KASPERSKY lab

Kaspersky Industrial CyberSecurity: Descripción general de la solución

www.kaspersky.com/ics
#truecybersecurity

Kaspersky Industrial CyberSecurity: descripción general de la solución

Los ataques a sistemas industriales van en aumento

Los ciberataques a sistemas de control industriales no solo van en aumento, sino que han pasado de ser especulativos a ser indiscutibles[1]. El 67 % de los administradores de seguridad de IT/OT perciben el nivel actual de ciberamenazas sobre los sistemas de control industrial (ICS) como crítico o alto, lo que representa un aumento de más del 43 % con respecto a las conclusiones del último año[2]. La interrupción de la cadena de suministro y del negocio se sitúa como la principal preocupación mundial en los últimos cinco años; los ciberriesgos son la principal inquietud emergente[3]. En lo que respecta a las empresas con sistemas de infraestructuras industriales o vitales, los riesgos nunca han sido tan abundantes. La seguridad industrial tiene consecuencias que van mucho más allá de la protección de las empresas y la reputación. Cuando se trata de proteger los sistemas industriales contra ciberamenazas, surgen consideraciones sociales, ecológicas y macroeconómicas específicas y significativas.

[1] PwC: Global State of Information Security (Estado global de la seguridad de la información), 2015.

[2] SANS 2016, State of ICS Security Survey (Encuesta sobre el estado de la seguridad de ICS)

[3] Allianz Risk Barometer (Barómetro de riesgos de Allianz), 2017

Tecnología operativa frente a tecnología de la información

Según lo definido en el estándar de automatización IEC 62443, un sistema de control industrial (ICS) es una recopilación de personal, hardware y software que puede afectar o influir en el funcionamiento seguro, y fiable de un proceso industrial (tecnológico).

Los sistemas de control industrial incluyen, entre otros:

- Sistemas de control distribuido (DCS), controladores lógicos programables (PLC), unidades terminales remotas (RTU), dispositivos electrónicos inteligentes (IED), control de supervisión y adquisición de datos (SCADA) y sistemas de diagnóstico.
- Interfaces internas, humanas, de red o de máquina asociadas utilizadas para proporcionar una funcionalidad operativa de control, seguridad y fabricación para procesos continuos; por lotes, discretos independientes y de otros tipos.

En un plano superior, todas las infraestructuras de sistemas industriales pueden descomponerse en dos dominios:

- Tecnología de la información (IT): sistemas necesarios para gestionar datos en el contexto de los objetivos empresariales
- Tecnología operativa (OT): sistemas necesarios para gestionar procesos físicos e industriales de automatización industrial.

Las estrategias de seguridad de IT suelen centrarse en la protección de datos y seguir los objetivos del modelo de "C-I-D": confidencialidad, integridad y disponibilidad (CID) de los datos. Sin embargo, para la mayoría de sistemas de OT, la ciberseguridad no se basa en los "datos", sino en la continuidad de los procesos tecnológicos. De este modo, y según el modelo de C-I-D, la "disponibilidad" es el objetivo principal de las estrategias de seguridad aplicadas a OT. Esto es lo que distingue las necesidades de la ciberseguridad industrial de los demás sistemas, lo que significa que incluso la solución de ciberseguridad clásica de IT más efectiva resulta inapropiada para su uso en sistemas de OT, poniendo así en riesgo la disponibilidad de los procesos (y en algunos casos la integridad).

Riesgos y amenazas

A pesar de la creciente concienciación frente a los ciberataques sobre sistemas de control industrial, muchos modelos de seguridad siguen rigiéndose por la anticuada creencia de que aislar físicamente los sistemas (a través de aislamiento físico air-gap) y la "seguridad por anonimato" es suficiente. Pero no es así. En la era de la Industria 4.0, la mayoría de las redes industriales no esenciales, están disponibles a través de Internet[4], sea o no por propia elección. Una extensa investigación de Kaspersky Lab ICS CERT, que utiliza datos de Kaspersky Security Network, indica que los PC industriales reciben ataques con regularidad del mismo malware genérico que afectan a los sistemas empresariales (IT), incluidos (entre otros elementos) conocidos troyanos, virus y gusanos. Durante la segunda mitad de 2016, los productos de Kaspersky Lab de todo el mundo bloquearon intentos de ataques en el 39,2 % de los ordenadores protegidos por Kaspersky Lab clasificados como componentes de infraestructura industrial[5].

