



# **DOTLAKE EN EL SECTOR DE AUTOMOCIÓN**

Whitepaper

# ¿PORQUÉ LA CIBERSEGURIDAD ES IMPRESCINDIBLE EN EL SECTOR DE LA AUTOMOCIÓN?

La creciente digitalización y conectividad en la industria automovilística ha brindado numerosas ventajas, pero también ha expuesto a los fabricantes de automóviles y empresas del sector a la amenaza constante de ciberataques. Estos ataques pueden tener consecuencias devastadoras, desde la pérdida de datos confidenciales hasta la manipulación remota de vehículos. En este artículo, examinaremos algunos de los ciberataques más importantes que han afectado a empresas automovilísticas en los últimos años, destacando la importancia de la seguridad cibernética en esta industria en constante evolución y como **Dotlake Cyber Threat API** te ayuda a monitorizar y prevenir los ataques.

**2015**

Ataque al sistema de entretenimiento y navegación de **Fiat Chrysler** donde se descubrió una vulnerabilidad que permitía a los hackers tomar el control remoto de un vehículo.

**2017**

Ransomware en **Honda** en el que los sistemas informáticos clave de la empresa fueron cifrados, lo que llevó a una interrupción significativa de la producción.

Ataque al sistema de acceso remoto de **Tesla** en el que un grupo de hackers logró comprometer el sistema de acceso remoto de **Tesla**

**2020**

**Hyundai** y **Mitsubishi Electric** sufrieron ciberataques comprometiendo tanto redes internas, como información confidencial de la empresa y su propiedad intelectual.

**Dotlake** se encarga de recopilar información de forma automatizada de la deep web, darknets, ransomsites y foros ciberdelictivos más importantes del mercado para que puedas consumirla de forma rápida y segura.

## ¿Qué te ofrece **Dotlake**?

- 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 todo lo relacionado con el sistema sin llave o 'keyless', que es uno de los ciberataques más comunes contra los vehículos y así asegurarte de que estás actualizado 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 del sector automovilístico 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

Los ciberataques en la industria automotriz han demostrado ser una amenaza real y preocupante en la era digital. Generando un impacto significativo, no solo en términos de **daños financieros**, sino también en la **confianza de los consumidores** y en la **reputación de las empresas**.

A medida que la industria automotriz continúa innovando y adoptando tecnologías emergentes como la conducción autónoma, la **ciber seguridad** debe convertirse en una **prioridad absoluta**.

Para detectar y solucionar las vulnerabilidades, es necesario enfrentarlas en todas las fases del proceso, desde la etapa de diseño y creación de los vehículos hasta la administración de la cadena de suministro y la protección de la información sensible.



Solo a través de un enfoque proactivo y la **colaboración continua** entre las empresas, los reguladores y los expertos en ciberseguridad, se podrá garantizar un futuro seguro y confiable para la industria automovilística en la era digital