Kaspersky OT CyberSecurity

Un ecosistema de seguridad ciberfísica
para empresas industriales

Solid Servicios

kaspersky BRING ON THE FUTURE

Kaspersky Sobre la ciberseguridad

Unified Industrial Safety Concept

Tecnologías

Una sólida selección de soluciones de seguridad industrial probadas, compatibles y aprobadas

Conocimiento

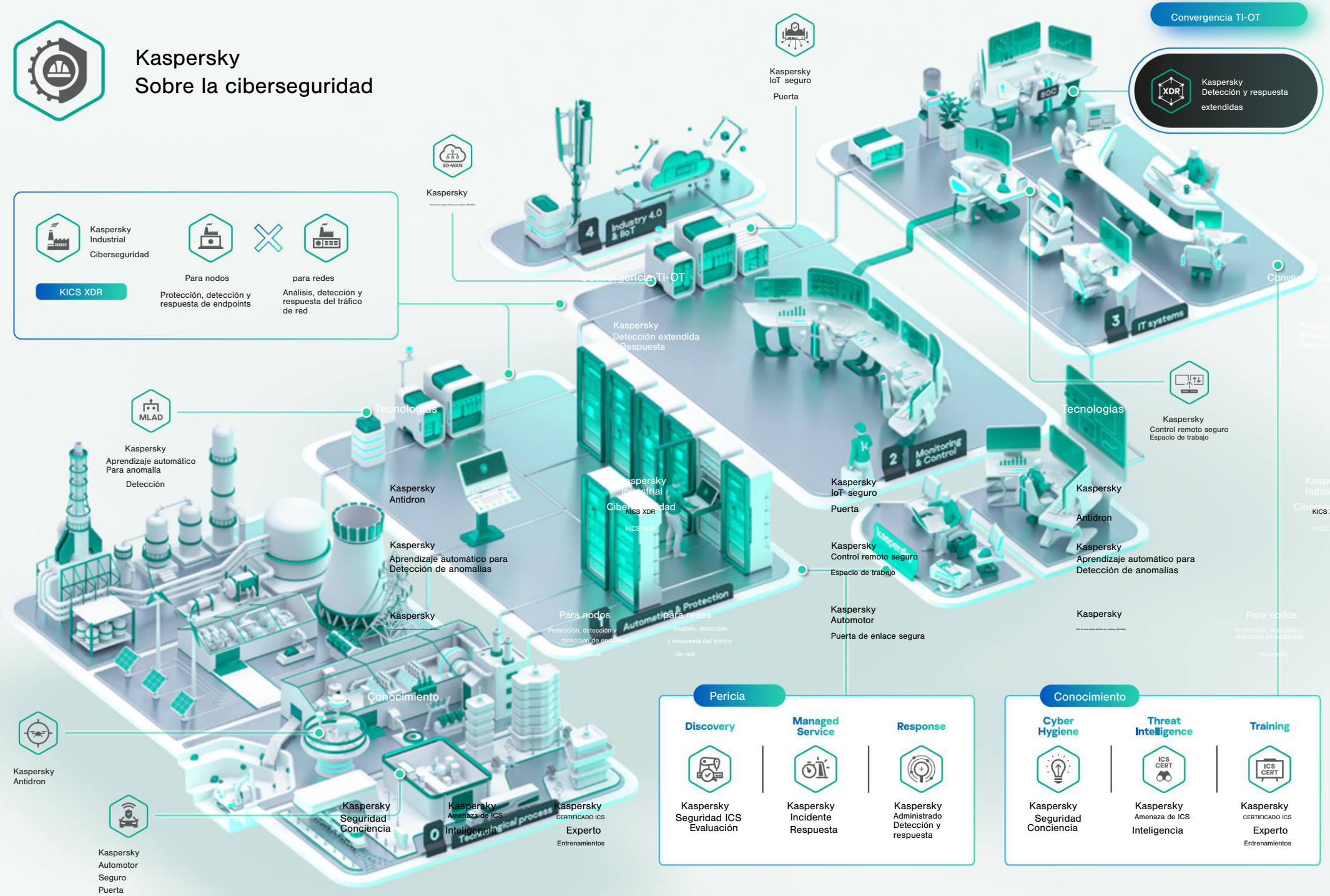
Análisis de amenazas confiables y capacitación integral en ciberseguridad industrial

Pericia

Una gama completa de servicios profesionales para una ciberseguridad industrial integral

Solid Servicios

Kaspersky
Sobre la ciberseguridad



Visita el sitio web

Kaspersky Industrial Ciberseguridad

XDR

TECNOLOGÍA

Solid Servicios

Native XDR platform to protect automation systems

- Revela amenazas ocultas, anomalías, vulnerabilidades e intentos de intrusión mucho antes de que se vuelvan peligrosos para sus operaciones.
- Certificado por proveedores de automatización y reguladores
- Sin efectos adversos sobre los procesos tecnológicos. Previene daños inaceptables
- Facilita la gestión de infraestructura de automatización distribuida y compleja y la respuesta a incidentes.
- Ayuda a mitigar los riesgos y mantener un registro de violaciones.

Advantages of the XDR platform

Cobertura de extremo a extremo para sistemas de automatización y control industrial (IACS). Protección para equipos Linux, Windows, aislados o de terceros, así como detección de anomalías y amenazas de red.

Auditoría de seguridad activa y/o pasiva de endpoints y redes.

Gestión centralizada de riesgos, políticas de seguridad y activos en todos los niveles del IACS.

Excelentes sistemas y visibilidad de red.
Investigació y reconstrucció de toda la cadena de muerte. Visualización de la progresió de incidentes en redes industriales y diferentes nodos.

Comprar a un socio Solicitar una demostración

Ficha de datos

es.ics.kaspersky.com

Visita el sitio web

Kaspersky Detección y respuesta extendidas

TECNOLOGÍA

Unified cybersecurity across the industrial and corporate segments of your enterprise

Gracias a la estrecha integración con Kaspersky Extended Detection & Response, la plataforma Kaspersky Industrial CyberSecurity permite nuevos escenarios que incluyen interacciones con soluciones de terceros, con capacidades de investigación y respuesta mejoradas. La plataforma también ayuda a proteger su empresa no solo en entornos industriales, sino también en aquellos en los que los entornos industriales y corporativos se superponen. Esto se logra gracias a la estrecha colaboración con la cartera de ciberseguridad informática de primera clase de Kaspersky.

De esta manera, los equipos de seguridad pueden formar una imagen holística del desarrollo de un incidente e identificar sus causas fundamentales para prevenir incidentes similares en el futuro.

