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: 01/02/2025	**Entry:** #3
Description	Financial services company has reached out to cybersecurity professionals to help with phishing alerts about a suspicious file being downloaded on an employee's computer. After investigating the email attachment file's hash, cybersecurity professionals see that the attachment has already been verified malicious.
Tool(s) used	
The 5 W's	• **Who**: Financial Services Company • **What**: Suspicious file → attachment file's hash =malicious • **Where**: Email (phishing) • **When**: From: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114> • Sent: Wednesday, July 20, 2022 09:30:14 AM • To: <hr@inergy.com> <176.157.125.93> Subject: Re: Infrastructure Egnieer role • **Why**:phing -cyberattack using social engineering techniques trying to exploit current employees to benefit their malicious actions
Additional notes	Furthermore, the alert severity is reported as medium. With these findings, I chose to escalate this ticket to a level-two SOC analyst to take further action as the playbook states.