

Kaspersky

Ciberseguridad de OT

Solución unificada diseñada específicamente
para la resiliencia de los sistemas ciberfísicos





Kaspersky Ciberseguridad de OT

Cuando la experiencia
ofrece resiliencia



Tecnologías industriales

Soluciones robustas de seguridad industrial: probadas, conformes y aprobadas



Conocimiento aplicable

Análisis de amenazas fiable y formaciones en ciberseguridad industrial integral



Experiencia probada en el campo

Una gama completa de servicios profesionales para una ciberseguridad sólida y holística



Kaspersky Next
XDR Expert

Convergencia de TI/TO

IT XDR

Tecnologías

Soluciones especializadas



Kaspersky
Antidrone



Kaspersky
Machine Learning
for Anomaly Detection



Kaspersky
SD-WAN



Kaspersky
Industrial
CyberSecurity

DR nativa para TO



for Nodes

Protección,
detección
y respuesta en
endpoints



for Networks

Análisis, detección
y respuesta de
tráfico de red

Soluciones de
Kaspersky OS



Kaspersky
Thin Client



Kaspersky
Automotive
Secure Gateway

Conocimientos

Ciber
Higiene



Kaspersky
Security
Awareness

Contra amenazas
frente
a amenazas



Kaspersky
ICS Threat
Intelligence

Formación



Kaspersky
ICS CERT
Training

Experiencia

Detección



Kaspersky
ICS Security
Assessment

Respuesta



Kaspersky
Incident
Response

Administrado
Protección



Kaspersky
Managed
Detection
and Response

Kaspersky

Ciberseguridad de OT

Cobertura completa para sistemas de misión crítica – entregada



Kaspersky Industrial CyberSecurity
DR nativa para TO



for Nodes
Protección, detección y respuesta en endpoints



for Networks
Análisis, detección y respuesta de tráfico de red



Kaspersky Next XDR Expert
Convergencia de TI/TO



Kaspersky Machine Learning for Anomaly Detection



Kaspersky Antidrone



Kaspersky Automotive Secure Gateway



Kaspersky SD-WAN

1 Automation & Protection

2 Monitoring & Control

kaspersky



Kaspersky Thin Client

3 IT systems

4 Industry 4.0 & IIoT

Experiencia

Detección



Kaspersky ICS Security Assessment

Respuesta



Kaspersky Incident Response

Protección gestionada



Kaspersky Managed Detection and Response

Conocimientos

Ciberhigiene



Kaspersky Security Awareness

Threat Intelligence



Kaspersky ICS Threat Intelligence

Formación



Kaspersky ICS CERT Training



**Kaspersky
Industrial
CyberSecurity**

Conciencia situacional de 360° y control de la exposición al riesgo

- **Inventario de activos y visibilidad de la red.** Realiza un seguimiento de todos los dispositivos conectados y sus configuraciones. Genera un gráfico de red y analiza los flujos de datos.
- **Eliminación de amenazas.** Identifica y mitiga amenazas en todos los hosts y redes, con información sobre las causas raíz y recomendaciones de respuesta seguras.
- **Evaluación de riesgos.** Evalúa las vulnerabilidades y monitoriza los cambios en la configuración de seguridad de los hosts, los dispositivos de red y los controladores

Ventajas principales



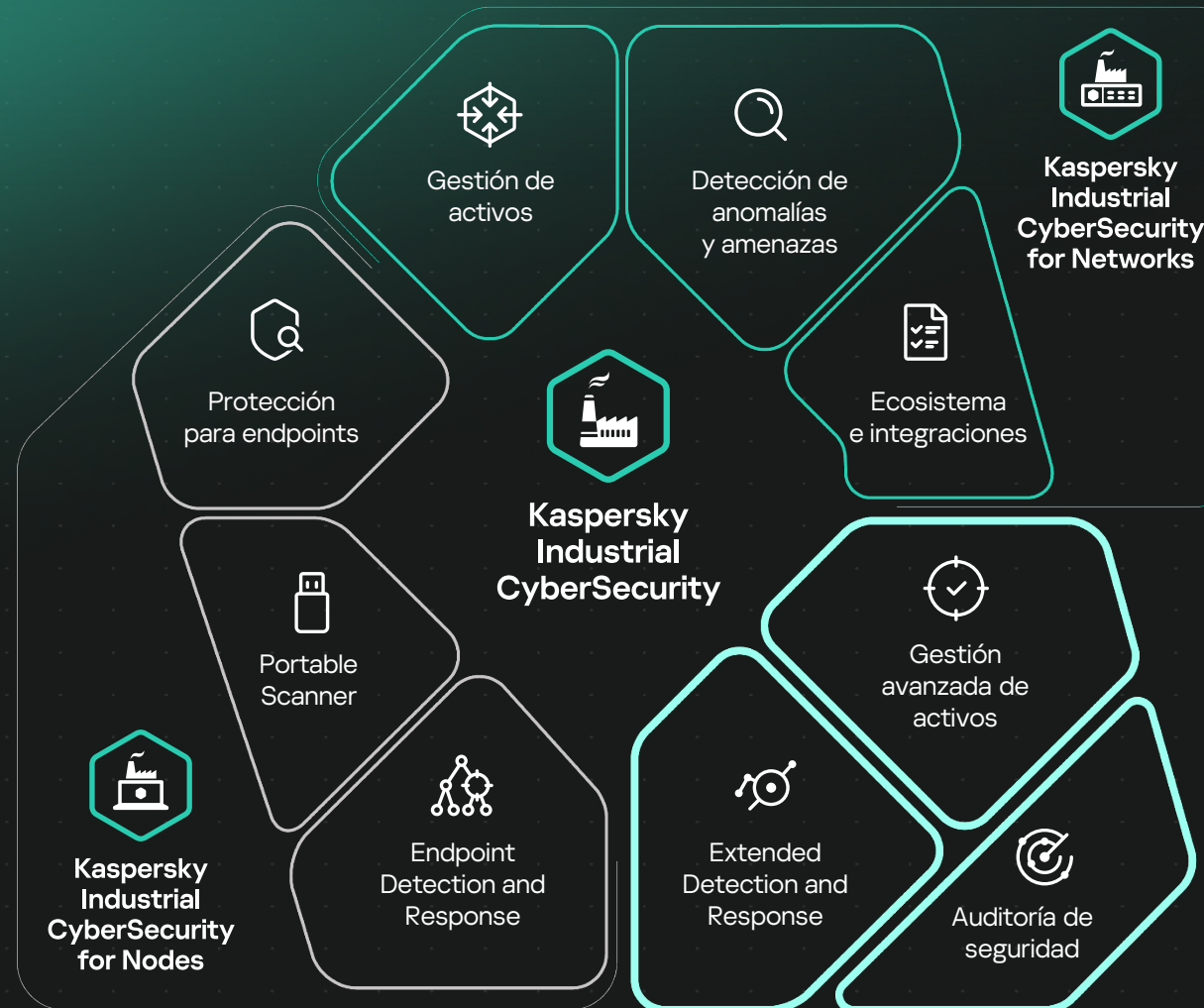
Compatibilidad probada y verificada con más de 200 sistemas y dispositivos de automatización industrial