Ejemplos de respuestas con KICS:

- Escaneo AV y actualización de bases de datos AV
- Lanzamiento de tareas
- Cambiar la autorización del nodo
- Aislamiento de nodos y procesos

Contáctenos

Ficha de datos

Visita el sitio web

MLAD

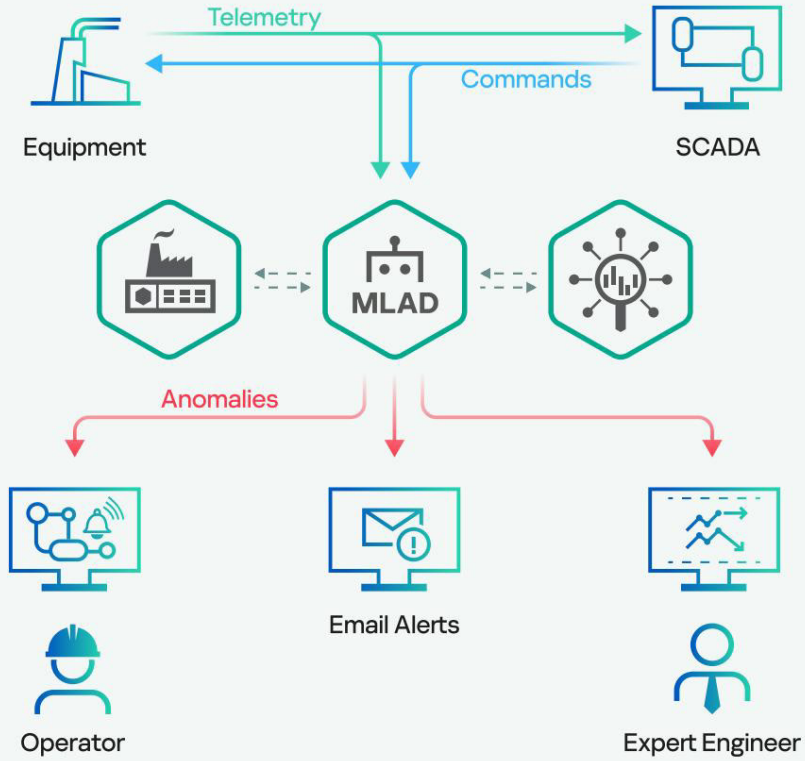
Kaspersky

Aprendizaje automático para la detección de anomalías

TECNOLOGÍA

Early anomaly detection and predictive analytics

- Detecta fallas de equipos y errores humanos mucho antes de que se vuelvan críticos, lo que ayuda a prevenir fallas y accidentes.
- Identifica acciones atípicas de los empleados o operaciones de equipos como señales de un ataque especializado o sabotaje.
- Combina la detección de anomalías con el análisis predictivo del estado y el ciclo de vida del equipo.



Ecosystem and artificial intelligence

Integración con KICS for Networks y KUMA: recibe telemetría y eventos de estos sistemas y envía alertas sobre anomalías detectadas

Aplica reglas de diagnóstico a los síntomas predefinidos del problema y aprendizaje automático para detectar cualquier desviación del comportamiento normal del equipo.

Utiliza IA para analizar la telemetría de procesos y eventos relacionados con las acciones de los empleados.

Solid Servicios

Visita el sitio web

SD-WAN

Kaspersky

Red de área amplia definida por software (SD-WAN)

TECNOLOGÍA

Kaspersky SD-WAN features:

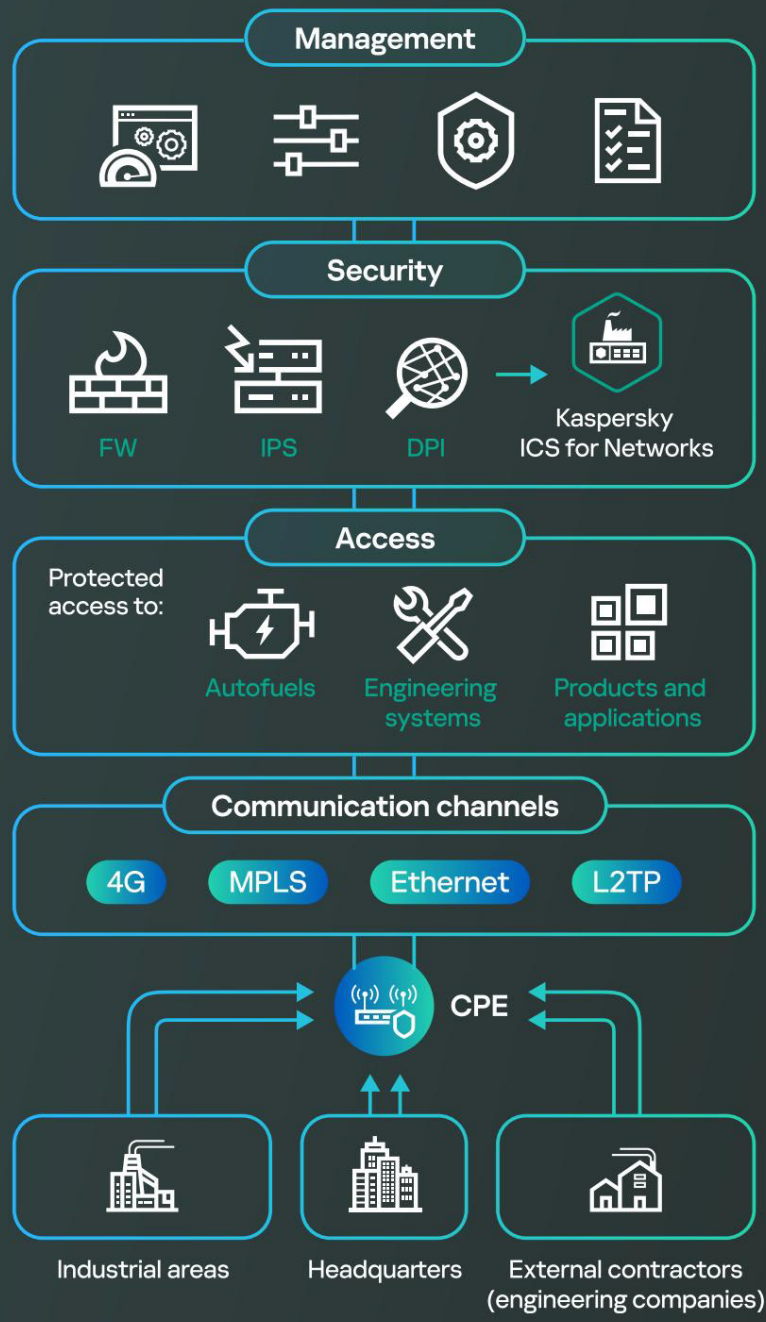
- Fácil escalabilidad
- Gestión cómoda
- Optimización de costes
- Seguridad centralizada

A single solution for reliable industrial networks

Kaspersky SD-WAN permite a las empresas construir una red tolerante a fallos, distribuida geográficamente y con gestión centralizada, al tiempo que garantiza la continuidad de los procesos de producción. La arquitectura de Kaspersky SD-WAN permite integrar fácilmente las herramientas de seguridad de Kaspersky y de terceros a través del administrador de funciones de red virtual (VNF).

