Una plataforma de Detección y Respuesta Extendida (XDR) que proporciona a las empresas industriales una seguridad integral

Kaspersky Industrial CyberSecurity

kaspersky bring on the future

Ataques de malware

En el primer trimestre de 2024, las organizaciones afectadas o los funcionarios responsables confirmaron públicamente un total de 30 incidentes de ciberseguridad, de los cuales el 64,5 % correspondió a la industria manufacturera.

Kaspersky ICS CERT, junio de 2024

Conozca más

Panorama de amenazas para la industria

La nueva realidad para los propietarios y operadores de infraestructuras industriales está marcada por el creciente interés de hackers activistas en los sistemas de automatización, requisitos normativos más estrictos, la convergencia entre IT y OT, y una mayor diversidad de ciberataques en el sector industrial. En el primer trimestre de 2024, las soluciones de Kaspersky bloquearon malware de 10,865 familias diferentes en sistemas de automatización industrial.

La proliferación de tecnologías digitales, generalmente vista como algo positivo, está eliminando la separación entre los entornos de IT y OT, que anteriormente protegía a este último de los ciberdelincuentes. Aunque basta con que una sola unidad flash entre en contacto con el entorno ICS para afectar gravemente la actividad principal de una empresa, un grupo de hackers con la motivación suficiente puede infiltrarse en las redes OT, causar daños significativos o incluso robar información valiosa. Si a esto sumamos la evolución de los estándares de automatización —que han pasado de ser recomendaciones generales a convertirse en requisitos legislativos— y la creciente necesidad de compartir mejores prácticas y gestionar riesgos, la ciberseguridad de las empresas industriales se presenta como un gran desafío.

ICS CERT de Kaspersky considera que las organizaciones de las siguientes industrias se enfrenten a ciberataques con una frecuencia cada vez mayor:

Petróleo, gas y productos químicos

La digitalización de la exploración, extracción, transporte y refinación —todos factores clave de competitividad para estas empresas— implica la integración de dispositivos IIoT, drones y robots, así como la implementación de soluciones de redes 5G, blockchain y realidad virtual, lo que aumenta la superficie de ataque para actividades maliciosas.

Fabricación crítica

Estas empresas buscan optimizar la relación costo-eficiencia mediante la implementación de tecnologías de vanguardia, la expansión de la conectividad, el uso de soluciones en la nube y la exploración de escenarios de convergencia entre IT y OT, lo que aumenta su exposición a amenazas nuevas y en constante evolución.

Minerales, metales y minería

Esta industria, un pilar fundamental de la fabricación crítica y relevante a nivel nacional, debe equilibrar los gastos con las tecnologías digitales y de automatización. La industria no debe subestimar la ciberseguridad, ya que es un objetivo para hackers activistas y atacantes altamente capacitados.

Electricidad, redes y servicios públicos

Las tecnologías emergentes y digitales son cruciales para impulsar la transición energética, mientras se preservan las infraestructuras heredadas, que continúan siendo el pilar de la mayoría de las instalaciones de energía. Aun así, representan el mayor riesgo y, por lo tanto, requieren mayores esfuerzos de ciberseguridad.

Los ataques a sistemas industriales, en particular a ICS y SCADA, están en aumento. Mientras tanto, las ciberamenazas actuales dirigidas a entornos industriales parecen resistir las soluciones convencionales. Frente a esta realidad, Kaspersky ofrece un enfoque integral para estas industrias. Descubra las historias de éxito de nuestros clientes, información sobre el panorama de amenazas y ofertas para escenarios específicos en nuestro sitio web.

Nunca ha sido tan importante elegir un socio de confianza que comprenda en profundidad las coincidencias entre la ciberseguridad corporativa e industrial y ofrezca una gama completa de tecnologías de seguridad de última generación.

Estos son los principales objetivos de los ataques APTs:

Propietarios y operadores de infraestructuras críticas

Organizaciones estratégicas de los sectores de petróleo y gas, productos químicos, energía y servicios públicos enfrentan consecuencias cada vez más graves por la interrupción de sus operaciones.

Fabricación crítica

Estas empresas, que van desde plantas individuales hasta instalaciones a nivel nacional e internacional, incluidas las de los sectores de metales y minería, agricultura y fabricación global, llevan a cabo operaciones de alto riesgo que implican costos significativos ante cualquier incidente.