El gusano "Kido" (también conocido como Conficker), aunque no es específicamente industrial, obligó a cortar el suministro de una central eléctrica nuclear alemana durante varios días en abril de 2016. El problema no se produjo por penetración directa del sistema de control de la central, sino mediante la infección de la red de la oficina adyacente.

Otra creciente amenaza para los ICS es el ransomware. La gama y diversidad del ransomware ha crecido masivamente entre 2015 y principios de 2017. La aparición del ransomware es muy significativa para el sector industrial; estas infecciones pueden causar daños de gran impacto y alcance en los sistemas críticos, lo que hace que los ICS sean un objetivo potencial particularmente atractivo, tal y como demuestran varios incidentes de ataques del ransomware contra los sistemas SCADA durante 2016. El ransomware diseñado para atacar sistemas industriales puede tener su propio plan: en lugar de cifrar datos, el malware puede empezar a interrumpir las operaciones o a bloquear el acceso a un activo clave.

Al igual que las amenazas genéricas, la seguridad industrial debe luchar contra el malware específico de ICS y ataques dirigidos: Stuxnet, Havex, BlackEnergy, PLC Blaster, Ladder Logic Bomb, Pin Control Attack: la lista crece rápidamente. Como los ataques Stuxnet y BlackEnergy han demostrado, una unidad USB infectada o un único correo electrónico de spear-phishing es todo lo que se necesita para que atacantes bien preparados crucen el aislamiento físico air-gap y penetren en una red aislada.

Muchos ataques dirigidos a complejos industriales utilizan la red corporativa y los ICS para lanzarse y propagarse. Por ejemplo, durante el ataque contra BlackEnergy en la red eléctrica de Ucrania en diciembre de 2015, que provocó un grave corte de suministro, los hackers utilizaron varios vectores de ataque. Primero robaron las credenciales de acceso al sistema SCADA del entorno corporativo mediante un ataque de spear-phishing. Después, los hackers comenzaron a apagar la red eléctrica manualmente y, a continuación, sembraron un programa KillDisk malicioso en la red industrial que borró o sobrescribió datos de los archivos esenciales del sistema, provocando el bloqueo de la máquina del operador. En paralelo, el centro de llamadas de la empresa fue objeto de un ataque DDoS para impedir que los clientes informaran del apagón.

Además del malware y los ataques dirigidos, las organizaciones industriales hacen frente a otras amenazas y riesgos para las personas, los procesos y la tecnología. Y subestimar estos riesgos puede tener graves consecuencias. Kaspersky Lab desarrolla soluciones y servicios para

[4] ICS and their online availability (ICS y su disponibilidad online), 2016, Kaspersky Lab

[5] Threat Landscape for Industrial Automation Systems for H2 (Panorama de amenazas de los sistemas de automatización industrial para el segundo semestre de 2016), Kaspersky Lab ICS CERT

ayudar a nuestros clientes a abordar y gestionar no solamente malware y ataques dirigidos, sino también otros muchos ciberincidentes y factores de riesgo, entre los que se incluyen:

- Errores de operadores o contratistas (terceros) de SCADA
- Acciones fraudulentas
- Cibersabotaje
- Problemas de cumplimiento
- Falta de concienciación y datos relevantes para la investigación forense

Necesidad de una ciberseguridad industrial especializada

Solo los proveedores de ciberseguridad que comprendan las diferencias entre las empresas industriales y las empresas estándar orientadas a los datos pueden ofrecer soluciones para satisfacer las singulares necesidades de seguridad de los sistemas de control industrial y su infraestructura. Forrester Research aconseja a las organizaciones industriales que están seleccionando proveedores de seguridad que "busquen experiencia especializada en el sector". Forrester identifica a Kaspersky Lab como uno de los pocos proveedores con experiencia especializada en este sector.

