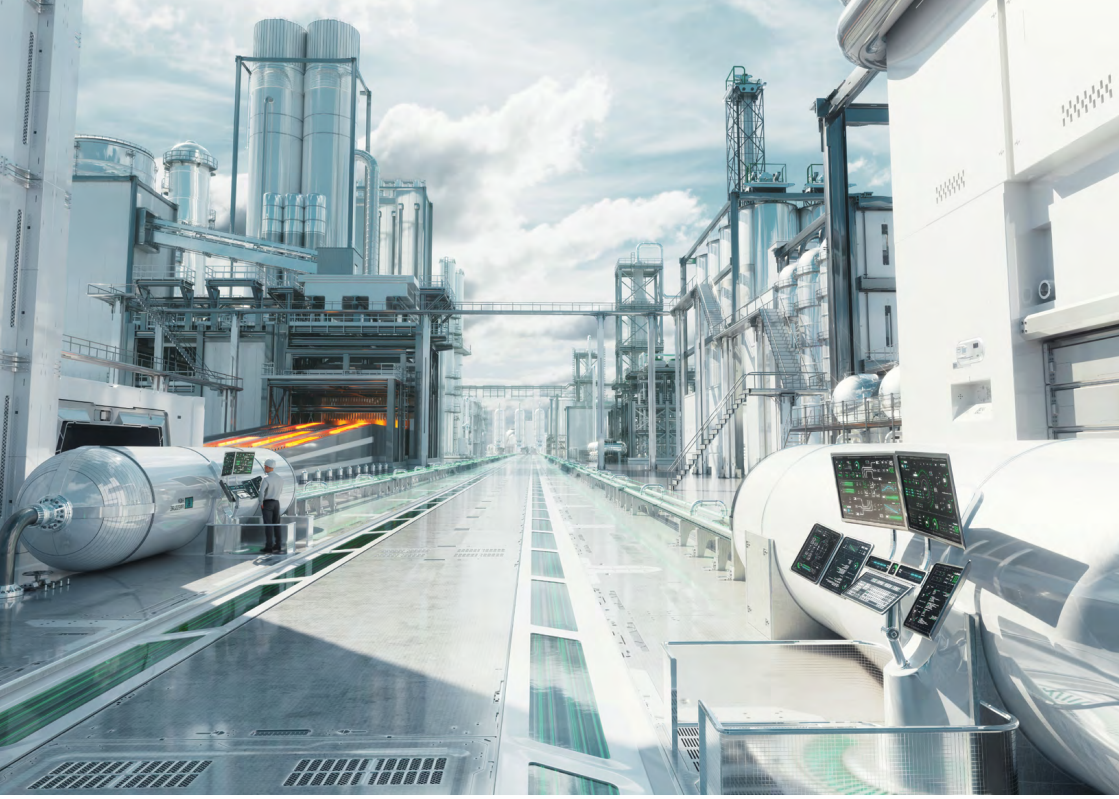


Kaspersky Industrial CyberSecurity: descripción general de la solución

kaspersky PREPARADOS PARA EL FUTURO

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity: descripción general de la solución

Introducción

Históricamente, las empresas industriales de todo el mundo han enfocado la ciberseguridad en sus redes de TI y TO (tecnología operativa) de manera diferente. La mayoría de las empresas ya cuentan con una detección de brechas y medidas de respuesta ante incidentes maduras en su infraestructura corporativa, pero cuando se trata de TO suelen confiar en un enfoque hermético clásico. Las empresas industriales se están volviendo cada vez más «digitales», invirtiendo cada vez más en tecnologías inteligentes, nuevos sistemas de automatización y la adopción de la Industria 4.0. Esto verdaderamente elimina la brecha entre los entornos de TI y TO que se utiliza para evitar que las ciberamenazas lleguen a los sistemas de control industriales. Según Kaspersky ICS CERT, en el primer semestre de 2019, el porcentaje de ordenadores ICS en los que se detectaron elementos maliciosos alcanzó el 41,2 %[1].

¿Cuáles son esas amenazas?

