Una plataforma de XDR
para la seguridad integral
de empresas industriales

Kaspersky Industrial CyberSecurity

kaspersky PREPARADOS PARA EL FUTURO

Ataques de malware

Desde principios de 2023, alrededor del 35 % de los ordenadores relacionados con el ICS han sido atacados por malware, casi un 5 % menos que el año anterior.

ICS CERT de Kaspersky, octubre de 2023

Más información

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

La nueva realidad de los propietarios y operadores de infraestructuras industriales está determinada por el interés creciente de los ciberactivistas en los sistemas de automatización, los altos requisitos regulatorios, la convergencia de TI/TO 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, de acuerdo a las estadísticas de Kaspersky ICS CERT).

La adopción de tecnologías digitales, que suele verse desde un punto de vista favorable, elimina la distancia entre los entornos de TI y TO, que solían proteger a este último de los ciberdelincuentes. Mientras que solo basta con que una sola unidad flash entre en contacto con el entorno de ICS para afectar gravemente al negocio principal de una empresa, un grupo de hackers motivados puede penetrar en las redes de TO y generar daños considerables o incluso robar información valiosa. Si a esto se suma la evolución de los estándares de automatización, de recomendaciones habituales 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 desafío formidable.

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

Petróleo, combustible y productos químicos

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

Empresas de manufactura industrial de alto perfil

Estas empresas tienen funciones sociales críticas y poseen datos valiosos que pueden aprovecharse para obtener beneficios financieros, resultando en enormes daños económicos y de reputación.

Minerales, metales y minería

La industria de los minerales, los metales y la minería se elige como objetivo por sus recursos valiosos, impacto financiero y cadenas de suministro interconectadas.

Energía, redes y servicios públicos

La función crucial que la industria de la energía, las redes y los servicio públicos desempeñan en nuestra vida diaria es la razón principal por la que son objetivos de ataques, que buscan generar caos o ejercer influencia.

La estabilidad de la producción y los procesos comerciales, así como la protección de los activos valiosos, están directamente relacionados al desarrollo sustentable de las empresas industriales y los centros de infraestructura crítica. Los ataques a los sistemas industriales, en particular ICS y SCADA, van en aumento. Mientras tanto, las ciberamenazas actuales enfocadas en entornos industriales parecen ser inmunes a las soluciones convencionales.

Elegir un partner de confianza, que tenga un gran conocimiento de las coincidencias entre la ciberseguridad corporativa e industrial, junto con la capacidad de brindar una gama completa de tecnologías de seguridad de última generación, nunca fue tan importante.

Entre los principales objetivos de ataques APT se encuentran los siguientes:

Propietarios y operadores de infraestructuras críticas

Las organizaciones públicas o gubernamentales estratégicamente importantes se enfrentan a peores consecuencias potenciales de interferencias operativas

Empresas industriales de alto perfil

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

Obtenga más información acerca de los ataques de TTP más habituales desplegados hacia organizaciones industriales

Más información

La plataforma de XDR KICS les permite a los usuarios tener una visión y un contexto más amplios: la cadena de incidentes en el nivel de la red y los 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 de red
- Transmisión de telemetría del host
- Supervisión de equipo
- Respuesta ante incidentes

Tecnologías de seguridad de ICS avanzadas

Kaspersky Industrial CyberSecurity (KICS) es una plataforma de detección y respuesta extendidas (XDR) para organizaciones industriales, diseñada y certificada especialmente para proteger a equipos, activos y redes de TO críticos de ciberamenazas. La plataforma incluye tecnologías integradas que protegen los componentes de automatización industrial y sistemas de control en cada nivel. KICS for Nodes es un software de protección, detección y respuesta de endpoints con funciones de auditoría de cumplimiento y sensores de endpoints. KICS for Networks está diseñado para el análisis, la detección y la respuesta del tráfico en la red de TO. La función de administración centralizada al nivel del sitio, esencial para la escalabilidad de las operaciones de seguridad de TO a un alto volumen de infraestructuras industriales de gran tamaño, diversas y distribuidas geográficamente, está integrada en la plataforma.