Kaspersky Lab: proveedor de ciberseguridad industrial de confianza

Como líder reconocido en ciberseguridad y protección industrial[6], Kaspersky Lab investiga y desarrolla continuamente soluciones que aborden mejor las amenazas en constante evolución contra infraestructuras críticas industriales. Desde la gestión de las operaciones hasta el nivel ICS y más allá, Kaspersky Lab desempeña un papel protagonista para ayudar al sector, los organismos reguladores y las agencias gubernamentales a nivel global a anticiparse a los cambios en el panorama de amenazas y a defenderse contra los ataques.

Como proveedor de seguridad de confianza y partner de organizaciones líderes en su sector que han confiado durante muchos años de nuestra protección antimalware, Kaspersky Lab colabora con los principales proveedores y organizaciones de automatización industrial, como Emerson, SAP, Siemens, Schneider Electric, Industrial Internet Consortium y muchos otros, para establecer compatibilidad, procedimientos especializados y marcos de cooperación que protejan los entornos industriales no solo frente a las amenazas existentes y emergentes, sino también contra los ataques dirigidos los ataques altamente dirigidos.

Kaspersky Lab ha desarrollado un portfolio de soluciones especializadas para responder a determinadas necesidades del mercado de ciberseguridad industrial: Kaspersky Industrial CyberSecurity (KICS). Estas soluciones proporcionan una seguridad eficaz contra las ciberamenazas en todas las capas de ICS, incluidos

[6] Gartner Market Guide for Operational Technology Security (Guía de mercado de Gartner para la tecnología de seguridad operativa), 2016

servidores SCADA, HMI, estaciones de trabajo de ingeniería, PLC y conexiones de red industriales, todo ello sin afectar a la continuidad operativa ni a la coherencia de los procesos tecnológicos.

De acuerdo con la estrategia de seguridad multicapa global de Kaspersky Lab, Kaspersky Industrial CyberSecurity ofrece una combinación de diversas metodologías de protección. Adoptar un enfoque integral en cuanto a ciberseguridad industrial (que va desde la predicción de posibles vectores de ataque, pasando por tecnologías de prevención y detección industrial especializada hasta llegar a la respuesta proactiva ante un ciberincidente), es la mejor garantía de que su empresa operará de forma segura y sin interrupciones.

La arquitectura de seguridad adaptable

Kaspersky Industrial CyberSecurity: servicios

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

Conocimiento (formación e inteligencia)

- **Formación:** Kaspersky Lab ofrece cursos de formación diseñados tanto para expertos en seguridad de IT/OT como para operadores e ingenieros de ICS. Durante la formación, los participantes adquieren un mayor conocimiento de las ciberamenazas pertinentes, sus tendencias de desarrollo y los métodos más eficaces para protegerse contra ellas. Los cursos también permiten a los profesionales de seguridad seguir desarrollando sus habilidades en áreas específicas, incluidos los Pen Testing de ICS y la ciencia forense digital.
- **Programas de concienciación:** Para aumentar la concienciación sobre las cuestiones de ciberseguridad industrial, además de promover las competencias necesarias para abordarlas y resolverlas, Kaspersky Lab ofrece formación basada en gamificación, para gestores de seguridad e ingenieros. Por

ejemplo, Kaspersky Industrial Protection Simulation (KIPS) simula ciberataques reales en sistemas de automatización industrial para mostrar los principales problemas asociados con la provisión de ciberseguridad industrial.

- **Informes de inteligencia:** Nuestro equipo de expertos de respuesta a ciberemergencias de ICS ha preparado para usted informes de inteligencia de seguridad actualizados.

Servicios expertos

- **Evaluación de ciberseguridad:** Para las organizaciones preocupadas por el impacto operativo potencial de la seguridad de IT/OT, Kaspersky Lab proporciona una evaluación de ciberseguridad industrial mínimamente invasiva. Al suponer un primer paso decisivo en el establecimiento de requisitos de seguridad en el contexto de las necesidades operativas, también puede proporcionar información significativa sobre los niveles de ciberseguridad, incluso sin ningún despliegue posterior de tecnologías de protección.
- **Integración de soluciones:** Si el sistema de control industrial de una organización tiene una arquitectura singular o se basa en componentes de hardware y software personalizados que no se utilizan ampliamente en el sector, Kaspersky Lab puede adaptar herramientas de ciberseguridad recomendadas para trabajar con estos sistemas. Este servicio incorpora asistencia para sistemas de hardware y software exclusivos, lo que incluye servidores SCADA privados, PLC y protocolos de comunicación industrial.
- **Investigación de 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; dentro de su marco de acción, los expertos de Kaspersky Lab clasifican cualquier muestra de malware proporcionada, analizan sus funciones y comportamiento, y desarrollan recomendaciones y un plan para extraerlo de los sistemas y revertir cualquier acción maliciosa.

