**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: 6/23/24**  Tuesday, 9am | **Entry:**  0001 | | |
| --- | --- | --- | --- |
| Description | Ransomware security incident | | |
| Tool(s) used | None | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who:** Unethical Hackers * **What:**Ransomware security incident * **When:** Tuesday 9am * **Where** US, small health care company - office * **Why** Employee responded to phishing email. Threat actors were able to access company data and encrypt all data. Threat actors are holding it for ransom. | | |
| Additional notes | How do we avoid events like this in the future? Education on Phishing needs addressing.  Should the company pay the ransom? | | |

| **Date:**  6/20/22 | **Entry:**  0002 | | |
| --- | --- | --- | --- |
| Description | Suspicious File download | | |
| Tool(s) used | SHA256 VirusTotal | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? Threat actor * **What** happened? 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. * **When** 6/20/22 1:20 pm IDS detects the executable file. * **Where** did the incident happen? Main office financial service company. * **Why** did the incident happen? Employee was tricked into opening a malicious file. | | |
| Additional notes | Need PD on identifying threats, also need to sanitize stations and check other stations for similar infections. | | |

| **Date:**  6/22/22 | **Entry:**  0003 | | |
| --- | --- | --- | --- |
| Description | Alert ticket was received to investigate a potential malicious phishing file. | | |
| Tool(s) used | SHA256 VirusTotal | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? “Clyde West” threat actor * **What** Phishing file opened and possible malware installed * **When** 6/22/22 9:30am * **Where** Office - HR * **Why** HR received an email with Resume and cover letter attached. Password was given to open the file. When the password was entered the file installed malware onto the employee’s computer. | | |
| Additional notes | Searched the Hash number provided on VirusTotal. 59 vendors identify it as malware. Alert ticket escalated to SOC 2. | | |

| **Date:**  12/28/22 | **Entry:**  0004 | | |
| --- | --- | --- | --- |
| Description | Security incident - individual was able to gain unauthorized access to customer personal identifiable information and financial information. 50,000 customer records were affected. The threat actor asked for ransom or will release data. | | |
| Tool(s) used | none | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? Threat Actor * **What** happened? Threat actor exploited a vulnerability in application that allow them access to customer data. * **When** did the incident occur? 12/28/22 7:20 pm * **Where** did the incident happen? Attack on e-commerce web application * **Why** did the incident happen? Threat actor discovered a vulnerability with the e-commerce web application. The 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. The vulnerability allowed the attacker to access customer purchase confirmation pages , exposing customer data. | | |
| Additional notes |  | | |