  **jude-reyes-pc**  **First accessed: January 31, 2023**  **Last accessed: July 09, 2023**  **roger-spence-pc**  **First accessed: January 31, 2023**  **Last accessed: July 09, 2023** | | |
| **RESOLVED IP ADDRESS POST RESULTS**  **40.100.174.34** | [**14:40:45**](https://demo.backstory.chronicle.security/assetResults?assetIdentifier=ashton-davidson-pc&assetType=hostname&namespace=%5Buntagged%5D&referenceTime=2023-01-31T14%3A40%3A45.000Z&selectedList=AssetViewTimeline&startTime=2023-01-31T14%3A34%3A05.000Z&endTime=2023-01-31T14%3A44%3A05.000Z&selectedTab=chart&selectedDestinationIp=40.100.174.34&selectedEventTimestamp=2023-01-31T14%3A40%3A45Z) **ashton-davidson-pc 40.100.174.34** | | |
| **POST RESULTS-**  **Port: [Unknown]**  **Resp. Code: 200**  **Resp. Size: 19,181 (bytes)**  **Port: [Unknown]**  **Resp. Code: 200**  **Resp. Size: 19,181 (bytes)** | | |
| **ADDITIONAL AFFECTED ASSETS** | **amir-david-pc**  **First accessed: January 31, 2023**  **Last accessed: January 31, 2023**  **ashton-davidson-pc**  **First accessed: January 31, 2023**  **Last accessed: January 31, 2023**  **bruce-monroe-pc**  **First accessed: January 31, 2023**  **Last accessed: January 31, 2023**  **coral-alvarez-pc**  **First accessed: January 31, 2023**  **Last accessed: January 31, 2023**  **emil-palmer-pc**  **First accessed: January 31, 2023**  **Last accessed: January 31, 2023**  **jude-reyes-pc**  **First accessed: January 31, 2023**  **Last accessed: January 31, 2023**  **roger-spence-pc**  **First accessed: January 31, 2023**  **Last accessed: January 31, 2023**  **warren-morris-pc**  **First accessed: January 31, 2023**  **Last accessed: January 31, 2023** | | |
| **ADDITIONAL DOMAINS** | **signin.accounts-gooqle.com**  **First accessed: January 31, 2023**  **Last accessed: July 09, 2023**  **signin.office365x24.com**  **First accessed: January 31, 2023**  **Last accessed: July 09, 2023** | | |
| Additional notes | Include any additional thoughts, questions, or findings.  **NAMES AND NUMBER OF ASSETS THAT HAVE ACCESSED THE DOMAIN**  **1.ashton-davidson-pc**  **First accessed: January 31, 2023**  **Last accessed: July 09, 2023**  **2. bruce-monroe-pc**  **First accessed: January 31, 2023**  **Last accessed: July 09, 2023**  **3. coral-alvarez-pc**  **First accessed: January 31, 2023**  **Last accessed: July 09, 2023**  **4. emil-palmer-pc**  **First accessed: January 31, 2023**  **Last accessed: July 09, 2023**  **5. jude-reyes-pc**  **First accessed: January 31, 2023**  **Last accessed: July 09, 2023**  **6. roger-spence-pc**  **First accessed: January 31, 2023**  **Last accessed: July 09, 2023** | | |
|  |  | | |

### 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. |
| --- |