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: 12/20/2023	**Entry: 2**
Description	File downloaded by employee executed a malicious payload on their computer. At 1:11 pm, the employee received an email containing a file attachment. At 1:13 pm the employee downloads and opens the file, which created multiple unauthorized executable files on their computer at 1:15, Our TDS detected these executables and sent out an alert to the SOC at 1:20.
Tool(s) used	Hash function in CLI. VirusTotal.com reporting

The 5 W's	Capture the 5 W's of an incident.
	• **Who** caused the incident?
	  ○ Employee, Malicious actor
	• **What** happened?
	  ○ Trojan virus found its way into an employee's computer through an email attachment, and began implementing malicious code
	• **When** did the incident occur?
	  ○ The incident occurred at 1:11pm
	• **Where** did the incident happen?
	  ○ The incident occurred on an employee's computer

	• **Why** did the incident happen? ○ The incident happened due, in part, to the negligence of the employee, who did not take necessary steps to ensure the source of the file was a legitimate one before opening it.
Additional notes	Include any additional thoughts, questions, or findings.