Plataforma OT XDR integrada de forma perfecta que resuelve múltiples desafíos, diseñada específicamente para infraestructuras críticas



Solución de baja huella que no afecta al rendimiento del sistema ni a la continuidad del proceso



**KICS y sus tecnologías básicas
están sujetas a auditorías líderes en la industria**



ISA/IEC 62443-4-1



SOC 2 Tipo 2



ISO/IEC 27001



GB 42250-2022

**Kaspersky Next
XDR Expert**

Protección integral en todos los segmentos industriales y corporativos de tu organización

Gracias a una integración estrecha con Kaspersky Next XDR Expert, la plataforma de Kaspersky Industrial CyberSecurity habilita nuevos escenarios que incluyen interacciones con soluciones de terceros y funcionalidades mejoradas de investigación y respuesta. La integración permite proteger tu empresa en la intersección de los entornos industriales y corporativos.

Los equipos de seguridad obtienen una vista unificada del desarrollo de un incidente e identifican sus causas raíz para evitar que se produzcan incidentes similares en el futuro.

Ventajas principales



Seguridad y soberanía de datos para infraestructuras convergentes de TI/TO/IoT que utilizan muchos activos



Interoperabilidad nativa en toda la cartera de productos de Kaspersky que proporciona integración impecable e incomparable

Fuentes de datos

Soluciones de
Kaspersky

Terceros

xFlows

Eventos

Integraciones



**Kaspersky
Anti Targeted
Attack**
NDR Enhanced



**Kaspersky
Threat Intelligence**



**Kaspersky
Managed Detection
and Response**

y más Integraciones de
Kaspersky o de terceros
a demanda

Datos

Respuesta

Kaspersky Next XDR Expert

Plataforma de gestión única abierta

Endpoint Detection
y respuesta gestionadas

Investigación
gráficos

Detección de
amenazas y
correlación cruzada

Gestión de
registros y lago
de datos

Paneles
e informes

Guías

Gestión de
casos

Gestión
centralizada
de activos

Terceros

Kit de
herramientas de
implementación

Datos

Respuesta

EDR con seguridad de entorno de prueba, correos electrónicos y entornos híbridos

Security Awareness, Sandbox,
seguridad del correo electrónico y de la nube híbrida



**Kaspersky
Automated Security
Awareness Platform**



**Kaspersky
Security for
Mail Server**



**Kaspersky
Hybrid Cloud
Security**



**Kaspersky
Sandbox**



Kaspersky Machine Learning for Anomaly Detection

Detección de anomalías temprana y análisis predictivo

- Detecta fallos en el equipo y errores humanos mucho antes de que se vuelvan críticos, lo que permite evitar errores y accidentes.
- Identifica acciones de empleados u operaciones de equipos atípicas, que pueden indicar un ataque especializado o de sabotaje.
- Identifica anomalías difíciles de detectar en el funcionamiento de sistemas ciberfísicos, generadas por pequeñas desviaciones en múltiples parámetros del proceso.

Integración con sistemas externos



Kaspersky MLAD recibe telemetría del proceso de KICS for Networks, sistemas industriales de automatización y dispositivos de IoT/IIoT



El procesador de eventos de MLAD intercambia mensajes CEF con fuentes externas: sistemas SIEM, IIoT y dispositivos de red



