Incident Handler's Journal – (Sample)

Date: Tuesday, April 15, 2025	**Entry:** 0001
Description	A *Ransomware* attack caused a shutdown of operations, seizing system resources and compromising personal data in the medical industry.
Tool(s) used	N/A
The 5 W's	Capture the 5 W's of an incident. ● Unethical Hackers ● Phishing Email delivered Ransomware ● Tuesday, 09:00 ● Phishing email; Possible motive: monetary gain
Additional notes	Screen filter emails? Incident handed off for HIPPA compliance or recovery? Pay Ransom?

Date: Thursday, April 24, 2025	**Entry:** 002
Description	Phishing Incident - A-2703 - malware Flagpro. Email sent to administrative head, implying an intentional attack

Tool(s) used	VirusTotal, Hash file, bfsvc.exe
The 5 W's	• **Who** caused the incident? threat actor BlackTech • **What** happened? <hr@inergy.com> <176.157.125.93> email sent • **When** did the incident occur? : Wednesday, July 20, 2022 09:30:14 AM • **Where** did the incident happen? Email client • **Why** did the incident happen? Phishing attack
Additional notes	Referred to playbook

Date: Friday, April 25, 2025	**Entry:** 003
Description	Forced Browsing Attack - eCommerce Vulnerability Breach. Previous transactions were accessed freely due to non-authenticated and archived data.
Tool(s) used	Web Server logs
The 5 W's	• External threat actor - • A forced browser attack vulnerability that accessed multiple confirmation pages • 3:13 p.m., PT, on December 22, 2022 and December 28, 2022 • Non-authenticated customers

---

Date: Monday, May 5, 2025	**Entry:** 004
Description	Parking Lot USB found
Tool(s) used	VM Sandbox
The 5 W's	• Indirect/direct Jorge Baily • A USB drive was found • Monday, May 5, 2025 • in the parking lot • **Why** did the incident happen?
Additional notes	Upon examining the USB (flash drive), Jorge Bailey saved several personal photos and company files (including vacation schedules, budget information). Also, included are personal information (PII) files. The information on the USB could have been tampered with by manipulating image files. Employee files contain personal information that could be used to track an employee's personal activities. Jorge's personal events may be compromised as well as hospital information that could lead to infiltration. The information on the drive may give an attacker information on potential employees. There are (2) files indicating current employee shift schedules and the employee budget.

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.

Reflections/Notes:

Monday, May 5, 2025

1. **Were there any specific activities that were challenging for you?** *Yes. I had to elaborate beyond what I felt was needed information. I typically get straight to the point in terms suitable for the level of knowledge needed.*
2. **Has your understanding of incident detection and response changed since taking this course?** *Yes. I know that a great deal more data must be documented to properly present the facts needed to mitigate possible future threats.*
3. **Was there a specific tool or concept that you enjoyed the most?** Splunk **Why?** Splunk has a better pleasing interface that is more intuitive and seemingly quicker. The data supported is searchable and efficient.