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: 1/5/25	**Entry:** 001
Description	This first journal entry is to document a scenario provided in the Google Cybersecurity course on Coursera. The specific scenario is as follows: A small U.S. health care clinic specializing in delivering primary-care services experienced a security incident on a Tuesday morning, at approximately 9:00 a.m. Several employees reported that they were unable to use their computers to access files like medical records. Business operations shut down because employees were unable to access the files and software needed to do their job. Additionally, employees also reported that a ransom note was displayed on their computers. The ransom note stated that all the company's files were encrypted by an organized group of unethical hackers who are known to target organizations in healthcare and transportation industries. In exchange for restoring access to the encrypted files, the ransom note demanded a large sum of money in exchange for the decryption key. The attackers were able to gain access into the company's network by using targeted phishing emails, which were sent to several employees of the company. The phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded. Once the attackers gained access, they deployed their ransomware, which encrypted critical files. The company was unable to access critical patient data, causing major disruptions in their business operations. The company was forced to shut down their computer systems and contact several organizations to report the incident and receive technical assistance.
Tool(s) used	I did not use any specific cybersecurity tools in analyzing this scenario. It

	doesn’t sound like any specific tools were used to identify the issue, and the scenario doesn’t go into any details about how the problem was actually addressed or if the ransom had to be paid.
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ A malicious threat actor (a black hat hacker group) gained access as a result of targeted phishing. ● **What** happened? ○ An employee fell victim to targeted phishing which allowed a malicious hacker group to install malware (ransomware) that encrypted the health care provider’s data and render their systems unusable. ● **When** did the incident occur? ○ As a hypothetical scenario there is no actual time and date involved. The scenario does list that employees became aware of the issue at 9am on the date of the scenario. ● **Where** did the incident happen? ○ The scenario involves an unspecified small US-based health care clinic. ● **Why** did the incident happen? ○ The incident was made possible by an employee failing to detect that they were the target of a phishing attack and inadvertently downloading malware.
Additional notes	This scenario is particularly short on details, and doesn’t really talk at all about the remediation steps taken other than shutting down computers to stop any further actions by the ransomware.

Date: 1/14/	**Entry:** 002
Description	This is another scenario provided as part of the Google cybersecurity certificate program on Coursera. The specific scenario is as follows: You are a level one security operations center (SOC) analyst at a financial services company. You have received an alert about a suspicious file being downloaded on an employee's computer. You investigate this alert and discover that the employee received an email containing an attachment. The attachment was a password-protected spreadsheet file. The spreadsheet's password was provided in the email. The employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer. You retrieve the malicious file and create a SHA256 hash of the file. You might recall from a previous course that a hash function is an algorithm that produces a code that can't be decrypted. Hashing is a cryptographic method used to uniquely identify malware, acting as the file's unique fingerprint. Now that you have the file hash, you will use VirusTotal to uncover additional IoCs that are associated with the file.
Tool(s) used	SHA256 hash, VirusTotal website
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ An unknown threat actor appears to have targeted the scenario employee with a trojan download. The employee who downloaded the file is primarily responsible for the incident. ● **What** happened? ○ The scenario's employee received an email containing a file attachment, which they downloaded and opened. The file then created multiple executable files on the employee's computer, which were detected by an IDS which alerted the SOC. ● **When** did the incident occur? ○ The initial email was received at 1:11pm, and the alert was sent to the SCO at 1:20pm ● **Where** did the incident happen?

	○ The scenario does not give any location information. Presumably this all happened within the hypothetical organization’s location. ● **Why** did the incident happen? ○ The hypothetical employee failed to follow proper safety precautions with an unknown file.
Additional notes	These scenarios are always very light on details, only providing the bare minimum of information needed to perform the requested steps. I suppose it’s unavoidable, but it’d be nice to have more real-world scenarios instead of these stripped down hypotheticals.

Date: 1/15/25	**Entry:** 003
Description	Yet another Coursera activity based on a provided scenario. Here is the specific scenario provided this time: You are a level-one security operations center (SOC) analyst at a financial services company. Previously, you received a phishing alert about a suspicious file being downloaded on an employee's computer. After investigating the email attachment file's hash, the attachment has already been verified malicious. Now that you have this information, you must follow your organization's process to complete your investigation and resolve the alert. Your organization's security policies and procedures describe how to respond to specific alerts, including what to do when you receive a phishing alert. In the playbook, there is a flowchart and written instructions to help you complete your investigation and resolve the alert. At the end of your investigation, you will update the alert ticket with your findings about the incident. The activity is directing me to follow step-by-step the instructions in the playbook as if I were truly a level 1 security analyst, including using Google doc-based forms as if it were a true ticketing application.
Tool(s) used	Hypothetical playbook “Phishing Playbook Version 1.0”;

The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ The unspecified user in the HR department who downloaded/opened the malicious attachment. ● **What** happened? ○ An apparent phishing email containing an attachment with known malicious file hash triggered an IDS alert with ticket ID A-2703. Ticket details indicate the user may have opened a malicious email and opened attachments or clicked links. ● **When** did the incident occur? ○ The email was sent 7/20/22 @ 9:30 AM (sender's time) ● **Where** did the incident happen? ○ Emailed to departmental inbox "hr@inergy.com" with IP address 176.157.125.93. ● **Why** did the incident happen? ○ The hypothetical unnamed user in HR who opened an obviously malicious file exhibited a stunning lack of judgement and/or serious deficiency in basic anti-phishing skills.
Additional notes	Within the scenario, I would be escalating this ticket to a level 2 SOC analyst immediately. External to the scenario, this is such a blatant phishing email that if someone were to actually download/install the attachment I would recommend mandatory retraining for that individual in basic anti-phishing practices.

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: Record additional notes.