**Kaspersky
SD-WAN**

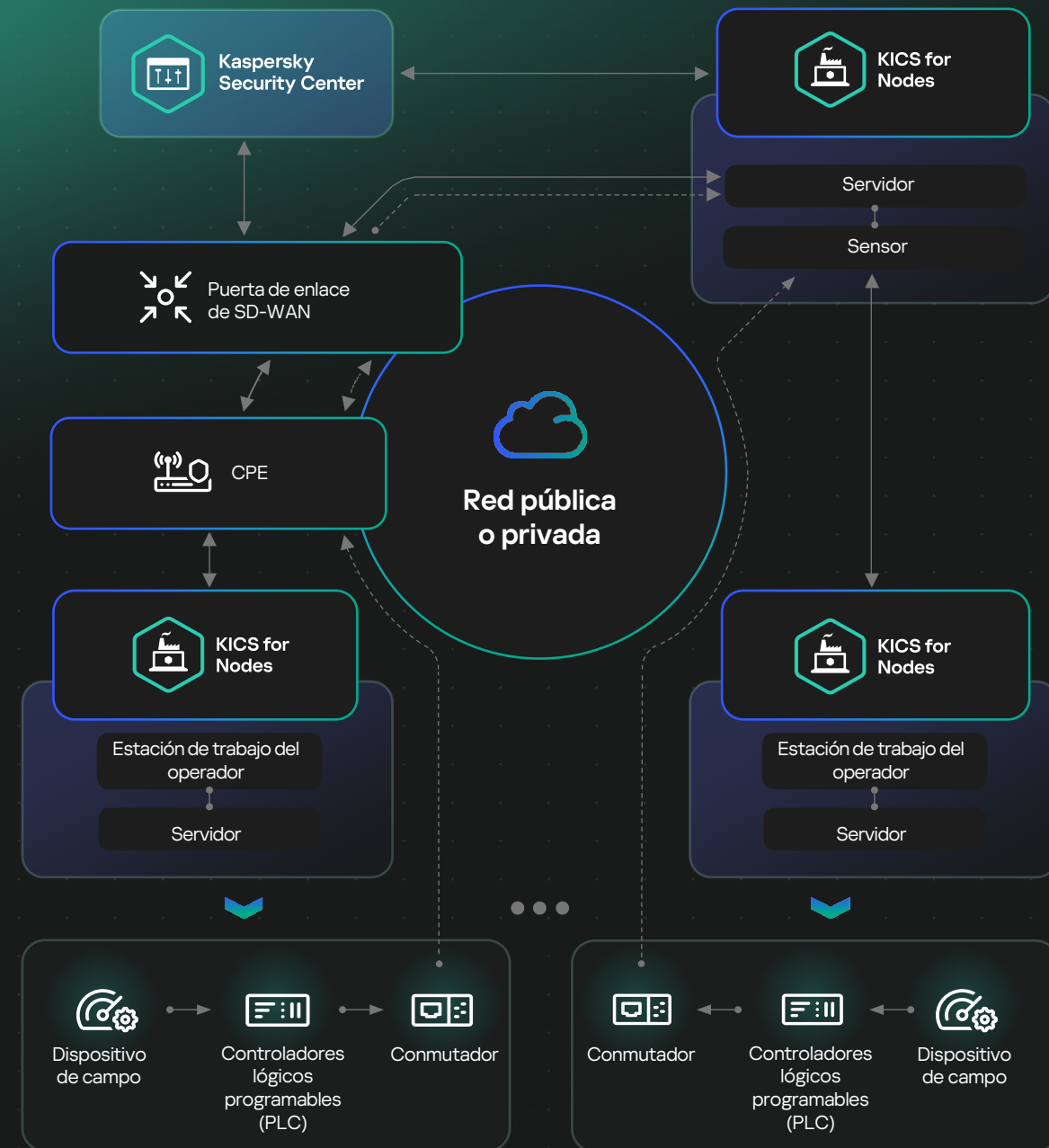
Una solución unificada que garantiza la confiabilidad de las redes industriales distribuidas

Kaspersky SD-WAN le permite a las empresas industriales construir una red resiliente y distribuida en diferentes regiones geográficas con administración centralizada, mientras garantiza la continuidad de los procesos industriales.

Kaspersky Industrial CyberSecurity puede aprovechar la infraestructura SD-WAN para recopilar tráfico industrial, proporcionar supervisión centralizada y proteger objetos y sistemas industriales distribuidos.

Ventajas principales

- ➔ Fácil escalabilidad
- 📄 Optimización de costes
- 👉 Administración práctica
- 🛡️ Seguridad centralizada



**Kaspersky
Antidrone**

Solución de defensa y supervisión de drones

Kaspersky Antidrone permite reducir el riesgo de interrupciones de procesos en empresas industriales dado que evita el ingreso de drones no autorizados a su territorio. El sistema analiza el espacio aéreo de manera automática, detectando y clasificando drones. Además, puede encontrar información acerca de lo que está ocurriendo en la interfaz web. En el caso de una amenaza, y siempre que se permita, los operadores pueden neutralizar el dron.

Kaspersky Antidrone es una solución modular que se puede implementar en establecimientos industriales de todos los tamaños. También ofrece un modo "amigo o enemigo", que permite que las organizaciones operen sus drones sin interferencias y evita que vehículos aéreos no tripulados y no autorizados ingresen al área.

