**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:**  2023-08-01 | **Entry:**  1 |
| Description | Ransomware incident |
| Tool(s) used | SIEM logs – Splunk Cloud |
| The 5 W's | Capture the 5 W's of an incident.   * A malicious actor sent phishing emails to company employees. One or more employees may have opened an attachment containing malware * Users reported not being able to log into their accounts. They saw popups on their screens demanding a ransom to unlock their accounts * Users reported the incident starting at 9:00AM on 8/1/2023 * Onsite, users tried to log into their workstations * One or more employees opened an attachment in phishing emails sent to the company. This caused the installation of malware and allowed access for the attacker into the network. The attacker then installed ransomware and encrypted data files. |
| Additional notes | Users should be trained on dealing with phishing emails. The network should be segmented to prevent complete system shutdown. |

|  |  |
| --- | --- |
| **Date:**  2023-08-03 | **Entry:**  2 |
| Description | Phishing incident |
| Tool(s) used | List any cybersecurity tools that were used. |
| The 5 W's | Capture the 5 W's of an incident.   * **Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114>** * **Phishing email was sent to HR** * **July 20, 2022 09:30:14 AM** * **User’s email** * **Phishing attack to install malware** |
| Additional notes | * Sender’s name, email, IP are suspicious * Grammatical and spelling errors in subject and message * Exe file attachment * Attachment file hash flagged as malicious on VirusTotal |

|  |  |
| --- | --- |
| **Date:**  2023-08-04 | **Entry:**  3 |
| Description | Investigate packet |
| Tool(s) used | Wireshark |
| The 5 W's | Capture the 5 W's of an incident.   * Source IP: 142.250.1.139 * ICMP, HTTP, DNS traffic * 11/23/2022 * Network traffic |
| Additional notes | No strange activity |

|  |  |
| --- | --- |
| **Date:**  08-04-2023 | **Entry:**  4 |
| Description | Signature examination and configuration in Suricata |
| Tool(s) used | Suricata |
| The 5 W's | Capture the 5 W's of an incident.   * Examined custom alert rule * Triggered suricata alert with sample pcap file * Examined fast.log and eve.json output files |
| Additional notes | Learned what signatures looked like in config and where to look for logs |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry:**  Record the journal entry number. |
| 2023-08-04 | Provide feedback for final report |
| Tool(s) used | Final report |
| The 5 W's | Capture the 5 W's of an incident.   * Outside malicious actor * User gained access to customer data and demanded ransom for not releasing it to the public * December 28, 2022, at 7:20 p.m., PT * Forced browsing on website * Software vulnerability allowed the user to view multiple invoices containing customer PII |
| Additional notes |  |

|  |  |
| --- | --- |
| **Date:**  2023-08-04 | **Entry:**  6 |
| Description | Examine failed logins in SIEM (Splunk) |
| Tool(s) used | Splunk Cloud |
| The 5 W's | Capture the 5 W's of an incident.   * Multiple failed logins to the mail server * Over 300 failed logins as root to the mail server were logged * 2/27/23 – 3/6/23 * Multiple IP sources trying to log into the mail server |
| Additional notes | Further investigation needed – possible attempt by malicious actors to access the mail server |

### 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. |