**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:1**  Date: 2024-04-08  Entry: 1 |
| Description | Exploration of Suricata alerts and logs. |
| Tool(s) used | Suricata for IDS/IPS and network analysis. |
| The 5 W's | Capture the 5 W's of an incident.   * Who: Unknown external actor. * What: Attempted network intrusion detected. * When: During routine monitoring. * Where: Company's main network gateway. * Why: Likely probing for vulnerabilities. |
| Additional notes | Configured Suricata to monitor network interfaces and apply custom rules |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry: 2**  2024-04-08 |
| Description | Creation and testing of custom Suricata rules. |
| Tool(s) used | Suricata rule syntax for custom intrusion detection. |
| The 5 W's | Capture the 5 W's of an incident.   * Who: Internal test by cybersecurity team. * What: Test custom IDS rules. * When: Post configuration of new rules. * Where: Test environment within corporate network. * Why: To ensure accuracy and reliability of alerts. |
| Additional notes | Include any additional thoughts, questions, or findings. |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry: 3**  Date: 2024-04-08 |
| Description | Analyzing alerts using Suricata's fast.log. |
| Tool(s) used | Used fast.log for quick analysis of alerts. |
| 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: 4**  Date: 2024-04-08 |
| Description | Detailed examination of network traffic via eve.json. |
| Tool(s) used | Used eve.json for detailed event logging and analysis. |
| 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 | Leveraged JSON format for better data processing and integration with other tools. |