Una plataforma XDR para ofrecer seguridad integral a empresas industriales

Kaspersky Industrial CyberSecurity

kaspersky BRING ON THE FUTURE

Atacados por malware

Desde principios de 2023, alrededor del 35 % de las computadoras vinculadas con ICS fueron atacadas por malware: casi un 5 % menos que el año anterior.

Kaspersky ICS CERT, octubre de 2023

Más información

Ciberamenazas a las que se enfrentan los sistemas de control industrial (ICS) y las empresas industriales

La nueva realidad de los propietarios y operadores de infraestructuras industriales se define por el creciente interés de los ciberactivistas en los sistemas de automatización, los altos requisitos regulatorios, la convergencia IT/OT y el aumento en la variedad de ciberataques en el sector industrial (un incremento de casi el 50 % en la primera mitad del 2023, en comparación con la segunda mitad del 2022, según las estadísticas del ICS CERT de Kaspersky).

La adopción de tecnologías digitales, que tiende a considerarse como algo positivo, elimina la distancia entre los entornos IT y OT que solía proteger a este último de los ciberdelincuentes. Mientras que es suficiente con que una sola unidad flash entre en contacto con el entorno del ICS para afectar de gravedad el negocio principal de una empresa, un grupo de hackers con la motivación necesaria puede penetrar en las redes OT y generar daños considerables o incluso robar información valiosa. Si a esto se agrega la evolución de los estándares de automatización (de recomendaciones generales a requisitos legislativos) y la creciente necesidad de compartir las mejores prácticas y gestionar riesgos, la ciberseguridad de las empresas industriales se convierte en un enorme desafío.

De hecho, el ICS CERT de Kaspersky ha notado un incremento en la frecuencia de ciberataques en las siguientes industrias:

Petróleo, gas y productos químicos

Dado el alto valor de los datos y sistemas que estas empresas controlan, son un objetivo atractivo para el ransomware y los actores maliciosos que buscan interrumpir operaciones o manipular precios.

Empresas de la industria manufactura de alto perfil

Estas empresas desempeñan funciones sociales críticas y poseen datos valiosos que pueden aprovecharse para obtener beneficios financieros, lo que provocaría enormes daños económicos y para su reputación.

Minerales, metales y minería

La industria de los minerales, los metales y la minería se convierten en un objetivo importante por sus valiosos recursos, su impacto financiero y las cadenas de suministro interconectadas.

Electricidad, redes y servicios públicos

La función crucial que la industria de la electricidad, las redes y los servicios públicos desempeñan en nuestra vida diaria es la razón principal por la que son objetivos de ataques, con el objetivo de generar caos o ejercer influencia.

La estabilidad de los procesos comerciales y de producción, así como la protección de activos valiosos, están directamente relacionadas con el desarrollo sustentable de las empresas industriales y las instalaciones de infraestructuras críticas. Los ataques a sistemas industriales, en particular a ICS y SCADA, están en aumento. Mientras tanto, las ciberamenazas modernas dirigidas a entornos industriales parecen ser inmunes a las soluciones convencionales.

Nunca fue tan importante elegir un partner de confianza, que conozca en profundidad las coincidencias entre la ciberseguridad corporativa e industrial, y pueda brindar una gama completa de tecnologías de seguridad de última generación.

Estos son los principales objetivos de los ataques APT:

Propietarios y operadores de infraestructuras críticas

Las organizaciones públicas o gubernamentales de importancia estratégica se enfrentan a potenciales peores consecuencias debido a interferencias operativas.

Empresas industriales de alto perfil

Ya sea que tengan una sola instalación u operen a escala nacional o internacional, estas empresas llevan a cabo operaciones de alto riesgo que implican incidentes de altos costos.

Obtenga más información acerca de los TTPs más habituales en los ataques que se lanzan contra organizaciones industriales.

