Incident handler's journal

Date: 20/01/2025	**Entry:** 1
Description	A small U.S. healthcare clinic has faced a significant security incident that has caused major disruption to its operations. It appears to be the result of a ransomware attack carried out by a skilled group of malicious hackers, with multiple employees reporting that their files have been encrypted and new ransom notes are appearing on their devices.
Tool(s) used	N/A
The 5 W's	● Who caused the incident? ○ The ransomware note suggests the involvement of an organized group of unethical hackers. Further investigation is required to identify the specific individuals or entities responsible. ● What happened? ○ The attackers sent multiple targeted phishing emails, each containing a malicious file attachment that, when downloaded, installed malware on the employees' devices. As a result, employees reported being unable to access critical files, such as medical records, rendering their computers unusable. This disruption forced the shutdown of business operations, as employees could not access the necessary files or software to perform their duties. Additionally, ransom notes appeared on employees' computers, demanding payment in exchange for decryption keys. ● When did the incident occur? ○ Tuesday approximately 9:00am

	● Where did the incident happen? ○ A small U.S. health care clinic specialized in delivering primary-care services ● Why did this attack happen? ○ The incident resulted from a successful phishing attack, which allowed the attackers to infiltrate the organization's network, deploy ransomware, and demand a ransom. The underlying motivations for the attack, whether financial or otherwise, have yet to be determined.
Additional notes	To prevent similar attacks in the future, staff should receive training on how to identify phishing emails.

Date: 20/01/2025	**Entry:** 2
Description	Received an alert of a suspicious file being downloaded onto an employee's computer.
Tool(s) used	● SHA256 hash ● Virustotal
The 5 W's	● Who caused the incident? ○ Unknown email sender ● What happened? ○ An employee downloaded a file attached in an email and opened it, which caused a malicious payload to be executed on their device.

	● When did the incident occur? ○ 1:11pm ● Where did this incident happen? ○ At a financial services company ● Why did this attack happen? ○ An employee downloaded the file as it wasn't stopped by the email filter which then led to the payload being executed
Additional notes	The behavior described by the employee matches the activity reported on VirusTotal, which includes actions such as creating new processes, modifying files, setting registry keys, and performing various other malicious activities. Future lessons to be learnt is improving the email filter, and also staff training on how to spot malicious emails.

Date: 21/01/2025	**Entry:** 3
Description	An alert came in for a phishing attempt with possible download of malware
Tool(s) used	Phishing Playbook
The 5 W's	● Who caused the incident? ○ The email address of the sender is Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114> ● What happened? ○ An employee was sent a phishing email that held a password-protected malicious file. The email was disguised as applying for a job with the attached file claiming to be a

	password protected resume. ● When did the incident occur? ○ Wednesday, July 20, 2022 09:30:14 AM ● Where did the incident happen? ○ Inergy ● Why did this attack happen? ○ The organization’s email filter did not detect/block the malicious file, which could have been done through the file’s SHA256 hash.
Additional notes	Check email filter rules to see why the email wasn’t blocked by the email filter in place.

Date: 21/01/2025	**Entry:** 4
Description	Final report review for data breach experienced at mid sized retail company.
Tool(s) used	N/A
The 5 W's	● Who caused the incident? ○ Not known ● What happened? ○ An employee was targeted with a ransom email in which the attacker claimed to have stolen consumer data and demanded a $25,000 payment in cryptocurrency. Subsequently, the employee received a second email that included proof of the stolen information and raised the ransom request to $50,000. ● When did the incident occur?

	○ December 22 2022, 3:13 pm PT ● Where did the incident happen? ○ Mid sized retail company, their e-commerce web application had a vulnerability ● Why did this attack happen? ○ The attacker took advantage of a vulnerability in the organization’s website through a forced browsing attack, which enabled them to access and steal customer purchase confirmation pages and sensitive customer data.
Additional notes	The website lacked sufficient security controls to prevent such an attack. In response, the organization is taking several actions, including conducting routine vulnerability scans, performing penetration tests, implementing allowlisting for a specific set of URLs, and ensuring that only authenticated users can access certain content.

Reflections/Notes:

1. Were there any specific activities that were challenging for you? Why or why not?
    a. The Suricata activity was the most time-consuming for me because it involves using the CLI, which made it more difficult to process all the information that was being output at once.
2. Has your understanding of incident detection and response changed since taking this course?
    a. Yes, definitely! I've learned a lot about the incident response lifecycle, especially how different tiers of security team members have distinct roles and responsibilities throughout the process.
3. Was there a specific tool or concept that you enjoyed the most? Why?
    a. I found Chronicle to be particularly fascinating because of its integration with VirusTotal. It provides powerful tools for further investigating related domains and IP addresses, which really added to the depth of the analysis.