**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:**  10/21/2023 | **Entry:**  001 |
| Description | Initial incident documentation for healthcare clinic ransomware attack. |
| Tool(s) used | None. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? *Unethical hackers through targeted phishing emails.* * **What** happened? *Ransomware attack leading to the encryption of critical files, disrupting business operations.* * **When** did the incident occur? *Tuesday morning at approximately 9:00 a.m.* * **Where** did the incident happen? *U.S. healthcare clinic specializing in primary care services.* * **Why** did the incident happen? *Attackers gained access through phishing emails with malicious attachments.* |
| Additional notes | What measures could the healthcare organization take to avoid a recurrence of such an event?  Is it advisable for the company to make the ransom payment in exchange for the decryption key? |

|  |  |
| --- | --- |
| **Date:**  10/29/2023 | **Entry:**  002 |
| Description | Analysis of a suspicious file using VirusTotal and identification of related IoCs. |
| Tool(s) used | VirusTotal |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? *Unknown attackers delivered the malicious file via email.* * **What** happened? *An employee received and executed a malicious file, resulting in the creation of unauthorized executable files.* * **When** did the incident occur? *The incident happened at 1:15 p.m. When unauthorized executable files were created on the employee's computer.* * **Where** did the incident happen? *The incident occurred on the employee's computer.* * **Why** did the incident happen? *The incident happened because the employee opened a password-protected spreadsheet file from an email that contained a malicious payload.* |
| Additional notes | The VirusTotal report on the SHA256 file hash (54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b) strongly indicates the file is malicious based on a high vendors' ratio, a negative community score, and multiple vendors flagging it as malicious. Additionally, the report provided various IoCs, including a SHA1 hash (e7d9cf0c6dd65f7393c15c31fca28f7ed9e7f67a), an IP address (185.53.178.7), and a domain name (mypc.com) associated with the malware. |

|  |  |
| --- | --- |
| **Date:**  10/30/2023 | **Entry:**  003 |
| Description | Investigating Malicious Email Attachment |
| Tool(s) used | VirusTotal, Phishing Playbook, Phishing Flowchart |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? *The incident was likely caused by an external threat actor, using the alias "Clyde West," who sent a phishing email.* * **What** happened? *A phishing email was received by the HR department, which contained a malicious attachment disguised as a resume and cover letter.* * **When** did the incident occur? *The malicious email was received on Wednesday, July 20, 2022, at 09:30:14 AM.* * **Where** did the incident happen? *The incident occurred in the organization's email system, specifically in the HR department.* * **Why** did the incident happen? *The incident was an attempt by the threat actor to exploit the recipient into opening the malicious attachment, possibly leading to malware installation or data theft.* |
| Additional notes | * The phishing email contained grammar errors ("writing for to express"), which is a common indicator of phishing attempts. * The mismatch between the sender's email address ("76tguyhh6tgftrt7tg.su") and the displayed name ("Def Communications") is suspicious. * The attachment "bfsvc.exe" is an executable file, which is uncommon for resume submissions and is a red flag for potential malware. * The malicious file hash provided in the additional information matches the hash of the attachment, confirming the malicious nature of the file. * Given the high severity of the alert, the suspicious nature of the email, and the confirmed malicious attachment, immediate escalation and further investigation are warranted. |

|  |  |
| --- | --- |
| **Date:**  10/30/2023 | **Entry:**  004 |
| Description | Final Report Analysis |
| Tool(s) used | N/A |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? *The incident was caused by an external threat actor who was able to exploit a vulnerability in the e-commerce web application. The identity of the threat actor remains unknown.* * **What** happened? *On December 28, 2022, an unauthorized individual gained access to customer personal identifiable information (PII) and financial data. This breach involved approximately 50,000 customer records and resulted in a potential financial loss of $100,000.* * **When** did the incident occur? *The incident began with a phishing attempt on December 22, 2022, when an employee received a ransom email. The second phase of the incident took place on December 28, 2022, when the attacker escalated their demands.* * **Where** did the incident happen? *The incident took place within the organization's e-commerce web application. The attacker exploited a vulnerability that allowed them to access and exfiltrate customer data.* * **Why** did the incident happen? *The incident occurred due to a vulnerability in the e-commerce web application, specifically a forced browsing attack. The attacker sought financial gain through the theft of customer data, demanding a cryptocurrency payment in exchange for not releasing the stolen data publicly.* |
| Additional notes | The incident investigation and response were conducted promptly, and the organization has taken steps to remediate the issue, including disclosing the breach to affected customers and offering identity protection services. Furthermore, the incident report provides clear recommendations for preventing future recurrences, emphasizing the importance of routine vulnerability scans, penetration testing, and implementing robust access control mechanisms. |

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