Obtenga más información sobre los ataques financieros y las APTs dirigidas a empresas industriales durante los primeros meses de 2024

Conozca más

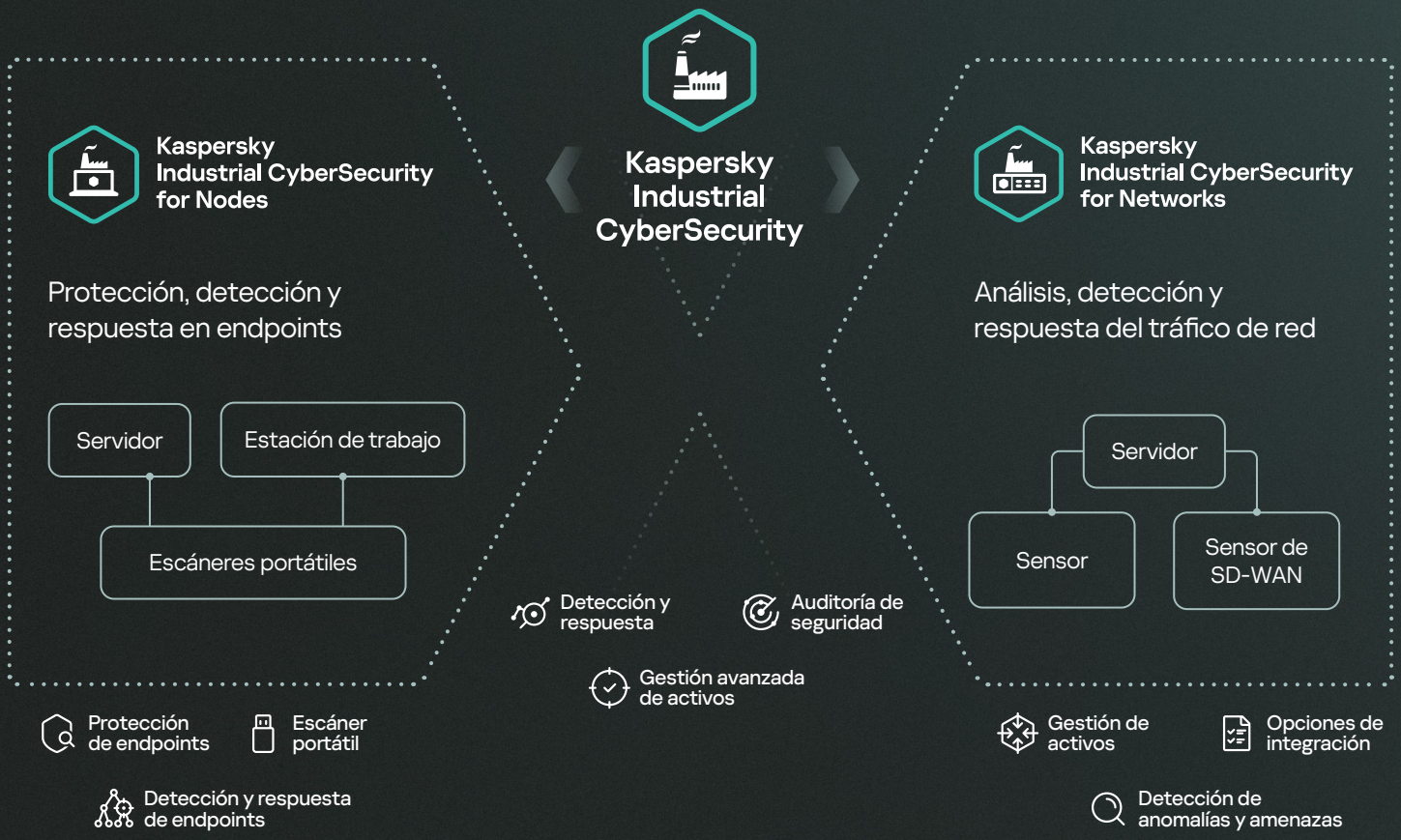
Tecnologías de seguridad avanzada ICS

La brecha entre los entornos de IT y OT, que antes protegía a estos últimos de los ciberdelincuentes, se está reduciendo cada vez más. Por ello, quienes poseen u operan sistemas físico-digitales deben contar con una solución de seguridad integral, proporcionada por un único proveedor y de nivel empresarial, para proteger la infraestructura crítica. **La plataforma XDR nativa de Kaspersky Industrial CyberSecurity (KICS)**, que incluye los componentes KICS for Networks y KICS for Nodes, protege las redes y los sistemas de automatización industrial.