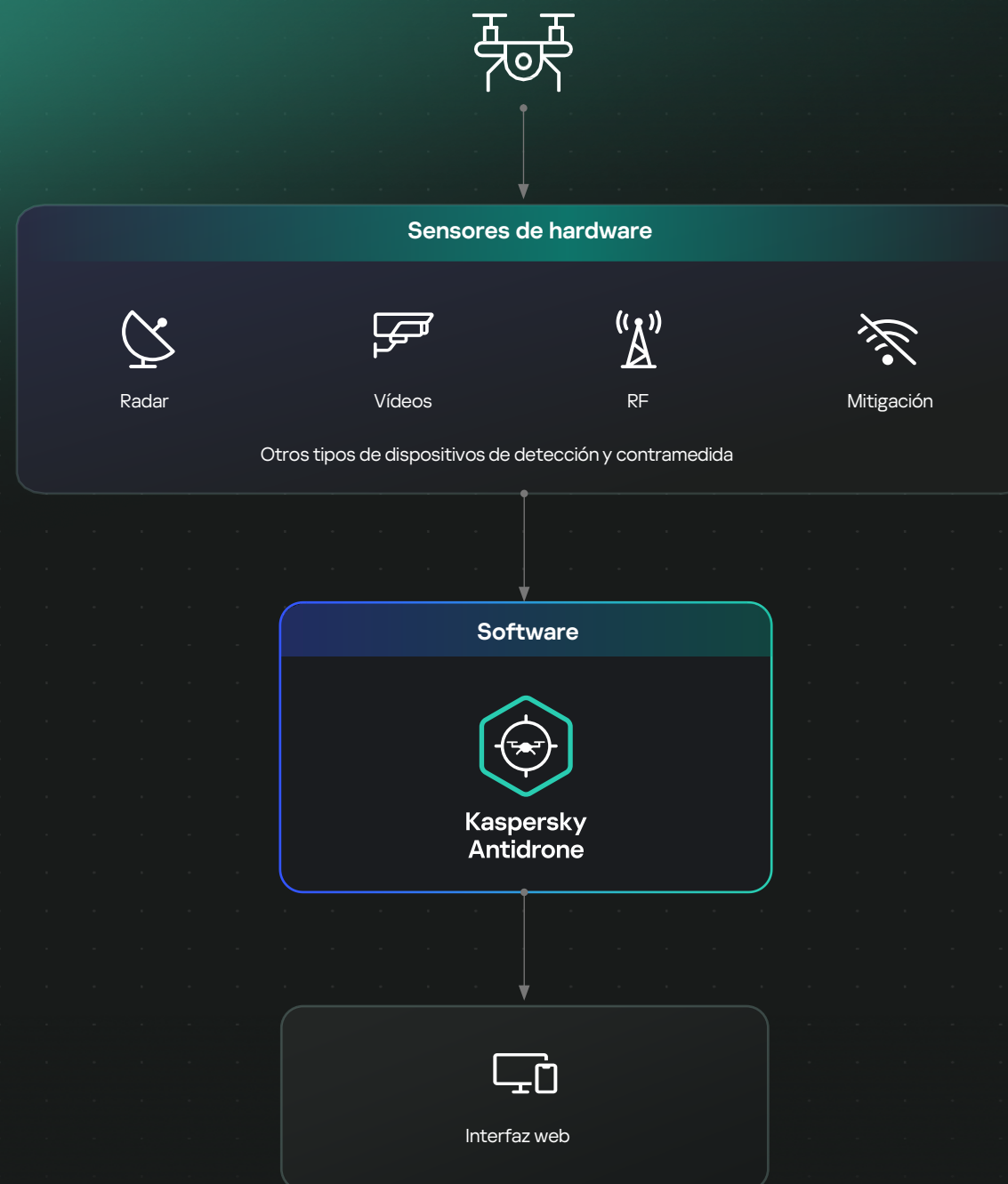
Ventajas principales



Kaspersky Antidrone admite la combinación y coordinación de radares, escáneres de RF, cámaras y emisores de interferencias de diferentes proveedores en un único sistema unificado.



La fusión multisensor mejora significativamente la fiabilidad de la detección en condiciones congestionadas, ruidosas o de baja visibilidad.



**Kaspersky
Thin Client**

Infraestructura de escritorio virtual y remota segura

Riesgo

Las estaciones de trabajo de los usuarios son uno de los objetivos más comunes de los ciberataques.

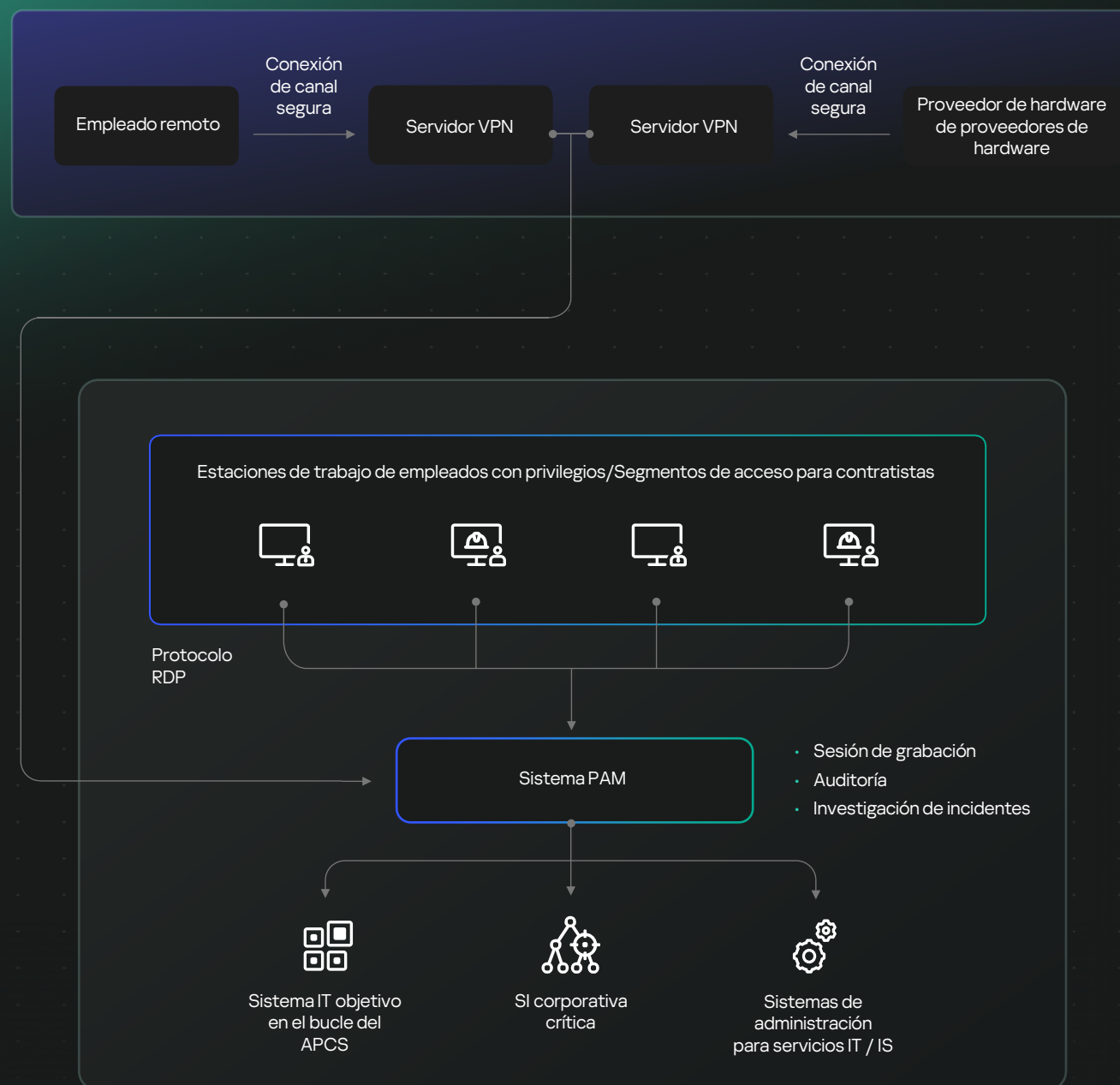
Solución

Kaspersky Thin Client es una solución para la construcción de una infraestructura funcional y administrada en clientes ligeros, con el sistema operativo con microkernel de Kaspersky: KasperskyOS.

