Ciberresiliencia industrial: ocho pasos para proteger su empresa

La ciberseguridad industrial puede resultar abrumadora. Obtenga claridad estructurando su estrategia con estos ocho pasos.

kaspersky bring on the future

Primera edición: febrero de 2025

Contenido

Introducción

Si la complejidad y la automatización ocupan un lugar destacado en su organización, es probable que su superficie de ataque sea amplia y ofrezca múltiples puntos de entrada para actores malintencionados. Nuestros expertos en ciberseguridad industrial supervisan los sistemas de control industrial (ICS) en todo el mundo, y una parte significativa de ellos son objeto de ataques cada mes. Los agresores aprovechan todo tipo de vectores: desde scripts maliciosos y páginas de phishing, hasta gusanos, virus y ransomware. Frente a ello, contamos con las capacidades para detectar, contener y combatir estas amenazas.

La mayoría de los ciberataques industriales comienza en la infraestructura de tecnología de la información (TI), en la cadena de suministro o a través de contratistas externos, antes de propagarse a los entornos de tecnología operativa (OT) y provocar interrupciones. Esto representa un riesgo crítico, ya que muchas organizaciones tienen una baja tolerancia al tiempo de inactividad y cualquier interrupción en la producción genera presión adicional por parte de terceros afectados. En el caso de las infraestructuras críticas, el impacto es aún mayor: las consecuencias no solo afectan a clientes, sino también a la ciudadanía, como ocurre en interrupciones del suministro eléctrico o de agua.

Un ataque consumado puede afectar no solo a la estrategia y la reputación de una organización, sino también provocar interrupciones en los procesos, interrupciones en la cadena de suministro, pérdidas financieras y problemas normativos. Por lo tanto, las empresas de alto perfil deben prestar especial atención a la ciberseguridad industrial, ya que constituye la piedra angular de toda estrategia de transformación digital bien fundamentada.

Mediante la adopción de prácticas integrales de seguridad TI-TO, las organizaciones pueden evitar interrupciones en operaciones críticas y mitigar la mayoría de los riesgos financieros, reputacionales y tecnológicos asociados a los ciberataques.

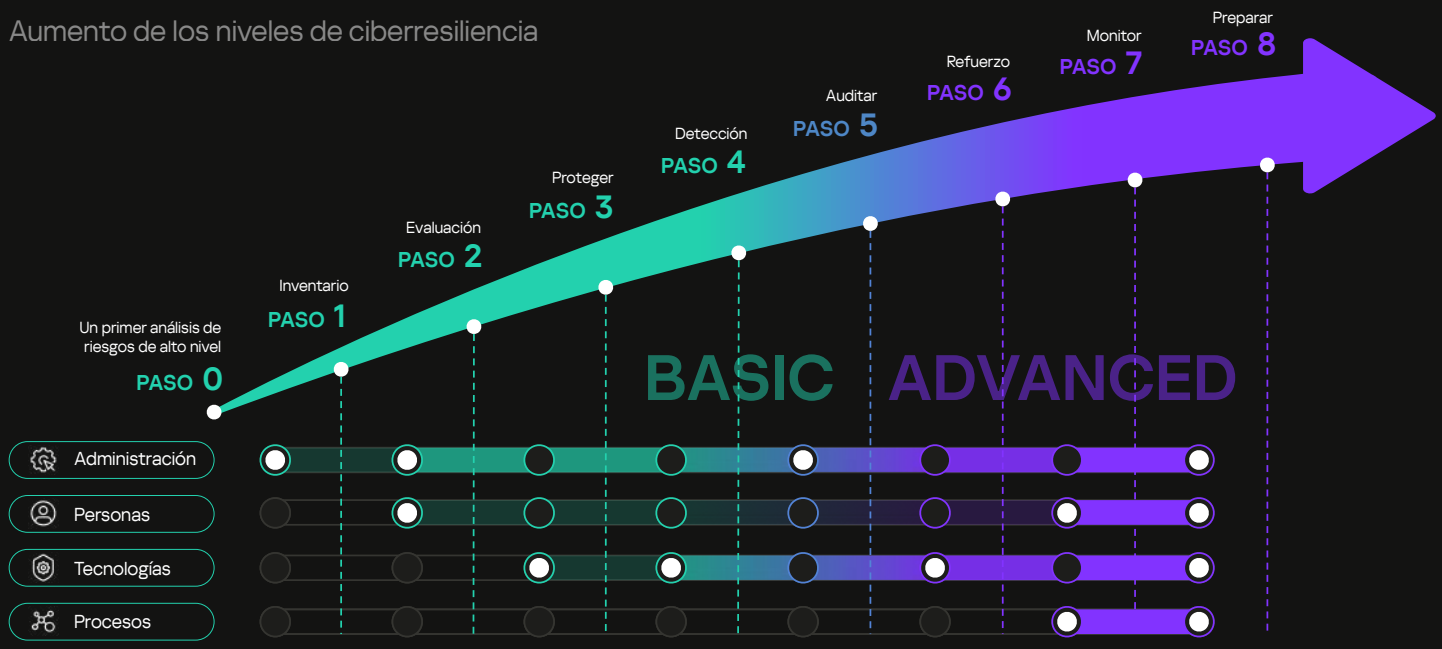
El punto de partida lógico

Una estrategia lógica debe comenzar con un análisis general de riesgos antes de abordar los pasos tangibles y factibles descritos en este documento: una especie de "paso cero". Esto forma parte del grupo de normas ISA/IEC 62443 y es la fase en la que se determinan los riesgos inaceptables que existen actualmente en la organización. Las pruebas resultantes son cruciales para obtener la aprobación de la alta dirección y el presupuesto. Según la ISA Global Cybersecurity Alliance, "facilita un método relativamente rápido para determinar las áreas de mayor riesgo dentro de un sistema de automatización".[1]

Sin embargo, la primera tarea que abordamos es el inventario de activos. Esto le garantizará una visibilidad total de su TO, lo que le permitirá realizar una evaluación detallada de los riesgos y definir las amenazas a las que se enfrenta su empresa. De este modo, podrá implementar numerosos niveles de seguridad (protección de endpoints, segmentación de redes, etc.) para frustrar las ciberamenazas dirigidas a los ICS. A partir de este punto, se trata de reforzar de forma constante y simultánea la tecnología de seguridad, el personal, los procesos y los sistemas de gestión de la seguridad.

En total, cubriremos ocho pasos que pueden ayudar a cualquier empresa industrial a desarrollar ciberresiliencia (o al menos hacerla más accesible). Estos pasos están alineados con las mejores prácticas descritas en numerosas guías, marcos y normas del sector, como la ISA/IEC 62443, y son especialmente útiles para las empresas industriales de alto perfil (las que se rigen por sus amplias infraestructuras). Esto se debe a que realizan operaciones de alto riesgo que conllevan importantes costos por incidentes y a que hacen hincapié en adoptar las mejores prácticas globales de gestión de la ciberseguridad.

Aumento de los niveles de ciberresiliencia



Las organizaciones gubernamentales, privadas y públicas también pueden beneficiarse de este plan. Su demanda de ciberseguridad y sus operaciones están reguladas por organismos gubernamentales, legislación nacional y normas internacionales específicas del sector. Estas organizaciones enfrentan consecuencias operativas potencialmente mucho más graves que la mayoría, en particular las siguientes:

- Petróleo, gas, petroquímica y química (offshore, transporte por oleoducto, refinerías, procesamiento petroquímico, etc.)
- Generación de energía térmica, nuclear o renovable; redes eléctricas (subestaciones de transmisión y distribución de energía, operadores de sistemas eléctricos, etc.) y empresas de servicios públicos
- Metales y minería (minería de metales ferrosos y no ferrosos, procesamiento y fabricación básica, minería del carbón, producción de cemento, etc.)
- Minerales y productos químicos (procesamiento de potasa, fosfato, nitrógeno, urea, amoníaco, etc.)
- Logística y transporte (aeropuertos, puertos marítimos, ferrocarriles, etc.)
- Industria manufacturera (electrónica, alimentación y bebidas, salud y farmacia, pasta y papel, etc.)

La mayoría de los pasos iniciales de esta guía son esenciales para lograr una **ciberresiliencia industrial básica**. Se trata de un área en la que el cumplimiento de las normas está muy extendido y que involucra protecciones fundamentales, a menudo reactivas. Estos últimos pasos facilitan en gran medida la **ciberresiliencia industrial avanzada**, que es proactiva, continua y eficaz contra las ciberamenazas sofisticadas, con el fin de minimizar el riesgo para las operaciones.

