Incident handler's journal

Date: August 10	**Entry:** 1
Description	US based health clinic ransomware attack
Tool(s) used	**N/A**
The 5 W's	The attack was done by a group of unethical hackers known for targeting companies in healthcare and transportation. The group of hackers targeted the healthcare clinics employees with phishing emails and those emails contained a malicious attachment to install malware once it was downloaded. The attack took place at a small U.S. based healthcare clinic on a Tuesday morning at exactly 9AM
Additional notes	They need a contingency plan and employee training. How can they prevent this from happening again?

Date: August 15	**Entry:** 2
Description	Phishing incident
Tool(s) used	Company Level 1 SOC Analyst playbook

The 5 W's	The phishing email was received and downloaded from a potential employee that sent an email to HR inquiring about a job from our website for an infrastructure engineer. The email had a resume and cover letter attachment which was password protected and after further investigation of the attachments file hash I found that it had already been verified as malicious. The incident took place on July 20, 2022 at 9:30:14 am
Additional notes	There were several red flags in the email that should have alerted a properly trained employee to open that attachment. Training is needed

---

Date: August 28	**Entry:** 3
Description	Data Breach final report review
Tool(s) used	Final Report
The 5 W's	On December 22, 2022 at 3;13pm an employee received a ransomware email in which the sender stated that they had stolen customer data and in exchange for not releasing that information they wanted $25,000. That employee took that email to be spam and deleted it but received another email on December 28,2022 with a sample of the customer data and an increased request for $50,000 at which point they notified our security team. The incident was because of a vulnerability in the web application which allowed the hacker to perform a forced browsing attack and modify data in the URL string.
Additional notes	ITo prevent future occurrences we will be performing routine vulnerability

	scans and implementing access controls that ensure only authenticated users are authorized access to content

---

Date: September 4	**Entry:** 4
Description	Security incident: Phishing
Tool(s) used	Chronicle SIEM
The 5 W's	An employee at our company received a phishing email in their inbox. Using Chronicle i found that GET and POST http request were made which could suggest a possible successful phish and that multiple assets could be impacted
Additional notes	Logs show that login information was submitted to the suspicious domain through POST request

---
