**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:**  09/08/24 | **Entry:**  #1 |
| Description | Documenting a cybersecurity incident |
| Tool(s) used | - |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: Group of unethical hackers. * **What**: A ransomware attack * **When**: Tuesday, 9:00 am. * **Where**: Health company * **Why**: The group of unethical hackers managed to gain access using a phishing attack. The attackers ran their ransomware on company’s systems, encrypting the data and asking for a large amount of money. |
| Additional notes | The healthcare company can prevent future incidents by implementing employee cybersecurity training, advanced email filtering, multi-factor authentication, regular data backups, and a strong incident response plan.  The company should avoid paying the ransom, as it does not guarantee data recovery. |

|  |  |
| --- | --- |
| **Date:**  10/09/24 | **Entry:**  #2 |
| Description | Verifying a file based on hash value |
| Tool(s) used | Virustotal |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: BlackTech, known threat actor. * **What**: A potentially malicious file was detected by various security vendors during a VirusTotal scan. * **When**: The exact date when the file was introduced into the environment isn't provided, but the VirusTotal report was generated when the hash was checked. * **Where**: The incident occurred wherever the malicious file was discovered, such as on a specific endpoint, server, or within the corporate network * **Why**: The file itself was designed to act as a backdoor or trojan, which indicates that the intent behind the attack could be to gain unauthorized access to systems |
| Additional notes | Sha256 hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b |

|  |  |
| --- | --- |
| **Date:**  10/09/24 | **Entry:**  #3 |
| Description | An employee downloaded a file which affected his system. |
| Tool(s) used | Virustotal |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: external threat * **What**: employee received an phishing email * **When**: During work hours, when the employee opened his email. * **Where**: On the employees machine. * **Why**: The incident happened because the employee fell victim to a phishing attack. |
| Additional notes | The malware has been already checked before, using it’s file hash. It is a known backdoor threat used by BlackTech. |

|  |  |
| --- | --- |
| **Date:**  11/09/2024 | **Entry:**  #4 |
| Description | The organization experienced a security incident during which an unauthorized individual gained access to customer Personally Identifiable Information (PII) and financial information. |
| Tool(s) used | **-** |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: An external threat actor. * **What**: Unauthorized access to customer PII and financial information via a web application vulnerability. * **When**: 28 December 2022, at 7:20 p.m. * **Where**: The organization's e-commerce web application. * **Why**: The attacker exploited a vulnerability in the web application, specifically a forced browsing attack, by modifying the order number in the URL string of purchase confirmation pages. This allowed unauthorized access to customer transaction data, which was then exfiltrated |
| Additional notes | - |

|  |  |
| --- | --- |
| **Date:**  12/08/2024 | **Entry:**  #5 |
| Description | Check ip adress |
| Tool(s) used | Google Chronicle |
| The 5 W's | Capture the 5 W's of an incident.   * **Who:** The incident was likely caused by an external threat actor who targeted multiple assets within the organization * **What**: A phishing attack was initiated, leading to unauthorized access to several organizational assets. The threat actor used malicious domains (signin.accounts-gooqle.com and signin.office365x24.com) to mimic legitimate login pages * **When**: The initial incident occurred on **January 31, 2023**, as indicated by the first access timestamps. * **Where**: The incident occurred within the organization's network, specifically involving multiple user workstations identified by their hostnames (e.g., amir-david-pc, ashton-davidson-pc, etc.). * **Why**: The incident occurred because the threat actor successfully lured users into interacting with phishing domains designed to look like legitimate sign-in portals. |
| Additional notes | - |

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

|  |
| --- |
| Reflections/Notes: Record additional notes.  **Were there any specific activities that were challenging for you? Why or why not?**  I found working with Google Chronicle and Splunk particularly challenging. With Google Chronicle, navigating the interface and understanding how to effectively query and analyze normalized data was confusing at first. What I learned from this experience was the importance of dedicating time to familiarize myself with new tools and seeking additional resources to overcome these challenges.  **Has your understanding of incident detection and response changed after taking this course?**  After taking this course, my understanding of incident detection and response has definitely evolved.  **Was there a specific tool or concept that you enjoyed the most? Why?**  I really enjoyed learning about network traffic analysis and using network protocol analyzer tools. It was my first time delving into this area, and I found it both challenging and exciting. |