DOTLAKE IN THE HEALTHCARE SECTOR

Whitepaper

DOTLAKE
DOTLAKE.IO

THE IMPORTANCE OF CYBERSECURITY IN THE **HEALTHCARE SECTOR**

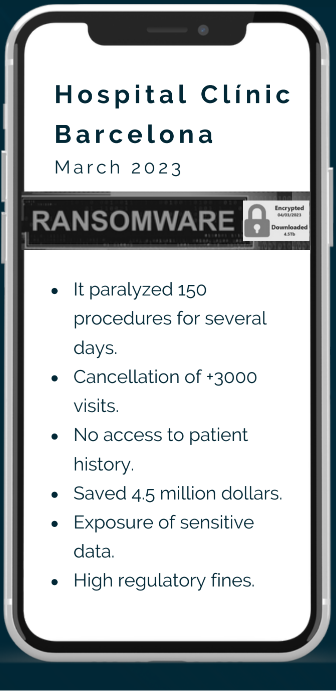
In the current world, the healthcare sector has become more reliant on technology to provide quality and efficient medical care. However, this growing interconnection has also increased exposure to cyber threats, with attacks on this sector **growing by 650%** in the last year, underscoring the urgent need for a robust cybersecurity infrastructure.

The healthcare sector stores a large amount of confidential patient data and carries out critical life-saving operations. The interconnection of systems, telemedicine, and cloud data storage have provided countless benefits, but have also created opportunities for devastating cyber attacks.

This whitepaper provides key recommendations for **strengthening healthcare system protection with Dotlake**.

PROTECTION OF SENSITIVE DATA

Medical, financial, and personal data stored within healthcare systems are valuable to cybercriminals. A security breach could lead to identity theft, financial fraud, and irreparable damage to both the patient's and hospital's reputation.



Hospital Clínic Barcelona

March 2023

- It paralyzed 150 procedures for several days.
- Cancellation of +3000 visits.
- No access to patient history.
- Saved 4.5 million dollars.
- Exposure of sensitive data.
- High regulatory fines.

AVAILABILITY OF MEDICAL SERVICES

Cyberattacks can disrupt the provision of vital medical services, jeopardizing the health and lives of patients. Electronic medical record systems and critical hospital infrastructures are attractive targets for attackers.

DATA INTEGRITY

The malicious alteration of electronic medical records or test results could lead to incorrect medical decisions and inappropriate treatments, jeopardizing patients' health.

To help you **monitor and prevent such attacks** even before they can pose a real threat, **Dotlake CTI** (Cyber Threat API) emerges. This solution is responsible for collecting information in an automated manner from the deep web, darknets, ransom sites, and the most significant cybercriminal forums in the market, so you can consume it quickly and safely.

What does Dotlake CTI offer you?

- **Detect real-time mentions at the earliest stage** of the supply chain, providing a rich contextual view and severity of each threat.
- **Receive early alerts** related to your company's assets, products, credentials, as well as mentions of your brand.
- **Access to a portal web** where you can thoroughly investigate your company's **risk level**.

And not only that...

With Dotlake, you'll also be able to stay informed about the **latest tactics, techniques, and procedures (TTPs)** being used by cybercriminals. For example, you can monitor what vulnerabilities companies in your sector are facing, ensuring you are updated and covered against constantly evolving threats.

By **digital surveillance** your assets, you can have control over all of them and even your suppliers, ensuring **no breaches in your supply chain**.

It will allow you to stay vigilant if companies in your same sector are undergoing "**Threat Hunting**" attacks, thus enabling you to detect in a timely manner that any vulnerabilities others have suffered cannot affect your company.

CONCLUSION

Cybersecurity in the healthcare sector is essential to **safeguard sensitive data**, **ensure the availability of medical services, and preserve the integrity of patient care**. Recent cyberattacks have shown the **devastating consequences** of cybersecurity negligence. By addressing these challenges with robust preventive measures offered by **Dotlake CTI**, the healthcare sector can continue to provide **safe and efficient care** in an increasingly complex digital environment.