[1] O'Brien, P. Cybersecurity Risk Assessment According to ISA/IEC 62443-3-2. ISA Global Security Alliance

1 Inventario:gestión de activos

Comience su viaje hacia la resiliencia de la ciberseguridad creando (o actualizando) el inventario de activos de su organización. Es aquí donde contabilizará todos sus sistemas, software, hardware, segmentos de red, conductos, vías de comunicación y dispositivos para comprender qué debe, y puede, protegerse. A continuación, puede empezar a planificar su estrategia de seguridad utilizando seguridad esencial (el antimalware, por ejemplo, se considera la protección básica para las organizaciones de baja madurez) y otras estrategias de mitigación avanzadas, como la segmentación.

El inventario de activos forma parte de su tecnología de gestión de la seguridad y debe madurar en simultáneo con su tecnología de seguridad. En última instancia, lo ayudará en su intento de lograr una **ciberresiliencia industrial básica**. Catalogar los componentes de hardware, software y red significa que podrá identificar los activos críticos y las vulnerabilidades potenciales, lo que facilita una protección específica que garantizará una seguridad adecuada de activos valiosos. Un inventario detallado de activos también le permite supervisar y gestionar el ciclo de vida de cada activo, lo cual simplifica el proceso de actualización y aplicación de parches.

Flujo de trabajo recomendado

1. **Defina sus objetivos**: defina el alcance del entorno industrial que va a evaluar y confirme los objetivos de su inventario de activos, como detallar todos los dispositivos, sistemas y sus interconexiones.

2. **Prepárese para la investigación**: reúna las herramientas y los recursos necesarios para la investigación.

3. **Utilice el sondeo activo**: aunque la supervisión activa suele evitarse en entornos industriales, es útil para obtener datos confiables de forma efectiva; puede hacerlo con seguridad si comprende y respeta las limitaciones y especificidades de sus equipos industriales.

4. **Mapee su red**: utilice herramientas de mapeo de red para identificar automáticamente los dispositivos conectados a su red industrial; esto garantiza la precisión de los datos. Opte por herramientas de exploración especializadas diseñadas para redes industriales. Las de propósito general, como Nmap y PowerShell, requieren conocimientos de los que carecen muchos (si no la mayoría) de los ingenieros y operadores de sitios, y su uso indebido en un entorno de control de supervisión y adquisición de datos (SCADA) puede dañar las operaciones.

5. **Proceda al inventario**: enumere los activos descubiertos en un inventario centralizado. Incluya todos los detalles disponibles de los activos; por ejemplo, fabricante del dispositivo, modelo, especificaciones de hardware, versión de firmware y software, servicios en ejecución/puertos abiertos y ubicación. Los activos a los que les faltan parámetros de datos clave pueden afectar la seguridad.

6. **Supervisión continua**: cree procesos para la supervisión continua que mantengan actualizado el inventario de activos y gestionen las vulnerabilidades.

Recuerde: Si no puede ver parte de su infraestructura, o no sabe que existe, no puede protegerla.

Tecnologías

Kaspersky Industrial CyberSecurity

¿Cómo Kaspersky puede ayudar?

Para obtener una visibilidad completa de su entorno de TO, considere probar la plataforma **Extended Detection and Response (XDR) de Kaspersky Industrial CyberSecurity (KICS)**, que comprende KICS for Nodes y KICS for Networks. KICS for Networks puede recuperar datos importantes de forma pasiva a partir de una copia duplicada del tráfico de red de TO proporcionada por equipos de red activos. Puede enriquecer estos datos con información adicional de telemetría recibida de endpoints industriales protegidos por KICS for Nodes, lo que ayuda a revelar áreas de la infraestructura de red no cubiertas por la supervisión pasiva del tráfico copiado (áreas ciegas). También hay otras características útiles, como el etiquetado, el estado de los activos y un diagrama de topología de red que muestra las conexiones físicas de la red y se construye automáticamente según el sondeo de equipos de red activos, lo cual destaca el estado de seguridad de los dispositivos.

El escáner portátil KICS también puede ahorrarle una gran cantidad de recursos a su empresa: se trata de una unidad flash conectable que recopila todos los datos de hardware y software automáticamente sin necesidad de usar atributos del administrador de sistemas, con lo que se obtienen datos que se exportan a un registro único de forma segura. Al mismo tiempo, la detección automatizada de activos permanentes y la detección de anomalías y hosts fraudulentos garantizan el descubrimiento inmediato de desviaciones.

Entre KICS for Nodes, KICS for Networks y el agente de endpoints, se recopilan datos sobre todos los aspectos cruciales de la infraestructura industrial:

- Dispositivos
- Aplicaciones
- Parches
- Usuarios
- Archivos ejecutables

Si estos datos no se recopilan y analizan, la organización no puede considerarse segura.

En definitiva, la plataforma XDR de KICS garantiza una alta cobertura de infraestructuras de automatización heterogéneas, y sus soluciones funcionan desde el primer momento.

Características aplicables de la plataforma KICS

KICS for Nodes	**Escáner portátil:** escáner de malware, escáner de Open Vulnerability and Assessment Language (OVAL) (vulnerabilidad, cumplimiento), captura de paquetes, inventario básico de activos
KICS for Networks	**Gestión de activos:** descubrimiento de activos, visibilidad de la red, cronología de la situación de la red
KICS: plataforma XDR nativa para TO	**Gestión avanzada de activos:** inventario de hardware de endpoints; inventario de aplicaciones, usuarios y parches; supervisión del tráfico en endpoints **Auditoría de seguridad:** análisis de vulnerabilidades, auditoría de cumplimiento, control de configuración

Experiencia

Kaspersky Professional Services

Si carece de recursos internos o busca una tranquilidad total, puede confiarle el proceso de descubrimiento de activos a nuestros expertos de **Kaspersky Professional Services (KPS).**

Ejemplos de marcos

Marco	Kaspersky OT CyberSecurity ayuda a cumplir la normativa			
ISA/IEC 62443-3-3[2]	SR 1.1*	SR 1.2	SR 1.3*	SR 7.8^
ISA/IEC 62443-3-2	ZCR 1.1	ZCR 2.2		
NIS2[3]	Artículo 21: Medidas de gestión de riesgos de ciberseguridad (apartado 2. [d, g, i] y apartado 3.)			
NIST SP 800-82r3[4]	6.1.1: Gestión de activos			
GB/T 44462.1[5]	7.3.5.5.2: Gestión de activos			

*Kaspersky puede ayudar a comprobar el cumplimiento de los requisitos.
^Tiene mayor efecto y valor.

¿Desea asistencia de mapeo detallada?
Comparta los detalles de su proyecto y obtenga ayuda de nuestros expertos: ICSExperts@kaspersky.com

[2] Sociedad Internacional de Automatización (2024). Serie de normas ISA/IEC 62443.
[3] Directiva (UE) 2022/2555 (Directiva NIS 2)
[4] NIST (septiembre de 2023). NIST SP 800-82r3: Guía para la seguridad de la tecnología operativa (TO). NIST Sociedad Internacional de Automatización.
[5] Asociación de Normas de Comunicaciones de China (CCSA). Ciberseguridad empresarial de Internet industrial. GB/T 44462.1 —2024.

2 Evaluación: análisis de riesgos detallado

El siguiente paso a tener en cuenta, suponiendo que haya ejecutado su evaluación de riesgos de alto nivel como "paso cero", es una evaluación detallada de los riesgos. Esto lo ayudará a obtener una comprensión concreta del nivel de riesgo actual de su organización, junto con los posibles vectores de amenaza y las contramedidas existentes o previstas. Es un aspecto crucial para lograr una **ciberresiliencia industrial básica** y está relacionado con su tecnología de gestión de la seguridad.

La evaluación detallada de los riesgos lo ayudará a cumplir los criterios de riesgo corporativos y permite la creación de requisitos de ciberseguridad detallados para cada zona. Las evaluaciones de riesgos cibernéticos son cruciales en entornos industriales, ya que permiten identificar amenazas ocultas, ayudándole a priorizar inversiones y prevenir interrupciones con consecuencias potencialmente catastróficas.

Flujo de trabajo recomendado

1. **Identifique las vulnerabilidades**: identifique las vulnerabilidades de los componentes críticos de su infraestructura, como los controladores lógicos programables (PLC) y los sistemas SCADA. Evalúe las posibles deficiencias del hardware, el software, las configuraciones de red y los procesos operativos.

2. **Evalúe las amenazas**: examine las posibles amenazas (posibles actores maliciosos; sus objetivos, enfoque de la actividad y capacidades; sus tácticas, técnicas y procedimientos [TTP]).

3. **Analice los impactos**: analice los posibles impactos de un ciberataque, como los peligros para la salud y la interrupción de las operaciones. Luego, defina las implicaciones financieras, reglamentarias y de seguridad de cada impacto potencial.

4. **Priorice los riesgos**: ordene los riesgos identificados en función del peligro que suponen y de la probabilidad de que se produzcan.

