**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:  Date:** 2023-08-15 **Entry #:** 1 |
| Description | **Description:** Investigated a suspected phishing attack targeting our company's email system. The incident required immediate attention to prevent potential data breaches and unauthorized access. |
| The 5 W's | * The 5 W's:   + Who: An external attacker posing as a known vendor.   + What: Sent fraudulent emails attempting to obtain employee login credentials.   + When: Detected on 2023-08-15 at 09:30 AM.   + Where: Targeted multiple employees across various departments via corporate email accounts.   + Why: Likely intended to gain unauthorized access to sensitive company information and exploit financial resources. |
| Additional notes | **NIST Incident Response Lifecycle Phase:** Detection and Analysis – Identified and analyzed the phishing attempt to assess the threat level and potential impact. |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry:**  **Date:** 2023-08-20 **Entry #:** 2 |
| Description | **Description:** Utilized Wireshark to analyze unusual network traffic reported by the monitoring system. The analysis aimed to identify potential security threats or malicious activities within the network. |
| The 5 W's | * Wireshark:   + Captured live network traffic for detailed inspection.   + Identified abnormal spikes in outbound traffic to unknown IP addresses.   + Filtered and analyzed packets to trace the source of suspicious activity.   + Assisted in determining that the traffic was caused by a misconfigured application, not malicious activity. |
| Additional notes | **Outcome:** Resolved the issue by reconfiguring the application settings, restoring normal network operations and preventing potential exploitation. |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry:**  **Date:** 2023-08-25 **Entry #:** 3 |
| Description | **Description:** Responded to a malware infection detected on an employee's workstation. Prompt action was necessary to contain and eradicate the threat to prevent lateral movement within the network. |
| The 5 W's | * The 5 W's:   + Who: Malware infiltrated through an employee inadvertently downloading a compromised file.   + What: A Trojan horse malware designed to steal sensitive data and provide remote access to attackers.   + When: Detected on 2023-08-25 at 02:15 PM.   + Where: Located on the employee's workstation connected to the corporate network.   + Why: The malware aimed to exfiltrate confidential information and compromise system integrity. |
| Additional notes | **NIST Incident Response Lifecycle Phase:** Containment, Eradication, and Recovery – Isolated the infected system, removed the malware, and restored the workstation to secure operational status. |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry:**  **Date:** 2023-08-30 **Entry #:** 4 |
| Description | **Description:** Employed Splunk for proactive monitoring and analysis of system logs to ensure ongoing security compliance and detect potential anomalies within the IT infrastructure. |
| The 5 W's | * Tool(s) Used:   + Splunk:   + Aggregated and indexed log data from various sources including servers, applications, and security devices.   + Created real-time dashboards to monitor key security metrics and system performance.   + Implemented automated alerts for predefined threat indicators and unusual activities.   + Conducted search queries to analyze historical data for trend analysis and reporting. |
| Additional notes | **Outcome:** Enhanced visibility into system operations, enabling early detection of potential threats and informed decision-making for security measures. |

|  |
| --- |
| Reflections/Notes:   **1. Were there any specific activities that were challenging for you? Why or why not?**   * Analyzing complex network traffic patterns using Wireshark was particularly challenging due to the volume and intricacy of the data. Distinguishing between legitimate and suspicious traffic required meticulous attention to detail and a deep understanding of network protocols.   **2. Has your understanding of incident detection and response changed since taking this course?**   * Yes, my understanding has significantly improved, especially regarding the structured approach provided by the NIST Incident Response Lifecycle. I now appreciate the importance of thorough preparation and systematic processes in effectively managing and mitigating security incidents.   **3. Was there a specific tool or concept that you enjoyed the most? Why?**   * I particularly enjoyed working with Splunk due to its powerful capabilities in aggregating and analyzing vast amounts of log data. The ability to create customizable dashboards and automated alerts made it an invaluable tool for maintaining robust security monitoring and swift incident response. |