**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:**  2024-09-05 | **Entry: #1** |
| Description | A small U.S. health care clinic experienced a security incident involving a ransomware attack. The attack began at approximately 9:00 a.m. on a Tuesday morning, disrupting business operations by encrypting the clinic's critical files. Employees were unable to access medical records and other essential systems. |
| Tool(s) used | No cybersecurity tools were directly mentioned in the scenario, but incident response tools like SIEM (Security Information and Event Management), antivirus/malware removal software, and email filtering systems could be involved in future responses. |
| The 5 W's | * **Who**: An organized group of unethical hackers, targeting the healthcare industry, caused the incident. The phishing email was directed at clinic employees. * **What**: The clinic’s computer systems were infected by ransomware via a phishing email, which led to encryption of critical files. A ransom note was left demanding payment for the decryption key. * **When**: The incident occurred on a Tuesday morning around 9:00 a.m., severely impacting business operations. * **Where**: The incident took place at a small U.S. health care clinic specializing in primary-care services. * **Why**: The incident happened due to successful phishing attacks, which allowed malware to be installed on the employees' computers. The attackers aimed to extort money by encrypting the clinic’s data and demanding a ransom in exchange for the decryption key. |
| Additional notes | This incident highlights the importance of phishing awareness and employee training, as well as the need for robust email filtering systems. A more detailed investigation will be needed to determine if there are further vulnerabilities in the network and how to prevent similar incidents in the future. |

|  |  |
| --- | --- |
| **Date:**  2024-09-16 | **Entry: #2** |
| Description | A suspicious file hash was reported during a cybersecurity incident investigation. The file was downloaded by an employee after receiving a phishing email with a password-protected spreadsheet. The malicious file caused the creation of unauthorized executable files on the system, prompting the need for further investigation using VirusTotal. |
| Tool(s) used | VirusTotal (<https://www.virustotal.com/>) for analyzing the SHA256 hash |
| The 5 W's | * **Who**: The incident was caused by an organized group of hackers who deployed ransomware through a phishing email. * **What**: The employee received a phishing email with a malicious attachment, downloaded the file, and opened it, triggering a payload that executed unauthorized files. * **When**: The incident began on September 16, 2024, with the email being opened at 1:13 PM, and unauthorized files being created shortly after. * **Where**: The incident occurred within the employee's computer network at a financial services company. * **Why**: The employee was tricked into opening a phishing email and executing the malware. |
| Additional notes | * IoCs identified include file system actions, process creation, and network communication. * A domain of interest, `org.misecure.com`, was identified, which may warrant further investigation. * The multiple `.tmp` files created raise suspicions of potential obfuscation or evasion tactics. * Company needs to ensure the organization has robust phishing training and potentiahttps://www.virustotal.com/lly implement stricter email filtering to prevent similar incidents from recurring. |

|  |  |
| --- | --- |
| **Date:**  2024-09-16 | **Entry: #3** |
| Description | The incident involved a data breach where an attacker gained unauthorized access to customer PII and financial information. Approximately 50,000 customer records were affected, leading to an estimated $100,000 in direct costs and potential revenue loss. The breach occurred due to a vulnerability in the e-commerce platform that allowed forced browsing attacks. |
| Tool(s) used | * Web application access logs * Vulnerability analysis tools (scanning, penetration testing) |
| The 5 W's | * **Who**: An external attacker exploited the e-commerce system vulnerability. * **What**: A data breach occurred due to a vulnerability that exposed customer information on purchase confirmation pages. The attacker threatened to release the stolen data unless paid in cryptocurrency. * **When**: The incident started on December 22, 2022, with the first extortion email, and escalated on December 28, 2022, when stolen data was demonstrated to the company. * **Where**: The breach originated from a vulnerability in the company’s e-commerce web application, particularly the purchase confirmation page. * **Why**: The attacker exploited a lack of proper access control mechanisms and URL validation on the e-commerce site. |
| Additional notes | Recommendations to avoid future incidents include routine vulnerability scans, penetration testing, and access control improvements such as allowlisting and authentication requirements for users accessing sensitive content. |

|  |  |
| --- | --- |
| **Date:**  2024-09-17. | **Entry: #4** |
| Description | Investigation of phishing alert involving suspicious domain `signin.office365x24.com`. POST requests to the `/login.php` page observed. Additional domain `signin.accounts-gooqle.com` associated with the same IP. Multiple affected assets identified. |
| Tool(s) used | Chronicle |
| The 5 W's | * **Who**: Phishing emails targeting employees. * **What**: Employees accessed the phishing domain `signin.office365x24.com` and sent POST requests to `/login.php`. Additional POST requests to another phishing domain `signin.accounts-gooqle.com`. * **When**: Initial access on January 31, 2023, and ongoing until July 9, 2023. * **Where**: Multiple employee computers across the company's network accessed phishing domains. * **Why**: Likely due to phishing emails, resulting in successful compromise of user credentials or data. |
| Additional notes | * **POST requests to the `/login.php` page**: Confirmed POST requests from `ashton-davidson-pc`, `emil-palmer-pc`, and `warren-morris-pc` to the domain `signin.office365x24.com` and `signin.accounts-gooqle.com`. * **Affected assets**: `ashton-davidson-pc`, `emil-palmer-pc`, `warren-morris-pc`, and `amir-david-pc` accessed the phishing domains. * **Additional domain and assets**: Discovered the domain `signin.accounts-gooqle.com`, associated with the same IP (`40.100.174.34`). The newly affected assets are `warren-morris-pc` and `amir-david-pc`. |

|  |  |
| --- | --- |
| **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:  **1. Were there any specific activities that were challenging for you? Why or why not?**  *I found the activities related to SIEM tools challenging because Splunk and Chronicle provide vast amounts of information, making them complex to use. These tools require a strong understanding of networks, OS, and applications. Suricata also presented a learning curve due to its detailed logging capabilities.*  **2. Has your understanding of incident detection and response changed since taking this course?**  *Yes, my understanding has significantly expanded, especially due to the advanced tools available today. The level of insight and functionality they offer truly surprised me.*  **3. Was there a specific tool or concept that you enjoyed the most? Why?**  *I particularly enjoyed using Suricata because it’s a powerful and free tool for logging events on devices, offering comprehensive visibility into network traffic.* |