Kaspersky Industrial

La seguridad cibernética

Una plataforma XDR para la seguridad empresarial industrial integral

Solid Servicios

kaspersky BRING ON THE FUTURE

Atacado por malware

Desde principios de 2023, alrededor del

35% de los ordenadores relacionados con ICS han sido atacados por malware, casi un 5% menos que el año anterior.

CERTIFICADO ICS de Kaspersky, octubre 2023

Aprende más

Amenazas cibernéticas que enfrentan los ICS y las empresas industriales

La nueva realidad para los propietarios y operadores de infraestructuras industriales está determinada por el creciente interés de los hacktivistas en los sistemas de automatización, los altos requisitos regulatorios, la convergencia IT-OT y el aumento de la variedad de ciberataques en el sector industrial (un aumento de casi el 50% en el primer semestre de 2023). en comparación con el segundo semestre de 2022, según las estadísticas de Kaspersky ICS CERT).

La penetración de las tecnologías digitales, que suele considerarse algo bueno, borra la brecha entre los entornos de TI y OT que solían proteger a estos últimos de los ciberdelincuentes. Mientras que una sola unidad flash introducida en el entorno ICS puede afectar gravemente el negocio principal de una empresa, un grupo de hackers motivado puede penetrar las redes OT y causar daños considerables y/o robar información valiosa.

Combinado con los estándares de automatización que evolucionan desde recomendaciones comunes hasta requisitos legislativos y la creciente necesidad de compartir mejores prácticas y gestionar riesgos, esto hace que la ciberseguridad de las empresas industriales sea un desafío formidable.

Kaspersky ICS CERT espera que las organizaciones de las industrias enfrenten ciberataques con una frecuencia cada vez mayor:

Los objetivos principales de los ataques APT incluirán:

Infraestructura crítica

propietarios y operadores Los gobiernos u organizaciones públicas estratégicamente importantes enfrentan consecuencias potenciales considerablemente mayores debido a la interferencia operativa.

De alto perfil

Actores industriales Desde una sola planta hasta escala nacional o internacional, estas empresas participan en operaciones de alto riesgo, que implican importantes costos de incidentes.

Petróleo, gas y productos químicos

El alto valor de los datos y sistemas que controlan estas empresas las convierte en un objetivo atractivo para el ransomware y los actores maliciosos que buscan interrumpir las operaciones o manipular los precios.

Fabricación industrial de alto perfil

Estas empresas desempeñan funciones sociales fundamentales y poseen datos valiosos que pueden explotarse para obtener beneficios financieros, lo que provoca enormes daños económicos y de reputación.

Minerales, metales y minería

La industria de los minerales, los metales y la minería es el objetivo por sus valiosos recursos, su impacto financiero y sus cadenas de suministro

interconectadas.

Energía, red y servicios públicos

El papel clave que desempeñan la energía, la red y los servicios públicos en nuestra vida diaria es la principal razón de los ataques destinados a crear caos o ejercer influencia.

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

Solid Servicios

Más información sobre lo común

TTP de ataques contra organizaciones industriales

Aprende más

Elegir un socio en el que pueda confiar, con un profundo conocimiento de las superposiciones entre la ciberseguridad industrial y corporativa y la capacidad de proporcionar una gama completa de tecnologías de seguridad de vanguardia nunca ha sido más importante.

La plataforma KICS XDR permite a los usuarios para ver el panorama más amplio y el contexto más amplio: la cadena de incidentes a nivel de red y punto final, parámetros precisos de activos, comunicación de red y mapas de topología incluso de segmentos donde la duplicación de tráfico aún no está disponible, y más.

Sensor de punto final

Proteccion
Estado

Seguridad
Auditoría

Red
Comunicaciones

Telemetría del host
Transmisión

Equipo
Supervisión

Incidente
Respuesta

Tecnologías de seguridad avanzadas de ICS

Kaspersky Industrial CyberSecurity (KICS) es un nativo extendido

Plataforma de detección y respuesta (XDR) para empresas industriales, especialmente diseñada y certificada para proteger equipos, activos y redes de OT críticos de amenazas iniciadas cibernéticamente. La plataforma comprende tecnologías integradas que protegen los componentes centrales del sistema de control y automatización industrial en todos los niveles. KICS for Nodes es un software de respuesta, detección y protección de terminales con funcionalidad de auditoría de cumplimiento y sensor de terminales. KICS for Networks está diseñado para el análisis, la detección y la respuesta del tráfico de redes OT. La función de gestión centralizada a nivel de sitio, esencial para escalar las operaciones de seguridad OT a un gran volumen de infraestructuras industriales grandes, diversas y distribuidas geográficamente, está integrada en la plataforma.

La integración perfecta entre los componentes de la plataforma proporciona visibilidad completa de múltiples redes OT y sistemas de automatización distribuidos geográficamente, lo que brinda una experiencia de cliente mejorada, conocimiento de la situación y flexibilidad de implementación. Con detección y respuesta extendidas, la plataforma KICS permite la convergencia IT-OT y ofrece numerosos beneficios para un solo proveedor.