Más información

KICS, la plataforma de XDR, les permite a los usuarios tener una visión y un contexto más amplios: la cadena de incidentes a nivel de red y endpoints, los parámetros precisos de los activos, la comunicación de la red y los mapas topológicos, incluso de los segmentos donde la duplicación de tráfico aún no está disponible, entre otras cosas.

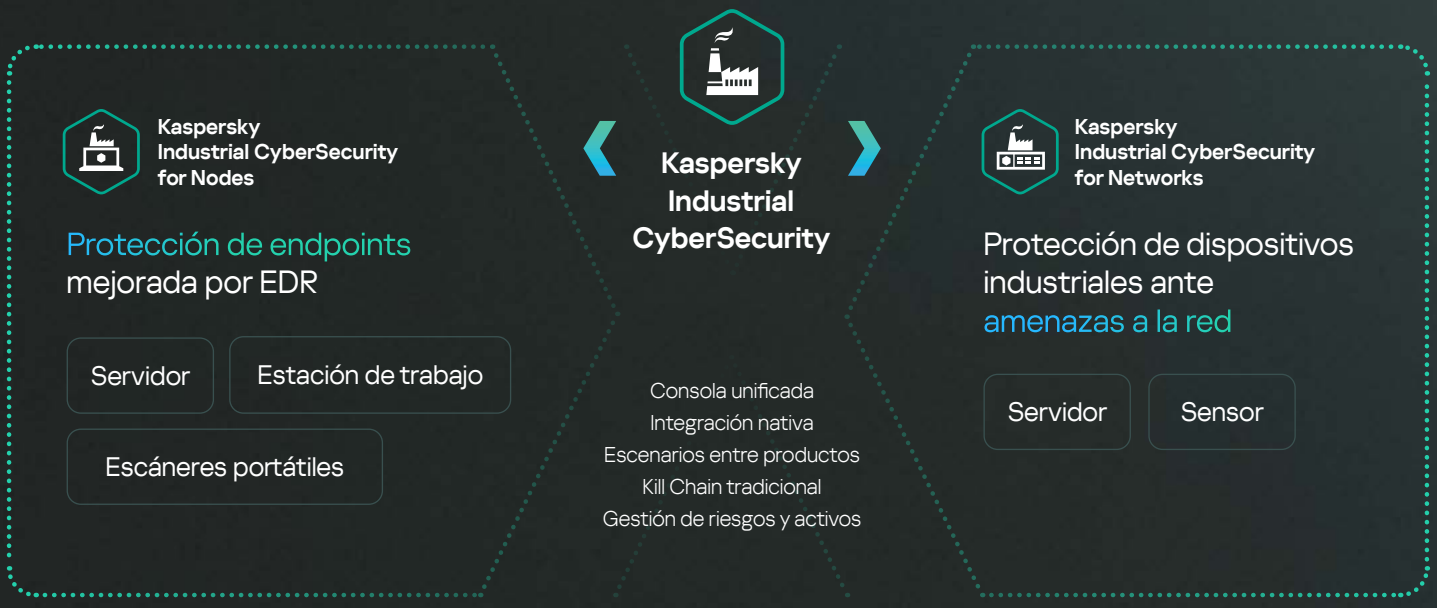
Sensor de endpoints

- Estado de la protección
- Auditoría de seguridad
- Comunicaciones en la red
- Transmisión de telemetría del host
- Supervisión de equipos
- Respuesta a incidentes

Tecnologías de seguridad avanzada ICS

Kaspersky Industrial CyberSecurity (KICS) es una plataforma de detección y respuesta extendida (XDR) para organizaciones industriales, diseñada y certificada especialmente para proteger equipos, activos y redes críticas OT ante ciberamenazas. La plataforma cuenta con tecnologías integradas que aseguran los componentes y sistemas de control de la automatización industrial en todos los niveles. KICS for Nodes ofrece protección, detección y respuesta en endpoints, incluyendo auditorías de cumplimiento y funcionalidades de sensor de endpoints. Por otro lado, KICS for Networks está especializado en el análisis, detección y respuesta de tráfico en redes OT. Adicionalmente, la plataforma incorpora una función de administración centralizada a nivel de sitio, crucial para expandir las operaciones de seguridad OT en diversas infraestructuras industriales de gran envergadura, repartidas en diferentes regiones geográficas.