En primer lugar, incluyen el riesgo de infección accidental por malware convencional. No tiene que ser un objetivo para convertirse en una víctima Una simple unidad flash o un mensaje de correo electrónico de tipo phishing con un troyano bancario o ransomware introducido involuntariamente en el entorno ICS puede afectar seriamente a la actividad principal de una empresa. Incluso si las infecciones accidentales no se producen con demasiada frecuencia, es evidente que un hacker motivado también puede penetrar en las redes de TO y causar daños considerables a la producción o equipos de gran valor, o bien robar información valiosa.

¿Cuáles son las medidas adecuadas de ciberseguridad ICS?

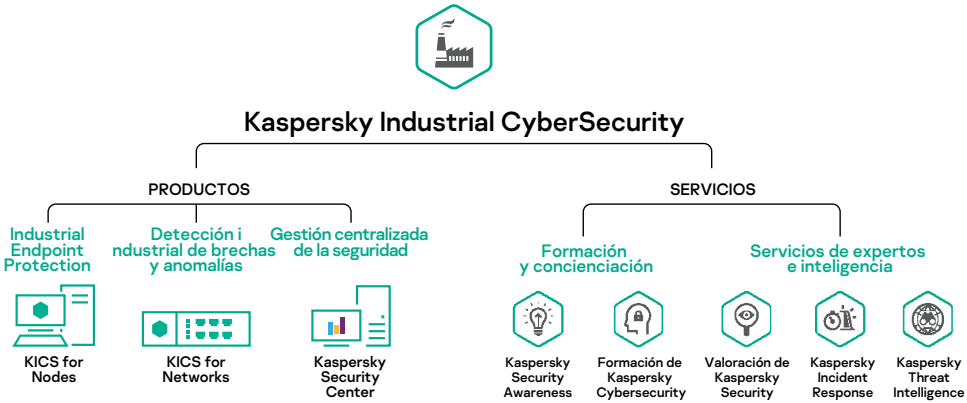
1. Protección de endopoints industriales para prevenir las infecciones accidentales y dificultar más las intrusiones motivadas.
2. Supervisión de la red de TO y detección de anomalías para identificar acciones maliciosas en el nivel de los controladores lógicos programables (PLC).
3. Programas de formación para los empleados con el fin de reducir los accidentes y minimizar el factor humano.
4. Servicios de expertos dedicados a investigar la infraestructura, llevar a cabo análisis de expertos o mitigar el impacto de un incidente.

1 Threat landscape for industrial automation systems, H1 2019, Kaspesky ICS CERT

¿Qué proporciona Kaspersky?

Kaspersky satisface todas las necesidades de ciberseguridad de las organizaciones industriales en su cartera de productos Kaspersky Industrial CyberSecurity(KICS). KICS ofrece un enfoque holístico de la ciberseguridad industrial, aportando valor en cualquier etapa del proceso de seguridad de la OT del cliente: desde la evaluación de la ciberseguridad y la formación en esta materia, hasta el uso de tecnologías avanzadas y la respuesta ante incidentes.

Componentes de Kaspersky Industrial CyberSecurity



En 2020, Kaspersky recibió la mención en el informe de Gartner «Panorama competitivo: seguridad de la tecnología operacional»[2] como proveedor representativo en 4 categorías de productos, incluidas:

- Seguridad de endpoints de TO
- Visibilidad y supervisión de la red de TO
- Detección de anomalías, respuesta ante incidentes y generación de informes
- Servicios de seguridad de TO[2].

ARC Advisory Group hace hincapié en que Kaspersky ofrece una combinación única de inteligencia de amenazas, aprendizaje automático, y la experiencia humana que aporta la protección ágil contra de cualquier tipo de amenaza[3].

Mientras tanto, un estudio de Forrester[4] indica un ROI del 368 % para una empresa que utiliza Kaspersky Industrial Cybersecurity, así como otros beneficios, como la asistencia técnica de expertos y la tranquilidad.

