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->(DD/MM/YY)

Date: (12/09/23)	**Entry: Incident #1**
Description	On Tuesday, September 12th at 09:00 AM MST, a small U.S based healthcare clinic was targeted by a malicious hacker group using ransomware/cryptoware to disrupt business operations. This malware was installed via phishing emails and malicious email attachments. The hacker group claims to undo encryption if the ransom is paid in full.
Tool(s) used	No tools have been used for this event
The 5 W's	Capture the 5 W's of an incident. • **Who =>** Incident was perpetrated by a malicious group of hackers(name unknown) • **What** => Malicious software was installed on end host, encrypting all data and halting critical and non critical business operations • **When** => Incident occurred on September 12, 2023 at 9:00 AM MST • **Where**=> Incident occurred in a small clinic located in the USA • **Why**=> Incident occurred due to a phishing email with a malicious payload, employee interaction was the trigger
Additional notes	-A social engineering and phishing awareness course for employees will be considered after the event has been remedied. -Ensure that all machines have the 'Autorun' function disabled -Possibly set up an application whitelisting security control to ensure that unauthorized programs are blocked from running

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.