La integración continua entre los componentes de la plataforma proporciona una visibilidad completa de las múltiples redes OT los sistemas de automatización distribuidos geográficamente. De esta manera, el cliente disfruta de una experiencia mejorada, puede conocer la situación y tiene flexibilidad en su implementación. Con detección y respuesta extendidas, la plataforma KICS permite la convergencia IT/OT y proporciona numerosos beneficios a proveedores únicos.



Puntos de aplicación de la plataforma

Convergencia de entornos OT y IT

DMZ/GTW

Entorno IT

Entorno OT

Kaspersky Industrial CyberSecurity for Nodes

- Estación de trabajo del operador
- Servidor SCADA
- Estación de trabajo de ingeniería
- Puerta de enlace ICS

Equipo de red

SPAN

Kaspersky Industrial CyberSecurity for Networks

- Unidad de Control de Bahía (BCU)
- Dispositivo electrónico inteligente (IED)
- Controladores lógicos programables (PLC)
- Relés de protección y sistema instrumentado de seguridad (SIS)
- Nodos aislados (verificación manual con el Escáner portátil KICS)

Detección temprana de anomalías y análisis predictivo

Kaspersky Machine Learning for Anomaly Detection (Kaspersky MLAD) es un sistema innovador que emplea una red neuronal para supervisar una gran variedad de datos de telemetría de forma simultánea. Detecta fallas del equipo y errores humanos (lo que permite evitar errores y accidentes), identifica acciones de empleados u operaciones de equipos atípicas, como indicios de un ataque especializado o de sabotaje, y combina la detección de anomalías con el análisis predictivo del estado de los equipos y el ciclo de vida.

Más información

Nivel físico

Protegido por los productos Kaspersky

Kaspersky Industrial CyberSecurity for Networks

KICS for Networks

Una solución patentada al nivel del protocolo para la supervisión y el análisis de tráfico de redes industriales, entregada como software o como un dispositivo virtual.

KICS for Networks identifica anomalías e intrusiones en el ICS de forma temprana, muestra cómo el ataque se desarrolla a través de la red y en los nodos (telemetría y kill chain de EDR), y garantiza que se realicen las acciones necesarias para evitar cualquier impacto negativo en los procesos industriales.

La solución permite detectar y clasificar riesgos en virtud de datos de vulnerabilidades, conexiones de la red y la función de diferentes activos, para prevenir incidentes.

Beneficios

Inventario de activos

Conjunto de datos e inventario de activos automáticos mediante métodos pasivos y activos de recopilación de datos

Inventario y visualización de la red

- Mapa de comunicaciones de la red
- Diagrama de topología de la red

Evaluación de riesgos y vulnerabilidades

- Gestión de riesgos y vulnerabilidades específicas del OT
- Puntuación y priorización automáticas
- Recomendaciones sobre la remediación de riesgos

Detección de anomalías en la red

Control de integridad de la red mediante la supervisión de desviaciones del punto de referencia y la detección de actividad maliciosa y sospechosa en la red

Control de procesos OT e inspección profunda de paquetes (DPI)

- Extracción de datos de las cargas útiles industriales
- Control de procesos en tiempo real
- Control de comandos industriales
- Supervisión avanzada de procesos OT con Kaspersky MLAD

Integración e intercambio de datos

- Información centralizada
- Integración con sistemas de clientes o de Kaspersky y terceros (IEC 104, OPC, CEF, Syslog, conectores basados en API)

Auditoría Centralizada de Cumplimiento para Nodos de Redes Industriales

KICS for Networks brinda una auditoría centralizada para los nodos de redes industriales. Incluye la capacidad de realizar auditorías en endpoints y hardware de red, tanto con agentes (usando KICS for Nodes) como sin agentes. Esta función se enfoca en identificar vulnerabilidades y asegurar el cumplimiento con los estándares industriales OVAL* y XCCDF**.