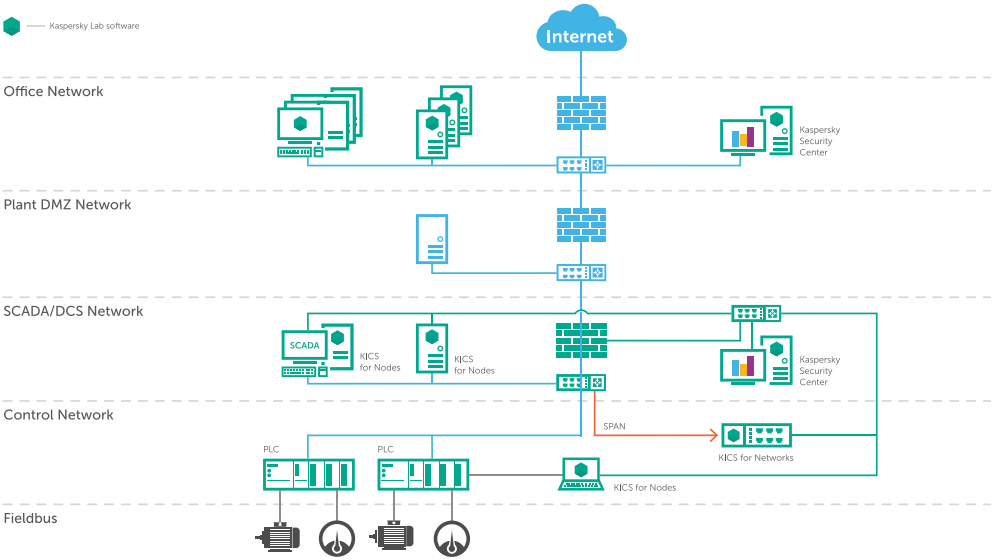
Kaspersky Industrial CyberSecurity: gestión centralizada de la seguridad

Kaspersky Security Center

A fin de garantizar los más altos niveles de protección frente a todos los vectores de ataque, la seguridad en la planta industrial debe funcionar en los niveles de nodo y de red. Para asegurar un control óptimo, facilidad de gestión y visibilidad, KICS, al igual que todas las tecnologías de protección de Kaspersky Lab, se controla mediante una única consola de administración, Kaspersky Security Center, que permite:

- Gestión centralizada de políticas de seguridad; posibilidad de establecer diferentes configuraciones de protección para los distintos nodos y grupos.
- Prueba simplificada de actualizaciones antes de su despliegue en la red, lo que garantiza la plena integridad del proceso.
- Acceso basado en funciones en línea con las políticas de seguridad y acciones urgentes.

Kaspersky Security Center garantiza facilidad de control y visibilidad, no solo de las capas industriales de varios centros, sino a través de las plantas de negocio circundantes, como se ilustra a continuación.



Kaspersky Security Gateway

KICS también puede enviar datos relacionados con eventos a otros sistemas, como SIEM, MES y soluciones de Business Intelligence. Notificación de todos los eventos y anomalías detectados a sistemas de terceros, lo que incluye SIEM, correo, servidores syslog y sistemas de gestión de redes a través de los protocolos CEF 2.0, LEEF y Syslog. Además de ayudar a detectar, contrarrestar e investigar los ataques cibernéticos, la supervisión de red industrial detallada facilita el mantenimiento predictivo.

Integración con interfaces hombre-máquina (HMI)

La solución puede enviar notificaciones de seguridad directamente a las HMI, lo que ofrece a los trabajadores de la planta industrial información específica para poder proporcionar una respuesta inmediata al ciberincidente y la derivación de este.

Kaspersky Industrial CyberSecurity for Nodes

KICS for Nodes fue diseñada específicamente para abordar las amenazas a nivel de operador en entornos de ICS. Protege los servidores ICS/SCADA, las HMI y las estaciones de trabajo de ingeniería contra varios tipos de ciberamenazas que pueden deberse a factores humanos, malware genérico, ataques dirigidos o sabotaje. KICS for Nodes es compatible tanto con los componentes de hardware y software de los sistemas de automatización industrial como con SCADA, PLC y DCS.