2 Gartner: Competitive Landscape: Operational Technology Security, marzo de 2020
https://ics.kaspersky.com/KICS-cited-in-Gartnercompetitive-landscape-OTsecurity

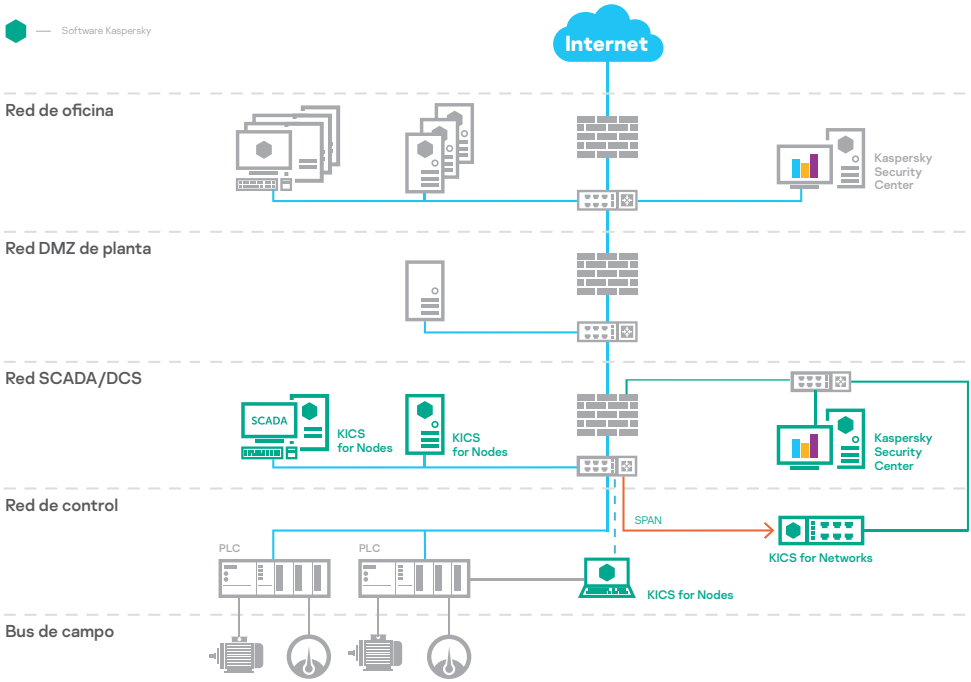
3 Arc Advisory: Kaspersky Moves Forward with Improved Cybersecurity Solutions, 2018

4 Forrester Research: The Total Economic Impact™ of Kaspersky Industrial CyberSecurity, April 2019.
https://www.kaspersky.com/ forrester-tei-for-kics

Productos

Los productos KICS están diseñados para asegurar de forma integral los elementos industriales de su organización: KICS for Nodes está dirigido a los endpoints industriales, mientras que KICS for Networks supervisa la seguridad de la red industrial.

Implementación de los productos de Kaspersky Industrial CyberSecurity



KICS for Networks

KICS for Networks es una solución de monitorización y visibilidad que se suministra como software o un dispositivo virtual, conectado pasivamente a la red ICS.

Ventajas:

- ✓ **Identificación de activos** identificación e inventario de activos de TO pasivos
- ✓ **Inspección de paquetes exhaustiva** análisis en tiempo casi real de telemetría de procesos técnicos
- ✓ **Control de la integridad de la red** detección de hosts y flujos de red no autorizados
- ✓ **Sistema de detección de intrusiones**envía alertas sobre actividades maliciosas en la red
- ✓ **Control de comandos** inspecciona los comandos en los protocolos industriales
- ✓ **Sistemas externos** capacidades de detección externas mediante integración API
- ✓ **El aprendizaje automático para la detección de anomalías (MLAD)** detecta anomalías cibernéticas o físicas a través de la telemetría y extracción de datos históricos en tiempo real (red neuronal recurrente)

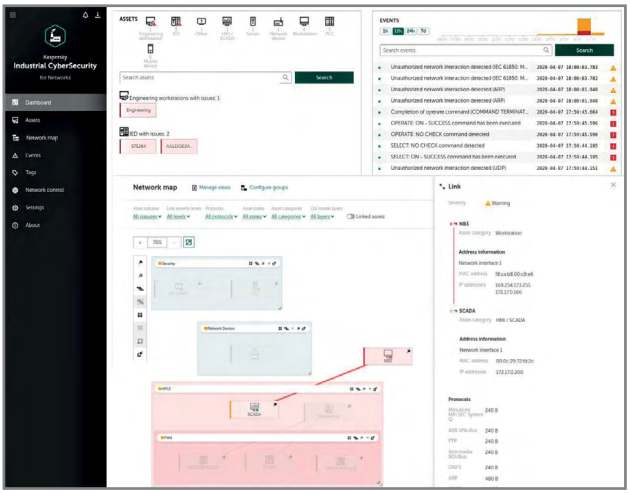
KICS for Networks detecta anomalías e intrusiones dentro de las redes ICS en sus primeras etapas y se asegura de que se emprendan las acciones necesarias se toman para evitar cualquier impacto negativo en los procesos industriales.

