Una plataforma de seguridad para la sostenibilidad de la empresa industrial y la transformación digital

Plataforma de Kaspersky Industrial CyberSecurity

kaspersky PREPARADOS PARA EL FUTURO

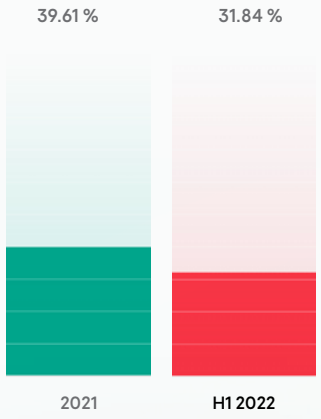
Ataques de malware

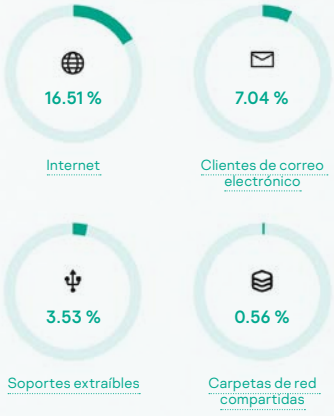
Desde principios de 2022, alrededor del 30 % de los ordenadores relacionados con el ICS han sido atacados por malware, casi un 10 % menos que el año anterior

Kaspersky ICS-CERT, Junio 2022

Más información

Porcentaje de ordenadores ICS en los que se han bloqueado objetos maliciosos desde principios de 2022





Las empresas industriales abordan la ciberseguridad en sus infraestructuras de TI y TO (tecnología operativa) de manera diferente. Muchas empresas ya cuentan con medidas desarrolladas de detección y respuesta en sus redes corporativas, pero cuando se trata de TO suelen confiar en un enfoque anticuado de aislamiento (Air Gapped). Las empresas industriales se están volviendo cada vez más «digitales» e invierten cada vez más en tecnologías inteligentes, nuevos sistemas de automatización y la adopción de información digital. Esto elimina verdaderamente el espacio entre los entornos de TI y TO, el cual se utilizaba para evitar que las ciberamenazas lleguen a los sistemas de control y automatización industrial.

Se puede ser un blanco, pero no la víctima

No hace falta ser un blanco para ser víctima de una brecha accidental en el espacio de aire o de una infección de malware. Una sola unidad flash, un teléfono móvil, un mensaje de correo electrónico de tipo phishing que logren penetrar en el entorno ICS puede afectar seriamente a la actividad principal de una empresa. A su vez, un grupo de piratas informáticos motivado puede penetrar en las redes de TO y causar daños considerables a los equipos, los procesos, la producción, la seguridad y la calidad, o robar información valiosa.

Ciberseguridad esencial para TO

Protección de endpoints

para sistemas autónomos y conectados. Una solución segura y probada debe ayudar a aplicar las políticas de seguridad, apoyar el cumplimiento de la normativa, realizar auditorías de seguridad, gestionar el inventario, ejecutar tareas de parcheo y recoger la telemetría precisa como un sensor de endpoint

Protección de redes

para la visibilidad de las comunicaciones, la detección de amenazas y la gestión de activos. El sistema de análisis del tráfico de red y de detección de intrusos controla la eficacia de la configuración del cortafuegos, la segmentación de la red y el cumplimiento del uso de la red y ayuda a brindar una respuesta manual segura

Programas de formación

para los empleados con el fin de reducir los accidentes y minimizar el factor humano (error humano)

Servicios expertos

dedicados a investigar la infraestructura, llevar a cabo análisis de expertos o mitigar el impacto de un incidente

Reconocimiento global

Frost and Sullivan ha reconocido a Kaspersky con el Premio a la empresa global del año 2020, según el análisis del mercado global de ciberseguridad industrial (TO/ICS)

En **la encuesta mundial anual de VDC**, Kaspersky fue el mejor proveedor en la categoría de ciberseguridad industrial, según las calificaciones generales de más de 250 profesionales cualificados de la comunidad de la automatización industrial

Lo que ofrece Kaspersky

La plataforma de Kaspersky Industrial CyberSecurity (KICS) de tecnologías integradas de forma nativa, junto con nuestra cartera de formación y servicios de expertos abordan todas las necesidades de ciberseguridad de las empresas industriales y los operadores de infraestructuras críticas.