La integración constante entre los componentes de la plataforma brinda una visibilidad total de múltiples redes de TO y sistemas de automatización distribuidos geográficamente y ofrece una mejor experiencia del cliente, conocimiento de la situación y flexibilidad de despliegue. Con detección y respuesta extendidas, la plataforma de KICS permite la convergencia TI/TO y proporciona numerosos beneficios para proveedores únicos.

Kaspersky Industrial CyberSecurity for Nodes

Protección de endpoints mejorada por EDR

- Servidor
- Estación de trabajo
- Escáneres portátiles

Kaspersky Industrial CyberSecurity

Consola unificada
Integración nativa
Escenarios de productos cruzados
Common Kill Chain
Gestión de riesgos y activos

Kaspersky Industrial CyberSecurity for Networks

Protección de dispositivos industriales de amenazas a la red

- Servidor
- Sensor

Medidas de respuesta

- Aislamiento del host
- Prevención de ejecución
- Cuarentena

Puntos de aplicación de la plataforma

Convergencia de entornos de TO y TI

DMZ/GTW

entorno de IT

Entorno de TO

Kaspersky Industrial CyberSecurity for Nodes

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

Equipos de red

SPAN

Kaspersky Industrial CyberSecurity for Networks

- Unidad de control de posición (BCU)
- Dispositivos electrónicos inteligentes (IED)
- Controladores lógicos programables (PLC)
- Protección de relés y sistema instrumentado de seguridad (SIS)
- Nodos aislados (comprobación manual con una herramienta de análisis portátil de KICS)

Nivel físico

Detección temprana de anomalías y análisis predictivo

Kaspersky Machine Learning for Anomaly Detection (Kaspersky MLAD) es un sistema innovador que utiliza una red neuronal para supervisar una gran variedad de datos de telemetría de forma simultánea. Detecta errores en el equipo y errores humanos, ayudando a evitar los fallos y los 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 análisis predictivo de la condición de los equipos y el ciclo de vida.

Más información

Protegido por productos de Kaspersky

Kaspersky Industrial CyberSecurity for Networks

KICS for Networks

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

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

La solución ayuda a detectar y clasificar los riesgos basándose en datos de vulnerabilidades y conexiones de red, así como en la función de los distintos activos, para prevenir incidentes.

Ventajas

Inventario de activos

Inventario de activos y recogida de datos automáticos mediante métodos pasivos y activos de recogida de datos

Inventario y visualización de red

- Mapa de comunicaciones de red
- Diagrama topológico de la red

Evaluación de la vulnerabilidad y los riesgos

- Gestión de vulnerabilidades y riesgos específicos de TO
- Calificación y priorización automáticas
- Recomendaciones para remediar los riesgos

Detección de anomalías de red

Control de la integridad de la red con supervisión de la desviación de la línea de base y detección de actividades maliciosas y sospechosas en la red

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

- Extracción de datos de cargas útiles industriales
- Control de procesos en tiempo real
- Control de mando industrial
- Supervisión avanzada de procesos de TO por Kaspersky MLAD

Integración e intercambio de datos

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

Cumplimiento centralizado auditoría 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 redes y endpoints para detectar vulnerabilidades y el cumplimiento de los estándares industriales OVAL* y XCCDF**.

- Auditoría de seguridad centralizada y automatizada para Windows, nodos Linux y dispositivos de red
- Auditoría de cumplimiento. Editor completo de controles de conformidad y parámetros
- Todos los informes y datos sobre activos están disponibles en un único lugar: la base de activos de KICS for Networks
- Bóveda protegida para credenciales de nodos
- Soporta cualquier base de datos OVAL de terceros o personalizada
- Base de datos de vulnerabilidades SCADA incorporada por ICS CERT

* Open Vulnerability and Assessment Language (OVAL)
** The Extensible Configuration Checklist Description Format (XCCDF)

Kaspersky Industrial CyberSecurity for Nodes

KICS for Nodes

Protección, detección y respuesta para endpoints de calidad industrial, testeada y certificada. Una solución de bajo impacto, compatible y estable para Linux, Windows y sistemas autónomos.