5. **Tenga en cuenta el cumplimiento y las mejores prácticas**: realice evaluaciones de riesgos con la profundidad y frecuencia descritas en los requisitos normativos o las mejores prácticas aplicables a su industria y región.

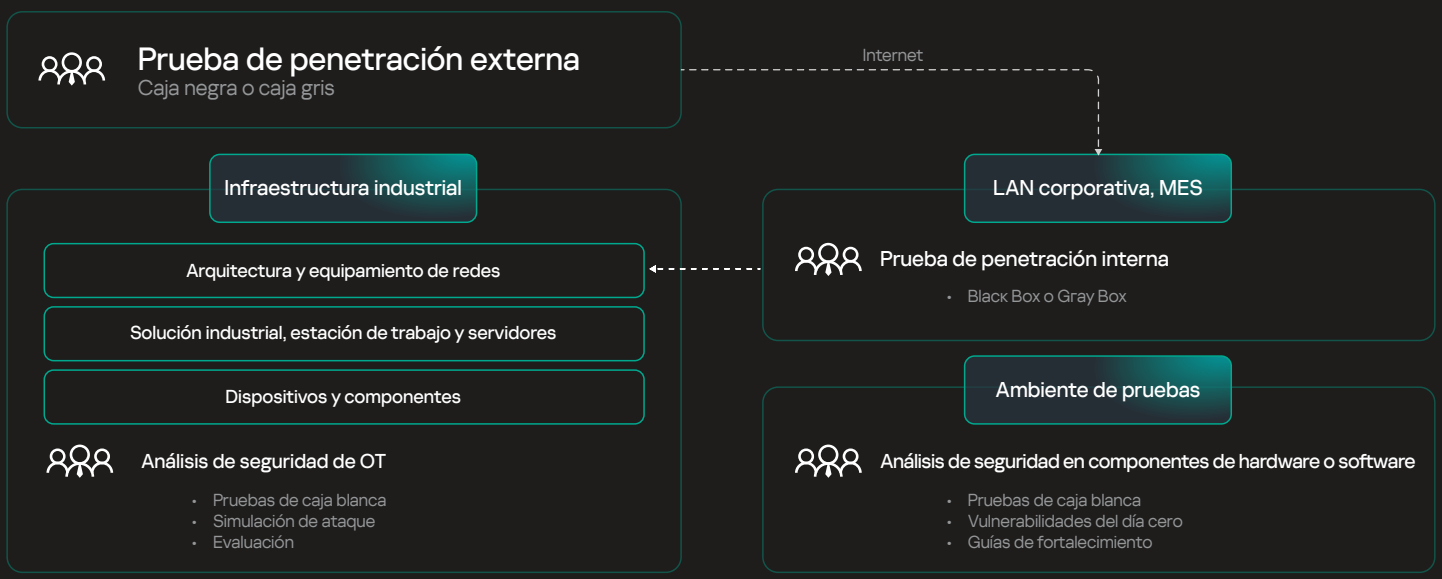
¿Cómo Kaspersky puede ayudar?

Experiencia

Kaspersky ICS Security Assessment

El servicio Kaspersky **ICS Security Assessments** identifica fallas en cada capa de su ICS, desde la seguridad física y de red hasta las vulnerabilidades específicas del proveedor en componentes ICS como sistemas SCADA y PLC. Determina la eficacia de sus medidas de seguridad existentes y proporciona las acciones únicas necesarias para reforzarlas.

Nuestro enfoque para la evaluación de la seguridad industrial



Conocimiento

Kaspersky ICS Threat Intelligence

Nuestro servicio **ICS Intelligence Reporting** proporciona información clave sobre amenazas y vulnerabilidades en entornos de tecnología operativa (TO), incluyendo análisis de gravedad y recomendaciones de mitigación. Esta información es especialmente útil durante la modelización de amenazas, el análisis de impacto y la priorización de riesgos.

Ejemplos de marcos

Marco	Kaspersky OT CyberSecurity ayuda a cumplir la normativa				
ISA/IEC 62443-3-2	ZCR 3 (TODOS)	ZCR 5.1^	ZCR 5.2^	ZCR 5.3	ZCR 5.4
	ZCR 5.5	ZCR 5.8	ZCR 5.10	ZCR 5.12^	ZCR 5.13^
NIS2	Artículo 21: Medidas de gestión de riesgos de ciberseguridad (apartado 2. [a, f]) Artículo 22: Evaluaciones coordinadas a nivel de la unión de los riesgos para la seguridad de las cadenas de suministro críticas (apartado 1.)				
NIST SP 800-82r3	3.3.6: Implementar un marco de gestión de riesgos para la OT 6.1.3: Evaluación de los riesgos				
GB/T 44462.1	7.3.5.2: Gestión de la seguridad				

^Tiene mayor efecto y valor.

¿Desea asistencia de mapeo detallada?
Comparta los detalles de su proyecto y obtenga ayuda de nuestros expertos: ICSExperts@kaspersky.com

3 Seguridad: controles de protección esenciales

En el mundo industrial, la seguridad esencial consiste en proteger el alma de las operaciones, con el fin de garantizar que cada proceso se desarrolle sin problemas, con seguridad y sin interrupciones. Su implementación lo ayuda a crear líneas de base de seguridad destinadas a mantener y proteger la ejecución de sistemas TO y la integridad de la configuración (así como a detectar, bloquear y remediar las ciberamenazas). Forma parte de su tecnología de seguridad y es la pieza central de su **ciberresiliencia industrial básica**. Sin embargo, si su objetivo es alcanzar una **ciberresiliencia industrial avanzada**, esta tecnología debe evolucionar con el tiempo.

Quizás el componente de seguridad esencial más reconocido sea la protección de endpoints, que protege los dispositivos (endpoints) dentro de sus entornos ICS y TO. Estos endpoints incluyen una amplia variedad de ICS, como servidores SCADA, interfaces hombre-máquina, historiadores de datos, estaciones de trabajo de ingeniería y paneles locales.

Flujo de trabajo recomendado

1. **Fortalezca y configure sus endpoints**: aplique configuraciones seguras para los endpoints, que se ajusten a las normas pertinentes de la industria. Reduzca su superficie de ataque; para ello, desinstale el software innecesario, cierre/elimine los servicios no requeridos y bloquee los puertos innecesarios, e instale regularmente actualizaciones de seguridad para el resto de su software y firmware. Comuníquese con el proveedor de ICS pertinente (proveedor u organización de servicios) para obtener la aprobación de estos cambios e implementarlos correctamente.

2. **Configure líneas de base de la integridad del sistema**: defina cómo son las operaciones estándar y seguras para cada sistema y cree configuraciones de línea de base, con el fin de capturar el estado del software, el firmware, las configuraciones y los patrones de comunicación de red. Será un punto de referencia para detectar y responder a las desviaciones.

3. **Implemente seguridad en los endpoints**: debido a la complejidad de los entornos industriales que incorporan tanto TI como TO, la mayoría de las soluciones estándar no son adecuadas. Elija software diseñado para entornos industriales como el suyo.

4. **Implemente mecanismos de control de acceso**: limite el personal que puede acceder a las configuraciones de los endpoints e interferir en ellas. Siga el principio del mínimo privilegio a la hora de diseñar funciones y asignar privilegios. Utilice modos de autenticación confiables recomendados por el proveedor del sistema de automatización, como la autenticación multifactor, y supervise los intentos de acceso a los endpoints para registrar los intentos no autorizados.

Muchos sistemas de control y automatización utilizados en las empresas industriales son conservadores o están desactualizados. Pueden llevar años funcionando sin mejoras sustanciales y se espera que sigan igual, lo que dificulta su protección. Estos sistemas son vulnerables de manera predeterminada y la implementación de protección de integridad (protección de línea de base) podría ser una medida de seguridad aplicable cuando no existe la posibilidad de aplicar parches.

Tecnologías

Kaspersky Industrial CyberSecurity for Nodes

¿Cómo Kaspersky puede ayudar?

KICS for Nodeses un software de protección de endpoints de OT óptimo y recomendado con un consumo mínimo de recursos. Combina funciones de protección, detección y respuesta, así como la integración de la plataforma KICS y la provisión de telemetría para el inventario y el análisis de riesgos tanto en sistemas de TO heredados como modernos.

Características aplicables de la plataforma KICS

KICS for Nodes	**Protección de endpoints:** prevención de amenazas en tiempo real, control de actividad local, control de actividad de red, supervisión de sistemas, ecosistemas e integraciones

Experiencia

Kaspersky Professional Services

Si desea saber si sus medidas de refuerzo tuvieron éxito antes de cualquier acción, **KPS Cybersecurity Health Check** es un buen punto de partida. Puede obtenerse de forma remota o en las instalaciones, y evaluará la eficacia de su enfoque e infraestructura de seguridad actuales de acuerdo con las mejores prácticas. Recibirá un informe en el que se detalla la investigación y todos los problemas de seguridad descubiertos, junto con nuestras recomendaciones de acuerdo con las normas de seguridad de la industria.