Los clientes ligeros, que no requieren refrigeración activa ni tienen componentes móviles, ofrecen rendimiento altamente confiable para entornos de producción.

Ventajas principales

- ✓ Seguridad desde el diseño
- ⚙️ Una única plataforma de administración para SI y TI
- ⌚ Integración de la infraestructura en tan solo dos minutos





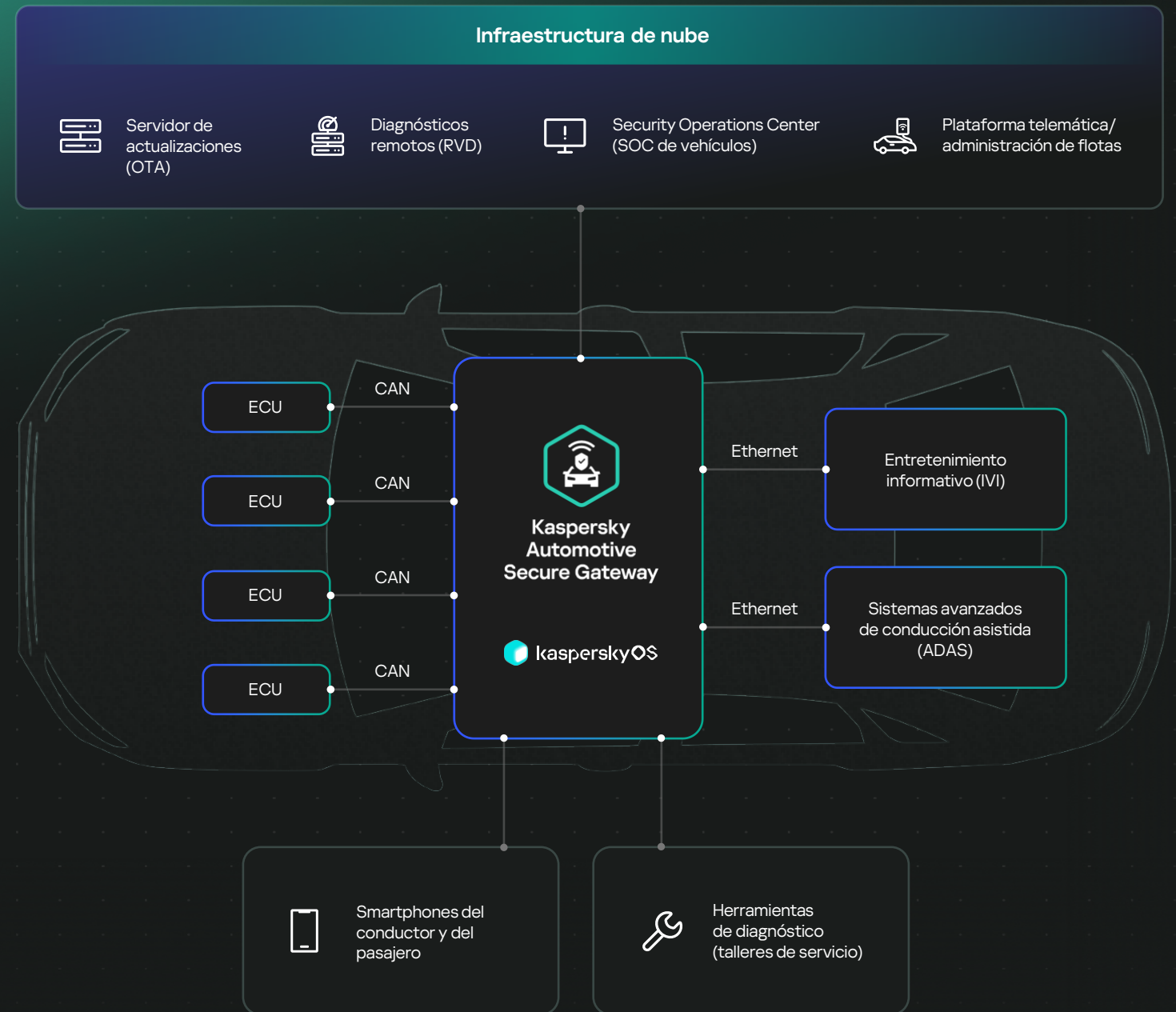
Kaspersky Automotive Secure Gateway

Creación de sistemas de TI confiables para vehículos conectados

- Puerta de enlace de software segura para vehículos conectados que también brinda las funciones de una unidad de control telemático (TCU)
- Seguridad a nivel de sistema operativo
- Cumplimiento con los requisitos más recientes para garantizar la ciberseguridad y la seguridad de los vehículos (ISO 26262, ISO/SAE 21434, UN R155, UN R156, Uptane)
- Comunicación segura y de confianza entre unidades electrónicas de la arquitectura E/E, así como entre estas unidades y los dispositivos de diagnóstico y de nube del vehículo conectado
- Implementación de diagnósticos remotos, actualizaciones seguras de la ECU por aire y otros servicios telemáticos

Ventajas principales

-  Seguridad incomparable e inmunidad cibernética para industrias con requisitos de alto nivel de seguridad de la información
-  Integración de una puerta de enlace segura y una unidad de control telemática en una solución única que reduce los costes
-  Los protocolos especializados ayudan a optimizar los gastos del tráfico móvil



Conocimientos



Kaspersky ICS Threat Intelligence



Análisis profundo de las ciberamenazas industriales y las vulnerabilidades para apoyar evaluaciones de riesgo eficaces, detección de ataques, e investigación y respuesta ante incidentes.

Respaldo por la experiencia sin igual de Kaspersky ICS CERT, el primer CERT privado en ciberseguridad industrial.