- Auditorías de seguridad centralizadas y automatizadas para dispositivos de red y nodos de Windows y Linux
- Auditoría de cumplimiento. Editor completamente funcional con verificaciones y parámetros de cumplimiento
- Todos los informes y datos de activos están disponibles en un solo lugar: la base de activos de KICS for Networks
- Bóveda protegida para credenciales de nodos
- Compatible con cualquier base de datos OVAL personalizada o de terceros
- Base de datos integrada de vulnerabilidades de SCADA realizada por ICS CERT

* Lenguaje abierto de evaluación y vulnerabilidad (OVAL)
** Formato de descripción de listas de comprobación de configuración ampliable (XCCDF)

Kaspersky Industrial CyberSecurity for Nodes

KICS for Nodes

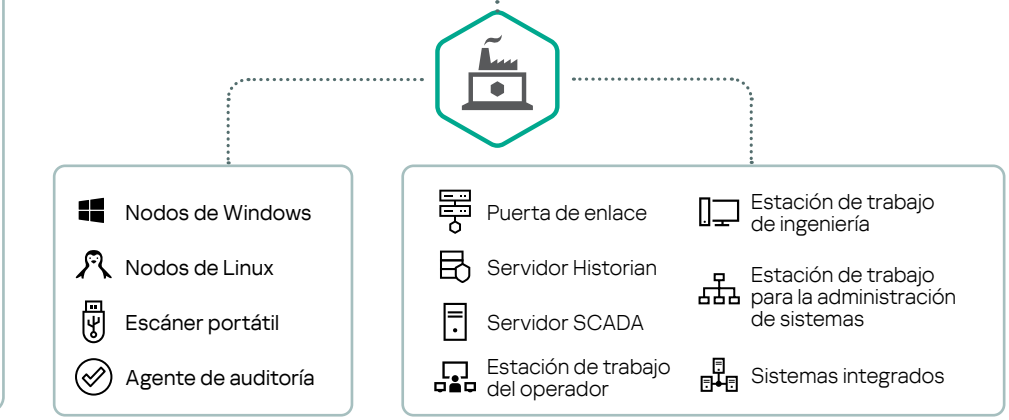
Esta solución ofrece protección, detección y respuesta de endpoints industriales de calidad comprobada y certificada. Esta solución es estable, de bajo impacto y compatible con sistemas Linux, Windows y otras plataformas independientes.

KICS for Nodes protege todos los endpoints de un sistema de automatización moderno, digital, administrado y distribuido. La solución recopila telemetría para crear una representación visual clara y detallada del progreso de un incidente en las estaciones de trabajo, los servidores, las puertas de enlace y otros endpoints. De este modo, se asegura a los administradores del sistema de automatización que se resolvió el incidente por completo y que no volverá a suceder.

El Escáner portátil de KICS for Nodes ejecuta una política de ciberseguridad en los mecanismos independientes, los sistemas de automatización o los equipos en los que no se puede instalar un software de seguridad. Debido a que tiene un impacto operativo muy bajo, no interfiere con las soluciones de seguridad existentes.

- Es una solución que no requiere instalación, brinda un conocimiento óptimo de la situación y proporciona una máxima visibilidad de las redes OT, incluyendo infraestructuras independientes.
- Le permite realizar análisis a pedido en múltiples máquinas durante las ventanas de mantenimiento de manera simultánea y proporciona informes convenientes.
- Lleva a cabo verificaciones de cumplimiento antimalware de los equipos que acceden al sitio de OT, incluso en computadoras de contratistas externos.