KICS for Networks es un producto de análisis de tráfico, detección y respuesta que ofrece supervisión de redes industriales, detección de intrusiones y capacidades de gestión de riesgos, además de auditar de forma centralizada los nodos de redes industriales para identificar vulnerabilidades y verificar el cumplimiento de los estándares del sector. **Por otro lado, KICS for Nodes** ofrece protección de endpoints a nivel industrial, con capacidades de detección y respuesta, además de funciones de auditoría de cumplimiento basadas en OVAL. Esta solución modular y de bajo impacto es compatible con Linux, Windows, sistemas heredados, sistemas independientes y PLC. La versión Escáner Portátil protege máquinas independientes y dispositivos de contratistas sin necesidad de instalación.

Combinados, estos componentes conforman la plataforma XDR de KICS, que proporciona un inventario centralizado de activos, gestión de riesgos y auditorías, permitiendo escalar la seguridad en infraestructuras distribuidas y diversas a través de una única plataforma, con un gráfico integral de incidentes, análisis y muchos otros recursos.

La plataforma XDR de KICS permite a los usuarios obtener una visión y un contexto más amplios; incluyendo la cadena de incidentes a nivel de red y endpoints, los parámetros precisos de los activos, los mapas de comunicación y la topología de la red, incluso en segmentos donde la duplicación de tráfico aún no está disponible, entre otros aspectos.



* Lenguaje abierto de evaluación y vulnerabilidad (OVAL)

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

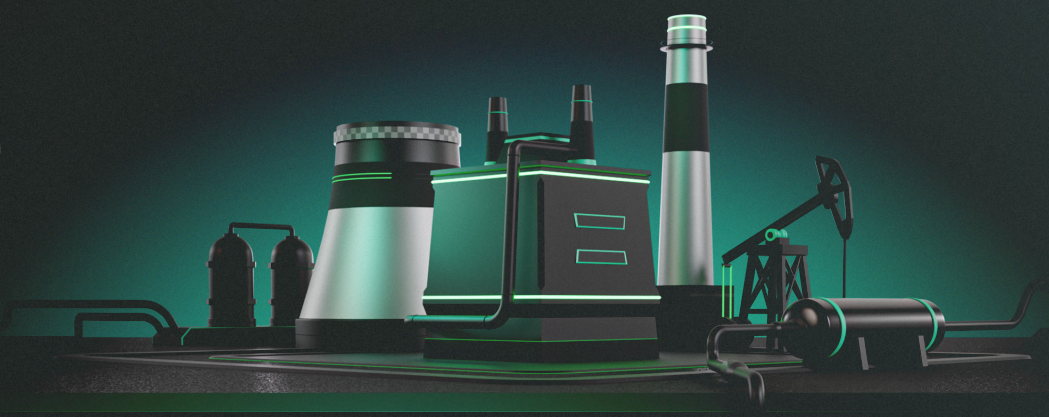
Kaspersky Industrial CyberSecurity for Networks

- 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)

Nivel físico

Detección temprana de anomalías y análisis predictivo

Kaspersky Machine Learning for Anomaly Detection (Kaspersky MLAD) es un sistema innovador que utiliza redes neuronales para supervisar simultáneamente una amplia variedad de datos de telemetría. Detecta fallas en los equipos y errores humanos (lo que permite prevenir errores y accidentes), identifica acciones atípicas de empleados o equipos como indicios de un ataque especializado o sabotaje, y combina la detección de anomalías con el análisis predictivo del estado de los equipos y su ciclo de vida.



Conozca más

Con protección de los productos de Kaspersky

Kaspersky Industrial CyberSecurity for Networks

KICS for Networks

Esta solución de supervisión y análisis de tráfico de redes industriales habilita la Inspección exhaustiva de paquetes (DPI) sobre protocolos industriales privados. Se entrega 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 los nodos (telemetría y cadena de ataques del EDR), y garantiza que se tomen las medidas necesarias para evitar cualquier impacto negativo en los procesos industriales.