Ventajas principales



Detección rápida de amenazas y amplias capacidades analíticas



Mayor eficacia en las investigaciones y en la búsqueda proactiva de amenazas



Información integral sobre amenazas y vulnerabilidades para una toma de decisiones informada

Solicitar una demo

Descripción general de la solución

Póngase en contacto con nosotros

Productos y servicios de Kaspersky Threat Intelligence

Inteligencia frente a amenazas legible por máquina

Kaspersky Threat Data Feeds





Kaspersky Threat Data Feeds



El servicio Kaspersky Threat Data Feeds proporciona inteligencia de amenazas en tiempo real para ayudar a las organizaciones industriales a proteger sus redes y sistemas de las ciberamenazas. Los feeds de datos ICS incluyen información sobre archivos maliciosos conocidos y las vulnerabilidades más recientes conocidas, comprobadas como explotables en sistemas de control industrial. Cuando están en contexto, estos datos permiten revelar un panorama general y responder las preguntas “quién”, “qué”, “dónde” y “cuándo” para identificar a los adversarios, tomar decisiones con mayor agilidad y responder con eficacia.

Ventajas principales



Respuesta mejorada y acelerada ante incidentes y aumento de las funcionalidades de análisis forense



Soluciones de seguridad reforzadas



Evita la filtración de activos confidenciales y propiedad intelectual

Ventajas:

Fuente de datos sobre hashes de ICS de Kaspersky

Inteligencia actualizada sobre amenazas para ICS y otros sistemas usados en TO con el fin de simplificar y automatizar la detección y la investigación oportuna de ataques

#

prevención

#

detección

#

investigación

Fuente de datos sobre vulnerabilidades de ICS de Kaspersky

Datos verificados y perfeccionados acerca de las vulnerabilidades halladas en el software y hardware de sistemas ICS y otros dispositivos empleados en entornos industriales, ofrecidos en un formato legible por máquinas

#

prevención

#

detección

#

investigación

Fuente de datos sobre vulnerabilidades industriales de ICS en formato OVAL

Fuente de datos actualizada periódicamente que contiene definiciones en formato OVAL para la detección automatizada de vulnerabilidades conocidas en sistemas SCADA y otros tipos de software industriales

#

detección



Kaspersky ICS Intelligence Reporting



El servicio Kaspersky ICS Threat Intelligence Reporting proporciona al cliente una inteligencia detallada y un mayor conocimiento de las campañas maliciosas que apuntan a las organizaciones industriales, así como información sobre las vulnerabilidades que se encuentran en los sistemas de control industrial más populares y las tecnologías subyacentes. La información detallada y adaptada a las organizaciones industriales permite a los clientes proteger activos críticos, incluidos componentes de software y hardware, y garantizar la seguridad y la continuidad de los procesos tecnológicos.

Los informes se entregan en el portal **Kaspersky Threat Intelligence** y también están disponibles a través de la API.

Ventajas principales



Detecta y evita amenazas notificadas para proteger los activos más importantes y para garantizar la seguridad y la continuidad del proceso tecnológico



Correlaciona la actividad maliciosa o sospechosa detectada con la investigación de Kaspersky para atribuir incidentes a campañas específicas e identificar amenazas

Ventajas:



Informes de APT

Informes sobre nuevas APT y campañas de ataque de volumen elevado dirigidas a organizaciones industriales, así como actualizaciones de amenazas activas



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 diversos sectores



El entorno de amenazas

Informes sobre cambios significativos en el entorno de amenazas para los sistemas de control industrial, factores críticos recién detectados que afectan los niveles de seguridad de ICS y la exposición de ICS a amenazas, con información regional, nacional y sectorial



Análisis y mitigación de vulnerabilidades

Nuestras asesorías proporcionan recomendaciones prácticas por parte de nuestros expertos de Kaspersky para ayudar a identificar y mitigar amenazas



Kaspersky Ask the Analyst

Kaspersky Ask the Analyst complementa la cartera de Kaspersky Threat Intelligence. Gracias a este servicio, podrás comunicarte con especialistas para obtener asistencia e información útil sobre amenazas y vulnerabilidades específicas a las que te enfrentas o que te interesan. Con estos datos, puedes mejorar tus defensas contra las amenazas que se dirigen tanto a tu organización como a tu infraestructura industrial.

Ventajas principales



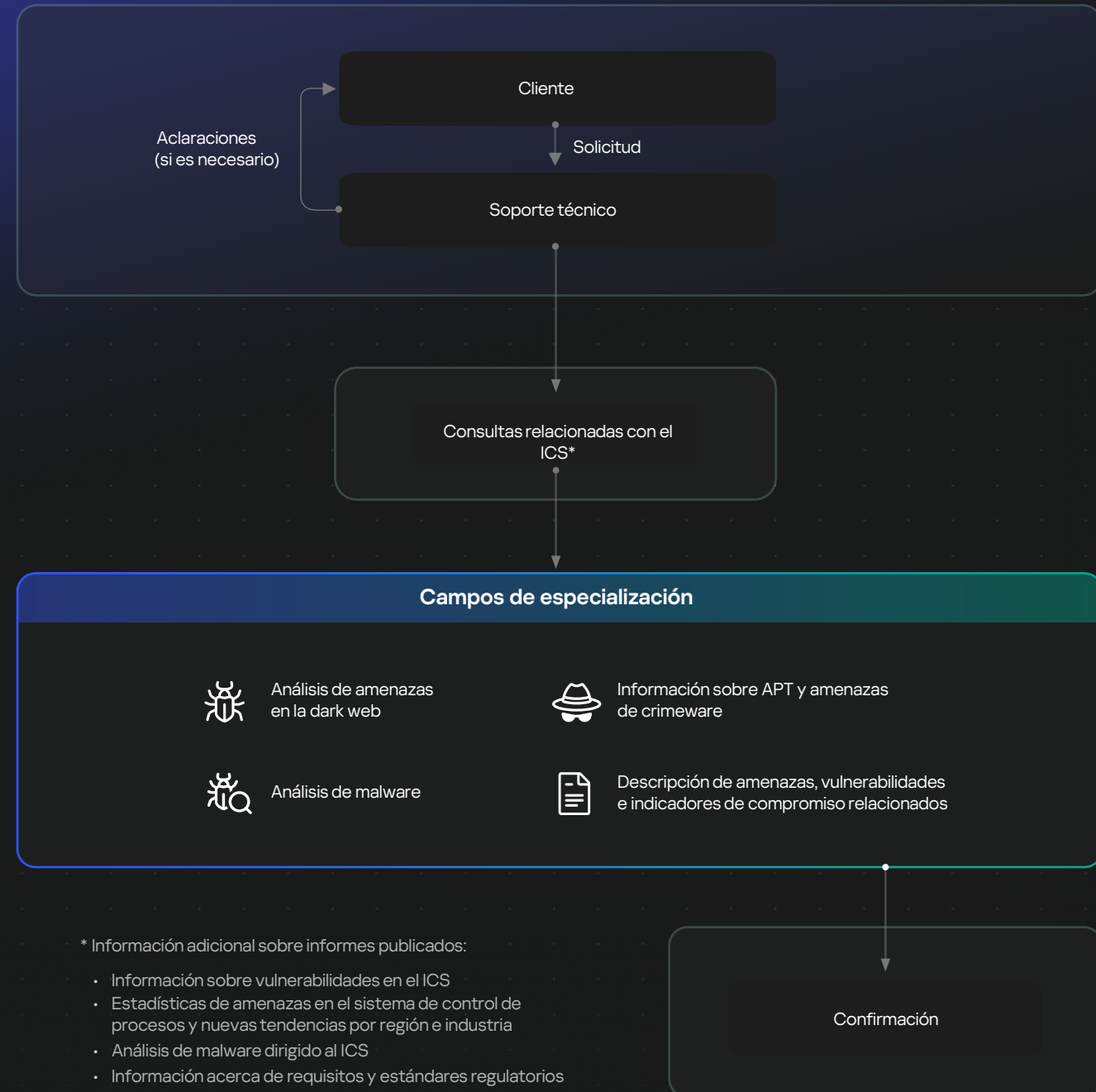
Acceso a los principales expertos en inteligencia frente a amenazas, incluidos los expertos en seguridad industrial de Kaspersky ICS CERT



