**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:**  September 16, 2024 | **Entry:**  Entry #1 | | |
| --- | --- | --- | --- |
| Description | Documentation of a security incident regarding ransomware being deployed on a small U.S. health care clinic. After deployment, users were unable to access important files to continue operations. | | |
| Tool(s) used | No cybersecurity tools were used in this incident. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who:** An organized group of unethical hackers caused this incident. * **What:** The health care clinic’s employees reported that they were unable to access important files such as medical records, and that on their computer screens a ransom note appeared that stated the company’s files would remain locked/encrypted until the ransom was paid to restore access to those files with the decryption key. * **When**: The security incident occurred on Tuesday, at approximately 9 a.m. * **Where**: The incident occurred at a small health care clinic. * **Why**: The attackers gained access to the clinic’s network by using phishing emails that were sent to several employees that contained a malicious attachment. When opened, it downloaded malware to the employees’ computer and allowed the attackers access to the network. The attackers then deployed their ransomware message that then encrypted the critical data of the clinic. | | |
| Additional notes | The clinic doesn’t seem to have a cybersecurity department as there were no efforts to contain the issue. They immediately had to request outside assistance to help resolve the issue, which will take time. | | |

| **Date:**  September 29, 2024 | **Entry:**  Entry #2 | | |
| --- | --- | --- | --- |
| Description | Analyzing an incident where an alert was received that a phishing email was received by an employee. There is a need to determine whether any other employees also received the same phishing email and have visited the domain associated with the email. | | |
| Tool(s) used | Google Chronicle: A SIEM tool that is developed by Google. This tool was used in this entry to retrieve information about the domain found in the phishing email. Information included incoming and outgoing requests from users/endpoints, the IP address associated with the domain, other sibling domains, etc. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: signin.office365x24.com, 40.100.174.34 * **What**: An alert was received that a phishing email was received by an employee. Some employee computers visited the domain associated with the phishing email. * **When**: 1/31/2023, 7/8/2023, 7/9/2023 * **Where**: Financial Services Company * **Why**: Company assets were compromised when employees received phishing emails. It seems that the ashton-davidson-pc and emil-palmer-pc were the assets that were compromised due to the POST event to /login.php indicating that these assets contacted the suspicious domain. | | |
| Additional notes | Accessed assets: ashton-davidson-pc, bruce-monroe-pc, coral-alvarez-pc, emil-palmer-pc, jude-reyes-pc, roger-spence-pc, warren-morris-pc  Total accessed assets: 7  Assets that had POST requests to domain: ashton, emil, warren | | |

| **Date:**  September 29, 2024 | **Entry:**  Entry #3 | | |
| --- | --- | --- | --- |
| Description | Monitoring traffic on the organization’s network utilizing Suricata to analyze a captured network traffic packet. Analyzing the logs associated with the output of running Suricata. | | |
| Tool(s) used | Suricata: Suricata is an open-source IPS/IDS/network analyzer tool. It was used to analyze a captured packet and perform signature analysis to generate the eve.json and fast.log files with alerts that were found from the analysis. Information was sorted through using special commands listed in the additional notes section. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: The security analyst (me) * **What**: Created custom rules used by Suricata to monitor network traffic captured in a packet capture file. Analyzed log data captured by Suricata. * **When**: November 23, 2022 * **Where**: The organization’s network * **Why**: Tasked with monitoring the organization’s network and capturing network packets with Suricata to analyze eve.json and fast.log output. | | |
| Additional notes | Commands utilized:  cat custom.rules  ls -l /var/log/suricata  sudo suricata -r sample.pcap -S custom.rules -k none  ls -l /var/log/suricata  cat /var/log/suricata/fast.log  cat /var/log/suricata/eve.json  jq . /var/log/suricata/eve.json | less  jq -c "[.timestamp,.flow\_id,.alert.signature,.proto,.dest\_ip]" /var/log/suricata/eve.json  jq "select(.flow\_id==1647223379236084)" /var/log/suricata/eve.json | | |

| **Date:**  September 29, 2024 | **Entry:**  Entry #4 | | |
| --- | --- | --- | --- |
| Description | Investigating an alert about a suspicious file being downloaded to an employee’s computer. When the file was opened, it executed a series of executables onto the computer. | | |
| Tool(s) used | VirusTotal | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: A malicious actor that sent a phishing email to a user. * **What**: An employee downloaded a file and opened it to find a malicious payload executed onto the computer. * **When**: 1:20pm * **Where**: A financial services company * **Why**: An employee received an email and downloaded a file, and then opened it to find a malicious payload executed onto the computer. A series of executables occurred and the IDS alerted the SOC that an intrusion occurred. | | |
| Additional notes | Yes, the file has been identified as malicious. The Vendor’s ratio of the file is 59/73 with the other 14 vendors reporting “undetected”. This means that the vendors overall say that the file is malicious. The community score is a -211, which suggests that the community also believes the file is malicious. In the Detection tab under “Security vendors’ analysis”, the file is flagged as malicious by the vendors and includes the name of the malware that was detected. With all the evidence collected, and is consistent, it’s concluded that the file is malicious. | | |

| **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. | | |

| **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. | | |

### 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?   *The Google Chronicle activity was challenging. There was a lot of information thrown at me at once and finding the areas that I was supposed to interact with was not straightforward in the beginning of the assignment. I had trouble finding items of interest that I could use to figure out what the assignment was asking me to record to finish the assignment.*   1. Has your understanding of incident detection and response changed since taking this course?   *Utilizing the tools, labs, and information given in this course helped me understand how much goes into incident detection and response. I can see why the incident response lifecycle is a cycle in that depending on the incident, the process can loop for a very long time. Before, I assumed that all things in cybersecurity were a streamlined process with a standard beginning and end.*   1. Was there a specific tool or concept that you enjoyed the most? Why?   *I enjoyed the use of Google Chronicle the most. Even though it was difficult to grasp at first due to so much information coming at once, realizing how useful of a tool it is made me more eager to become more comfortable with it.* |
| --- |