Gestión de activos

Detección de activos
Proporciona información detallada sobre los activos mediante una base de datos de vulnerabilidades, la priorización de riesgos y un sondeo activo y seguro

Visibilidad de la red
Supervisa el tráfico, crea mapas topológicos y controla la situación de la red a lo largo del tiempo para obtener mayor visibilidad

Herramientas para analizar el tráfico
Controla y analiza las sesiones de red, permitiendo el almacenamiento y la exportación de datos detallados sobre el tráfico

Ventajas

- Ideal para protocolos y aplicaciones industriales Soporte para diversos protocolos OT, dispositivos y ataques de red, con compatibilidad para la importación de proyectos externos
- Reglas preconfiguradas para establecer auditorías de seguridad
- Interfaz fácil de usar e informes personalizables
- Conciencia sobre los riesgos en infraestructuras distribuidas
- Ingesta de muestras de tráfico desde distintos orígenes: sensores de redes propias, sensores SD-WAN, sensores en endpoints y sensores portátiles

Ecosistema e integraciones

Ecosistema
Descubra las amplias capacidades del ecosistema de Kaspersky mediante la integración con las siguientes soluciones y una estrategia de ciberseguridad unificada en todos nuestros productos:

- Kaspersky Next XDR Expert
Más información

- Kaspersky IoT Secure Gateway (KISG)
Más información

- Kaspersky Machine Learning for Anomaly Detection (MLAD)
Más información

- Kaspersky Software-Defined Wide Area Network (SD-WAN)
Más información

Gestione todos los elementos del ecosistema desde una única consola.

Integraciones con terceros
Disfrute de una compatibilidad sin inconvenientes a través de una amplia variedad de plataformas y herramientas de seguridad externas

Detección de anomalías y amenazas

Detección de intrusiones
Basada en firmas y un motor estadístico que identifica ataques de fuerza bruta o intentos de exploración

Control de la integridad de la red
El sistema aprende las interacciones normales de la red y notifica cualquier desviación

Detección de anomalías
Identifica anomalías en paquetes básicos y a nivel de protocolo
Puede ampliarse con MLAD

DPI de protocolos industriales
Mantiene el control de comandos y procesos, y realiza un seguimiento eficiente de los datos de telemetría

Correlación de eventos
Los eventos de seguridad se asocian con la clasificación MITRE y se integran en una única cadena de ataques

Kaspersky Industrial CyberSecurity for Nodes

KICS for Nodes

Protección, detección y respuesta de endpoints de calidad industrial, comprobada y certificada. Es una solución estable, de bajo impacto y compatible con Linux, Windows y sistemas independientes.

KICS for Nodes protege todos los endpoints de los sistemas de automatización digital actuales, tanto administrados como distribuidos. La solución recopila telemetría para crear una representación visual clara y detallada del progreso de un incidente en las estaciones de trabajo, servidores, puertas de enlace y otros endpoints. De este modo, garantiza a los administradores del sistema de automatización que el incidente se ha resuelto por completo y que no vuelva a ocurrir.

Protección de endpoints

Prevención de amenazas en tiempo real
Lleva a cabo análisis personalizados y bajo demanda de unidades extraíbles y áreas críticas para detener exploits y proteger archivos

Control de la actividad local
Gestiona dispositivos y sistemas Wi-Fi mientras garantiza la integridad en proyectos con PLC para obtener toda la información sobre la actividad local

Control de la actividad de la red
Gestiona firewalls en los hosts y bloquea sesiones de red para garantizar la protección frente a amenazas en la red

Supervisión del sistema
Verifiqua la integridad de los archivos, controla los accesos al registro y detecta amenazas en los logs del sistema para garantizar la seguridad del sistema operativo

Detección y respuesta en endpoints

Detección
Analiza indicadores de compromiso (IoC) y disfruta de las características integrales de supervisión e informes

Respuesta
Evita ejecuciones, pone archivos en cuarentena (o los elimina), inicia o finaliza procesos, aísla redes y mucho más

- Nodos de Windows
- Escáner portátil
- Nodos de Linux
- Agente de auditoría

Escáner portátil

Análisis de malware
Realiza análisis antimalware en equipos independientes y en todas las computadoras de la planta industrial

Análisis OVAL
Fortalece sus políticas de ciberseguridad en máquinas independientes con análisis manuales sobre vulnerabilidades y cumplimiento

Obtención de paquetes
Recoge y analiza el tráfico de red para ofrecer plena visibilidad de lo que ocurre, incluso en infraestructuras aisladas

Inventario básico de activos
Recopila datos integrales sobre hardware y software con una solución poco exigente

Ventajas

- Bajo impacto en dispositivos protegidos y consumo de recursos configurable
- Compatibilidad con SO heredados y proveedores de automatización industrial
- Configuración de seguridad básica y opciones avanzadas para proteger los hosts de cualquier amenaza
- Implementación modular y configuración no intrusiva
- Compatibilidad con PLC: Siemens SIMATIC S7-300, S7-400, S7-400H, S7-1500, S7-1200, SIPROTEC 4, Schneider Electric Modicon M340, M580, dispositivos CODESYS V3 y Fastwel CPM723-01
- Opciones de licencias flexibles (de 1 mes a 5 años)
- Configuraciones predefinidas verificadas y eficientes para los ICS más conocidos

