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: 11/07/2024	**Entry: 1**
Description	This entry analyzes an incident at a small healthcare clinic in the U.S.. Based on the description provided, it seems as though this was a ransomware attack conducted by a known group of unethical hackers.
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ The incident was caused by a known group of unethical hackers targeting organizations in healthcare and transportation industries ● **What** happened? ○ Employees became unable to access any files or systems required to perform their jobs. A ransom note indicated that the group of hackers had encrypted the files and systems. The note demanded a large sum of money in exchange for the decryption key allowing the files and systems to be decrypted. ● **When** did the incident occur?

	○ Tuesday morning at approximately 9:00 am. ● **Where** did the incident happen? ○ A small healthcare clinic in the United States. ● **Why** did the incident happen? ○ The group of hackers were able to gain access to the network by using targeted phishing emails. Once the attachment in the email was downloaded, the attackers were able to gain access to the network and encrypt the targeted systems.
Additional notes	In order to prevent an attack like this in the future, technical controls such as email phishing in addition to managerial controls such as frequent training for employees regarding the dangers of phishing and how to identify a similar attack. Since this is a known group of hackers, have similar attacks occurred at other healthcare clinics?

Date: 12/18/2024	**Entry: 2**
Description	This entry analyzes an incident at a financial services company. An employee has downloaded a suspicious file contained in an email onto their computer. We have created a file hash from the suspicious file for investigation.
Tool(s) used	● VirusTotal
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ The incident was caused by an unknown threat actor who emailed the malicious file to an employee

	● **What** happened? ○ The employee downloaded and executed the malicious file on their computer. Through investigation, it has been determined that the executed file was malicious. Because of this, and because the incident has been deemed of medium severity, the alert has been escalated. ● **When** did the incident occur? ○ The malicious file was downloaded at 1:13 p.m. ● **Where** did the incident happen? ○ A financial services company ● **Why** did the incident happen? ○ An employee downloaded a password-protected spreadsheet that was attached to an email. When the employee accessed the spreadsheet using the password contained in the email, a malicious payload was executed on their computer.
Additional notes	● Utilizing the tool VirusTotal, it was determined that the file executed on the employee's computer was malicious. The file hash has been flagged as malicious by over 50 security vendors. The malicious file makes contact with several domains and IP addresses once executed as determined through execution in a controlled environment. In order to prevent a similar incident from occurring in the future, phishing training can be conducted with company employees to make them aware of the dangers of suspicious emails. ● The alert has been escalated past tier 1

Date: 12/18/2024	**Entry: 3**
Description	A retail organization suffered from an incident in which a threat actor was able to gain access to over 50,000 customer records including PII and financial information. An investigation was performed and the incident is now closed.
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ A threat actor who gained access to customer information due to a vulnerability in the e-commerce web application ● **What** happened? ○ An employee at the retail organization received multiple emails demanding compensation in return for customer data not being released to the public. Samples of the stolen customer data were sent to the employee and an investigation into how this data was stolen was launched. ● **When** did the incident occur? ○ December 28th, 2022 at 7:20 p.m. PT ● **Where** did the incident happen? ○ A retail organization with over 80% of sales being accounted for by e-commerce ● **Why** did the incident happen? ○ A vulnerability in the e-commerce web application allowed the threat actor to input different order numbers into the url string. As a result, the attacker was able to view thousands of customer purchase confirmation pages. The attacker was able to gain access to customer order numbers due to a single log source showing an exceptionally high number of sequentially listed customer order numbers.

Additional notes	● In order to fix the vulnerability and to prevent additional future incidents from occurring in the future, the organization plans to take the following actions: ○ Perform routine vulnerability scans and penetration testing ○ Implement the following access control mechanisms: ■ Implement allowlisting to allow access to a specified set of URLs and automatically block all requests outside of this URL range ■ Ensure that only authenticated users are authorized access to content

Date: 12/19/2024	**Entry: 4**
Description	An employee at a financial services company has received an email with a suspicious attachment. Using Chronicle, we investigate the suspicious domain.
Tool(s) used	● VirusTotal ● Chronicle
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ The incident was caused by an unknown threat actor who emailed the malicious file to an employee ● **What** happened? ○ The employee downloaded and executed the malicious file on their computer. Through investigation, it has been determined that the executed file was malicious. Because of this, and

	○ because the incident has been deemed of medium severity, the alert has been escalated. ● **When** did the incident occur? ○ The malicious file was downloaded at 1:13 p.m. ● **Where** did the incident happen? ○ A financial services company ● **Why** did the incident happen? ○ An employee downloaded a password-protected spreadsheet that was attached to an email. When the employee accessed the spreadsheet using the password contained in the email, a malicious payload was executed on their computer.
Additional notes	Assets accessing the signin.office365x24.com domain: 1. ashton-davidson-pc 2. bruce-monroe-pc 3. coral-alvarez-pc 4. emil-palmer-pc 5. jude-reyes-pc 6. Roger-spence-pc Assets making post requests to the signin.office365x24.com domain: 1. ashton-davidson-pc 2. Emil-palmer-pc Assets accessing the IP 40.100.174.34: 1. amir-david-pc 2. ashton-davidson-pc 3. bruce-monroe-pc 4. coral-alvarez-pc 5. jude-reyes-pc 6. roger-spence-pc 7. warren-morris-pc Assets making post requests to the IP 40.100.174.34:

	1. ashton-davidson-pc 2. emil-palmer-pc 3. warren-morris-pc Domains associated with the IP 40.100.174.34: 1. signin.accounts-google.com 2. signin.office365x24.com

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?
    a. I think that the last journal entry utilizing Chronicle was the most challenging for me. This is because I needed to explore a new tool with a great amount of information on the screen at once. However, once I got the hang of the SIEM tool and understood how the information was organized, it became simpler to me and I was able to find all of the information that I needed.
2. Has your understanding of incident detection and response changed since taking this course?
    a. I now understand to a greater extent how security analysts respond to incidents. Throughout the course, we went into detail of the NIST Incident Response Lifecycle which further helped me understand the steps in responding to an incident. I learned how to use different tools such as Wireshark, tcpdump, Splunk, and Chronicle to analyze network traffic as well as logs. Finally, I learned how to

use documentation to effectively respond to an incident. Overall, I learned a great deal in this course along with the other courses that I have taken so far.

3. Was there a specific tool or concept that you enjoyed the most? Why?
    a. The tool which I enjoyed using the most was Wireshark. This is because the GUI which it utilizes allows for the efficient organization of network traffic. Individual packets were colored according to their protocols and it was very easy to access additional information related to each packet. While I found tcpdump easy to use as well, I enjoyed Wireshark's interface.