KICS for Nodes protege cada endpoint de un sistema de automatización moderno, digital, gestionado y distribuido. La solución recoge la 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, asegurando a los administradores del sistema de automatización que un incidente se ha resuelto completamente y no volverá a suceder.

El escáner portátil KICS for Nodes ejecuta una política de ciberseguridad a las máquinas autónomas, los sistemas de automatización o los equipos en los que no se puede instalar un software de seguridad. Gracias a su una huella operativa muy baja, no interfiere con las soluciones de seguridad existentes.

- Solución sin instalación que proporciona el máximo conocimiento de la situación y visibilidad de TO incluso para una infraestructura autónoma.
- Permite realizar análisis a demanda en varios equipos simultáneamente durante las ventanas de mantenimiento, y proporciona informes prácticos.
- Realiza comprobaciones de conformidad antimalware de los equipos que acceden a un emplazamiento de TO, incluidos los ordenadores de terceros contratistas.

- Control de dispositivos
- Control de integridad de archivos
- Control de integridad de PLC
- Anti-Cryptor
- Prevención de exploits
- Prevención contra amenazas de red
- Inspector de registros de Windows
- Control Wi-Fi
- Gestión de firewalls
- Monitor de registro
- Auditoría de seguridad
- Agente EDR
- Sensor de endpoints (integración con KICS for Networks)

- Nodos Windows
- Nodos Linux
- Escáner portátil
- Oficial de auditorías

- Puerta de entrada
- Servidor Historian
- Servidor SCADA
- Estación de trabajo del operador
- Estación de trabajo de ingeniería
- Estación de trabajo de gestión del sistema
- Sistemas integrados

Ventajas

Bajo impacto

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

Compatibilidad

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

Protección ampliada

- Protección contra malware, ransomware y exploits
- Análisis de registros
- Control de firewall
- Tecnología ICS EDR integrada
- Actualizaciones de la base de datos aislada

Despliegue modular

- Opciones flexibles y ajustes seguros y no intrusivos diseñados para TO
- La arquitectura modular permite seleccionar solo los componentes de protección necesarios

Soporte 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

Auditoría

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

Factores de eficacia de Kaspersky XDR

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

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

Inteligencia sobre amenazas específicas de TO para aprovechar la experiencia de Kaspersky en el ámbito de la protección contra amenazas en entornos industriales

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

Un **único proveedor** para aprovechar al máximo el apoyo y la colaboración de los proveedores, incluido el suministro puntual de actualizaciones y parches

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

Los ataques a los sistemas industriales, en particular ICS y SCADA, van en aumento. Elegir un socio en el que puedas confiar, con un profundo conocimiento de los solapamientos entre la ciberseguridad industrial y corporativa y la capacidad de proporcionar una gama completa de tecnologías punteras de ciberseguridad industrial y corporativa, nunca ha sido tan importante.

Kaspersky XDR es la herramienta perfecta para crear un entorno de trabajo seguro y libre de amenazas. Su compatibilidad con una gran variedad de productos de seguridad facilita el establecimiento de un ciberespacio seguro, proporcionando opciones específicas para el sector de tu empresa y protegiéndola de cualquier amenaza, por grande o pequeña que sea. Las opciones de integración de Kaspersky XDR permiten proporcionar una visión unificada y global de las amenazas, equipando a tu equipo de seguridad con todas las herramientas y datos que necesitan para proteger a tu empresa de las amenazas actuales y potenciales.

Más información

Convergencia de TI/TO
con Kaspersky Hybrid XDR

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

ICS CERT

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 100 certificados de interoperabilidad con soluciones de proveedores de automatización

Eficacia demostrada de la tecnología, cumplimiento de normas 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

www.kaspersky.es

#kaspersky
#bringonthefuture