Ejemplos de marcos

Marco	Kaspersky OT CyberSecurity ayuda a cumplir la normativa				
ISA/IEC 62443-3-3	SR 1.6	SR 2.1	SR 2.3	SR 2.4	SR 2.5
	SR 2.8	SR 3.2	SR 4.1*	SR 7.2^	SR 7.7
NIS2	Artículo 21: Medidas de gestión de riesgos de ciberseguridad (apartado 2. [d, e, j]) Artículo 25: Normalización (apartado 1.)				
GB/T 44462.1	7.3.1.1 Seguridad de host ICS				

*Kaspersky puede ayudar a comprobar el cumplimiento de los requisitos.
^Tiene mayor efecto y valor.

¿Desea asistencia de mapeo detallada?
Comparta los detalles de su proyecto y obtenga ayuda de nuestros expertos: ICSExperts@kaspersky.com

4 Detección: monitoreo de anomalías y amenazas

La detección de amenazas y anomalías es un componente crucial de una buena estrategia de ciberseguridad. Sin embargo, en ningún ámbito esto es más cierto como en las organizaciones industriales, debido a la complejidad de sus sistemas, la confidencialidad de sus procesos y su carácter crítico. La aplicación de estas medidas tecnológicas de seguridad no solo lo ayudará a identificar las amenazas en una fase temprana, sino también a comprender cómo se desarrollan los ataques. Esto le permitirá responder con rapidez, evitar interrupciones operativas y reforzar su postura de seguridad, actividades que evidencian una **ciberresiliencia industrial avanzada**.

Muchas de las tecnologías utilizadas habitualmente en las soluciones de ciberseguridad también son beneficiosas para el personal de ingeniería. Por ejemplo, las siguientes capacidades mejorarían enormemente la experiencia digital de un ingeniero en sistemas de automatización responsable:

- Visibilidad de la red y detección de anomalías
- Inspección profunda de paquetes (DPI) de comunicaciones industriales con funcionalidades de aprendizaje automático (ML)
- Sistema de control de configuración
- Auditoría detallada del sistema

Estas características son otra forma de aumentar la seguridad de las operaciones internas de mantenimiento y la visibilidad de la actividad de contratistas externos, ya que actúan como potentes herramientas independientes de diagnóstico del sistema.

Flujo de trabajo recomendado

1. **Implemente su conjunto de herramientas**: elija las herramientas y tecnologías adecuadas para la detección de amenazas y anomalías; por ejemplo, los sistemas de detección de intrusiones en la red (IDS/NIDS) lo ayudarán a supervisar el tráfico y la actividad de la red. El análisis del tráfico de red ayuda a diferenciar los comportamientos normales de los anormales en los procesos industriales.

2. **Recopile datos**: optimice la recopilación de datos de numerosas fuentes (piense en el tráfico de red de todos los segmentos y hosts disponibles; telemetría de sistemas Linux y Windows; registros de SCADA, PLC/dispositivo final inteligente y otros controladores y equipos de red; visualización de la topología real de la red y el flujo de datos, etc.) recopilando datos en una plataforma centralizada para su correlación y análisis.

3. **Establezca un comportamiento de referencia**: defina el comportamiento "normal" de las operaciones en los sistemas industriales y fije parámetros para detectar desviaciones.

4. **Busque anomalías**: identifique comportamientos anómalos mediante análisis estadísticos y modelos basados en ML.

5. **Detecte amenazas**: utilice mecanismos de detección para identificar peligros conocidos y actividades maliciosas, pero sea consciente de que la experiencia en TO por sí sola no es suficiente. Existe una creciente superposición entre los activos de TO, los dispositivos de Internet de las cosas (IoT) y los sistemas de TI, y cada uno de ellos debe estar protegido por igual para minimizar el riesgo de interrupción. Por lo tanto, es crucial buscar proveedores de seguridad de TO que prosperen en entornos digitalmente convergentes.

6. **Repare**: limite el impacto de cualquier infracción posible, identifique la causa y aplique una estrategia de corrección integral.

7. **Esté preparado para el futuro**: sin importar la madurez actual de su sistema, asegúrese de definir los próximos pasos para una mejor integración. El objetivo debe ser adoptar la convergencia TI-TO en un centro de operaciones de seguridad (SOC) unificado, cerrar las brechas de visibilidad y tratar a la seguridad TI-TO como una sola entidad. Entre los beneficios de ampliar su SOC para cubrir las TO (creando una instalación a nivel de empresa) se incluyen la mejora del intercambio de información, una mayor visibilidad para los responsables de seguridad y la reducción del tiempo necesario para detectar y mitigar las amenazas.

Tecnologías

Kaspersky Industrial CyberSecurity for Networks

¿Cómo Kaspersky puede ayudar?

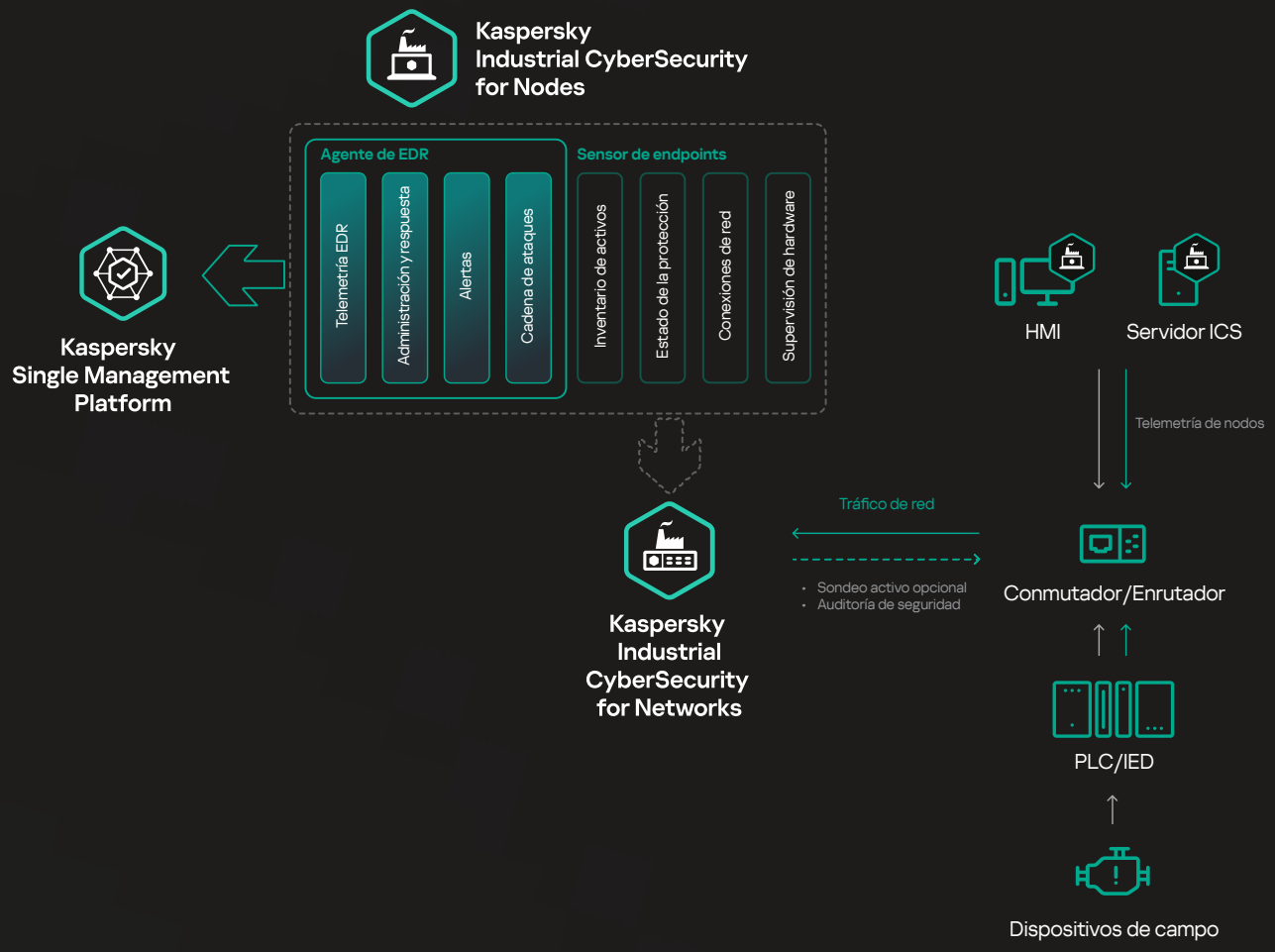
Su proveedor debe ser capaz de funcionar eficazmente en las instalaciones, en entornos difíciles y en áreas de baja conectividad de red (si fuera necesario). Por lo tanto, es fundamental contar con un proveedor de seguridad para entornos de TO que pueda abordar retos complejos de ciberseguridad mediante capacidades avanzadas que se integren con su cartera tecnológica existente y evolucionen con el tiempo.