Amenazas y factores de riesgo	Tecnologías de Kaspersky Lab
Ejecución de software no autorizado	Modos de marcado en lista blanca, prevención o solo detección (registro en lugar de bloqueo)
Malware	Motores de detección antimalware avanzados basados en firmas; motor de detección basado en la nube, que utiliza la nube pública de Kaspersky Lab (KSN) o la nube privada (KPSN)
Cryptors, incluido el ransomware	Anti-Cryptor
Ataques de red	Firewall basado en host
Conexión de dispositivos no autorizados	Control de dispositivos
Conexiones inalámbricas no autorizadas	Control de la red Wi-Fi
Falsificación de programas de PLC	Comprobación de integridad de PLC
Específicos de ICS: aislamiento físico air-gap; falsos positivos para software/ procesos de ICS, etc.	Actualizaciones de confianza, que han sido probadas con software de los principales proveedores industriales; certificación de productos por parte de los principales proveedores de automatización industriales.

Lista blanca de aplicaciones

La naturaleza relativamente estática de las configuraciones endpoint de ICS implica que las medidas de control de integridad son mucho más eficaces que en redes corporativas dinámicas. Las tecnologías de control de integridad de KICS for Nodes incluyen:

- Control de la instalación y el inicio de las aplicaciones de acuerdo con políticas de marcado en lista blanca (prácticas recomendadas para redes de control industrial) o lista negra.
- Control del acceso de las aplicaciones a los recursos del sistema operativo: archivos, carpetas, registro del sistema, etc.
- Control de todo tipo de archivos ejecutables que se ejecutan en entornos Windows, lo que incluye: .exe, .dll, .ocx, controladores, ActiveX, scripts, intérpretes de línea de comandos y controladores de modo kernel.

- Actualización de datos de reputación de la aplicación.
- Categorías de aplicaciones predefinidas y definidas por el cliente para gestionar las listas de aplicaciones controladas.
- Ajuste de controles de aplicaciones para diferentes usuarios.
- Modos de prevención o de solo detección: bloquear cualquier aplicación que no esté en la lista blanca, o bien, en modo de "vigilancia", permitir la ejecución de aplicaciones que no estén en la lista blanca pero registrando su actividad en Kaspersky Security Center, donde se pueden evaluar.

Control de dispositivos

Gestión de acceso a dispositivos extraíbles, periféricos y buses del sistema, según la categoría del dispositivo, la familia y el ID de dispositivo específico.

- Compatibilidad con enfoques de lista blanca y lista negra.
- Asignación detallada de políticas, por equipo y por usuario, a un solo usuario/equipo o un grupo de usuarios/equipos.
- Modos de prevención o de solo detección.

Firewall basado en host

Configuración y ejecución de las políticas de acceso a la red para nodos protegidos tales como servidores, HMI o estaciones de trabajo. La función principal incluye:

- Control del acceso a redes y puertos restringidos.
- Detección y bloqueo de ataques de red lanzados desde fuentes internas, como equipos portátiles de contratistas, que pueden introducir malware para intentar analizar e infectar el host en cuanto se une a la red industrial.

Control de la red Wi-Fi

Esto permite la supervisión de cualquier intento de conexión a redes Wi-Fi no autorizadas. La tarea Control de Wi-Fi se basa en la tecnología de denegación predeterminada, que implica automáticamente el bloqueo de conexiones a cualquier red Wi-Fi "no permitida" en la configuración de la tarea.

Comprobación de integridad de PLC

Esto habilita un control adicional sobre las configuraciones de PLC mediante comprobaciones periódicas de determinados servidores protegidos por Kaspersky Lab. Las sumas de comprobación resultantes se comparan con valores "patrón" guardados y se informa de las desviaciones.