KICS for Networks es una solución que no depende de ningún dispositivo y que permite al cliente elegir el proveedor de dispositivos informáticos industriales de su confianza.

La interfaz de CCI for Networks muestra un panel en vivo y un mapa de la red, lo que permite trabajar con los activos y eventos de seguridad.

Ejemplo de dispositivo de KICS for Networks

Interfaz de KICS for Networks



KICS for Nodes

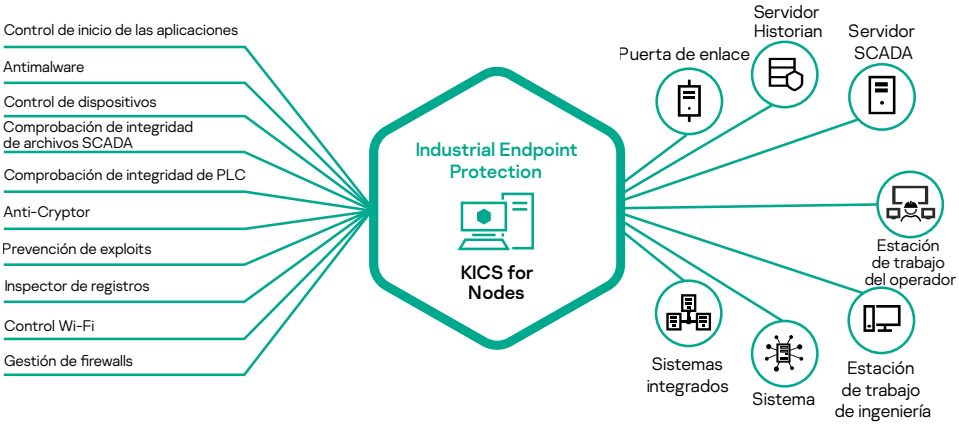
KICS for Nodes es un producto de seguridad de endpoint de TO, que se suministra como software para máquinas basadas en Linux y Windows.

Ventajas:

- ✓ **Bajo impacto en los equipos protegidos**
- ✓ **Mayor compatibilidad**
- ✓ **Protección contra malware avanzada**
- ✓ **Control del entorno**

KICS for Nodes fue especialmente diseñado para consumir una cantidad mínima de recursos. Construido sobre la seguridad y los sistemas integrados, sus arquitectura modular significa que solo tiene que instalar los componentes de protección que necesita. Los componentes de protección se pueden configurar en modo de prevención de amenazas o solamente de detección. Este enfoque es ideal para máquinas heredadas de bajo rendimiento que requieren la máxima potencia de cálculo disponible.

Funciones de KICS for Nodes y endpoints compatibles



«Hemos decidido asociarnos con Kaspersky Lab porque Kaspersky Industrial CyberSecurity podía implementarse mientras nuestras operaciones seguían ejecutándose, y porque la solución es compatible con los sistemas de control que utilizamos».

Jan Houben, director de planta, AGC Glass Germany GmbH

KICS for Nodes protege los nodos industriales de los distintos tipos de ciberamenazas que pueden provenir de factores humanos, malware genérico, ataques selectivos o sabotaje. KICS for Nodes es compatible tanto con los componentes de software y hardware de los sistemas de automatización industrial como con SCADA, PLC y DCS.

Kaspersky Security Center

Kaspersky Security Center es una solución de gestión de seguridad centralizada. Proporciona control y visibilidad de las capas industriales en múltiples sitios, así como las redes empresariales circundantes.