Ya sea que esté iniciando la convergencia de sus procesos y tecnologías de ciberseguridad, o explorando funciones avanzadas como la búsqueda de amenazas, la visualización integrada de la cadena de ataque TI-TO o el análisis de causa raíz, en Kaspersky podemos ayudarle. Prosperamos en entornos convergentes y contamos con la experiencia necesaria para gestionar la triple amenaza: TI, TO e IoT.

KICS for Networksanaliza el tráfico de la red industrial para identificar desviaciones en los valores de los parámetros del proceso, detectar indicios de ataques a la red y supervisar el funcionamiento y los estados actuales de los dispositivos en la red. La combinación de DPI de protocolos industriales y capacidades IDS permite identificar y mitigar potenciales ciberamenazas en tiempo real. Esto permite proteger los entornos de ICS del acceso no autorizado, el malware y otras actividades maliciosas.

Cuando KICS for Networks se combina con **KICS for Nodes**, se desbloquean las capacidades de la plataforma XDR para TO, concretamente la detección y la respuesta. Esto incluye una única vista de la cadena de ataques, un enriquecimiento de alertas, etc. y facilita la supervisión de muestras de tráfico de red de sistemas aislados a través del escáner portátil KICS (con veredictos estándar de KICS for Networks).

Intercambio de datos de los componentes de la plataforma XDR de KICS



Características aplicables de la plataforma KICS

KICS for Networks	**Detección de amenazas y anomalías en la red:** detección de intrusiones, detección de anomalías, control de la integridad de la red, DPI de protocolos industriales y correlación de eventos
KICS for Nodes	**Detección y respuesta para endpoints:** análisis de detección, informes, medidas de respuesta, ecosistema e integraciones
KICS: plataforma XDR nativa para TO	**Detección y respuesta ampliadas:** vista única de la cadena de ataques, enriquecimiento de alertas, prevención de ejecución, aislamiento de host y archivos e integración de firewall

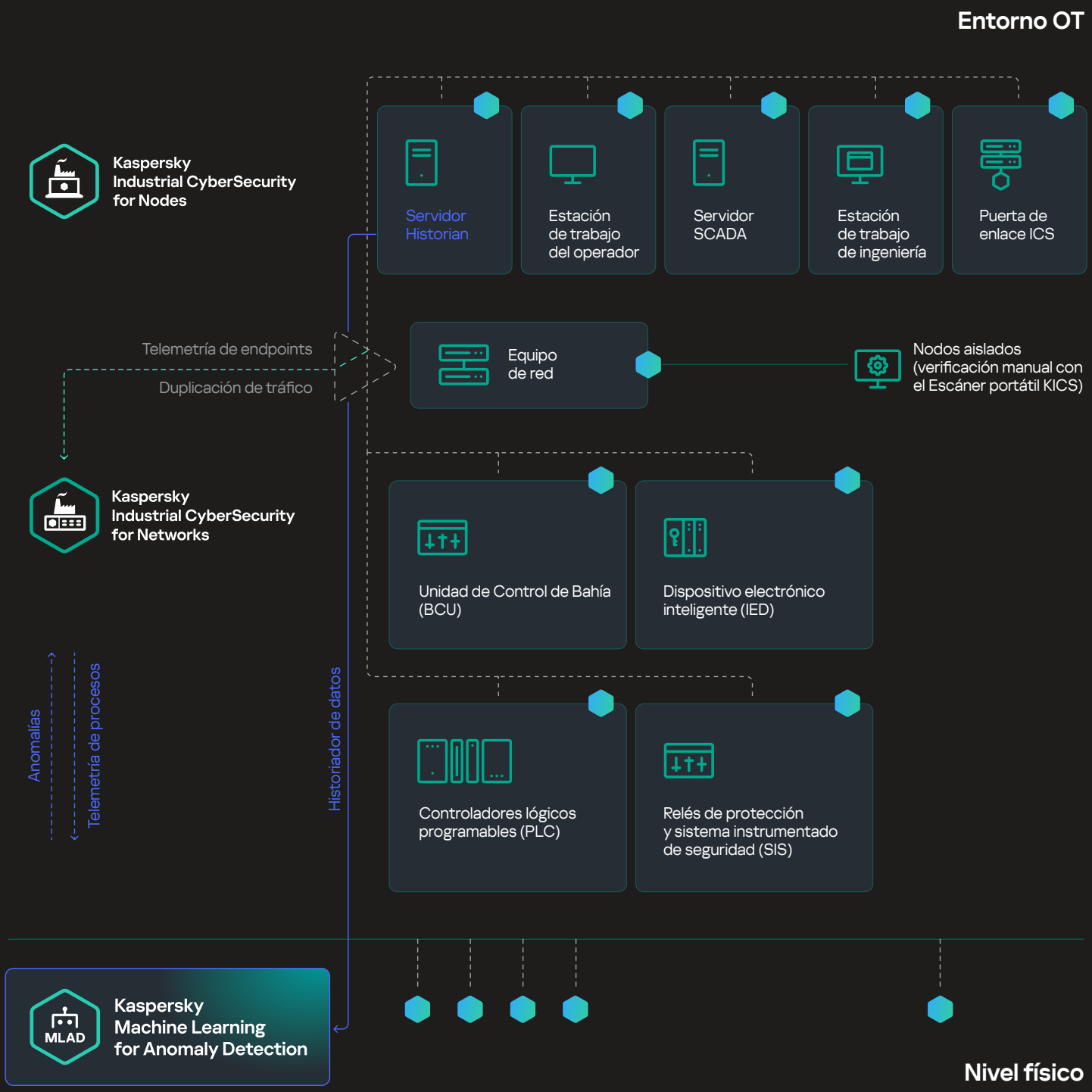
Tecnologías

Kaspersky Machine Learning for Anomaly Detection

A pesar de la exhaustividad de KICS, siempre existe el riesgo de que su organización se enfrente a amenazas avanzadas desconocidas o a ataques de día cero. Estos ataques nunca se pueden abordar por completo, por eso diseñamos **Machine Learning for Anomaly Detection (MLAD)**, una extensión de KICS y gemelo digital de los activos industriales con capacidades de ML. Pero si bien MLAD puede sobresalir como última línea de defensa prediciendo anomalías, también sirve como herramienta digital para supervisar y optimizar los indicadores clave de rendimiento de los procesos tecnológicos.

Cuando se combinan, MLAD y KICS for Networks detectan tanto las amenazas conocidas como las anomalías. Mientras que KICS for Networks detecta y bloquea rápidamente los peligros según vulnerabilidades o firmas conocidas, MLAD rastrea continuamente patrones sutiles o complejos que podrían indicar una amenaza desconocida grave, como un grupo de amenazas persistentes avanzadas.

Detección de anomalías en procesos tecnológicos basada en ML



Tecnologías

Kaspersky Next XDR Expert

Kaspersky Next XDR Core es ideal para los clientes que ya implementan soluciones de EDR y no quieren volver a comprarlas, por lo cual prefieren extender las funcionalidades con un motor de correlaciones, respuestas automatizadas y conectores externos.

Se basa en Open Single Management Platform, una plataforma de tecnología abierta que permite la integración con aplicaciones de Kaspersky y de terceros en un único sistema de seguridad para ofrecer escenarios de aplicaciones cruzadas. Las características de correlación cruzada (SIEM) de nuestro XDR le permiten a KICS centralizar la gestión en múltiples ubicaciones industriales, mientras correlaciona y recopila datos de fuentes externas dentro de los objetos industriales.

Ejemplos de marcos

Marco	Kaspersky OT CyberSecurity ayuda a cumplir la normativa			
ISA/IEC 62443-3-3	SR 1.11 SR 3.1^	SR 2.2 SR 3.5^	SR 2.10 SR 3.8	SR 2.12 SR 5.3
NIS2	Artículo 21: Medidas de gestión de riesgos de ciberseguridad (apartado 2. [b, c, d, e]) Artículo 23: Obligaciones de información (apartado 4. [todos])			
NIST SP 800-82r3	4.1: Gestión del riesgo de seguridad de TO			
GB/T 44462.1	7.3.3.2. Seguridad perimetral			

*Kaspersky puede ayudar a comprobar el cumplimiento de los requisitos.
^Tiene mayor efecto y valor.