- Puerta de enlace
- Servidor Historian
- Servidor SCADA
- Estación de trabajo del operador
- Sistemas integrados
- Estación de trabajo para la gestión de sistemas
- Estación de trabajo de ingeniería

En la plataforma de KICS y más allá

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

XDR nativo para TO

Los componentes fundamentales de Kaspersky Industrial CyberSecurity, KICS for Networks y KICS for Nodes, están diseñados para integrarse sin inconvenientes con nuestro ecosistema, permitiendo una experiencia unificada y coherente. Al combinarse, estos componentes conforman la plataforma XDR nativa, que integra funcionalidades adicionales valiosas en múltiples productos

Gestión avanzada de activos

Inventario de hardware de endpoints
Obtenga una visibilidad integral de todos los dispositivos conectados en su infraestructura para asegurar un seguimiento preciso de sus activos y fortalecer la gestión de la seguridad.

Inventario de parches, usuarios y aplicaciones
Reciba información detallada sobre implementaciones de software, accesos de usuarios y estados de parches en su entorno. Además, obtenga datos enriquecidos para gestionar posibles vulnerabilidades y mitigarlas de forma adecuada.

Supervisión del tráfico de endpoints
Controla continuamente los flujos de datos en cada endpoint para detectar rápidamente patrones inusuales o posibles amenazas, garantizando una respuesta oportuna ante actividades sospechosas.

Auditoría de seguridad

Análisis de vulnerabilidades
Examina en detalle sus activos para identificar debilidades de seguridad, aumentar la conciencia sobre los riesgos, responder oportunamente y fortalecer su posición general en materia de seguridad.

Auditoría de cumplimiento
Realiza auditorías con y sin agentes para verificar el cumplimiento de los estándares de la industria OVAL y XCCDF*. Incluye un editor completamente funcional, una base de datos centralizada de informes, una bóveda segura para las credenciales de los nodos y mucho más.

Control de la configuración
Garantiza una configuración segura de sus activos, supervise los cambios relacionados con los riesgos de seguridad y mantenga la integridad fundamental de los activos de hardware y software.

Detección y respuesta

Detección
Optimiza y mejora la identificación de amenazas mediante la correlación de eventos en hosts de red, con una vista unificada de la cadena de ataques. Además, proporciona datos enriquecidos sobre las alertas en la red para obtener información más detallada de los incidentes.

Respuesta
Reduce las amenazas mediante la prevención de ejecuciones, el aislamiento de hosts y la cuarentena de amenazas, mientras que las integraciones eficientes con firewalls potencian su capacidad para responder de manera rápida y eficaz ante incidentes de seguridad.

XDR abierto para OT

Extienda la funcionalidad de sus soluciones EDR mediante un motor de correlación, respuestas automáticas y conectores externos, potenciando la capacidad de la plataforma KICS con la solución Kaspersky XDR Core. Aproveche las siguientes características:

- Supervisión integral y correlación de eventos de seguridad informática (SIEM), integrada con múltiples sistemas
- Gestión y enriquecimiento de la inteligencia de amenazas

XDR único para IT y OT

Dé un paso más y aproveche la más reciente convergencia de IT y OT. Combine la plataforma KICS con nuestro paquete Kaspersky Next XDR Expert y disfrute de las mejores funcionalidades de la industria en protección de endpoints, beneficiándose de las siguientes características:

- Un único gráfico de investigación, junto con manuales de estrategias y gestión de incidentes, todo desde la Plataforma de Administración Única de Kaspersky
- Protección compleja para la infraestructura de IT (IT XDR)

XDR industrial

Kaspersky Industrial CyberSecurity

Conozca más

Kaspersky Single Management Platform

XDR corporativo

Kaspersky Next XDR Expert

Conozca más

* Formato de descripción de listas de comprobación de configuración ampliable (XCCDF)

27 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 200 certificados de compatibilidad con soluciones de proveedores de automatizaciones

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

Conozca más

latam.kaspersky.com

© 2024 AO Kaspersky Lab. Las marcas comerciales y marcas de servicios registradas pertenecen a sus legítimos propietarios.

#kaspersky
#bringonthefuture