Incident Manager Log

Date: 2025–05-05	**Entrance** : 1
Description	Cybersecurity incident report involving ransomware that caused a major service disruption at a small US primary care clinic.
Tool(s) used	None
QQQOP	• **Who:** An organized hacker group known for targeting the healthcare and transportation sectors. • **What:** A security incident involving ransomware • **Where :** In a small healthcare company, located in the United **States** • **When:** Tuesday morning, around 9 a.m. • **Why:** The incident was caused by a group of malicious hackers who gained access to the company's systems through a **ransomware attack** (phishing attack) . They then deployed their ransomware within the company's systems and encrypted critical files. The group is demanding a large ransom in exchange for the decryption key, suggesting a clear financial motivation.
Other remarks	**1. Prevention** : The company could reduce future risks by: • Training its employees to recognize phishing attempts. • Implementing a powerful email filter. • Performing regular, offline backups. • Updating systems and software regularly. **2. Pay the ransom?:** Payment is not **recommended** by the competent authorities (e.g. FBI, ANSSI), because: • There is no guarantee of data recovery. • This fuels the business model of cybercriminals. • Alternatives exist through recovery specialists or through backups (if available).