¿Desea asistencia de mapeo detallada?
Comparta los detalles de su proyecto y obtenga ayuda de nuestros expertos: ICSExperts@kaspersky.com

5 Auditoría: verificación de políticas y cumplimiento

Para hacerse una idea realista de la ciberseguridad de su organización, debe centrarse en el cumplimiento y realizar auditorías de seguridad periódicas. Estas evaluaciones sistemáticas están relacionadas con su tecnología de gestión de la seguridad y son una parte fundamental de la **ciberresiliencia industrial básica** que puede determinar si se está alineando con los criterios y alcanzando los puntos de referencia. Son los guardianes de su entorno industrial y garantizan que las operaciones no solo funcionen con eficacia, sino también con seguridad y dentro de los límites normativos. El resultado debería ser una mayor adhesión a las mejores prácticas y, en última instancia, sistemas más robustos.

Flujo de trabajo recomendado

1. **Identifique los marcos**: confirme las normas y reglamentos más relevantes de su industria (por ejemplo, NIST SP 800-82, ISA/IEC 62443, RGPD, etc.).

2. **Implemente controles técnicos**: lo ayudarán a demostrar el cumplimiento de las normas reglamentarias y a identificar las áreas de mejora.

3. **Organice talleres de evaluación de riesgos**: realice periódicamente talleres centrados en el análisis de riesgos en el contexto industrial. Incluya las principales partes interesadas cuya función sea identificar y evaluar los riesgos asociados a los procesos, sistemas y activos. Desarrolle y aplique procedimientos de fortalecimiento y reconfiguración para reducir los riesgos.

4. **Realice auditorías de seguridad**: lleve a cabo auditorías de seguridad periódicas para evaluar la eficacia de sus controles técnicos mediante la identificación de brechas. Lo ideal es recurrir tanto a auditores internos como externos.

Tecnologías

Kaspersky Industrial CyberSecurity

¿Cómo Kaspersky puede ayudar?

La **plataforma XDR nativa para TO de KICS** admite auditorías de seguridad activas y pasivas de endpoints y redes, lo que le permite conseguir más con menos recursos. Nuestra auditoría de cumplimiento centralizada de los nodos de la red industrial se basa en la norma OVAL, que identifica y supervisa los riesgos y las vulnerabilidades específicos de TO.

KICS for Networks. Evaluación de vulnerabilidades, riesgos y la configuración de seguridad de TO

Característica	Auditoría de seguridad	
Subcaracterística	Auditoría de vulnerabilidad y cumplimiento (OVAL +XCCDF)	Control de configuración
Datos	• Vulnerabilidades de sistemas operativos y software • Vulnerabilidades de software del ICS • Cumplimiento de la configuración de seguridad recomendada • Cumplimiento de los estándares normativos	• Usuarios y grupos • Aplicaciones y parches • Servicios • Objetos de inicio • Controladores • Tareas programadas
Métodos de recopilación de datos	Sin agente • SSH	Industrial • Protocolo nativo ICS**
	Agente • de KICS for Nodes	
Fuentes de datos	Estaciones de trabajo, servidores y dispositivos de red basados en Linux	Controladores Industriales: Siemens, Schneider Electric, Allen-Bradley, Emerson DeltaV
	Estaciones de trabajo y servidores Windows y Linux	

* - Lenguaje abierto de evaluación y vulnerabilidad (OVAL)
- Formato de descripción de listas de comprobación de configuración ampliable (XCCDF)

** s7comm; Modbus; Ethernet/IP, Emerson DeltaV

Características aplicables de la plataforma KICS

KICS: plataforma XDR nativa para TO	**Auditoría de seguridad:** análisis de vulnerabilidades, auditoría de cumplimiento, control de configuración
KICS for Nodes	**Escáner portátil:** escáner OVAL (vulnerabilidades, cumplimiento)

Ejemplos de marcos

Marco	Kaspersky OT CyberSecurity ayuda a cumplir la normativa
ISA/IEC 62443-3-3	SR 1.5 SR 1.7 SR 2.9 SR 2.11 SR 3.4 SR 3.7 SR 3.9 SR 6.1 SR 7.6^
NIS2	Artículo 20: Gobernanza (apartado 1.) Artículo 21: Medidas de gestión de riesgos de ciberseguridad (apartado 2. [d, e, f, i])
NIST SP 800-82r3	3.3.1: Establecer la gobernanza de la ciberseguridad de OT
GB/T 44462.1	7.3.2.3 Seguridad de la configuración 7.3.4.2. Seguridad para aplicaciones ICS

^Tiene mayor efecto y valor.

¿Desea asistencia de mapeo detallada?
Comparta los detalles de su proyecto y obtenga ayuda de nuestros expertos: ICSExperts@kaspersky.com

6 Refuerzo: zonas y conductos

Las zonas son conjuntos de redes, dispositivos y servicios agrupados según su función, criticidad y requisitos de seguridad. Son la base de la segmentación y la supervisión y el control del acceso y pueden ser esenciales para el cumplimiento. Los conductos, por su parte, representan las vías de comunicación que unen zonas o las conectan a redes externas. Su función está en el control del tráfico, el cifrado, el filtrado de seguridad y la redundancia y resiliencia. Juntos, forman parte de su tecnología de seguridad y son cruciales para alcanzar una **ciberresiliencia industrial avanzada**.

El modelado inicial de zonas y conductos desempeña un papel clave en la organización y protección de la arquitectura de red de los entornos TO y debe realizarse antes de su evaluación detallada de los riesgos. Este paso, sin embargo, se refiere a la mejora de las zonas y los conductos, ya que su organización debería estar ahora en condiciones de identificar incidentes y violaciones de políticas en las zonas y utilizar el flujo de datos real para mejorar la arquitectura.

Puede mitigar los riesgos cibernéticos y mantener la integridad operativa revisando sus zonas y conductos y aplicando las siguientes medidas.

Flujo de trabajo recomendado

1. **Mejore continuamente la segmentación de la red y determine las restricciones de flujo de información necesarias**: el diseño de la infraestructura de red no es un proceso estático; redefina los límites lógicos y agrupe los componentes según la evolución de las funciones, la criticidad y los requisitos de seguridad (por ejemplo, 1. control de procesos, 2. operaciones).

2. **Mapee las zonas**: diseñe un mapa físico y lógico de las interconexiones entre zonas.

3. **Modele los conductos**: enumere los que conectan zonas y redes externas y determine los controles de seguridad (firewall, etc.) que implementará en cada punto; confirme los requisitos para un acceso seguro, como los mecanismos de autenticación.

4. **Implemente y configure**: segmente la red según sus zonas y conductos, implemente controles de seguridad y acceso y supervise las anomalías.

5. **Pruebe su configuración**: utilice evaluaciones de vulnerabilidad y pruebas de penetración para confirmar la eficacia de sus zonas y conductos. Las reglas de configuración del firewall (regla por defecto, limpieza de las no utilizadas, etc.) deben probarse antes de la implementación.

¿Cómo Kaspersky puede ayudar?

Tecnologías

Kaspersky Thin Client

El acceso remoto seguro a la infraestructura de TO les permite a los ingenieros y operadores supervisar y controlar los sistemas a distancia, lo que puede ayudar a optimizar la producción, reducir el tiempo de inactividad y mejorar la programación del mantenimiento. Pero la arquitectura industrial de IoT-nube es compleja y si dichas conexiones están expuestas a vulnerabilidades, las ventajas potenciales pueden verse pronto superadas por los riesgos de un ciberataque. **Kaspersky Thin Client** simplifica la migración de una infraestructura de escritorio local a una infraestructura Thin Client confiable, fácil de gestionar y con inmunidad cibernética para la conexión segura a escritorios virtuales, incluida una zona de confianza para conectar a los usuarios a la infraestructura industrial.

