Incident handler's journal

Date: 2025-01-15	**Entry:** #1
Description	Documenting a cybersecurity incident that occurred in the USA
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ An organized group of known threat actors. ● **What** happened? ○ A ransomware security incident ● **When** did the incident occur? ○ Tuesday at 9 AM ● **Where** did the incident happen? ○ At a healthcare clinic in the US ● **Why** did the incident happen? ○ The threat actors gained access to the company's system through a phishing attack. Once inside, they deployed ransomware that encrypted critical and confidential files. The ransom note demanded payment in exchange for the decryption key, indicating that the primary motivation for this attack was financial gain.
Additional notes	1. Should the company pay the ransom to get the decryption key? 2. What could the company do to prevent any similar incidents from happening in the future? 3. What other areas the company can improve to strengthen to mitigate

	common targetted attacks?

Date: 2025-01-16	**Entry:** #2.
Description	Investigating a suspicious file that was downloaded onto an employee's computer.
Tool(s) used	Sha256sum VirusTotal Phishing playbook
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ Advanced threat actor likely named BlackTech ● **What** happened? ○ An employee received an email containing an attachment with a password. The employee downloaded and opened the file, which resulted in the creation of an unauthorized executable. The intrusion detection system (IDS) detected this activity and triggered an alarm to the Security Operations Center (SOC). ● **When** did the incident occur? ○ Email received: 1:11 PM ○ File downloaded and opened: 1:13 PM ○ Executable files created: 1:15 PM ○ IDS detection: 1:20 PM ● **Where** did the incident happen? ○ Financial Services Company

	● **Why** did the incident happen? ○ The incident occurred because a threat actor successfully deployed a phishing email, convincing the employee to download and open a malicious file. When the file was opened, an unauthorized executable was triggered. The root cause appears to be a combination of social engineering and insufficient user awareness or email security controls. No critical data has been reported as compromised so far. **Escalation Details** Escalation Reason: The email attachment has been confirmed as malicious using VirusTotal. Given the severity of the findings and the confirmed threat, the incident is being escalated for further investigation and remediation. Next Steps: The incident has been escalated to a Level 2 SOC analyst for deeper analysis, containment and remediation.
Additional notes	1. What can the company do to prevent unauthorized attachments from being downloaded? 2. What can the security team do to prevent unauthorized executables from running?

Date: 2025-01-17	**Entry:** **#3**
Description	Documenting a security incident that occurred before starting working
Tool(s) used	Final Report

The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ A threat actor or threat actors ● **What** happened? ○ An employee received two emails on separate occasions from the same sender. The first email claimed that customer data had been stolen and demanded a ransom of $25,000. The second email included a sample of the stolen data and an increased ransom demand of $50,000. The employee deleted the first email, assuming it was spam, but notified the security team after receiving the second email. ● **When** did the incident occur? ○ December 22, 2022, at 3:13 p.m. PT: The first email was received, claiming customer data was stolen with a ransom demand of $25,000. ○ December 28 2022 at 7:20 p.m. PT: The second email was received, including a sample of stolen data and a higher ransom demand of $50,000. ● **Where** did the incident happen? ○ Retail Company ● **Why** did the incident happen? ○ The incident occurred because the attackers exploited a vulnerability in the e-commerce web application. This allowed them to perform a forced browsing attack by modifying the order number in the URL of a purchase confirmation page. This vulnerability provided access to sensitive customer transaction data, which was then exfiltrated.
Additional notes	1. The principle of least privilege could have helped limit the damage from this incident by restricting access to sensitive data. 2. Ignoring or deleting the first email was not a viable option. A clear

	process should be established for handling these types of scenarios, such as promptly reporting suspicious emails to the security team for further investigation.

Date: 2025-01-21	**Entry:** #4
Description	Investigating a phishing email received by an employee., containing a suspicious domain name: `signin.office365x24.com`.
Tool(s) used	Google Chronicle
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ Unknown threat actor/s attempting to impersonate office365 service ● **What** happened? ○ An employee received a phishing email containing a suspicious domain name (`signin.office356x24.com`). The domain appears to mimic Office365, potentially aiming to steal employee credentials. Investigating to identify whether other employees have received similar emails and if they have interacted with the suspicious domain. ● **When** did the incident occur? ○ 2023-Jan to 2023-July ● **Where** did the incident happen? ○ Financial Company

	● **Why** did the incident happen? ○ Threat actors sent a phishing email to impersonate a legitimate service (Office365), exploiting social engineering tactics to lure employees into visiting a malicious domain and providing sensitive information.
Additional notes	● VirusTotal Report Results: ○ The domain `signin.office365x24.com` has been flagged as malicious/phishing by multiple vendors on VirusTotal. ● Affected Assets: ○ A total of 6 assets have interacted with the domain. ■ Assets with POST Requests (data likely sent): ashton-davidson-pc (multiple POST requests) emil-palmer-pc (multiple POST requests) ○ Other assets observed: bruce-monroe-pc coral-alvarez-pc jude-reyes-pc Roger-spence-pc ● Related Indicators of Compromise (IoCs): ○ A related domain, `signin.accounts-gooqle.com`, was identified from resolved IPs. This domain impersonates Google's sign-in service and does not yet have VirusTotal results. ○ Additional Affected Assets for signin.accounts-gooqle.com: ■ Assets with POST Requests (data likely sent): warren-morris-pc ■ Other assets observed: amir-david-pc

Date: 2025-01-21	**Entry:** #5
Description	Analyzing a packet capture file.
Tool(s) used	Wireshark using Try Hack Me and completed carnage room
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? NA ● **What** happened? NA ● **When** did the incident occur? NA ● **Where** did the incident happen? NA ● **Why** did the incident happen? NA
Additional notes	The GUI interface of Wireshark along with the advanced features available to filter and apply themes to the filtered data is exciting to see.