- Control de dispositivos
- Control de integridad de los archivos
- Control de integridad de PLC
- Protección contra cifradores
- Prevención de exploits
- Prevención de amenazas de red
- Inspector del registro de Windows
- Control de Wi-Fi
- Administración de firewall
- Supervisor del registro
- Auditoría de seguridad
- Agente de EDR
- Sensor de endpoints (integración con KICS for Networks)



Beneficios

Bajo impacto

- Bajo impacto sobre los dispositivos protegidos para un mejor rendimiento del sistema
- Sin necesidad de reinicio para realizar instalaciones, actualizaciones o mejoras
- Modo de solo detección disponible
- Consumo de recursos del sistema configurable

Compatibilidad

- Compatible con sistemas operativos heredados, desde Windows XP SP2 y Windows Server 2003 SP1
- Compatible con proveedores de automatización industrial
- Escáner portátil como opción sin instalación

Protección extendida

- Protección frente a malware, ransomware y exploits
- Análisis de registros
- Control de firewall
- Tecnología integrada de EDR para ICS
- Actualizaciones de bases de datos aisladas

Implementación modular

- Opciones flexibles y configuración segura y no intrusiva, diseñadas para TO
- La arquitectura modular permite seleccionar solo los componentes de protección requeridos

Compatible con PLC

- Siemens SIMATIC S7-300, S7-400, S7-400H, S7-1500, S7-1200, SIPROTEC 4
- Schneider Electric Modicon M340, M580
- Dispositivos basados en CODESYS V3
- Fastwel CPM723-01

Auditar

- Auditoría de cumplimiento y seguridad integral basada en el estándar abierto OVAL

Factores de efectividad de Kaspersky XDR

Comprensión contextual de características, requisitos, sistemas especializados, consideraciones operativas y protocolos únicos

La integración con ICS permite tener una visibilidad integral y analizar el comportamiento del sistema y el tráfico de la red industrial

Inteligencia de amenazas específicas de OT para aprovechar la experiencia de Kaspersky en el área de protección de amenazas en entornos industriales

Personalización y configuración para adaptar la solución a su nivel de tolerancia al riesgo, la arquitectura de su red y sus necesidades de cumplimiento regulatorio específicas

Un **proveedor único** para aprovechar al máximo la colaboración y la asistencia de proveedores, que abarca actualizaciones y parches oportunos

Ciberseguridad unificada en todos los segmentos industriales y corporativos de la empresa

Los ataques a sistemas industriales, en particular a ICS y SCADA, están en aumento. Nunca ha sido tan importante elegir un partner de confianza que conozca en profundidad las similitudes entre la ciberseguridad corporativa e industrial, y que pueda ofrecer una gama completa de tecnologías de ciberseguridad corporativas e industriales de última generación.

Kaspersky XDR es la herramienta perfecta para crear un entorno de trabajo seguro y sin amenazas. Debido a que es compatible con diversos productos de seguridad, permite establecer un ciberespacio seguro, al brindar opciones específicas para la industria de su empresa y protegerla de cualquier amenaza, sin importar qué tan pequeña o tan extensa sea. Las opciones de integración de Kaspersky XDR permiten acceder a una vista unificada e integral de las amenazas, lo que le proporciona a su equipo de seguridad todas las herramientas y los datos necesarios para proteger su empresa de las amenazas actuales y potenciales.

Más información

Convergencia de TI/TO con Kaspersky Hybrid XDR

Ciberseguridad IT

Más información

Ciberseguridad OT

Más información

Límite del entorno

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

ICS CERT

ICS CERT: división internacional propia de investigación en seguridad sobre tecnología operativa (OT) e Internet de las cosas (IoT)

Experiencia probada en la industria de la seguridad de IT y OT, con numerosos premios y logros

Más de 100 certificados de interoperabilidad con soluciones de automatización

Efectividad de la tecnología probada y cumplimiento con estándares y requisitos

Clientes en todo el mundo

ROSATOM NORNICKEL EuroChem

NLMK TATNEFT ROSSETI Wintershine

alperia PacificLight КазМунайГаз AGC

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Networks

Más información

latam.kaspersky.com

#kaspersky
#bringonthefuture