Tecnologías

Kaspersky SD-WAN

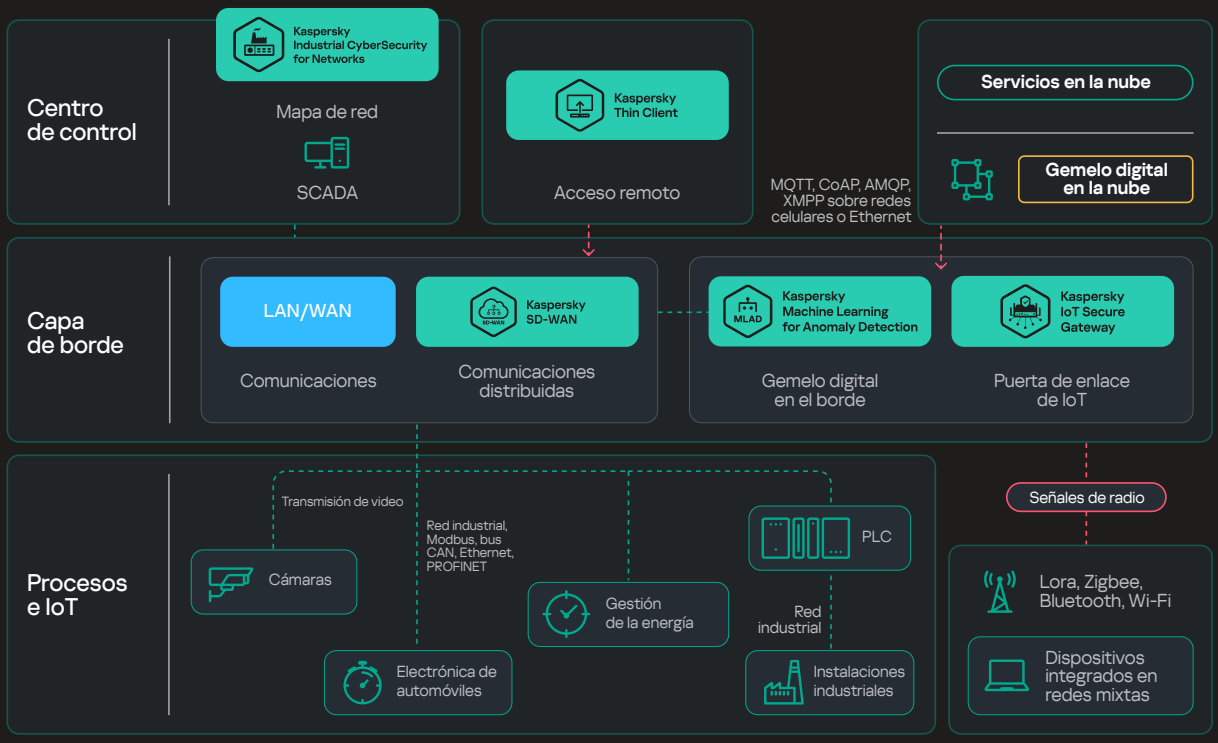
Kaspersky SD-WAN se diseñó para construir redes seguras y tolerantes a fallas con gestión unificada, lo que es esencial para las organizaciones industriales que abarcan una gran cantidad de sucursales, equipos distribuidos, recursos en la nube y empleados remotos. Le permite desplegar automáticamente herramientas de control del tráfico y de seguridad (tanto propias como de terceros) desde el primer momento. No solo garantizará que la transmisión de datos sea más segura que nunca, sino que también es escalable, fácil de gestionar y rentable.

Tecnologías

Kaspersky IoT Secure Gateway

KISG, parte de **Kaspersky IoT Infrastructure Security**, puede instalarse entre la infraestructura de TO y las redes de datos externas, a fin de bloquear los ataques a ICS, equipos y canales de intercambio de información. Se crea de acuerdo con los principios de la seguridad por diseño, no requiere protección adicional y admite aplicaciones de terceros para procesos perimetrales. (Este escenario es aplicable a dispositivos inteligentes conectados o expuestos a redes públicas).

KICS for Networks proporciona control de violación de políticas de zonas y conductos



Características aplicables de la plataforma KICS

KICS for Networks	**Ecosistema e integraciones:** Una serie de integraciones de terceros o sinergia dentro de la cartera de ciberseguridad de TO Kaspersky: - Kaspersky Next XDR Expert - Kaspersky IoT Secure Gateway (KISG) - Kaspersky Machine Learning for Anomaly Detection (MLAD) - Kaspersky Software-Defined Wide Area Network (SD-WAN)

Ejemplos de marcos

Marco	Kaspersky OT CyberSecurity ayuda a cumplir la normativa				
ISA/IEC 62443-3-3	SR 1.11	SR 1.13	SR 3.6	SR 5.1^	SR 5.2^
NIS2	Artículo 21: Medidas de gestión de riesgos de ciberseguridad (apartado 2. [h, i, j])				
NIST SP 800-82r3	4.1: Gestión del riesgo de seguridad de TO				
GB/T 44462.1	7.3.3.1. Seguridad de la arquitectura				

^Tiene mayor efecto y valor.

¿Desea asistencia de mapeo detallada?
Comparta los detalles de su proyecto y obtenga ayuda de nuestros expertos: ICSExperts@kaspersky.com

7 Supervisión: operaciones de seguridad maduras

El SOC es el corazón de su capacidad defensiva proactiva, pero no basta con establecer uno o contratar a un tercero imparcial. Confiar en medidas básicas y sistemas SIEM no será suficiente en un panorama de amenazas en constante evolución, en el que las ciberamenazas son muy sofisticadas. Estas medidas son necesarias, sí, pero por sí solas carecen del análisis proactivo y contextual necesario para gestionar ataques complejos.

Después de implementar un SIEM, su organización debe esforzarse por conseguir un SOC maduro y habilitado para XDR. Cuando los procesos eficaces, como la seguridad de los sistemas (evaluación, implementación y sostenibilidad) y la gestión de incidentes (detección, respuesta y recuperación) cuentan con el apoyo de expertos, se sabe que se está desarrollando una **ciberresiliencia industrial avanzada**.

Su organización debe evolucionar continuamente su capacidad defensiva con inteligencia de amenazas y características de respuesta a incidentes en cuanto ocurren. Un SOC reforzado puede investigar, contener y mitigar rápidamente las amenazas, a fin de minimizar los daños y reducir el tiempo de recuperación, características de la **ciberresiliencia industrial avanzada**.

Flujo de trabajo recomendado

1. **Establezca las metas del SOC**: describa sus objetivos y decida si formará parte de su organización, se tercerizará o será una combinación de ambos, en función de la disponibilidad de recursos.

2. **Desarrolle el SOC**: equípelo de personal, herramientas de supervisión de la seguridad y búsqueda de amenazas, herramientas e infraestructura de recopilación y análisis de artefactos, sistemas de triaje de incidentes y plataformas de colaboración.

3. **Aumente la capacidad humana**: mejore la calificación de los analistas del SOC en ciberseguridad industrial y asegúrese de que comprenden los entornos y protocolos de TO (o subcontrate a especialistas).

4. **Forme un equipo de respuesta a incidentes**: reúna a especialistas en TI, ciberseguridad y TO en un solo equipo y defina funciones y responsabilidades para la detección, el análisis, la priorización, la contención y la recuperación. Nombre a las partes interesadas principales del ámbito jurídico, financiero, de marketing, etc., que ayudarán en los elementos de respuesta no técnicos, como la elaboración de informes reglamentarios y la gestión de los medios de comunicación.

5. **Perfeccione el plan de respuesta a incidentes**: debería haber esbozado su plan de respuesta a incidentes como parte de sus políticas; agregue un toque con los siguientes elementos:

- categorización de los incidentes y niveles de gravedad
- partes interesadas
- acciones específicas de investigación y respuesta
- protocolos de comunicación e información
- pasos de recuperación
- Etc.

¿Cómo Kaspersky puede ayudar?

Ya sea que tenga su propio SOC o esté buscando una solución SOC de terceros completamente desarrollada, le ofrecemos tecnología, conocimientos y experiencia.

Tecnologías

Kaspersky Next XDR Expert

Aunque es posible construir su SOC utilizando una solución XDR de su elección antes de agregar nuestras capacidades de respuesta a incidentes, inteligencia de amenazas e incluso detección y respuesta gestionadas (MDR),**Kaspersky Next XDR Expert** es la elección por excelencia. Ofrece ciberseguridad unificada en todos los segmentos industriales y corporativos de su empresa, lo que facilita una verdadera convergencia TI-TO (en operaciones de seguridad) cuando se combina con KICS. Su detección de amenazas mejorada, respuesta automatizada y visibilidad en tiempo real proporcionan la defensa proactiva definitiva, mientras que la asistencia prémium las 24 horas del día, los 7 días de la semana proporciona tranquilidad en torno a la continuidad de la actividad empresarial.

Experiencia

Kaspersky Incident Response

El servicio **Kaspersky ICS Incident Response Handbook** tiene como objetivo crear un conjunto de escenarios detallados e instrucciones para todas las fases de respuesta a incidentes relevantes para su organización. Tenemos en cuenta todos los aspectos importantes, incluida la estructura organizativa y los recursos humanos disponibles, los sistemas de ciberseguridad en uso y los productos ICS en funcionamiento.

Capacidades maduras de Kaspersky Next XDR Platform

Conocimiento

Kaspersky ICS Threat Intelligence

Si lo que busca es simplemente información, nuestro servicio**ICS Threat Intelligence**le permite acceder en tiempo casi real a los indicadores de peligro de las amenazas relacionadas con OT, además de un análisis en profundidad de los ataques dirigidos a las empresas industriales.