Información contextual detallada y personalizada para realizar investigaciones efectivas



Instrucciones detalladas de nuestros expertos sobre cómo responder con rapidez y eficacia ante las amenazas y vulnerabilidades





Póngase en contacto con
nosotros
[Probar ahora](#)
[Más información](#)



Kaspersky
Security
Awareness

Transforma a tus empleados en un firewall humano

La cartera de Kaspersky Security Awareness ayuda a desarrollar una cultura sólida de ciberseguridad en todos los niveles de tu organización:

- **Kaspersky Interactive Protection Simulation (KIPS):** simulación basada en juegos adaptada a escenarios industriales (generación de energía, petróleo y gas, petroquímicos, etc.). Demuestra de qué forma la ciberseguridad puede afectar el rendimiento de la empresa, lo que les permite a los gerentes experimentar el impacto de las decisiones estratégicas.
- **Kaspersky Automated Security Awareness Platform (ASAP):** desarrolla un comportamiento seguro en la fuerza laboral a través de capacitaciones interactivas y ataques de phishing simulados para brindar a los empleados el conocimiento y las habilidades básicas de ciberseguridad industrial.
- **Formación para ejecutivos de Kaspersky:** un curso práctico que permite a las personas encargadas de la toma de decisiones y a los líderes funcionales comprender mejor el panorama de la ciberseguridad.

Principales temas tratados

✉ Correo electrónico

🌐 Sitios web
e Internet

🔑 Contraseñas
y cuentas

💬 Redes sociales
y servicios de mensajería

🏭 Industrial
cybersecurity

💻 Seguridad para PC

📱 Dispositivos
móviles

📄 Datos
confidenciales

🔒 RGPD

🔒 Seguridad física
de los datos

💳 Seguridad de las tarjetas
bancarias y PCI DSS

🧠 Inteligencia artificial
y redes neuronales

👤 Datos personales



Póngase en contacto
con nosotros
[Catálogo de la
formación](#)



Kaspersky
ICS CERT
Training

Aprendizaje aplicado

Nuestro programa de capacitación sobre ICS se ha diseñado para permitir que los profesionales de tecnología de la información (IT), tecnología operativa (OT) y seguridad de la información (IS), así como los gerentes y otros empleados, puedan ampliar sus conocimientos sobre ciberseguridad industrial y obtener habilidades prácticas especializadas.

Habilidades prácticas de especialistas de Kaspersky



Ciencia forense digital
y respuestas ante incidentes



Exploración de vulnerabilidades
en dispositivos de TO/IoT
y software industrial



Programas de formación
multidisciplinar
para especialistas
en IT, OT y IS.





Kaspersky
ICS Security
Assessment

Garantía de resiliencia cibernética en entornos de TO

Riesgo

Una sola vulnerabilidad es todo lo que se necesita para que los ciberdelincuentes tomen el control de todo un sistema industrial

Solución

Un enfoque integral para identificar vulnerabilidades y debilidades de seguridad en infraestructuras industriales

Ventajas principales

- Fortalece los controles de seguridad para proteger a operadores, ingenieros y otro personal
- Identifica vulnerabilidades que los hackers podrían explotar para interrumpir líneas de ensamblaje, equipos de fabricación o sistemas robóticos
- Protege los diseños, proyectos y programas de fabricación contra el robo
- Prevén infracciones que podrían comprometer la calidad o la seguridad del producto

Enfoque de Kaspersky respecto a la evaluación de la seguridad industrial



Prueba de penetración externa
Caja negra o caja gris

Internet

Infraestructura industrial (OT)

- Arquitectura y equipo de red
- Solución, estación de trabajo y servidores industriales
- Dispositivos y componentes

Dispositivos
y componentes



Análisis de seguridad de OT

- Pruebas de caja blanca
- Simulación de ataques
- Evaluación

LAN corporativa, MES



Prueba de penetración interna
Caja negra o caja gris

Prueba
entorno



Análisis de seguridad de componentes
de hardware y software

- Pruebas de caja blanca
- Vulnerabilidades de día cero
- Guías de fortalecimiento