Medidas de respuesta

Aislamiento del host

Prevención de ejecución

Cuarentena

Solid Servicios

Puntos de aplicación de la plataforma

Convergencia
of OT and IT
environments

entorno de TI

DMZ/GTW

OT medio ambiente

Kaspersky
Industrial CyberSecurity
for Nodes

Operador
Puesto de trabajo

SCADA
Servidor

Ingeniero
Puesto de trabajo

ICS
Puerta

Equipo de
red

DURAR

Kaspersky
Industrial CyberSecurity
for Networks

Control de Bahía
Unidad (BCU)

Electrónica
inteligente
Dispositivo (DEI)

Lógica programable
Controladores(PLC)

Sistema instrumentadode
seguridad y protecciónde
relés (SIS)

Nodos aislados
(comprobación manual
con Escáner portátil KICS)

anomalía temprana
detection and
predictive analytics

Kaspersky Machine Learning para la detección de anomalías (Kaspersky MLAD) es un sistema innovador que utiliza una red neuronal para monitorear simultáneamenteuna amplia gama de datos de telemetría.

Detecta fallas en los equipos y errores humanos, lo que ayuda a prevenir fallas y accidentes, identifica acciones atípicas de los empleados u operaciones del equipo como signos de un ataque o sabotaje especializado y combina la detección de anomalías con el análisis predictivo del estado y el ciclo de vida del equipo.

Nivel físico

Aprende más

Protegido por productos Kaspersky

Solid Servicios

Kaspersky Industrial CyberSecurity for Networks

KICS for Networks

Una solución patentada a nivel de protocolo para monitoreo de redes industriales y análisis de tráfico, enviada como software o como dispositivo virtual.

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

La solución ayuda a detectar y clasificar riesgos en función de datos de vulnerabilidades y conexiones de red, así como el papel de varios activos, para prevenir incidentes.

Beneficios

Inventario de activos

Inventario automático de activos y recopilación de datos utilizando métodos pasivos y activos de recopilación de datos.

Inventario y visualización de redes

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

Vulnerabilidad y Evaluación de riesgos

- Gestión de riesgos y vulnerabilidades específicas de OT
- Puntuación y priorización automática
- Recomendaciones de remediación de riesgos

Anomalía de la red Detección

Control de integridad de la red con monitoreo de desviación de referencia y detección de actividad de red maliciosa y sospechosa.

Control de procesos OT y paquetes profundos Inspección (DPI)

- Extracción de datos de carga útil industrial.
- Control de procesos en tiempo real
- Control de mando industrial
- Monitoreo avanzado de procesos OT por Kaspersky MLAD

Integración y

El intercambio de datos

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

Auditoría de cumplimiento centralizada de nodos de redes industriales

KICS for Networks ofrece auditoría centralizada de nodos de redes industriales, incluida la auditoría basada en agentes (a través de KICS for Nodes) y sin agentes de hardware de red y puntos finales para detectar vulnerabilidades y el cumplimiento de los estándares industriales OVAL* y XCCDF**.

- Auditoría de seguridad centralizada y automatizada para Windows, nodos Linux, dispositivos de red.
- Auditoría de cumplimiento. Editor completamente funcional para controles y parámetros de cumplimiento.
- Todos los informes y datos de activos están disponibles en un solo lugar: base de activos de KICS for Networks
- Bóveda protegida para credenciales de nodos
- Soporte de tercero o personalizado bases de datos OVAL
- Base de datos de vulnerabilidades SCADA incorporada por ICS CERT

Solid Servicios

* Lenguaje abierto de evaluación y vulnerabilidad (OVAL)
** El formato de descripción de lista de verificación de configuración extensible (XCCDF)

Kaspersky Industrial CyberSecurity for Nodes

KICS for Nodes

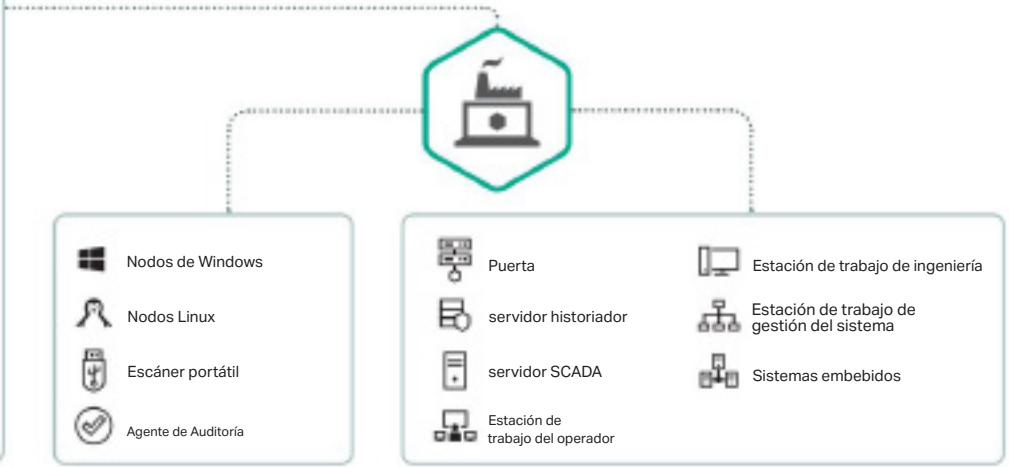
Protección, detección y respuesta de endpoints de grado industrial, probadas y certificadas. Una solución estable, compatible y de bajo impacto para Linux, Windows y sistemas independientes.

