DARKTRACE INDUSTRIAL



# Ciberdefensa para petróleo y gas

En los últimos años, la industria de petróleo y gas ha visto cómo se acelera la digitalización de sus operaciones. A medida que el sector cosecha enormes beneficios como una mayor eficacia y agilidad, este movimiento también ha cambiado radicalmente el paradigma de la seguridad. Las empresas de petróleo y gas se ven obligadas ahora a proteger dispositivos de campo, sensores y sistemas de control conectados, así como sistemas heredados, a menudo con poco ancho de banda y en ubicaciones remotas y desafiantes.

> Con la convergencia de la tecnología operativa (OT) y la tecnología de la información (TI), la industria se enfrenta tanto a las amenazas cibernéticas tradicionales como a nuevos ataques contra entornos industriales.

Estos entornos ciberfísicos mixtos presentan una serie única de desafíos para los equipos de seguridad sometidos a presión. Las soluciones tradicionales para proteger las redes informáticas no están preparadas para este fin: resultan insuficientes para defender estos complejos entornos híbridos contra un adversario en constante evolución.

> Darktrace proporcionará a los clientes información e inteligencia procesable para que puedan identificar y neutralizar estas amenazas con mayor rapidez y proteger los activos críticos frente a ataques dañinos y costosos.
>
> **Aymeric Sarrazin, vicepresidente senior de Siemens**

Big West Oil LLC

DOLPHIN ENERGY دولفين للطاقة

## Amenazas en números

### **68%** de las empresas de petróleo y gas se han enfrentado a algún peligro en 2016-17

Según Ponemon Institute, el 68% de la empresas de este sector han visto su ciberseguridad comprometida al menos un vez. Una de las principales vulnerabilidades es el envejecimiento y obsolescencia de los sistemas de control, de los que se depende en todas las etapas, desde la exploración y producción, al refinado y distribución. A menudo, estos han sido creados mucho antes de que la ciberseguridad fuera considerada una prioridad empresarial, por lo que son mucho más difíciles de parchear, lo que da lugar a vulnerabilidades en la seguridad de las infraestructuras dejando a las empresas expuestas a ataques malintencionados.

### **46%** de los ciberataques en entornos de OT pasan desapercibidos

Ponemon Institute también informó de que una media del 46% de todos los ataques cibernéticos que se producen el entorno de las OT pasan inadvertidos. Teniendo en cuenta los numerosos elementos distintos que participan en los procesos del petróleo y el gas, así como el gran número de sistemas que funcionan en tándem, lograr visibilidad a través de infraestructuras distribuidas y sitios remotos es increíblemente difícil de lograr. Sin embargo, esta falta de visibilidad significa que los atacantes pueden mantener un bajo perfil en entornos de OT durante largos períodos de tiempo, lo que les permite llegar a comprender profundamente la red antes de atacar.

### **29%** de las empresas de petróleo y gas no disponen de una visión en tiempo real de las ciberamenazas

Para proteger adecuadamente las redes de las que dependen las empresas de petróleo y gas, resulta fundamental detectar las amenazas en tiempo real. La detección temprana es clave para detener las amenazas en sus inicios y defender los entornos de OT antes de que se vea comprometida la eficacia operativa. Dada la tradicional pila de seguridad de las redes de OT, las empresas de petróleo y gas necesitan implementar tecnologías innovadoras con capacidad de autoaprendizaje para defenderse contra un panorama de amenazas en constante cambio.

## Darktrace Industrial

Algunas de las empresas más importantes del mundo de petróleo y gas confían en Darktrace Industrial para defender sus complejos entornos industriales de ciberamenazas. Ya se trate del sector upstream, midstream o downstrean, Darktrace Industrial se puede implementar en entornos industriales, en cada etapa de las operaciones, para proteger la producción y el transporte de petróleo y gas.

Darktrace Industrial es la tecnología de Ciber IA líder mundial que implementa un 'sistema inmunológico' en tiempo real para ambos entornos, TI y OT, para defender los dispositivos conectados en red de todo el espectro de ciberamenazas, desde ataques de ramsomware a velocidad de la máquina hasta cibercampañas de bajo perfil, sutiles y furtivas, en redes.

Basado en inteligencia artificial de nivel empresarial, Darktrace Industrial aprende el 'patrón de vida' de cada controlador y estación de trabajo de la red de control y de cada usuario y dispositivo de la red corporativa, llegando a comprender profundamente la 'forma de ser' de todo el entorno. Esta paulatina comprensión de lo 'normal' permite a Darktrace Industrial detectar los primeros indicadores de una amenaza incipiente sin depender de reglas, firmas ni presuposiciones.

Gracias a la capacidad para reconocer los diversos y complejos entornos en los que operan las empresa de petróleo y gas, Darktrace Industrial también puede soportar un ancho de banda reducido, así como entornos inhóspitos, empleando robustos sensores industriales.

> La exclusiva tecnología de autoaprendizaje de Darktrace Industrial representa un cambio radical en la defensa de los entornos industriales, permitiendo proteger entornos únicos sin distinguir OT, TI ni dispositivos del IoT.

Las implementaciones remotas en plataformas pueden incluir análisis y creación de modelos locales, así como una correlación central para la monitorización de la seguridad de todos los activos.

## Darktrace Industrial en acción

### Descargas sospechosas e infección de Serpent ransomware

En una empresa integrada de refinado y suministro de petróleo, Darktrace Industrial identificó los primeros signos de una infección de ransomware en la red de la empresa. Además de la escritura de sus propios archivos de notas de rescate, se detectó que un dispositivo de escritorio estaba estableciendo una serie de conexiones a destinos externos extraños a través de un servidor proxy para, a continuación, descargar archivos maliciosos.

El dispositivo procedió a realizar distintas consultas de directorios SMB, aumentando la serie de acciones anómalas. Habiendo identificado el ransomware con antelación, Darktrace Industrial fue capaz de reconocer que esta actividad coincidía estrechamente con el patrón de comportamientos de la infección del ransomware Serpent.

Darktrace Industrial alertó al equipo de seguridad sobre este patrón de comportamientos incriminatorio antes de que la infección fuera capaz de propagarse en el entorno de las OT.

### Reconocimiento detectado desde un dispositivo externo incluido en la lista negra

En el corazón de una empresa de producción de petróleo y gas se detectaron actividades de reconocimiento interno. Se descubrió que un dispositivo externo, incluido en una lista negra, con una dirección IP en China se estaba conectando a varios elementos clave de la infraestructura de la red mediante una VPN. Después de conectarse brevemente al controlador de dominio, seguidamente se conectaba a la computadora y el servidor de correo electrónico de un empleado, intentando acceder a través de tres puntos de entrada diferentes. El dispositivo fue incluso más lejos y llegó a comprobar la presencia de un honeypot, que podría haber señalado su presencia.

Darktrace Industrial detectó este intento de exploración maliciosa en sus primeras etapas, proporcionando al equipo de la posibilidad de reforzar sus defensas para garantizar que no se producía ningún riesgo.


### Contacto

Norteamérica: +1 (415) 229 9100
Europa: +44 (0) 1223 394 100
Asia-pacífico: +65 6804 5010
América Latina: +55 11 97 242 2011

**info@darktrace.com**
**darktrace.com/industrial**