**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:**  April 16, 2024 | **Entry:**  1 |
| Description | Initial journal entry documenting a security incident at a U.S. health care clinic. |
| Tool(s) used | Antivirus Software, SIEM. |
| The 5 W's | * An organized group of unethical hackers targeted the health care clinic. * The clinic's computer systems were compromised by ransomware, encrypting critical files. * The incident occurred on Tuesday morning at approximately 9:00 a.m. * The incident happened at the U.S. health care clinic. * The incident occurred due to employees unknowingly downloading malware from phishing emails. |
| Additional notes | This incident underscores the importance of cybersecurity awareness training for employees and robust email filtering mechanisms to detect and prevent phishing attacks. |

|  |  |
| --- | --- |
| **Date:**  April 16, 2024 | **Entry:**  2 |
| Description | Follow-up journal entry regarding the impact of the security incident on the clinic's operations. |
| Tool(s) used | Endpoint Detection and Response, Backup and Recovery Solutions. |
| The 5 W's | * An organized group of unethical hackers targeted the health care clinic. * The clinic's computer systems were compromised by ransomware, encrypting critical files. * The incident occurred on Tuesday morning at approximately 9:00 a.m. * The incident happened at the U.S. health care clinic. * The incident occurred due to employees unknowingly downloading malware from phishing emails. |
| Additional notes | The clinic experienced significant disruptions in business operations due to the inability to access critical patient data. Recovery efforts are underway, but the long-term impact remains uncertain. |

|  |  |
| --- | --- |
| **Date:**  April 17, 2024 | **Entry:**  3. |
| Description | Further investigation into the attack vectors used by the hackers. |
| Tool(s) used | Intrusion Detection System (IDS), Email Security Platform. |
| The 5 W's | * An organized group of unethical hackers targeted the health care clinic. * The clinic's computer systems were compromised by ransomware, encrypting critical files. * The incident occurred on Tuesday morning at approximately 9:00 a.m. * The incident happened at the U.S. health care clinic. * The incident occurred due to employees unknowingly downloading malware from phishing emails. |
| Additional notes | Investigation revealed that the hackers gained access through targeted phishing emails, highlighting the need for enhanced email security measures. |

|  |  |
| --- | --- |
| **Date:**  April 18, 2024 | **Entry:**  4. |
| Description | Initial steps taken to mitigate the impact of the security incident. |
| Tool(s) used | Vulnerability Scanning Tools, Firewall, Intrusion Prevention System (IPS). |
| The 5 W's | * An organized group of unethical hackers targeted the health care clinic. * The clinic's computer systems were compromised by ransomware, encrypting critical files. * The incident occurred on Tuesday morning at approximately 9:00 a.m. * The incident happened at the U.S. health care clinic. * The incident occurred due to employees unknowingly downloading malware from phishing emails. |
| Additional notes | Immediate actions include isolating infected systems, contacting law enforcement, and engaging cybersecurity experts for assistance in remediation efforts. |

### 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?   Exploring signatures and logs with Suricata was an engaging activity, although it presented some challenges along the way. Understanding the intricacies of Suricata's rule syntax and how to examine logs required careful attention to detail effectively. The process of examining a rule in Suricata involved deciphering its components, such as the condition, action, and options, which could be complex at times. Moreover, triggering a rule and analyzing the alert logs demanded a thorough understanding of network traffic patterns and potential threat indicators. This task required patience and persistence to interpret the output and identify suspicious activities accurately.   1. Has your understanding of incident detection and response changed after taking   this course?  Yes, my understanding of incident detection and response has evolved after completing this course. Through hands-on activities throughout the course, I gained practical insights into the techniques and tools used in incident detection. Moreover, learning about incident response playbooks provided a structured approach to handling security incidents effectively. The incident response playbook is a comprehensive guide outlining predefined steps, procedures, and roles during an incident. It helps streamline the response process, ensuring a coordinated and efficient response to security incidents while minimizing potential damage and downtime.   1. Was there a specific tool or concept that you enjoyed the most? Why?   One specific tool that stood out to me and that I enjoyed using the most was Splunk. Splunk's powerful querying and visualization capabilities make it invaluable for analyzing vast amounts of log data and gaining actionable insights into security incidents. Its user-friendly interface and flexible search language allow quick and efficient data analysis, facilitating rapid incident response and investigation. Additionally, Splunk's integration with other security tools and its ability to generate customizable dashboards make it a versatile solution for monitoring and managing security events effectively. Overall, the intuitive nature and robust features of Splunk make it a preferred choice for security analysts and incident responders. |