Al utilizar la infraestructura SD-WAN con Kaspersky ICS for Networks, puede organizar un sistema de protección y monitoreo centralizado para numerosos sitios industriales distribuidos.

Contáctenos



Visita el sitio web

Kaspersky
Antidron

TECNOLOGÍA

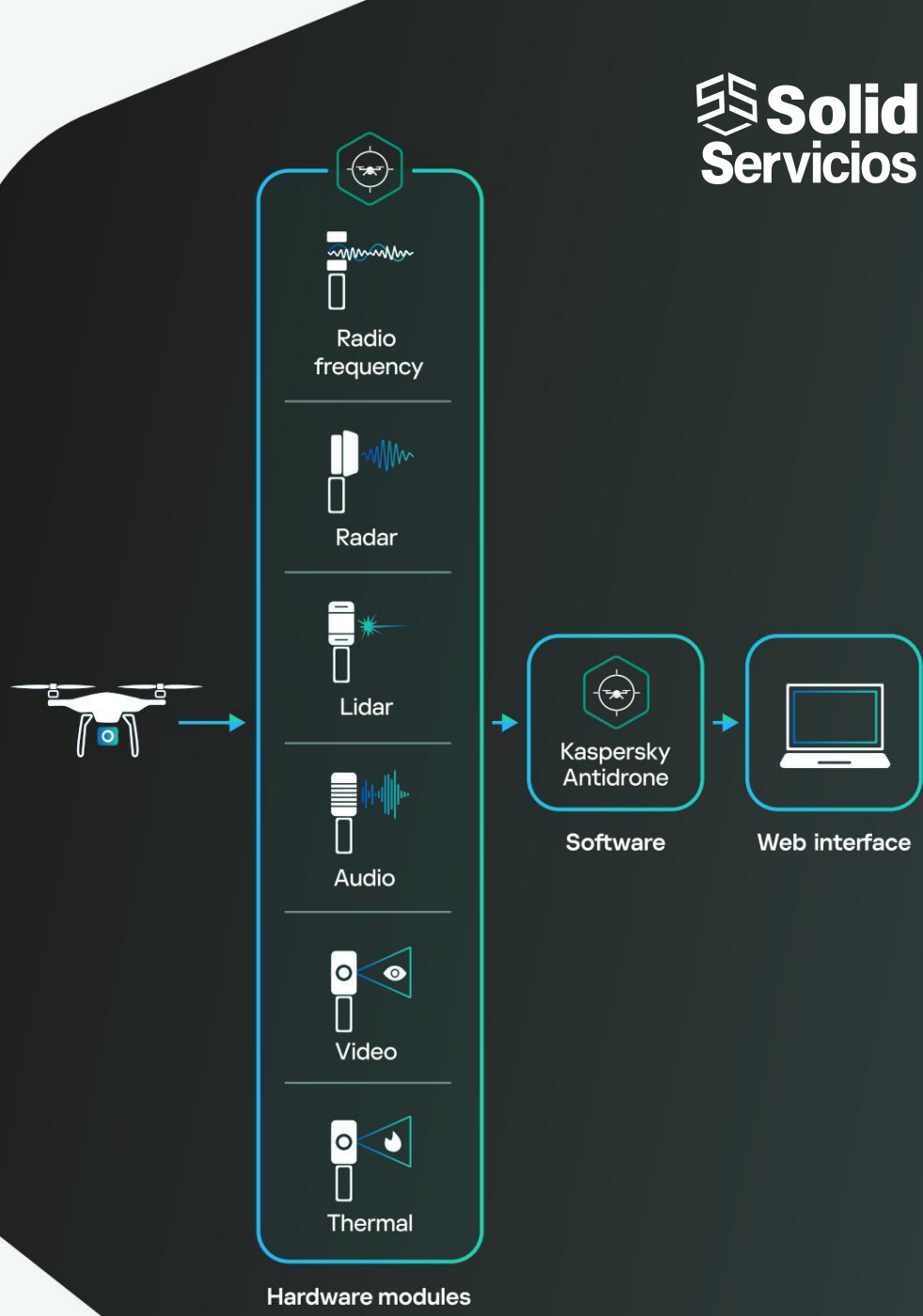
Key Features

- Detección y seguimiento de drones
- Clasificación de drones mediante redes neuronales
- Interferencia direccional y omnidireccional

Drone monitoring and defense solution

Kaspersky Antidrone reduce la probabilidad de que se produzcan interrupciones de procesos en las empresas industriales al impedir que drones no autorizados entren en su territorio. El sistema escanea automáticamente el espacio aéreo, detectando y clasificando los drones. La información sobre lo que está sucediendo se muestra en la interfaz web. En caso de amenaza, y con los permisos adecuados, el operador puede neutralizar el dron.

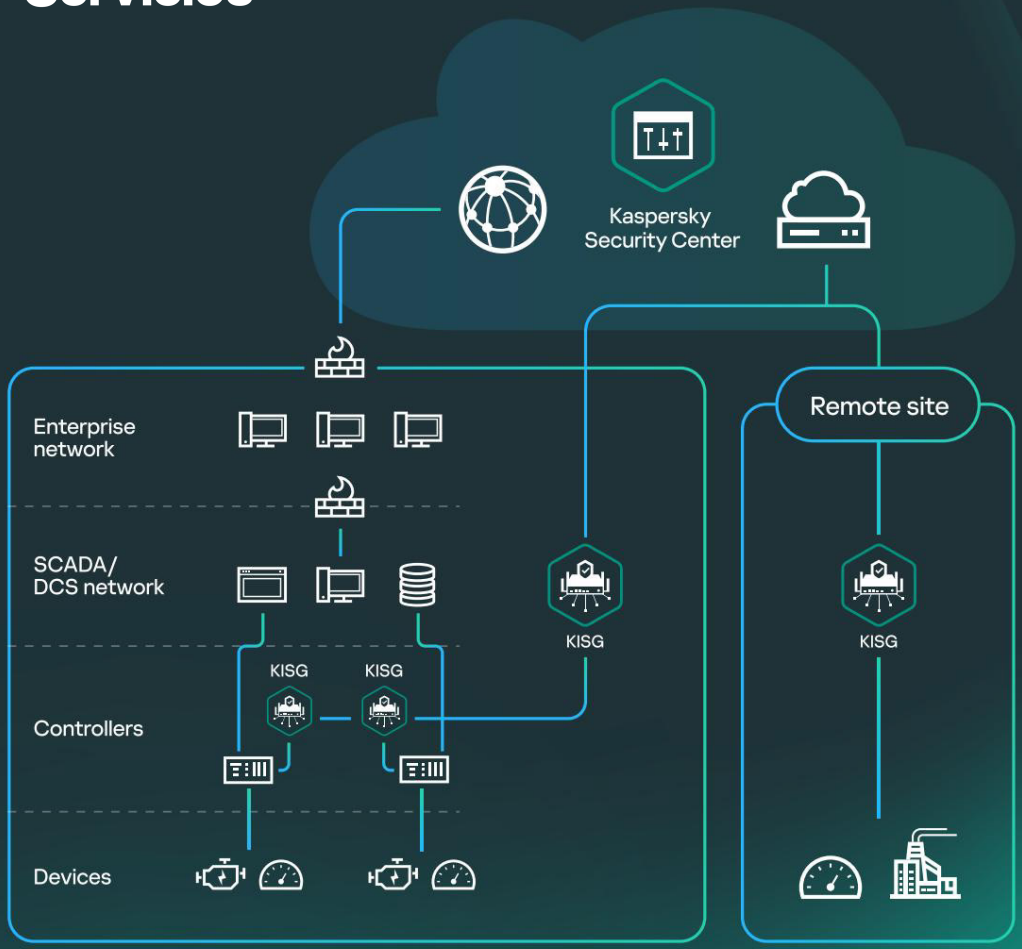
La solución Kaspersky Antidrone es modular y se puede aplicar a instalaciones industriales de cualquier tamaño. La solución también admite el modo de funcionamiento “amigo-enemigo”, lo que permite a los clientes utilizar sus propios drones y evitar la intervención de vehículos aéreos no tripulados ilícitos.



