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: Record the date of the journal entry. **8/10/2023**	**Entry:** Record the journal entry number. **1**
Description	Provide a brief description about the journal entry. **On a Tuesday, a primary-care healthcare clinic faced a breach locking computers and disrupting operations. Hackers via email attachments encrypted patient data, demanding payment in a ransom note. Shutdown and external aid were required.**
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? • An organized group of unethical hackers. • **What** happened? • A ransomware security incident. • **When** did the incident occur?

	• 09:00 on Tuesday. • **Where** did the incident happen? • A small U.S Healthcare clinic. • **Why** did the incident happen? • Unauthorized access to the company's systems was acquired by ethical hackers through a phishing attack. Ransomware was launched, encrypting sensitive and confidential information. This was probably motivated for monetary gain, seeing as that's what was demanded in return.
Additional notes	Include any additional thoughts, questions, or findings. What are ways that this can be prevented from ever happening again?

Date: Record the date of the journal entry. 8/16/2023	**Entry:** Record the journal entry number. 2
Description	Provide a brief description about the journal entry. **A financial company's level one SOC analyst investigated a suspicious download on an employee's computer. The employee opened a password-protected spreadsheet attachment, triggering a malicious payload. Using a generated SHA256 hash, the analyst used VirusTotal to identify related Indicators of Compromise (IoCs).**
Tool(s) used	List any cybersecurity tools that were used.

	VirusTotal
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • Blacktech, a threat group • **What** happened? • An employee accidentally downloaded trojanware • **When** did the incident occur? • 1311 to 1320 pm today. • **Where** did the incident happen? • At a financial services company • **Why** did the incident happen? • To gain unauthorized access to company information.
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry. 8/18/2023	**Entry:** Record the journal entry number. 3
Description	Provide a brief description about the journal entry. **As a new level-one SOC analyst at a mid-sized retail company, I'm undergoing initial training while delving into the company's security protocols. The recent data breach involving over a million users has spurred the team into action, seeking to avert similar occurrences. Although the breach predates my arrival, I've been tasked with**

	scrutinizing the conclusive report to aid in preventing future incidents.
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? A malicious threat actor. • **What** happened? An email was received by an employee showing a portion of customer data and demanding money in return for not releasing said data onto public forums. • **When** did the incident occur? December 28, 2022 • **Where** did the incident happen? Mid-sized retail company. • **Why** did the incident happen? For money. The attacker held the data hostage for money.
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry. **8/21/2023**	**Entry:** Record the journal entry number. **4**
Description	Provide a brief description about the journal entry. **At a financial firm, I, a security analyst, am alerted about an employee's**

	phishing email. The email contains a dubious domain, signin.office365x24.com. My task is to check if other employees got such emails and visited the domain. I'll utilize Chronicle for the investigation.
Tool(s) used	List any cybersecurity tools that were used. **Chronicle**
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? **Domain name = office365x24.com** • **What** happened? An employee received a phishing email with a suspicious domain name in the email's body. • **When** did the incident occur? • **Where** did the incident happen? At a financial services company • **Why** did the incident happen? An employee opened an email with a suspicious domain name which prompted a more in-depth search.
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.

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: There weren't any particularly challenging activities. Most were straightforward for the most part, with very few throwing in material that was not explored more in-depth, however using the resources available made everything much more understandable and approachable. Yes, I've realized incident and response is more than simply fixing a vulnerability and stopping threats, but also communicating with your team and keeping documentation of all that happens for potential future events. Even going as far as to implement controls and protocols to not only prevent but stop future attacks. I enjoyed using Splunk. I feel the GUI was very easy to understand and use. I can definitely see myself using it in the future.