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 27, 2023	**Entry:** 01-2023
Description	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 Phishing attack by email, business interruption, ransomware was deployed encrypting the organization's computer files
Tool(s) used	No tools have been used for detection (IPS or IDS)

The 5 W's	Capture the 5 W's of an incident. ● **Who** A group of unethical hackers who are known to target organizations in healthcare and transportation industries. ● **What** Attackers deployed ransomeware ● **When** Tuesday morning, at approximately 9:00 a.m. ● **Where** At a health Care Company and the interruption put an halt on all operations. ● **Why** Through a phishing attack the attackers who are unethical hackers, managed to gain access to company network system and encrypt sensitive data and display the ransom and demand for money on the companies computer. Their motive seems to be financial since they offered the encryption key after payment.
Additional notes	Q: information on the email would help to narrow down the path of attack point, was it social engineering or was this a random attack.

Reflections/Notes: Should Ransomware be paid? How can the Clinic prevent this type of attack from happening again.

Date: Mon Oct 2. 2023	**Entry:** 02-2023
Description	As a SOC Analyst I am tasked with an alert about a suspicious file that has been downloaded at a financial service company. 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. Password protected file came with an email as attachment. Employee was provided the password in the same email and proceeded to download -> Open -> input provided password -> malicious payload executed on
Tool(s) used	Virustotal.com, Pyramid of Pain
The 5 W's	Capture the 5 W's of an incident. ● **WHO:** unknown malicious actor ● **WHAT:** An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b ● **WHEN:** At 1:13pm the incident happened and at 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file ● **WHERE:** In the office of the employee at the financial service company ● **WHY:** Employee believed it was a spreadsheet for work, downloaded and executed instructions in email
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: Wed Oct 04, 2023	**Entry:** 03-2023
Description	Level 1 SOC Team Playbook phishing alert, suspicious file has been downloaded on employees computer.
Tool(s) used	Virustotal.com,
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? Email with attachment coming from unknown ● **What** happened? Email received with malicious attachment ● **When** did the incident occur? Wednesday, July 20, 2022 09:30:14 AM ● **Where** did the incident happen? work station computer ● **Why** did the incident happen? The instructions in the email was executed and caused an
Additional notes	Misspelling in email (subject line and body) Email address was suspect in the first place.
	The email address it self is suspicious and the mail client has identified a malicious file as attachment.

Date: Sun Oct, 08 2023	**Entry:** 04-2023
Description	Checking with SPL for failed SSH logins
Tool(s) used	SPLUNK
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? Unknown ● **What** happened? attempted error login check ● **When** did the incident occur? 27/02/2023 ● **Where** did the incident happen? index=main host=mailsv fail* root ● **Why** did the incident happen? unknown
Additional notes	Include any additional thoughts, questions, or findings.

Date: Sun, Oct, 09	**Entry:** 05-2023
Description	Employee email received phishing email at a financial service company. Reviewing alert and identifying a suspicious domain contained in the emails body signin.office365x24.com Checking if other employees received same email as well.
Tool(s) used	Google Chronicle, Virus Total

The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? Kamtron Systems Pvt. Ltd. “malicious malware” ● **What** happened? Employee **user=warren-morris** clientIP=10.200.8.18 received phishing email and 6 employees got infected ashton-davidson-pc First accessed: January 31, 2023 Last accessed: July 09, 2023 bruce-monroe-pc First accessed: January 31, 2023 Last accessed: July 09, 2023 coral-alvarez-pc First accessed: January 31, 2023 Last accessed: July 09, 2023 emil-palmer-pc First accessed: January 31, 2023 Last accessed: July 09, 2023 jude-reyes-pc First accessed: January 31, 2023 Last accessed: July 09, 2023 roger-spence-pc First accessed: January 31, 2023 Last accessed: July 09, 2023 ● **When** did the incident occur? Jan 31st 2023 ● **Where** did the incident happen? the domain signing.office365x24.com maps to 40.100.174.34 Two POST requests were made to the signin.office365x24.com domain. ● **Why** did the incident happen? The POST requests were sent to http://signin.office365x24.com/login.php. The http://accounts-gooqle.com/login.php URL is used by the additional domain accounts-gooqle.com.

Additional notes	1st quarrying signin.office365x24.com Virus Total shows 5 detections 2 security vendors flagged this URL as malicious 6 Assets are infected Category: Drop site for logs or stolen credentials Two post request found

Date: Tues Oct 10 2023	**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:** 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:** 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?**

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.

2. **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.

3. **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