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: 25/11/25	**Entry: # 1**
Description	A security incident occurred in a small U.S. health care clinic on Tuesday 25/11/2025 by 9:00 am.Several employees reported that they were unable to use their computers to access files like medical records.Emails containing malicious attachment that installed malwares on employees computer were downloaded on employee computers.The deployed ransomware and critical files were encrypted.
Tool(s) used	**None**
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • An organised group of unethical hackers were able to gain access into the company's network by using targeted phishing emails. • **What** happened? • Attackers were able to gain access into the company's network by using targeted phishing emails.Business operations shut down because employees were unable to access the files and software needed to do

	their job due to ransomware deployed by attackers.The company was forced to shut down their computer systems. • **When** did the incident occur? • Tuesday morning, at approximately 9:00 a.m. 25/11/25 • **Where** did the incident happen? • At a small U.S. health care clinic specializing in delivering primary-care services • **Why** did the incident happen? • An organized group of unethical hackers left a ransom note stating that the company's files were encrypted and demanded money in exchange for the decryption key •
Additional notes	Include any additional thoughts, questions, or findings 1. The company should adopt measures to prevent such security incidents from happening again. 2. The company should seek the services of experts to give technical assistance

---

Date: 26/11/25	**Entry: #2**
Description	**Investigate suspicious file hash**
Tool(s) used	YARA-SIGNATOR V0.60”
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • "Felix Bilstein - yara-signator at cocacoding dot com"

	• **What** happened? • received an alert about a suspicious file being downloaded on an employee's computer. • **When** did the incident occur? • 31/10/2024 1:11pm • **Where** did the incident happen? • financial services company • **Why** did the incident happen? • The employee downloaded the file, then entered the password to open the file.
Additional notes	• Felix Bilstein is the author of the attack and used social engineering to launch the attack, • Employees should be educated about malware.

Date: 27/11/25	**Entry: #3**
Description	**a phishing incident / ticket alert**
Tool(s) used	**Malware**
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • Clyde West • **What** happened? • received a phishing alert about a suspicious file being downloaded on an employee's computer.

	• **When** did the incident occur? • Wednesday, July 20, 2022 09:30:14 AM • **Where** did the incident happen? • At a financial services company • **Why** did the incident happen? • The incident happened due to the downloaded malicious attachment from the email sent from a threat actor
Additional notes	Phishing attempt possible download of malware , The severity of the alert is considered medium and a level two SOC analyst has been notified for further action

---

Date: 27/11/202	**Entry: # 4**
Description	INCIDENT FINAL REPORT
Tool(s) used	
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • An external threat actor • **What** happened? • Customer (PII) and financial information data theft • **When** did the incident occur? • December 28, 2022, at 7:20 p.m., • **Where** did the incident happen?

	• A mid-sized retail company with physical store locations also conducting operations in e-commerce, • **Why** did the incident happen? • a vulnerability in the e-commerce web application allowed the attacker to perform a forced browsing attack and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page. This vulnerability allowed the attacker to access customer
Additional notes	To prevent future recurrences, we are taking the following actions: Perform routine vulnerability scans and penetration testing. Implement the following access control mechanisms: Implement allowlisting to allow access to a specified set of URLs and automatically block all requests outside of this URL range. Ensure that only authenticated users are authorized access to content.

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: Record additional notes.