Solicitar una demostración Hoja de datos

antidrone.kaspersky.com

Solid Servicios



aprotech

El desarrollo técnico y comercial de esta solución está a cargo de Adaptive Production Technologies LLC
(Aprotech, una subsidiaria de Kaspersky)

Contáctenos Solicite una demostración Hoja de datos

Visita el sitio web

Kaspersky IoT seguro Puerta

TECNOLOGÍA

Key Features

- Recopilación y transporte seguros de datos desde dispositivos IoT a plataformas digitales y en la nube
- Kaspersky Cyber Immunity basado en KasperskyOS proporciona la resistencia «innata» a la gran mayoría de tipos de ciberataques sin herramientas de seguridad adicionales
- Transparencia de infraestructura, gestión centralizada de eventos y optimización de la producción

Trusted data for business development in Industry 4.0

La solución consta de Kaspersky IoT Secure Gateways basados en KasperskyOS y la consola de administración Kaspersky Security Center (KSC). Las puertas de enlace recopilan y transfieren de forma segura datos desde los equipos a plataformas digitales y en la nube, lo que proporciona inteligencia empresarial de alta calidad para optimizar la producción y prevenir incidentes. La consola permite mapear eventos de diferentes fuentes y administrar hasta 100.000 estaciones de trabajo físicas, virtuales y en la nube.

Visita el sitio web

Kaspersky Control remoto seguro

Espacio de trabajo

TECNOLOGÍA

Product Application

Riesgo

Las estaciones de trabajo de los usuarios se encuentran entre los objetivos más comunes de los ciberataques.

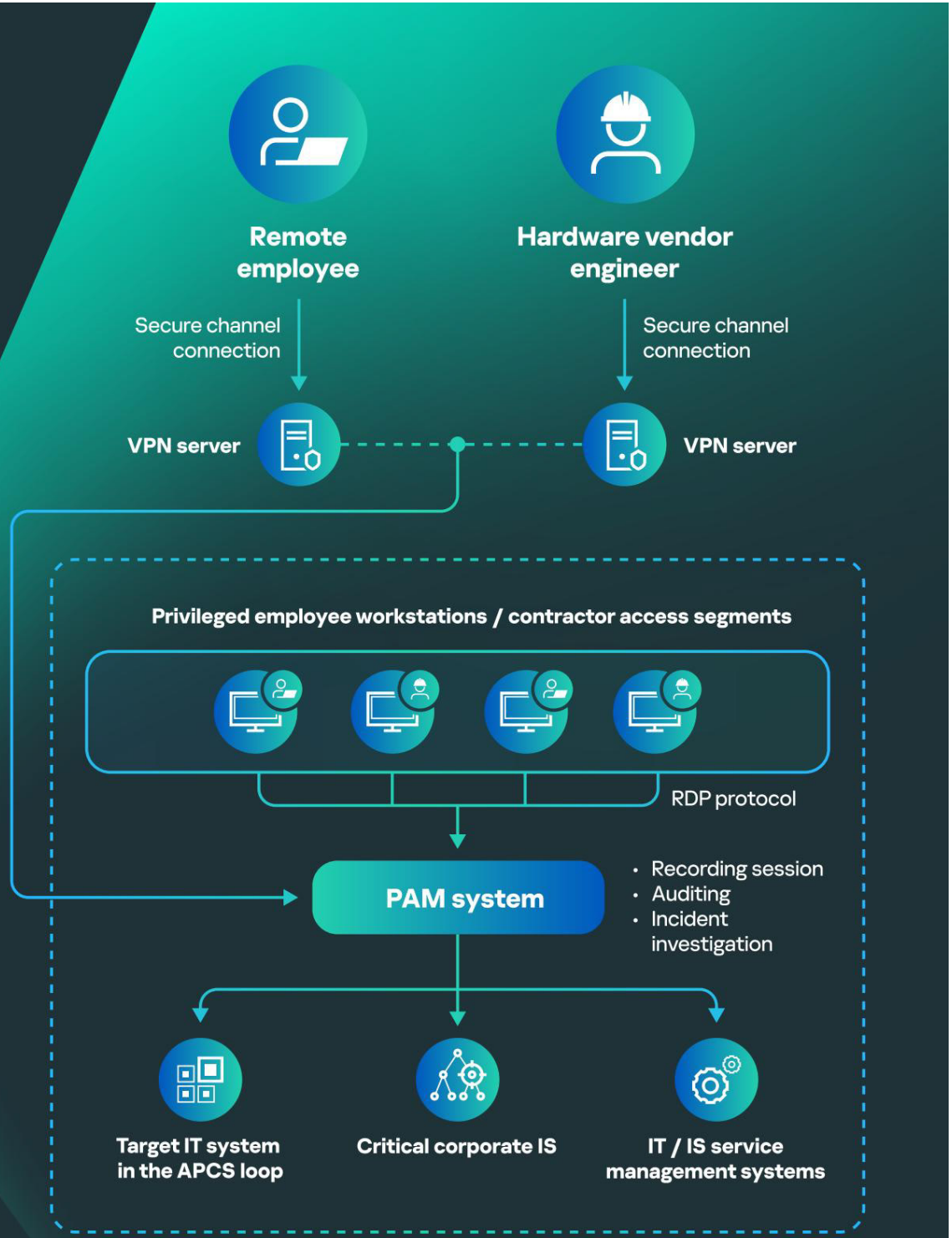
Solución

Espacio de trabajo remoto seguro de Kaspersky (KSRW) es una solución para construir una infraestructura administrada y funcional de clientes ligeros basada en el propio microkernel de Kaspersky.

