**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:** July 23, 2023 | **Entry:**  #1 |
| Description | Documenting a cybersecurity incident  This incident occurred in the two phases:   1. **Detection and Analysis**: The scenario outlines how the organization first detected the ransomware incident. For the analysis step, the organization contacted several organizations for technical assistance. 2. **Containment, Eradication, and Recovery**: The scenario details some steps that the organization took to contain the incident. For example, the company shut down their computer systems. However, since they could not work to eradicate and recover from the incident alone, they contacted several other organizations for assistance. |
| Tool(s) used | None |
| The 5 W's | * **Who**: An organized group of unethical hackers * **What**: A ransomware security incident * **Where**: At a health care company * **When**: Tuesday 9:00 a.m. * **Why**: The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key. |
| Additional notes | 1. How could the health care company prevent an incident like this from occurring again? 2. Should the company pay the ransom to retrieve the decryption key? |

|  |  |
| --- | --- |
| **Date:** July 25 2023 | **Entry:** #2 |
| Description | Analyzing a packet capture file |
| Tool(s) used | For this activity, I used Wireshark to analyze a packet capture file. Wireshark is a network protocol analyzer that uses a graphical user interface. The value of Wireshark in cybersecurity is that it allows security analysts to capture and analyze network traffic. This can help in detecting and investigating malicious activity. |
| The 5 W's | * **Who**: N/A * **What**: N/A * **Where**: N/A * **When**: N/A * **Why**: N/A |
| Additional notes | I've never used Wireshark before, so I was excited to begin this exercise and analyze a packet capture file. At first glance, the interface was very overwhelming. I can see why it's such a powerful tool for understanding network traffic. |

|  |  |
| --- | --- |
| **Date:** July 25 2023 | **Entry:**  #3 |
| Description | Capturing my first packet |
| Tool(s) used | For this activity, I used tcpdump to capture and analyze network traffic. Tcpdump is a network protocol analyzer that's accessed using the command-line interface. Similar to Wireshark, the value of tcpdump in cybersecurity is that it allows security analysts to capture, filter, and analyze network traffic. |
| The 5 W's | * **Who**: N/A * **What**: N/A * **Where**: N/A * **When**: N/A * **Why**: N/A |
| Additional notes | I'm still new to using the command-line interface, so using it to capture and filter network traffic was a challenge. I got stuck a couple of times because I used the wrong commands. But after carefully following the instructions and redoing some steps, I was able to get through this activity and capture network traffic. |

|  |  |
| --- | --- |
| **Date:** July 27 2023 | **Entry:**  #4 |
| Description | Investigate a suspicious file hash |
| Tool(s) used | For this activity, I used VirusTotal, which is an investigative tool that analyzes files and URLs for malicious content such as viruses, worms, trojans, and more. It's a very helpful tool to use if you want to quickly check if an indicator of compromise like a website or file has been reported as malicious by others in the cybersecurity community. For this activity, I used VirusTotal to analyze a file hash, which was reported as malicious.  This incident occurred in the **Detection and Analysis** phase. The scenario put me in the place of a security analyst at a SOC investigating a suspicious file hash. After the suspicious file was detected by the security systems in place, I had to perform deeper analysis and investigation to determine if the alert signified a real threat. |
| The 5 W's | * **Who**: An unknown malicious actor * **What**: An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b * **Where**: An employee's computer at a financial services company * **When**: At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file * **Why**: An employee was able to download and execute a malicious file attachment via e-mail. |
| Additional notes | How can this incident be prevented in the future? Should we consider improving security awareness training so that employees are careful with what they click on? |

|  |  |
| --- | --- |
| **Date:** July 29 2023 | **Entry:**  #5 |
| Description | As a level-one Security Operations Center (SOC) analyst at our financial services company, I have been tasked with responding to an ongoing security incident. This incident involves a phishing alert indicating that a suspicious file has been downloaded onto an employee's computer. Following the investigation of the email attachment's hash, it has been confirmed that the attachment is indeed malicious. To address this threat effectively, I am following our organization's established process, as outlined in our playbook, to conduct a thorough investigation and resolve the alert. |
| Tool(s) used | In the course of this investigation, I leveraged the following tools:  VirusTotal: This tool was employed to analyze the suspicious file with the SHA-256 hash 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b. |
| The 5 W's | * **Who**: An unknown malicious actor * **What**: An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b * **Where**: An employee's computer at a financial services company * **When**: At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file * **Why**: An employee was able to download and execute a malicious file attachment via e-mail. |
| Additional notes | The alert detected that an employee downloaded and opened a malicious file from a phishing email. There is an inconsistency between the sender’s email address “76tguy6hh6tgftrt7tg.su’” the name used in the email body “Clyde West,” and the sender’s name, “Def Communications.” The email body and subject line contained grammatical errors. The email’s body also contained a password-protected attachment, “bfsvc.exe,” which was downloaded and opened on the affected machine. Having previously investigated the file  hash, it is confirmed to be a known malicious file. Furthermore, the alert severity is reported as medium. With these findings, I chose to escalate this ticket to a level-two SOC analyst to take further action. |