KICS for Nodes protege cada punto final en 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 estaciones de trabajo, servidores, puertas de enlace y otros puntos finales, asegurando a los administradores de sistemas de automatización que un incidente se ha solucionado por completo y

KICS for Nodes Portable Scanner aplica una política de ciberseguridad en maquinaria, sistemas de automatización o equipos independientes en los que no se puede instalar software de seguridad. Con una huella operativa muy baja, no interfiere con las soluciones de seguridad existentes.

- Solución sin instalación que proporciona máxima conciencia situacional y visibilidad OT incluso para una infraestructura independiente.
- Le permite realizar análisis bajo demanda en varias máquinas de mantenimiento simultáneamente y proporciona informes convenientes.
- Realiza comprobaciones de cumplimiento antimalware de los equipos que acceden a un sitio OT, incluidas las computadoras de contratistas externos.

- Control del dispositivo
- Control de integridad de archivos
- Control de integridad del PLC
- Anticriptador
- Prevención de exploits
- Prevención de amenazas de red
- Inspector de registro de Windows
- Control Wi-Fi
- Gestión de cortafuegos
- Monitor de registro
- Auditoría de seguridad
- Agente EDR
- Sensor de punto final (integración con KICS para redes)



Beneficios

Bajo impacto

- Bajo impacto en dispositivos protegidos para un mejor rendimiento del sistema
- No es necesario reiniciar para la instalación, actualización o mejora
- Modo de solo detección disponible
- Recurso del sistema ajustable consumo

Compatibilidad

- Compatibilidad con sistemas operativos heredados a partir de Windows XP SP2 y Windows Servidor 2003 SP1
- Compatibilidad con proveedores de automatización industrial
- Escáner portátil como opción sin instalación

Protección extendida

- Protección contra malware, ransomware y exploits
- Análisis de registros
- Control de cortafuegos
- Tecnología ICS EDR incorporada
- Actualizaciones de bases de datos aisladas

Implementación modular

- Opciones flexibles y configuraciones seguras no intrusivas diseñadas para OT
- La arquitectura modular permite seleccionar solo los componentes de protección necesarios

soporte de 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
- Fastwell CPM723-01

Auditoría

- Auditoría integral de seguridad y cumplimiento basada en estándares abiertos de OVAL

Solid Servicios

Kaspersky XDR

factores de efectividad

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

La integración con ICS permite una visibilidad y un análisis integrales del tráfico de la red industrial y del comportamiento del sistema.

Inteligencia de amenazas específica de la experiencia de Kaspersky en el área del entorno industrial

protección contra amenazas

Personalización y configuración para adaptar la solución a las necesidades específicas de tolerancia al riesgo, arquitectura de red y cumplimiento normativo.

Un único proveedor para aprovechar al máximo el soporte y la colaboración de los proveedores, incluido el suministro de actualizaciones y parches oportunos.

Unified cybersecurity al otro lado de los segmentos industriales y corporativos de su empresa

Los ataques a sistemas industriales, en particular ICS y SCADA, van en aumento. Elegir un socio en el que pueda confiar, con un profundo conocimiento de las superposiciones entre la ciberseguridad industrial y corporativa y la capacidad de proporcionar una gama completa de tecnologías de ciberseguridad industrial y corporativa de vanguardia nunca ha sido más importante.

Kaspersky XDR es la herramienta perfecta para crear un entorno de trabajo seguro y libre de amenazas. Su compatibilidad con una variedad de productos de seguridad facilita el establecimiento de un ciberespacio seguro, brindando opciones específicas de la industria para su empresa y protegiéndola de cualquier amenaza, sin importar cuán grande o pequeña sea. Las opciones de integración de Kaspersky XDR le permiten brindar una visión unificada y global de las amenazas, equipando a su equipo de seguridad con todas las herramientas y datos que necesitan para proteger su negocio de amenazas actuales y potenciales.

Aprende más

IT–OT convergence con Kaspersky Híbrido XDR

Ciberseguridad TI

Aprende más

Kaspersky Extendido Detección y Respuesta

OT Ciberseguridad

Aprende más

Límite ambiental

Solid Servicios

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

ICS CERT

ICS CERT — propio internacional

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

Efectividad tecnológica comprobada, cumplimiento de estándares y requisitos.

Clientes en todo el mundo

ROSATOM · NORNICKEL · EuroChem · NLMK · TATNEFT · ROSSETI · Wintershine · alperia · PacificLight · КазМунайГаз · AGC

Kaspersky Industrial

La seguridad cibernética

Kaspersky Industrial

Ciberseguridad para nodos

Aprende más

Kaspersky Industrial

CiberSeguridad para Redes

www.solidservicios.com
contacto@solidservicios.com
tel. 800 872 9898 | 800 777 2908

Solid Servicios

#kaspersky
#bringonthefuture