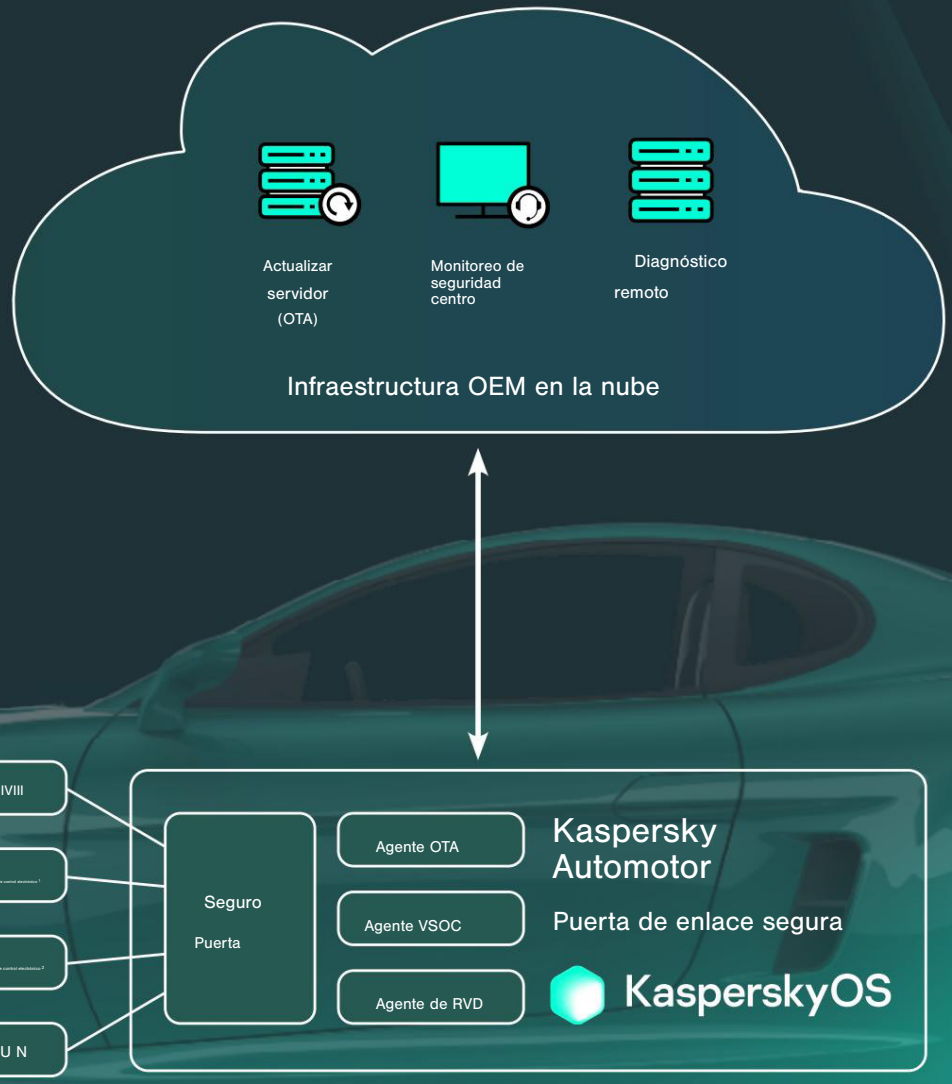
Sistema operativo KasperskyOS

Cyber Immune Thin Client infrastructure

Los clientes ligeros Cyber Immune como parte de Kaspersky Secure Remote Workspace proporcionan una conexión segura a los escritorios virtuales, incluida una zona confiable para conectar a los usuarios a la infraestructura industrial.



Solid Servicios



AUTOSAR

Contáctenos

Ficha de datos

Visita el sitio web

Kaspersky Automotor

Puerta de enlace segura

TECNOLOGÍA

Vehicle protection

- Acceso no autorizado
- Ataques dirigidos a la ECU
- Ataques a través de sistemas de información y entretenimiento de vehículos (IVI)
- Diagnósticos maliciosos
- Compromiso del sistema de actualización
- Conexiones y flujos de datos no controlados, interrupción de la comunicación

Key Benefits

- Solución segura por diseño
- Ayuda a cumplir con las regulaciones de ciberseguridad.
- 4 en 1: puerta de enlace conectada, puerta de enlace de seguridad, Maestro OTA y agente VSOC
- Cumplimiento de ISO21434, ISO26262, AUTOSAR Adaptativo, Uptane

Solid Servicios

Comprensión profunda de las amenazas y vulnerabilidades de la ciberseguridad industrial para una evaluación eficiente de riesgos, detección exitosa de ataques, investigación de incidentes y respuesta.

Respaldado por la experiencia y conocimientos incomparables

de Kaspersky ICS CERT, el primer CERT privado en ciberseguridad industrial.

Key Features

- Detección rápida de amenazas y amplias capacidades analíticas
- Aumenta la eficacia de las investigaciones y búsquedas activas de amenazas.
- Información completa sobre amenazas y vulnerabilidades para una toma de decisiones informada

Solicitar una demostración Descripción general de la solución Contáctenos

Manténgase por delante de sus adversarios con información detallada Visibilidad de las ciberamenazas dirigidas a su organización

Solid Servicios

Kaspersky
Amenaza de ICS
Fuentes de datos

Un conjunto de fuentes de datos de inteligencia sobre amenazas actualizadas periódicamente y adaptadas a las necesidades específicas de la ciberseguridad industrial

Threat Intelligence
Automatic data streams

Sistema de control de acceso de Kaspersky
Inteligencia de amenazas
Informes

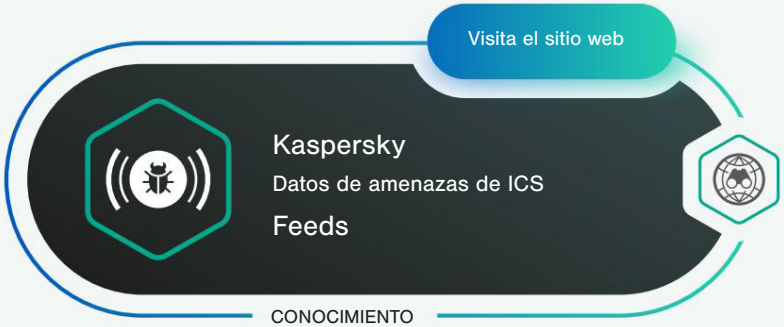
Proporciona un mayor conocimiento sobre las campañas maliciosas dirigidas a organizaciones industriales, así como información sobre Vulnerabilidades encontradas en los sistemas de control industrial más

populares

Kaspersky
Pregúntale a la

Analista

Un servicio para que los clientes soliciten orientación y conocimientos expertos sobre amenazas específicas que enfrentan o en las que están interesados.



El servicio Kaspersky Threat Data Feed ofrece información de inteligencia sobre amenazas en tiempo real para ayudar a las organizaciones industriales a proteger sus redes y sistemas de las ciberamenazas. Los feeds de datos incluyen información sobre malware conocido, sitios web de phishing, vulnerabilidades y exploits más recientes y otros tipos de ciberamenazas. Si se los pone en contexto, los datos pueden revelar más fácilmente el "panorama general" y usarse para responder a las preguntas "quién, qué, dónde, cuándo" para identificar a sus adversarios, tomar decisiones rápidas y actuar.