|  |  |
| --- | --- |
| **Date:** July 31 2023 | **Entry:**  #6 |
| Description | Review a final report |
| Tool(s) used | No specific tools were used for this entry; it involves the review of a final incident report. |
| The 5 W's | * **Who**: The incident involved an unknown attacker who gained unauthorized access to customer Personally Identifiable Information (PII) and financial data. * **What**: The security incident occurred on December 28, 2022, at 7:20 p.m. PT, resulting in unauthorized access to approximately 50,000 customer records, leading to an estimated financial impact of $100,000. * **Where**: The incident took place within the organization's infrastructure, specifically related to vulnerabilities in the e-commerce web application. * **When**: The incident timeline began on December 22, 2022, when the attacker sent the first email to an employee. The second email, containing a sample of stolen customer data and an increased payment demand, was received on December 28, 2022. * **Why**: The attack was initiated with the intention of extorting a cryptocurrency payment by threatening to expose stolen customer data. |
| Additional notes | This review of the final incident report highlights the key details of the security incident, including its timeline, impact, and the actions taken to respond and remediate. It emphasizes the importance of implementing security measures, such as routine vulnerability scans, access controls, and user authentication, to prevent similar incidents in the future. The incident has been successfully resolved, and the recommendations outlined in the report will guide the organization's efforts to enhance security and protect customer data moving forward. |

|  |  |
| --- | --- |
| **Date:** Aug 2 2023 | **Entry:**  #7 |
| Description | Explore signatures and logs with Suricata |
| Tool(s) used | Suricata |
| The 5 W's | * **Who**: As a security analyst, I am responsible for monitoring network traffic on my employer's network using Suricata. * **What**: In this task, I explored Suricata's custom rules and ran tests using the sample.pcap file to trigger alerts. I also examined the resulting logs in both the fast.log and eve.json files. * **Where**: The activity took place within the network infrastructure of my employer's organization. * **When**: The task was carried out on August 2, 2023, as part of ongoing network security monitoring. * **Why**: The purpose of this task was to test and validate custom rules in Suricata against sample network traffic data to ensure the effectiveness of the network intrusion detection system (NIDS). |
| Additional notes | In this exercise, I interacted with Suricata, a powerful network intrusion detection system, to better understand its signature-based detection capabilities. By exploring custom rules, running tests with the sample.pcap file, and analyzing the generated logs (both in the fast.log and eve.json formats), I gained valuable insights into how Suricata can be configured and utilized to enhance network security and identify potential threats. This hands-on experience will contribute to improving the organization's network defense capabilities. |

|  |  |
| --- | --- |
| **Date:** Aug 4 2023 | **Entry:**  #8 |
| Description | Perform a query with Splunk |
| Tool(s) used | Splunk |
| The 5 W's | * **Who**: I am a security analyst employed at Buttercup Games, an e-commerce store. * **What**: In this task, I was assigned to investigate potential security issues with the mail server by examining failed SSH logins for the root account. * **Where**: The investigation took place within the network infrastructure of Buttercup Games. * **When** The query was executed on August 4, 2023, as part of proactive security monitoring. * **Why**: The objective was to identify and analyze any failed SSH login attempts for the root account, which could indicate a security concern or potential breach. |
| Additional notes | In the capacity of a security analyst, I leveraged Splunk's capabilities to query and analyze log data related to SSH login attempts on the mail server. This investigation is crucial to identifying and addressing potential security issues promptly. Effective querying and analysis of log data is a vital skill for incident detection and response, enabling rapid action to mitigate security threats and vulnerabilities. |

|  |  |
| --- | --- |
| **Date:** Aug 6 2023 | **Entry:**  #9 |
| Description | Perform a query with chronicle |
| Tool(s) used | Chronicle |
| The 5 W's | * **Who**: I am a security analyst working at a financial services company. * **What**: In this task, I was assigned to investigate a security incident involving a phishing email with a suspicious domain name, "signin.office365x24.com," identified in an employee's inbox. * **Where**: The investigation took place within the network infrastructure and email systems of the financial services company. * **When**: The query and investigation were initiated on August 6, 2023, as part of the incident response process. * **Why**: The objective was to determine if other employees had received phishing emails containing the same suspicious domain and whether any of them had visited the domain. This investigation is crucial for identifying potential phishing campaigns and mitigating security risks. |
| Additional notes | Using Chronicle, a cloud-native SIEM tool, I conducted a query to search for related phishing emails with the domain "signin.office365x24.com." This investigation aims to identify any similar security threats affecting multiple employees within the organization. Chronicle's capabilities are instrumental in efficiently searching and analyzing security data to respond effectively to potential incidents and protect the company's sensitive information. |

|  |
| --- |
| Reflections/Notes:   1. **Were there any specific activities that were challenging for you? Why or why not?**   I really found the activity using tcpdump challenging. I am new to using the command line, and learning the syntax for a tool like tcpdump was a big learning curve. At first, I felt very frustrated because I wasn't getting the right output. I redid the activity and figured out where I went wrong. What I learned from this was to carefully read the instructions and work through the process slowly.   1. **Has your understanding of incident detection and response changed after taking this course?**   After taking this course, my understanding of incident detection and response has definitely evolved. At the beginning of the course, I had some basic understanding of what detection and response entailed, but I didn't fully understand the complexity involved. As I progressed through the course, I learned about the lifecycle of an incident; the importance of plans, processes, and people; and tools used. Overall, I feel that my understanding has changed, and I am equipped with more knowledge and understanding about incident detection and response.   1. **Was there a specific tool or concept that you enjoyed the most? Why?**   I really enjoyed learning about network traffic analysis and applying what I learned through network protocol analyzer tools. It was my first time learning about network traffic analysis, so it was both challenging and exciting. I found it really fascinating to be able to use tools to capture network traffic and analyze it in real time. I am definitely more interested in learning more about this topic, and I hope to one day become more proficient in using network protocol analyzer tools. |