Kaspersky Managed Detection and Response

Con tecnología de IA. Perfeccionada por humanos

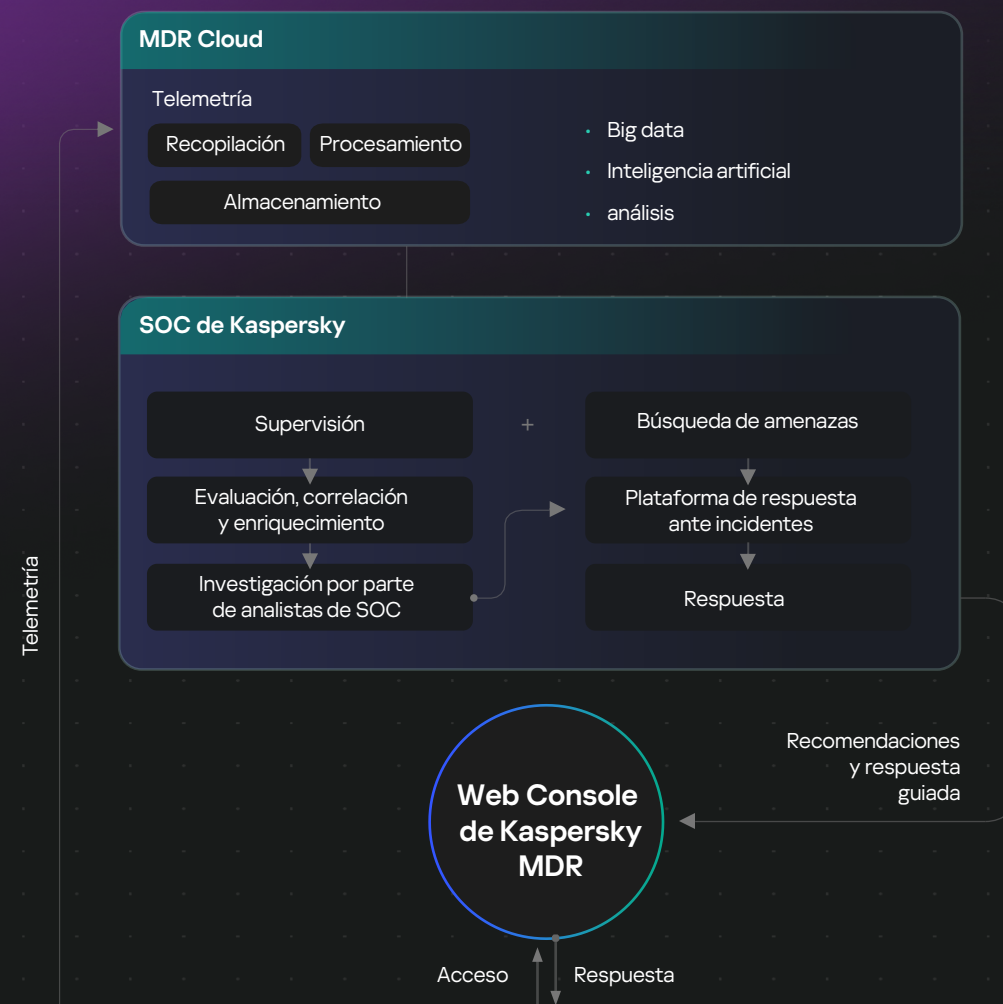
- Búsqueda, detección y eliminación continuas de amenazas que tienen como objetivo a tu organización industrial
- Menos costes de seguridad, dado que eliminas la necesidad de contratar a nuevos expertos en ciberseguridad
- Obtén todas las ventajas de un SOC sin tener que crearlo internamente

Un 22 % de nuestros clientes pertenece al sector industrial

Consulta el [informe de analistas](#) de MDR para obtener más información

Ventajas principales

-  Detección proactiva de amenazas: indicadores de ataque patentados permiten identificar amenazas en el sistema de control
-  Respuesta guiada automatizada (con investigación forense completa y análisis de malware disponible a pedido)
-  Experiencia en ciberseguridad de ICS: respaldada por uno de los equipos de detección de amenazas proactiva con más experiencia y éxito de la industria



Infraestructura industrial y corporativa del cliente



Kaspersky
Industrial CyberSecurity
for Nodes

Servidor

Sistema integrado

Estación de trabajo

Puerta de entrada



Soluciones de protección de
Kaspersky para infraestructura de IT

Servidor

PC

Red

Equipo virtual

Equipo portátil



**Kaspersky
Incident Response**

Gestión de las consecuencias de una brecha en la seguridad

Riesgo

Los incidentes que afectan a infraestructuras críticas requieren la experiencia adecuada para llevar a cabo una respuesta en instalaciones industriales. Las acciones incorrectas y tardías pueden aumentar significativamente el daño de un ataque.

Solución

- Eliminación rápida de las consecuencias de un incidente por parte del equipo global de respuesta a emergencias de Kaspersky
- Asistencia durante todo el ciclo de investigación y respuesta a incidentes
- Inteligencia, recopilación y reparación basadas en nuestras propias herramientas innovadoras
- Experiencia bajo demanda e intercambio de conocimientos con tus equipos

Componentes del servicio



Respuesta a incidentes:
investigación y eliminación de
amenazas



Ciencia forense digital
Análisis de las pruebas digitales



Análisis de malware
Obtén una vista detallada de los
archivos utilizados en un ataque

Explora el panorama de un mundo cibernético con el [informe global](#) del servicio de Kaspersky Security



Un socio de confianza



30 años de experiencia de primer nivel y petabytes de datos sobre amenazas



ICS CERT — división internacional de investigación de seguridad de OT / IoT propia



Experiencia probada en la industria de la seguridad de TI y tecnología operativa (TO), con numerosos premios y logros



Más de 200 certificados de interoperabilidad con soluciones de proveedores de automatización



Eficacia demostrada de la tecnología, cumplimiento de normas y requisitos de la industria

Más sobre
soluciones
de TO

Más sobre
soluciones
de TI

Póngase en
contacto con
nosotros