What you get:

Sistema de control de acceso de Kaspersky

Fuente de datos hashes

Inteligencia de amenazas actualizada para ICS y otros sistemas utilizados en OT para simplificar y automatizar la detección e investigación oportuna de ataques

#prevención

#detección

#investigación

Sistema de control de acceso de Kaspersky

Fuente de datos sobre vulnerabilidades

Datos verificados y refinados sobre vulnerabilidades descubiertas en software y hardware de Sistemas ICS y otros sistemas utilizados en entornos industriales, proporcionados en un formato legible por máquina

#prevención

#detección

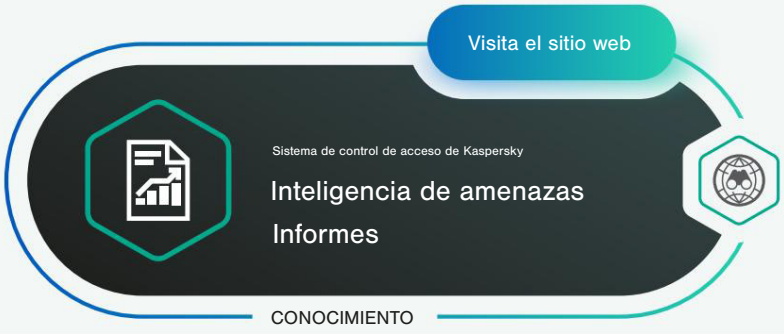
#investigación

Datos de vulnerabilidad de ICS Feed en formato OVAL

Un feed actualizado periódicamente que contiene Definiciones de OVAL para la detección automatizada de vulnerabilidades conocidas en sistemas SCADA y otro software industrial

#detección

Solid Servicios



Kaspersky ICS Threat Intelligence Reporting proporciona información detallada y un mayor conocimiento de las campañas maliciosas dirigidas a las organizaciones industriales, así como información sobre las vulnerabilidades detectadas en los sistemas de control industrial más populares y las tecnologías subyacentes. La información detallada adaptada a las organizaciones industriales ayuda a los clientes a proteger los activos críticos, incluidos los componentes de software y hardware, y a garantizar la seguridad y la continuidad del proceso tecnológico.

Los informes se envían a través de Kaspersky Threat Intelligence Portal o se puede acceder a ellos mediante API.

What you get:

Informes de APT

Informes sobre nuevas APT y campañas de ataques de gran volumen dirigidas a organizaciones industriales y actualizaciones sobre amenazas activas.

El panorama de amenazas

Informes sobre cambios significativos en el panorama de amenazas para los sistemas de control industrial, factores críticos recientemente descubiertos que afectan los niveles de seguridad de los ICS y la exposición de los ICS a amenazas, incluida información regional, nacional y específica de la industria.

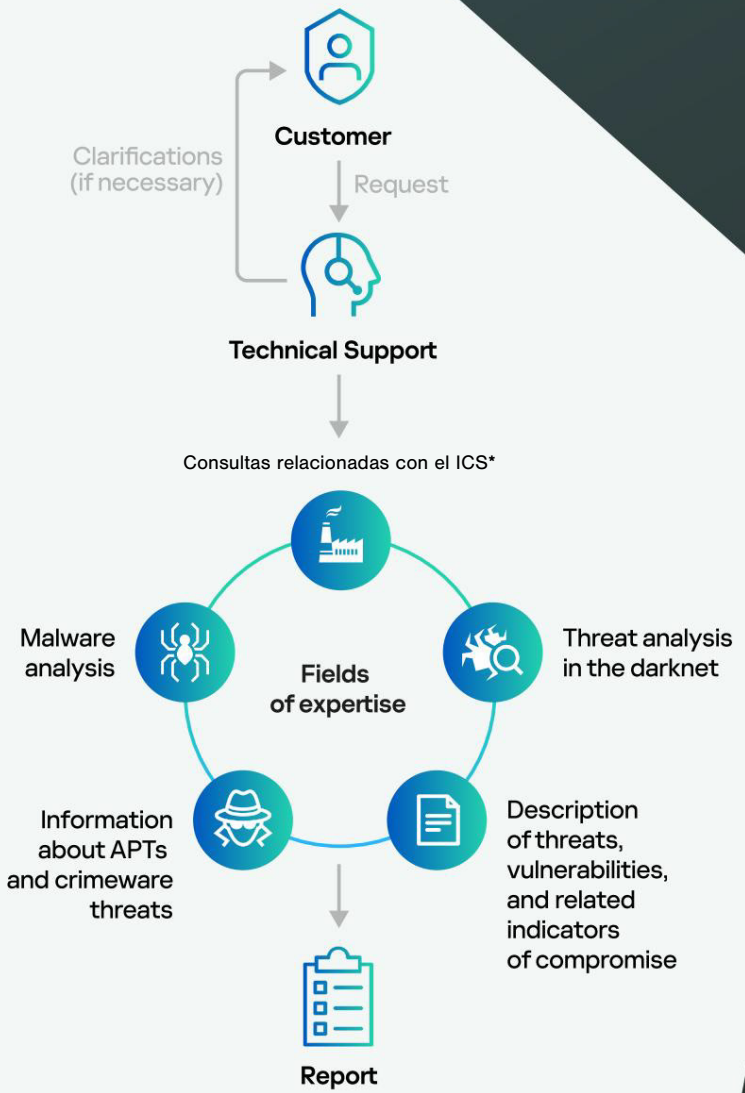
Vulnerabilidades encontradas

Informes sobre vulnerabilidades identificadas por Kaspersky en los productos más populares utilizados en sistemas de control industrial, Internet industrial de las cosas e infraestructuras en diversas industrias.

Análisis y mitigación de vulnerabilidades

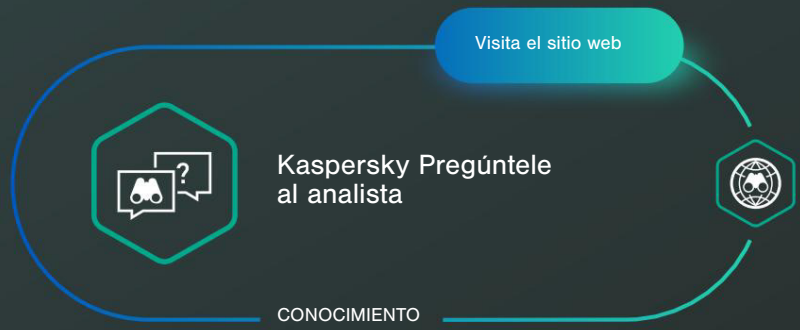
Nuestros avisos brindan recomendaciones prácticas de los expertos de Kaspersky para ayudar a identificar y mitigar amenazas.

