



DOTLAKE EN EL SECTOR INDUSTRIAL

Whitepaper

DOTLAKE EN EL SECTOR INDUSTRIAL

En la era de la digitalización y la automatización, el sector industrial se ha transformado significativamente para aprovechar los **avances tecnológicos** y **mejorar la eficiencia operativa**. Sin embargo, esta creciente dependencia de la tecnología también ha **incrementado la exposición a ciberamenazas** que podrían tener impactos devastadores en la seguridad y la economía.

España se sitúa como el cuarto país en Europa con más ataques al sector industrial, con un 26,3%, por detrás de Portugal, Estonia y Letonia.

¿Qué es **Dotlake**?

Dotlake es una solución de ciberinteligencia que se encarga de recopilar información de forma **automatizada** de la open y deep web, incluidos **ransomsites, mercados de fraude, grupos y canales de telegram y foros ciberdelictivos** más importantes del mercado.

SolarWinds

2020

Los atacantes comprometieron actualizaciones de software de SolarWinds, lo que les permitió acceder a numerosas organizaciones gubernamentales y privadas.

Hyundai y Mitsubishi Electric

2020

Estas empresas sufrieron vieron comprometidas tanto redes internas, como información confidencial de la empresa y su propiedad intelectual.

Colonial Pipeline

2021

Una importante red de oleoductos en EEUU, sufrió un ataque de ransomware que resultó en la interrupción de la distribución de combustible en la costa este.

¿Cómo te puede ayudar **Dotlake**?

- Detecta **menciones a tu marca, activos digitales** relevantes para tu empresa **o credenciales** de tus empleados en **tiempo real** en la etapa más temprana de la amenaza con nuestro **sistema de alertas automatizado**.
- **Accede a nuestro portal** donde poder investigar en profundidad los datos encontrados, la actividad de los ciberdelictivos y **contextualizar** la **gravedad** de la exposición.
- **Protege tu propiedad intelectual** garantizando la producción continua y la preservación de la confianza de los clientes

Y no solo eso...

Con Dotlake además podrás estar informado de cuales son las últimas tácticas, técnicas y procedimientos (**TTPs**), explorar que vulnerabilidades sufren empresas de tu mismo sector (**Threat Hunting**), detección de un posible fraude y protección de personas de alto cargo de tu empresa...