Incident handler's journal

Date: July 17, 2025	**Entry:** #1
Description	Summary of the ransomware attack that occurred at a small U.S. health care clinic. Employees were not able to access patient files as unethical hackers encrypted all their files through a malicious file downloaded by employees in a phishing email.
Tool(s) used	None.

The 5 W's	Capture the 5 W's of an incident.
	• **Who** caused the incident?
	  ○ Unethical hackers
	• **What** happened?
	  ○ Employees received a phishing email with a malicious attachment that they installed and encrypted all their files.
	• **When** did the incident occur?
	  ○ Tuesday morning, approximately 9AM
	• **Where** did the incident happen?
	  ○ A small U.S. health care clinic.
	• **Why** did the incident happen?
	  ○ The incident occurred when malicious hackers exploited a phishing attack to infiltrate the company's systems. Once inside, they deployed ransomware that encrypted essential files. The attackers were likely financially motivated, as they left a ransom note demanding a significant payment in return for the decryption key.

Additional notes	1. Should we train employees to be able to identify phishing emails? 2. How should we proceed to retrieve the encrypted files?

Incident handler's journal

Date: July 19, 2025	**Entry:** #2
Description	Malicious phishing email with confirmed malware attachment investigated and contained.
Tool(s) used	Hash analysis system (confirmed malicious file)

The 5 W's	Capture the 5 W's of an incident.
	• **Who** caused the incident?
	  ○ External threat actor using email address: Def Communications <76tguyhh6tgftrt7tg.su> from IP 114.114.114.114
	  ○ Internal recipient: hr@inergy.com (176.157.125.93)
	• **What** happened?
	  ○ Phishing email delivered with malicious executable attachment (bfsvc.exe)
	  ○ Email used social engineering tactics (job application pretext with password-protected attachment)
	  ○ Attachment confirmed malicious via hash analysis: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
	• **When** did the incident occur?
	  ○ Email sent: Wednesday, July 20, 2022 09:30:14 AM
	  ○ Alert generated: Current investigation period
	• **Where** did the incident happen?
	  ○ Target: hr@inergy.com mailbox
	  ○ Source: External domain (.su TLD - suspicious)
	  ○ Network: Internal corporate email system
	• **Why** did the incident happen?

	○ Targeted phishing attack using job application social engineering ○ Attacker attempted to bypass security by password-protecting malicious file ○ Likely reconnaissance of company structure (targeting HR department)
Additional notes	

Incident handler's journal: Data Leak Incident

Date: July 21, 2025	**Entry:** #3
Description	Confidential company documents were accidentally shared publicly on social media.
Tool(s) used	NIST guidelines for access controls
The 5 W's	Capture the 5 W's of an incident. • **Who:** Sales team member and business partner • **What:** Internal documents about new products got shared on social media by mistake • **When:** During a business call, then posted online afterwards • **Where:** Started in a team meeting, then shared in video call, finally posted on social media • **Why:** Employee had access to too many files and forgot the rules about sharing
Additional notes	**Main problem:** People had access to files they didn't need for their job. **Solution:** Only give people access to what they need and remove access when done. This shows why the least privilege rule is important - only give minimum access needed.

Incident handler's journal: Network Monitoring Practice

Date: July 24, 2025	**Entry:** #4
Description	Practiced using Suricata tool to watch network traffic and create alerts.
Tool(s) used	Suricata (network monitoring tool), sample network data files, log analysis commands.
The 5 W's	Capture the 5 W's of an incident. • **Who:** Me (learning exercise) • **What:** Set up a rule to detect when someone visits websites, then checked the alerts it created • **When:** Training session • **Where:** Practice lab environment • **Why:** Learning how to monitor networks for suspicious activity
Additional notes	Created my first Suricata rule that watches for web requests (HTTP GET). The rule worked and caught 2 examples from the test data. Learned that eve.json files have more detailed info than fast.log files. The jq command helps read JSON files better. This is useful for spotting bad network activity in real networks.

Incident Handler's Journal - Reflections/Notes

Course Reflection Questions

1. **Were there any specific activities that were challenging for you? Why or why not?**

The phishing email analysis was particularly challenging because it required understanding multiple technical components simultaneously. Learning to interpret hash values, trace IP addresses, and recognize social engineering tactics while maintaining attention to detail proved demanding but valuable for developing comprehensive threat assessment skills.

2. **Has your understanding of incident detection and response changed since taking this course?**

My understanding has evolved from viewing incidents as isolated technical problems to recognizing them as complex security events requiring systematic investigation. The structured approach using the 5 W's framework and proper documentation has shown me that effective incident response relies heavily on methodical analysis and clear communication.

3. **Was there a specific tool or concept that you enjoyed the most? Why?**

I found Suricata network monitoring most engaging because it provides real-time visibility into network traffic patterns. Creating custom rules and analyzing the resulting alerts gave me practical hands-on experience in proactive threat detection, which feels more dynamic than reactive incident response alone.