**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:** 8/23/23 | **Entry: #1** |
| Description | Documenting a cybersecurity incident.   1. Detection and Analysis: This incident outlines how an organization first detected the ransomware incident. For analysis the organization contacted several outside organizations for technical assistance. 2. Containment, Eradication and Recovery: The scenario details steps that were taken by the organization to contain the incident such as shutting down their computer systems. Since they could not work to eradicate and recover from the incident alone, they contacted other organizations for assistance. |
| Tool(s) used | None |
| The 5 W's | * Who- Group of unethical hackers. * What- A ransomware incident. * When- Tues morning at 9:00 am * Where- At a small U.S health care clinic that delivers primary care services. * Why- The incident occurred as the unethical hackers gained access to the company’s system through a phishing attack. They then launched ransomware on the system which encrypted critical files. They left a note to demand a large sum of money in exchange for the decryption key. |
| Additional notes | 1. How can the company prevent an incident like this again? 2. Should the company pay for the decryption key? |

|  |  |
| --- | --- |
| **Date:** 8/24/23 | **Entry: #2** |
| Description | Documenting a security incident involving phishing. |
| Tool(s) used | I used VirusTotal, which is a tool that analyzes files and URLs for malicious content like viruses, worms, and more. I used VirusTotal to analyze a file hash that was reported as malicious.  This incident occurred during the Detection and Analysis phase. The scenario put me as a security analyst at a SOC investigating a suspicious file hash. Once the file was detected by the security systems, I needed to perform a deeper investigation to determine if the alert was a real threat. |
| The 5 W's | * Who- Unknown malicious actor. * What- Email attachment with a malicious known file hash was opened by unsuspecting employee. Malicious file attachment with SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab5   27f6b.   * When- Weds at 1:20pm alert was sent to SOC after the intrusion detection system detected the file. * Where- At a financial services company. * Why- Employee downloaded and executed a malicious file attachment via an e-mail they received. |
| Additional notes | How can we prevent this in the future? Should we consider security awareness training for employees to learn to be careful with what attachments and links they click on? |

|  |  |
| --- | --- |
| **Date:** 8/25/23 | **Entry: #3** |
| Description | Reviewing affected assets and events. |
| Tool(s) used | For this activity I used Chronicle, a cloud-native tool, to investigate a security incident involving phishing answers a few questions. |
| The 5 W's | * **Who**: N/A * **What**: N/A * **When**: N/A * **Where**: N/A * **Why**: N/A |
| Additional notes | Noticed that 6 assets had accessed the domain: emil-palmer-pc, ashton-davidson-pc,  roger-spence-pc, jude-reyes-pc, coral-alvarez-pc, and bruce-monroe-pc.  Determined per ET intelligence Rep list that signin.office365x24.com is a drop site for logs and stolen credentials. Several of the assets accessed this domain and had 2 POST requests made to this domain. Multiple assets might have been impacted by the phishing campaign. Had a difficult time following directions to find all the different assets and IP addresses to review. With more practice I was able to gain a better understanding of what I was reviewing and what to look for when reviewing the information. |

|  |  |
| --- | --- |
| **Date:** 8/25/23 | **Entry: #4** |
| Description | Evaluating possible security issues with the mail server. |
| Tool(s) used | Splunk Cloud to learn to upload data and perform basic searches on the data. |
| The 5 W's | * **Who**: N/A * **What**: N/A * **When**: N/A * **Where**: N/A * **Why**: N/A |
| Additional notes | Searched for failed logins to the mail server. Found a few potential login failures that need to be investigated to determine if they are related to possible security issues. Had a difficult time reading the interface. It was very overwhelming at first. However, the information you receive can be very helpful and I can see why this tool would be used to parse through data as the filters can really helpful pinpoint what you are looking for. |

|  |
| --- |
| Reflections/Notes:   1. Were there any specific activities that were challenging for you? Why or why not? Using the Splunk tool created some obstacles as there was a lot of information to search for and sift through. The Chronicle tool presents similar challenges but seemed to have a more user-friendly format that could be followed. 2. Has your understanding of incident detection and response changed since taking this course? I did not have much knowledge of the details that go into incident detection and response. However, I have a much greater appreciation of the time and detail that goes in to securing companies and individuals from these events. 3. Was there a specific tool or concept that you enjoyed the most? Why? I really enjoyed the playbook scenario that used VirusTotal as it gave me a real look at a possible scenario that could happen. Since social engineering is one of the biggest threats to cybersecurity I liked that it gave me a hands on practice with going through a few simple steps in a playbook on how to respond to the issue. |

### 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.