Experiencia

Kaspersky Managed Detection and Response

También podemos ofrecerle servicios SOC dedicados y exhaustivos a través de **Kaspersky MDR**. Está disponible tanto para los segmentos industriales como corporativos de su empresa, y proporciona la experiencia y los recursos necesarios para rastrear ciberamenazas industriales y responder de manera adecuada.

Ejemplos de marcos

Marco	Kaspersky OT CyberSecurity ayuda a cumplir la normativa	
ISO/IEC 27001	SR 3.3	SR 6.2^
NIS2	Artículo 21: Medidas de gestión de riesgos de ciberseguridad (apartado 2. [b, c]) Artículo 23: Obligaciones de información (apartado 4. [todos])	
NIST SP 800-82r3	3.3.8: Desarrollar una capacidad de respuesta a incidentes	
GB/T 44462.1	7.3.5.5. Gestión de las operaciones	

^Tiene mayor efecto y valor.

¿Desea asistencia de mapeo detallada?
Comparta los detalles de su proyecto y obtenga ayuda de nuestros expertos: ICSExperts@kaspersky.com

8 Preparación: tolerancia a las fallas y capacidad de respuesta

A menudo, se pasa por alto el elemento humano en la ciberseguridad. La tecnología es tan buena como quienes la configuran y la utilizan, lo que significa que cada empleado o contratista es un punto de acceso potencial a su organización. Y cuando se trata de prevenir un ataque, o de responder eficazmente a un incidente, las personas son su mayor activo.

La tolerancia a las fallas, por otro lado, está relacionada con su tecnología de gestión de la seguridad y garantizará que pueda resistir y recuperarse de un incidente cibernético sin comprometer la continuidad operativa. Su ICS debería seguir funcionando durante un ataque, y es en este paso donde pondrá a prueba esta teoría. Recuerde que estos sistemas pueden degradarse con el tiempo, por lo que debe garantizar su disponibilidad frente a la degradación y la denegación de servicios (DoS).

La ciberresiliencia industrial avanzada solo puede lograrse cuando los diversos ICS son resistentes a diferentes tipos de eventos DoS, incluida la indisponibilidad parcial o completa de la funcionalidad del sistema a diferentes niveles. Lo más importante es que los incidentes de seguridad de los ICS no afecten a la seguridad (como los sistemas instrumentados de seguridad).

Mediante la realización de ejercicios de "tormenta cibernética" que simulan ciberataques a gran escala, puede poner a prueba la infraestructura que construyó en los pasos anteriores, para asegurarse de que todo funciona durante la degradación del sistema o los ataques DoS. Los ICS también deben tener la capacidad de volver a un estado seguro conocido luego de una interrupción o falla.

Flujo de trabajo recomendado

1. **Capacite a su equipo**: es fundamental que su personal posea las competencias técnicas y los conocimientos necesarios para proteger su entorno industrial exclusivo. Debe establecer capacitaciones periódicas centradas en la ciberseguridad delICS, SCADA y TO y tener en cuenta lo siguiente:
   - mejorar la capacitación de los empleados de toda la organización para que sean más resilientes a la suplantación de identidad, la ingeniería social, etc.
   - realizar ejercicios prácticos y simulacros para fortalecer la capacidad de respuesta.

2. **Fomente la colaboración entre equipos**: las unidades de TI, OT y ciberseguridad deben trabajar en grupo para aumentar la tolerancia a fallas y la eficacia de la respuesta. Para lograrlo, realice lo siguiente:
   - organice ejercicios y simulacros conjuntos para mejorar la comunicación y la coordinación durante los incidentes;
   - desarrolle una comprensión compartida de las dependencias operativas y los sistemas críticos;
   - realice periódicamente ejercicios de simulación y simulacros de crisis para poner a prueba su plan de respuesta a incidentes con las partes interesadas.

3. **Practique la resiliencia**: incorpore la tolerancia a las fallas en los sistemas centrales para mantener la operatividad bajo presión. Para lograrlo, realice lo siguiente:
   - instale mecanismos de respaldo para los componentes críticos de la infraestructura;
   - audite periódicamente la resiliencia del sistema;
   - cree planes de contingencia y respaldos para los escenarios más catastróficos.

4. **Realice retrospectivas de respuesta a incidentes**: no se trata solo de tener un plan de respuesta a incidentes y unos procedimientos establecidos; debería realizar una retrospectiva completa después de cada incidente cibernético para aprender las lecciones y volver más fortalecido, con un plan actualizado.

¿Cómo Kaspersky puede ayudar?

Conocimiento

Kaspersky Security Awareness

Los ciberdelincuentes utilizarán al personal como punto de entrada a sus sistemas. Para la resiliencia humana, proporcióneles a las personas los conocimientos en ciberseguridad que necesitan mediante **Kaspersky Security Awareness Training**.

Conocimiento

Kaspersky ICS CERT Training

Para mejorar las capacidades de sus profesionales de seguridad de TI y TO, involúcrelos con nuestro amplio programa de capacitación **ICS CERT**. Esto incluye Kaspersky Digital Forensics e Incident Response in ICS, que les permite llevar a cabo investigaciones forenses en entornos industriales y proporcionar análisis y recomendaciones de expertos.

Ejemplos de marcos

Marco	Kaspersky OT CyberSecurity ayuda a cumplir la normativa		
ISA/IEC 62443-3-3	SR 7.1	SR 7.4	SR 7.5
NIS2	Artículo 21: Medidas de gestión de riesgos de ciberseguridad (apartado 2. [b, c, g])		
NIST SP 800-82r3	3.3.2: Construir y entrenar un equipo multifuncional para implementar el programa de ciberseguridad de TO 3.3.5: Establecer un Programa de capacitación de concienciación en ciberseguridad para el entorno de TO 4.3.5: Evaluación		
GB/T 44462.1	7.3.5. Gestión de la seguridad		

^Tiene mayor efecto y valor.

¿Desea asistencia de mapeo detallada?
Comparta los detalles de su proyecto y obtenga ayuda de nuestros expertos: ICSExperts@kaspersky.com

Conclusión

Las organizaciones conectan cada vez más sus ICS a Internet en busca de una ventaja competitiva, pero esto las hace vulnerables a las ciberamenazas. Por lo tanto, se requieren esfuerzos multidireccionales para desarrollar entornos TO seguros, y esto incluye profesionales de ciberseguridad de TO con conocimientos más allá de la seguridad de TI. Esta experiencia es lo que hace tan valiosa nuestra división de investigación de seguridad ICS.

Afortunadamente, su organización puede proteger a sus grupos de interés de la pérdida de activos críticos (y de las implicaciones económicas y de seguridad nacional asociadas) aplicando principios básicos de diseño de ciberresiliencia industrial.

Lograr una **ciberresiliencia industrial avanzada** le permitirá a su organización resistir ataques maliciosos dirigidos a operaciones industriales e incluso impedir que los adversarios que penetren en su perímetro controlen, examinen o roben sistemas de misión crítica.

Ya protegimos a más de 1.000 clientes industriales y contamos con una amplia experiencia en la adopción de normas y mejores prácticas internacionales. Basándonos en esta experiencia, definimos ocho pasos estratégicos que se aplican universalmente a los sistemas de automatización tanto en la fase de diseño como en la operativa:

1. Mantener un inventario de activos de software, hardware y redes industriales. Esto es crucial para la seguridad basada en el riesgo.

2. Ejecutar una evaluación detallada de los riesgos para tener un conocimiento concreto de los riesgos de seguridad específicos de su organización. Esto lo ayudará a planificar contramedidas eficaces.

3. Implementar seguridad esencial, como la protección de endpoints, para proteger los dispositivos de sus entornos ICS y TO.

4. Llevar a cabo la detección de amenazas y anomalías, lo que le permitirá identificar las amenazas en una fase temprana y comprender cómo se desarrollan los ataques.

5. Realizar auditorías periódicas de seguridad y cumplimiento para garantizar que las operaciones se desarrollan sin problemas y dentro de los límites normativos.

6. Mejorar el modelado de zonas y conductos para optimizar la arquitectura del entorno de TO. Esto le permitirá mitigar los riesgos y mantener la integridad operativa.

7. Lograr operaciones de seguridad maduras a través de un SOC habilitado para XDR. Esto le permitirá investigar, contener y mitigar rápidamente las amenazas.

8. Aumentar la tolerancia a las fallas y la capacidad de respuesta, para que su empresa pueda resistir y recuperarse de un incidente cibernético sin comprometer la continuidad operativa.

Debido a que prosperamos en la intersección de la seguridad corporativa e industrial, estamos perfectamente posicionados para ayudarlo a lograr una protección sustentable de la infraestructura crítica y corporativa y podemos ayudarlo en cada uno de estos pasos.

Más información en nuestro sitio web:
https://lp.kaspersky.com/global/industrialcyberresilience

Primera edición: febrero de 2025