Protección antimalware avanzada

Las mejores tecnologías proactivas de detección y prevención de malware de Kaspersky Lab se han adaptado y rediseñado para satisfacer el consumo elevado de recursos y los requisitos de disponibilidad del sistema. Nuestra protección antimalware avanzada se ha diseñado para trabajar de forma eficaz incluso en entornos estáticos o raramente actualizados. El antimalware de Kaspersky Lab abarca toda la gama de tecnologías, lo que incluye:

- Detección de malware basada en firma.
- Detección por acceso y a petición.
- Detección en memoria (residente).
- Detección de ransomware a través de la tecnología especial Anti-Cryptor.
- Kaspersky Security Network (KSN) y Kaspersky Private Security Network (KPSN) posibilitan el mejor servicio de detección de malware.

Actualizaciones de confianza

Para garantizar que las actualizaciones de seguridad no tienen ningún impacto en la disponibilidad del sistema protegido, se realizan comprobaciones de compatibilidad antes del lanzamiento de las versiones de base de datos/componentes y de las actualizaciones de software/configuración del sistema de control de procesos. Los posibles problemas de consumo de recursos pueden abordarse desde una serie de diferentes escenarios:

- Kaspersky Lab realiza pruebas de compatibilidad de actualización de la base de datos con el software del proveedor de SCADA en el banco de pruebas de Kaspersky Lab.
- El proveedor de SCADA realiza comprobaciones de compatibilidad.
- Kaspersky Lab comprueba las actualizaciones de la base de datos de seguridad por usted: se integran imágenes de SCADA, estación de trabajo, servidor y HMI en el banco de pruebas de Kaspersky Lab.
- Las actualizaciones de seguridad de Kaspersky Lab se prueban en su centro y se automatizan a través de Kaspersky Security Center.

Kaspersky Industrial CyberSecurity for Networks

La solución de seguridad a nivel de red de Kaspersky Lab funciona en el nivel de protocolo de comunicación industrial (Modbus, conjunto IEC, ISO, etc.), analizando el tráfico industrial para encontrar anomalías a través de la tecnología avanzada DPI (inspección exhaustiva de paquetes). También se proporciona control de la integridad de la red y capacidades IDS.

Amenazas y factores de riesgo	Tecnologías de Kaspersky Lab
Aparición de dispositivos de red no autorizados en la red industrial	El control de integridad de la red detecta dispositivos nuevos/desconocidos.
Aparición de comunicaciones no autorizadas en la red industrial	El control de integridad de la red supervisa las comunicaciones entre dispositivos conocidos/ desconocidos.
Comandos de PLC maliciosos de: • Operador o un tercero (por ejemplo, contratista) por error • Persona interna (acciones fraudulentas) • Atacante/malware	DPI industrial analiza las comunicaciones desde y hacia los PLC y control de los comandos y los valores de parámetros del proceso tecnológico.
Ataques de red	Un avanzado sistema de detección de intrusiones identifica todos los patrones de ataque de redes conocidos, incluida la explotación de vulnerabilidades en software y hardware industrial
Falta de datos para la investigación y el análisis forense	Herramientas forenses: supervisión y registro seguro de eventos en la red industrial sospechosos y ataques detectados

Inspección no intrusiva del tráfico de red industrial

KICS for Networks proporciona una supervisión de anomalías del tráfico de red pasiva y de seguridad de red al mismo tiempo que se mantiene invisible para los posibles atacantes. La instalación es tan sencilla como activar/configurar la duplicación de puertos; la sencilla integración de un dispositivo de hardware o un dispositivo virtual/de software en el equipo de red industrial existente se logra a través del puerto SPAN del conmutador o dispositivo TAP existente. KICS for Networks cuenta con una arquitectura modular: los sensores pueden implementarse de manera independiente a partir de una unidad de control central.

DPI industrial para la detección de anomalías

KICS for Networks proporciona a los usuarios industriales una plataforma fiable para supervisar el flujo de comandos de control de proceso y los datos de telemetría, lo que permite, entre otras cosas:

- Detección de cualquier comando que pudiera volver a configurar un PLC o cambiar el estado del PLC.
- Cambios de los parámetros de control en los procesos tecnológicos.
- Protección contra amenazas externas al mismo tiempo que se mitiga el riesgo de interferencias internas "avanzadas" por parte de ingenieros, operadores de SCADA u otro personal interno con acceso directo a los sistemas.

