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: Record the date of the journal entry.	**Entry: 1** 04/12/2025
Description	Documenting a cybersecurity incident involving a ransomware attack at a U.S. health care clinic.
Tool(s) used	**Phishing Emails:** Delivered malicious attachments to employees. **Malware:** Installed upon execution of the attachment. **Ransomware:** Encrypted key business and patient files. **Social Engineering:** Used to deceive employees into opening malicious attachments.
The 5 W's	Capture the 5 W's of an incident. - **Who:** An organized group of unethical hackers known to target the health care and transportation sectors - **What:** A ransomware security incident - **Where:** At a small U.S. health care clinic - **When:** Tuesday, 9:00 a.m.

	- **Why:** The hackers gained access by sending targeted phishing emails containing a malicious attachment. After an employee opened the file, malware was installed and ransomware was deployed, encrypting important medical and business files. The attackers demanded a large sum of money in exchange for the decryption key. Their motivation appears to be financial.
Additional notes	- How can the clinic better train employees to recognize phishing emails in the future?

Date: Record the date of the journal entry.	**Entry: 2** 4/22/25
Description	Documenting a cybersecurity incident involving a phishing email attack that targeted a financial services firm.
Tool(s) used	Intrusion Detection System (IDS): Detected unauthorized executable files. VirusTotal: Used to analyze the SHA256 hash of the malicious file.
The 5 W's	**Who:** A threat actor who delivered a crafted phishing email to an employee. **What:** A phishing attack that led to malware execution and multiple unauthorized executables. **Where:** At a financial services company. **When:** Tuesday, 1:11 p.m. to 1:20 p.m. **Why:** The attacker tricked the employee into downloading and opening a malicious file using social engineering. The file deployed malware, which was

	later detected by the IDS. The motivation appears to be data compromise or persistence.
Additional notes	How can phishing simulations and user awareness training be improved to help employees recognize suspicious emails and avoid opening potentially harmful attachments in the future? The file's SHA256 hash was 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b and was submitted to VirusTotal for further investigation.

Date: Record the date of the journal entry.	**Entry: 3** **4/22/25**
Description	Documenting a phishing incident involving a malicious password-protected attachment sent to an employee at Inergy.
Tool(s) used	SERVER-MAIL: Initial phishing alert detection VirusTotal: File reputation and hash analysis
The 5 W's	Who: An unknown external attacker using the spoofed sender address 76tguyhh6tgftrt7tg.su and IP 114.114.114.114 targeted an Inergy employee. What: A phishing email containing a password-protected malicious attachment

	posing as a resume/cover letter. The password (“paradise”) was included in the body of the email to avoid detection. Where: The targeted employee’s inbox — `hr@inergy.com` When: Alert received via SERVER-MAIL on April 24, 2025 Why: The attacker attempted to lure the employee into opening the malicious attachment, likely with the intent to execute malware and gain access to internal systems.
Additional notes	- The subject line of the email contained a typo (“Infrastructure Egnieer role”), and the message included multiple grammar issues—both indicators of phishing. - The attachment hash was submitted to VirusTotal and returned malicious results. - I escalated the ticket to a Level 2 SOC analyst and updated the ticket status accordingly. - Recommend increased employee awareness around password-protected attachments and implementing automatic quarantine for similar future messages.

Date: Record the date of	**Entry: 4** **4/22/25**

the journal entry.	
Description	Documenting a security incident where an attacker exploited a vulnerability in the organization’s e-commerce web application, leading to unauthorized access of customer personal identifiable information (PII) and financial data.
Tool(s) used	Web Server Logs: Analyzed access patterns Internal Monitoring Systems: Alerted security team to suspicious access Manual Log Review: Identified forced browsing attack pattern
The 5 W's	Capture the 5 W's of an incident. ● **Who:** An unknown external attacker exploiting an insecure direct object reference (IDOR) vulnerability in the organization's web application. ● **What:** The attacker modified URL parameters to access customer order confirmation pages, exposing sensitive customer PII and financial information. ● **Where:** The organization’s e-commerce web application (purchase confirmation pages). ● **When:** Confirmed breach on December 28, 2022, at 7:20 p.m. PT. ● **Why:** The vulnerability allowed unauthorized access without authentication by manipulating the order number in the URL string. The attacker exfiltrated customer data and attempted to extort the organization for $50,000.
Additional notes	Highlighted the importance of prompt reporting of suspicious emails by employees to avoid delays in incident response.

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.