



DOTLAKE EN EL SECTOR SALUD

Whitepaper

LA IMPORTANCIA DE LA CIBERSEGURIDAD EN EL **SECTOR SALUD**

En el mundo actual, el sector de la salud se ha vuelto más dependiente de la tecnología para brindar atención médica de calidad y eficiencia. Sin embargo, esta creciente interconexión también ha aumentado la **exposición a amenazas cibernéticas**, creciendo un **650% los ataques** a este sector durante el último año, lo que subraya la necesidad urgente de una sólida infraestructura de ciberseguridad.

El sector salud almacena una gran cantidad de datos confidenciales de pacientes y realiza operaciones críticas para salvar vidas. La interconexión de sistemas, la telemedicina y el almacenamiento de datos en la nube han brindado innumerables beneficios, pero también han creado oportunidades para ataques cibernéticos devastadores.

Este whitepaper ofrece recomendaciones clave para **fortalecer con Dotlake** la protección de los sistemas de salud.

PROTECCIÓN DE DATOS SENSIBLES

Los datos médicos, financieros y personales almacenados en los sistemas de salud son valiosos para los ciberdelincuentes. Una violación de seguridad podría llevar al robo de identidad, fraude financiero y un daño irreparable a la reputación del paciente y del hospital.



DISPONIBILIDAD DE SERVICIOS MÉDICOS

Los ataques cibernéticos pueden interrumpir la prestación de servicios médicos vitales, poniendo en peligro la salud y la vida de los pacientes. Los sistemas de registro médico electrónicos y las infraestructuras críticas de hospitales son objetivos atractivos para los atacantes.

INTEGRIDAD DE LOS DATOS

La alteración maliciosa de los registros médicos electrónicos o los resultados de las pruebas podría conducir a decisiones médicas incorrectas y tratamientos inapropiados, poniendo en peligro la salud de los pacientes.

Para **ayudarte monitorizar y prevenir dichos ataques** incluso antes de que puedan suponer una amenaza real aparece **Dotlake CTI** (Cyber Threat API), una solución que se encarga de recopilar información de forma automatizada de la deep web, darknets, ransomsites y foros ciberdelinquentes más importantes del mercado para que puedas consumirla de forma rápida y segura.

¿Qué te ofrece Dotlake CTI?

- **Detectar menciones en tiempo real** en la etapa más temprana de la cadena de suministro, proporcionando una rica visión contextual y gravedad de cada amenaza.
- **Recibir alertas tempranas** relacionadas los **activos**, productos, credenciales de tu empresa, así como menciones a tu marca.
- **Acceso a un portal** donde poder investigar en profundidad el **nivel riesgo** de tu empresa.

Y no solo eso...

Con Dotlake además podrás estar informado de cuales son las últimas **tácticas, técnicas y procedimientos (TTPs)** que están utilizando los ciberdelincuentes. Por ejemplo, podrás monitorizar ante que vulnerabilidades se están enfrentando empresas de tu sector y así asegurarte de que estás actualizado y cubierto frente a las amenazas que están en constante evolución.

Mediante la **vigilancia digital** de tus **activos**, podrás tener control sobre todos ellos e incluso de tus **proveedores** para así no sufrir ninguna brecha en tu cadena de suministro.

Además te permitirá **mantenerte alerta**, si empresas de tu mismo sector están siendo atacadas "**Threat Hunting**", y así poder detectar a tiempo que cualquier vulnerabilidad que hayan sufrido otros no pueda afectar a tu compañía.

CONCLUSIÓN



La ciberseguridad en el sector salud es esencial para **proteger datos sensibles, garantizar la disponibilidad de servicios médicos y preservar la integridad de la atención al paciente**. Los recientes ataques cibernéticos han demostrado las **consecuencias devastadoras** de la negligencia en la seguridad cibernética. Al abordar estos desafíos con medidas preventivas sólidas ofrecidas por **Dotlake CTI**, el sector salud puede continuar brindando **atención segura y eficiente** en un entorno digital cada vez más complejo.