Ventajas:

✓ **Gestión de sistemas**
- Recopilación de datos de sistemas centralizados
- Implementación de software centralizado
- Detección de vulnerabilidades y gestión de parches
- Ampliación de las funciones de gestión de clientes

✓ **Gestión de políticas**
- Gestión de políticas de seguridad centralizada
- Programación y ejecución de tareas a distancia

✓ **Informes y análisis**
- Registro de eventos
- Paneles e informes
- Notificaciones por SMS/ correo electrónico

✓ **INTEGRACIÓN CON SIEM**
- Arcsight, Splunk, Qradar
- Servidor Syslog

✓ **INTEGRACIÓN HMI**

✓ **INTEGRACIÓN DE PANEL MES**
- información de estado y la entrega de información a HOSTS COMPATIBLES CON IEC 104/OPC 2.0

Kaspersky Industrial CyberSecurity: servicios

Nuestro paquete de servicios constituye una parte importante del catálogo de productos de KICS: ofrecemos el ciclo completo de servicios de seguridad, desde la evaluación de la ciberseguridad industrial hasta la respuesta ante incidentes.

«Su experiencia en el campo de la ciberseguridad ICS, su profesionalidad y la complejidad de su solución en comparación con otros proveedores, nos ha aportado un gran valor y nos ha garantizado un futuro brillante para la estrategia de seguridad de nuestra empresa».

Ondřej Sýkora, responsable de C&A, Plzeňský Prazdroj

Servicios expertos

- **Evaluación de la ciberseguridad industrial:** Kaspersky proporciona una evaluación de la ciberseguridad industrial mínimamente invasiva, que incluye pruebas de penetración externa e interna, evaluación de la seguridad de TO y evaluación de la seguridad de soluciones de automatización. Los expertos de Kaspersky proporcionan una perspectiva de gran valor sobre la infraestructura de una empresa y aportan recomendaciones sobre cómo reforzar la postura de ciberseguridad de ICS.

- **Inteligencia frente a amenazas:** los análisis actualizados, recopilados por expertos de Kaspersky, ayudan a mejorar la protección de los clientes frente a ciberataques a objetivos industriales. Se proporcionan como fuentes de información o informes personalizados de TI y satisfacen las necesidades específicas de los clientes en función de los parámetros de software regionales, del sector e ICS.

«Mediante la práctica y el aprendizaje de los conocimientos del equipo de Kaspersky, hemos aumentado nuestra protección frente a las amenazas a la ciberseguridad».

Yu Tat Ming, director general, PacificLight.

«Kaspersky Lab era la mejor empresa para ofrecer formación sobre habilidades en ciberseguridad industrial profesional para nuestro grupo ICS».

Søren Egede Knudsen, director técnico, Ezenta

- **Respuesta ante incidentes:** en caso de producirse un incidente de ciberseguridad, nuestros expertos recopilan y analizan los datos, reconstruyen la cronología del incidente, determinan las posibles fuentes y la motivación, y desarrollan un plan de corrección. Además, Kaspersky Lab ofrece un servicio de análisis de malware mediante el cual los expertos de Kaspersky Lab clasifican cualquier muestra de malware proporcionada, analizan sus funciones y comportamiento, y desarrollan recomendaciones y un plan para eliminarlo de los sistemas y revertir cualquier acción maliciosa.

Formación y concienciación

- **Formación y concienciación sobre ciberseguridad industrial:** módulos interactivos de formación presencial o en línea, y juegos de diberseguridad para empleados que interactúan con los sistemas informáticos industriales y sus gerentes. Los participantes adquieren una nueva visión del panorama de amenazas y los vectores de ataque actuales en relación con el entorno industrial, pueden analizar casos prácticos y adquieren habilidades de trabajo con ciberseguridad. El curso presencial se puede personalizar y adaptar para llevarse a cabo en uno o dos días.

- **Programas de formación de expertos:** los profesionales de la ciberseguridad dispone de los módulos de formación Pruebas de penetración en ICS y Análisis forense digital de ICS. Los participantes adquieren todos los conocimientos avanzados necesarios para llevar a cabo análisis de penetración integrales o análisis forenses digitales en entornos industriales. Incluyen certificación.

Más información sobre KICS en
https://ics.kaspersky.com

#Kaspersky
#BringontheFuture

www.kaspersky.es

IIC MEMBER industrial internet CONSORTIUM

OPC FOUNDATION MEMBER

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2018

* Premio al logro científico y tecnológico de Internet líder en el mundo en la III Conferencia Mundial de Internet

** Premio especial de la Feria Industrial Internacional de China (CIIF) en 2016