Solid Servicios



* Información adicional sobre los repositorios publicados:

- Información sobre vulnerabilidades de ICS
- Estadísticas de amenazas a los sistemas de control de procesos y nuevas tendencias por región e industria
- Análisis de malware dirigido al ICS
- Información sobre requisitos y normas reglamentarias.



What you get:

Kaspersky Ask The Analyst complementa nuestra cartera de Kaspersky Threat Intelligence. Con este servicio, puede ponerse en contacto con expertos para obtener asistencia e información útil sobre amenazas y vulnerabilidades específicas a las que se enfrenta o que le interesan. Con estos datos, puede mejorar sus defensas contra amenazas que afectan tanto a su organización en su conjunto como a su infraestructura industrial.

Key Benefits

Acceso a los principales expertos en inteligencia de amenazas, incluidos expertos en seguridad industrial de

Certificado ICS de Kaspersky

Información contextual personalizada y detallada para investigaciones

efectivas

Instrucciones detalladas de nuestros expertos sobre cómo responder rápidamente a las amenazas y vulnerabilidades

Solid Servicios

Visita el sitio web

Kaspersky
Conciencia de seguridad

CONOCIMIENTO

Visita el sitio web

Kaspersky
CERTIFICADO ICS

Capacitaciones de expertos

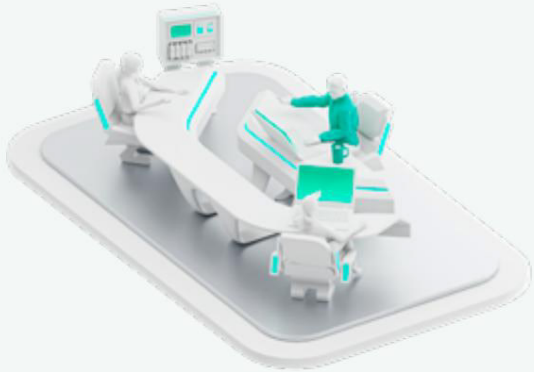
CONOCIMIENTO

Increase employee cyber-literacy

- Materiales de formación que dotan a sus empleados de los conocimientos necesarios sobre los aspectos más importantes de la ciberseguridad industrial, aumentando el nivel de concienciación en todos los niveles de la organización.
- Kaspersky Interactive Protection Simulation: capacitación basada en juegos a través de simulaciones empresariales que presentan una multitud de escenarios en diferentes industrias: energía térmica, energía hidroeléctrica, petróleo y gas, petroquímica, explotaciones petroleras, etc.
- Kaspersky Automated Security Awareness Platform (ASAP): módulos de aprendizaje interactivos y ataques de phishing simulados diseñados para fomentar un comportamiento ciberseguro

Applied learning

Nuestro programa de capacitación en ICS ha sido diseñado especialmente para garantizar que los profesionales de tecnología de la información (TI), tecnología de operaciones (OT) y seguridad de la información (SI), así como los gerentes y otros empleados, puedan ampliar sus conocimientos de ciberseguridad industrial y adquirir habilidades prácticas especializadas.

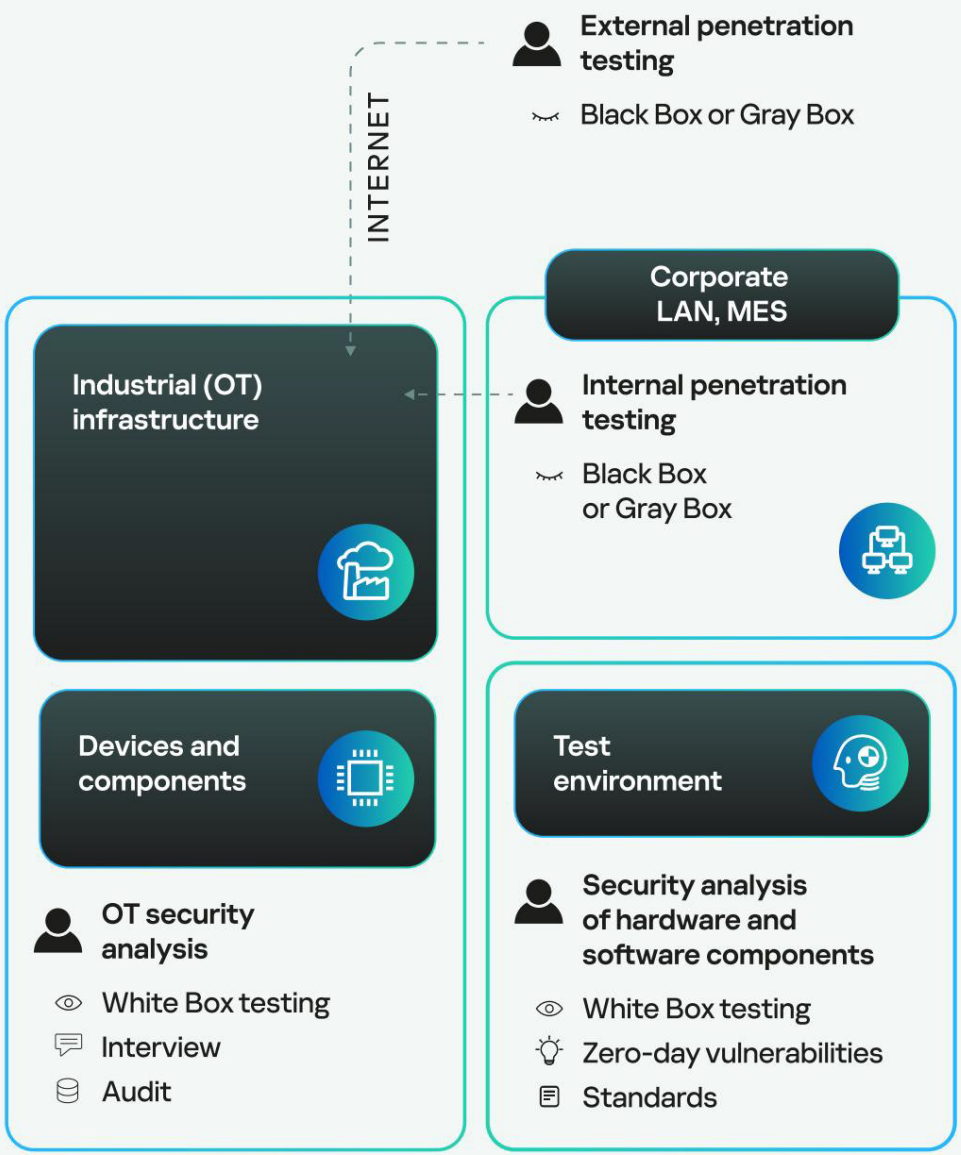


Major topics covered

- Correo electrónico
- Sitios web e Internet
- Contraseñas y cuentas
- Redes sociales y mensajeros
- Ciberseguridad industrial
- Seguridad de la PC
- Dispositivos móviles
- Datos confidenciales
- Seguridad de tarjetas bancarias y PCI DSS
- RGPD