Aprendizaje mecánico

Nuestro DPI industrial no solo se puede configurar conforme a un enfoque estándar basado en reglas, también puede detectar anomalías dentro de los procesos industriales a través de un potente modelo de previsión basado en LSTM. La capacidad de aprendizaje mecánico ofrece una detección de anomalías industriales a un nuevo nivel, lo que posibilita el descubrimiento de incidentes en las redes industriales más complejas y que se reconfiguran con frecuencia.

Control de la integridad de la red para proporcionar seguridad e inventario de activos

KICS for Networks permite la identificación de todos los activos de red conectados vía Ethernet, lo que incluye servidores SCADA, HMI, estaciones de trabajo de ingeniería, PLC y RTU. Todos los dispositivos nuevos o desconocidos y sus comunicaciones se detectan automáticamente. Esto permite a los equipos de seguridad crear un inventario propio, fiable y seguro de activos de red, en lugar de utilizar herramientas de gestión de activos de OT/IT potencialmente vulnerables que suelen ser objetivo de los atacantes.

Herramientas forenses

La solución de Kaspersky Lab ofrece a los usuarios industriales un sistema de registro seguro que proporciona herramientas digitales para el análisis de datos y análisis forense. El sistema también impide la realización de cambios en los registros de ICS.

Servicios adicionales para Kaspersky Industrial Cybersecurity

Kaspersky Security Network

Kaspersky Security Network (KSN) es una arquitectura distribuida basada en la nube que se dedica a recopilar y analizar inteligencia de amenazas de seguridad a partir de millones de nodos de todo el mundo. KSN no solo detecta y bloquea las nuevas amenazas y ataques de día cero, sino que también ayuda a localizar e incluir en listas negras las fuentes de ataques online, proporcionando datos de reputación para sitios web y aplicaciones.

Todas las soluciones corporativas de Kaspersky Lab, incluidas las soluciones industriales, se pueden conectar a KSN en caso necesario. Las principales ventajas incluyen:

- Índices de detección superiores.
- Tiempos de reacción reducidos; las respuestas basadas en firma tradicionales tardan horas, mientras que: KSN responde en aproximadamente 40 segundos.
- Menores tasas de falsos positivos.
- Consumo de recursos reducido para las soluciones de seguridad en las instalaciones.

Kaspersky Private Security Network (KPSN)

Para las organizaciones que tienen preocupaciones muy concretas sobre la privacidad de los datos, Kaspersky Lab ha desarrollado una opción denominada Kaspersky Private Security Network. Ofrece casi todas las ventajas de KSN, pero sin enviar ningún tipo de información fuera de la red.

KPSN puede desplegarse en el centro de datos de cualquier organización. Los especialistas de IT internos mantienen todo el control sobre la herramienta. Las instalaciones locales de KPSN pueden ayudar a satisfacer los requisitos de cumplimiento específicos de cada país u otra legislación sectorial específica.

Principales funciones de KPSN:

- Servicios de reputación de archivos y direcciones URL: los hash MD5 de archivos, las expresiones regulares para direcciones URL y los patrones de comportamiento de malware se almacenan, clasifican y despliegan de forma centralizada y con rapidez hasta el cliente.
- Record Management System (RMS): a veces el software de seguridad comete errores y clasifica incorrectamente archivos o direcciones URL como fiables/no fiables. RMS actúa como un freno de "falsos positivos", rectificando los errores y analizando de forma continua para mejorar la calidad
- Inteligencia e información basadas en la nube.

Kaspersky® Industrial CyberSecurity

Kaspersky Industrial CyberSecurity es un conjunto de tecnologías y servicios diseñada para proteger niveles de tecnología operativa y elementos de su organización, lo que incluye servidores SCADA, paneles HMI, estaciones de trabajo de ingeniería, PLC, conexiones de red e incluso ingenieros, sin afectar a la continuidad operativa ni a la coherencia de los procesos tecnológicos.

Más información en **www.kaspersky.com/ics**

Todo sobre ciberseguridad ICS:
https://ics-cert.kaspersky.com
Noticias de ciberamenazas: **https://securelist.lat/**

#truecybersecurity

www.kaspersky.es

IIC MEMBER industrial internet CONSORTIUM

OPC® FOUNDATION MEMBER

CYBER SECURITY EXCELLENCE AWARDS ★ FINALIST ★ 2017

* 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