Incident handler's journal

Date: 25/08/2023	**Entry: EN001**
Description	A security incident has occurred at a U.S. Healthcare clinic. The incident involved unethical hackers and resulted in the encryption of all organization files and software, rendering them unavailable due to a ransomware attack.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **What:** The incident was caused by unethical hackers who executed a ransomware attack. • **WHO**: Malicious actor or Hacker. • **When:** The incident took place on Tuesday at 9:00 am. • **Where:** The incident occurred at the healthcare clinic, in several employees' machines. • **Why:** The motivation behind the attack seems to be financial gain. The hackers are demanding a monetary payment to release the encrypted data.
Additional notes	The attack targeted several employees' machines at the clinic. The hackers gained access through a phishing attack, wherein employees received an email with a malicious attachment. This indicates that employees might not be familiar with email attacks and security practices.

Date: 28/08/2023	**Entry: EN002**
Description	An alert has been received about a suspicious file being downloaded on an employee's

	computer in a financial services company and working as a SOC analyst. (Ticked A-2703)
Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. ● An external and malicious actor caused the incident; ● A suspicious file was downloaded and executed on the employee's computer; ● Early in the afternoon, at 1:11 p.m; ● On the employee's computer from the company; ● The incident happens because the employee received an email containing an attachment and the password and he downloaded it;
Additional notes	After a short investigation I realize the attachment was a spreadsheet file and the password was provided in the email. After the download a malicious payload was executed on the computer;

Date: 28/08/2023	**Entry: EN003**
Description	Analize and evaluation of security incident with ticket A-2703;
Tool(s) used	Playbook
The 5 W's	Capture the 5 W's of an incident. ● The incident was caused by an external incoming email; ● An employee downloaded a suspicious attachment on his computer; ● Early in the morning at 9:30 AM; ● In the employee's workstation at the company; ● Because the email has a malicious payload inside the attachment, after the download it was executed on the computer;

Additional notes	The phishing alert appears to be legitimate due to several critical indicators present in the email. Firstly, the sender's email is from an unfamiliar domain, resembling that of a temporary email service. Secondly, the presence of misspellings and errors serves as an additional red flag, suggesting potentially fraudulent activity. Lastly, it is important to note that if the email claims to contain a resume in a spreadsheet format, the attachment's file extension should not be associated with executable files

---

Date: 28/08/2023	**Entry: EN004**
Description	Review of the final report about data breach incident;
Tool(s) used	Final Report
The 5 W's	Capture the 5 W's of an incident. ● The incident was caused by an external malicious actor; ● A vulnerability in the e-commerce web application was exploited and customer´s data was collected; ● The first hacker contact was in December 22 at 3:13 pm and the second in December 28; ● The contact was made to an employee’s email; ● The reason seems to be financial, because a first cryptocurrency payment demand was made in the first contact and when ignored, the demand increase in the second contact;
Additional notes	After analysis the vulnerability was found in the web application and seems to allow the access to thousands of purchase and customer’s data.