Practical skills from Kaspersky experts

- Informática forense digital y respuesta a incidentes
- Exploración de vulnerabilidades en dispositivos OT/IoT y software industrial
- Programas de capacitación multifuncional para expertos en TI, OT e IS



Visita el sitio web

Kaspersky
Seguridad ICS
Evaluación

PERICIA

Analysis of your industrial infrastructure's security

Un enfoque integral para identificar vulnerabilidades y debilidades de seguridad en infraestructuras industriales, que incluye:

- Superficie de ataque
- El nivel de seguridad de la infraestructura de red industrial, DCS y dispositivos industriales
- Riesgos de compromiso de sistemas críticos

Checking critical components

- Tráfico de red, incluidos protocolos industriales
- Componentes de control de procesos: SCADA, PLC, contadores inteligentes, etc.
- Elementos físicos del sistema de control de procesos automatizados
- Arquitectura de red, incluidas las redes ACS

Solid Servicios

Visita el sitio web

Kaspersky Detección gestionada y Respuesta

PERICIA

Key Features

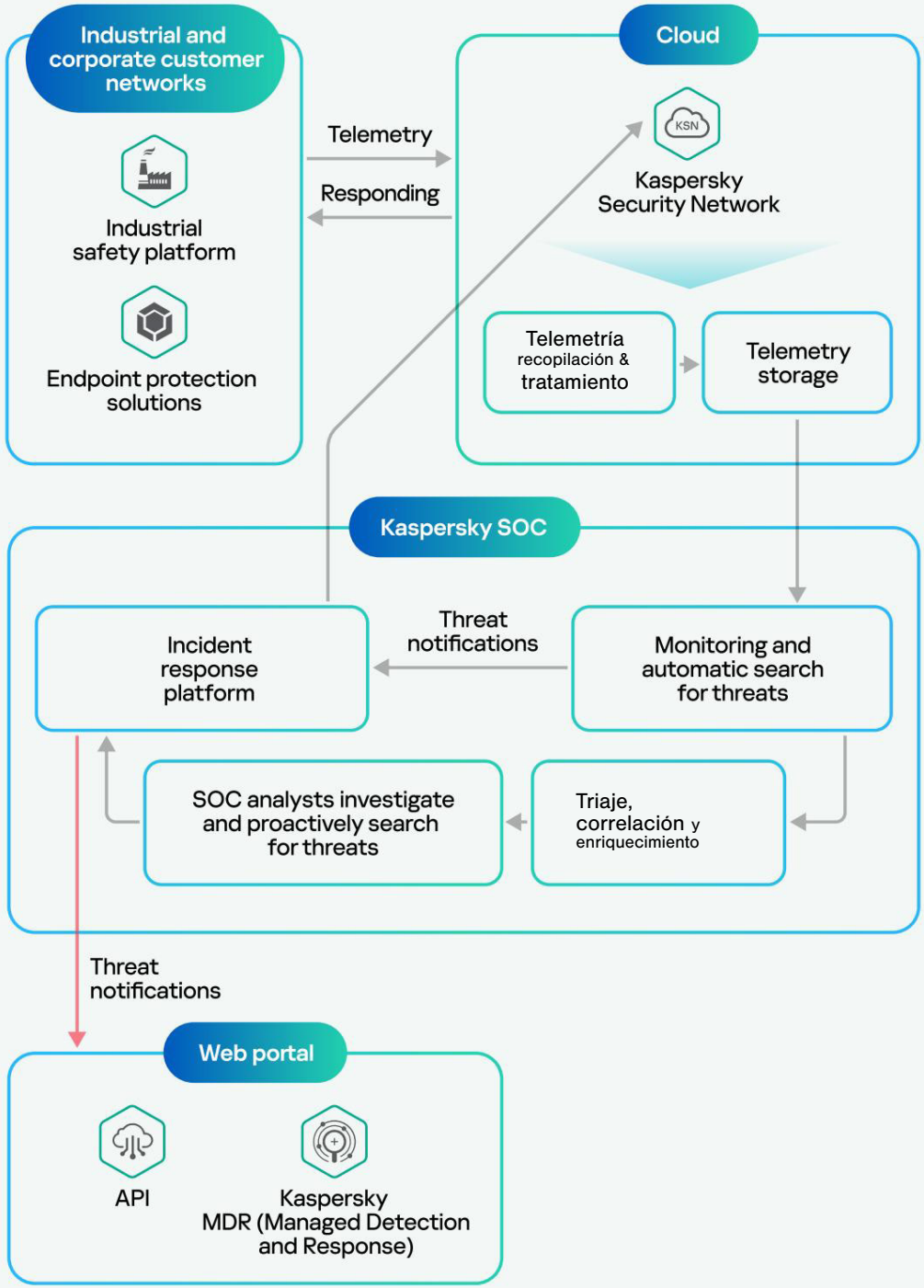
- Detección proactiva de amenazas: los indicadores de ataque patentados ayudan a rastrear amenazas no detectadas dentro del sistema de control
- Respuesta automatizada y guiada (con investigación forense completa y análisis de malware disponibles a pedido)
- Experiencia en ciberseguridad de ICS: respaldada por uno de los equipos de detección de amenazas proactivas más exitosos y experimentados de la industria

What you get:

- Búsqueda, detección y eliminación continua de amenazas dirigidas a su empresa industrial.
- Reducción de costes de seguridad al eliminar la necesidad de contratar nuevos expertos en ciberseguridad
- Todos los beneficios clave de un SOC, sin necesidad de establecerlo Uno en casa

El 25% de nuestros clientes protegidos son del sector Industrial

Consulte el informe del MDR para obtener más información



Visita el sitio web

Kaspersky
Respuesta a incidentes

PERICIA

Responding to incidents

Riesgo

Una vulnerabilidad es suficiente para que los cibercriminales obtengan el control de sistemas industriales enteros

Solución

- Eliminación rápida de las consecuencias de un incidente por parte del Equipo de Respuesta a Emergencias Globales de Kaspersky
- Análisis de las causas, fuentes y consecuencias. del incidente • Vista

detallada del malware utilizado

- Soporte adicional de Kaspersky ICS-CERT

Service composition

Respuesta al incidente:
Investigación y eliminación de

amenazas

Informática forense digital:
Análisis de evidencia digital

Análisis de malware:
Obtenga una vista detallada de los archivos

utilizados en un ataque

Solid Servicios

The partner you can trust

26 años de experiencia de clase mundial y petabytes de datos sobre amenazas

ICS CERT

ICS CERT — certificación internacional propia

División de investigación de seguridad OT/IoT

Experiencia comprobada en la industria de seguridad de TI/OT con numerosos premios y logros

Más de 100 certificados de

interoperabilidad con soluciones de proveedores de automatización

Eficacia tecnológica comprobada, cumplimiento de normas y requisitos

www.solidservicios.com
800 872 9898 | 800 777 2908

Solid Servicios