La plataforma es un elemento clave en un ecosistema único para las empresas industriales que incluye:

- Las mejores soluciones corporativas de Kaspersky, que ofrecen una verdadera convergencia TI-TO y los múltiples beneficios del enfoque de un solo proveedor
- Varias soluciones especializadas para la seguridad ciberfísica, la seguridad del IdC industrial, el aprendizaje automático, el espacio de trabajo remoto seguro y muchas otras más que aportan una escalabilidad ágil e ilimitada

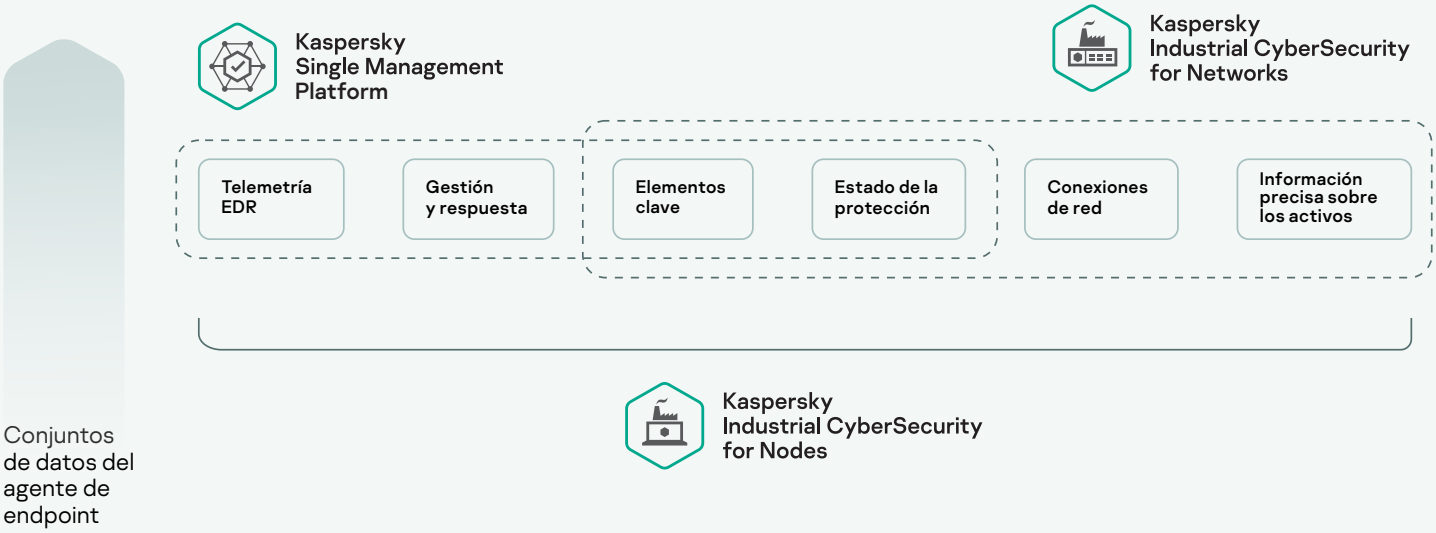
La plataforma de Kaspersky Industrial CyberSecurity es un líder en las siguientes categorías:

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

Cuando se utilizan en conjunto, el usuario ve el panorama general y el contexto más amplio: la cadena de incidentes a nivel de red y endpoints, los parámetros precisos de los activos, la comunicación de la red y los mapas de topología (incluso de los segmentos en los que la duplicación del tráfico aún no está disponible) y demás.

Productos

KICS es una plataforma de ciberseguridad de TO diseñada para la protección integral de los componentes principales del sistema de control y automatización industrial en todos los niveles. 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.



KICS for Nodes es un software de protección, detección y respuesta de endpoints con funciones de auditoría de cumplimiento y sensores de endpoints.

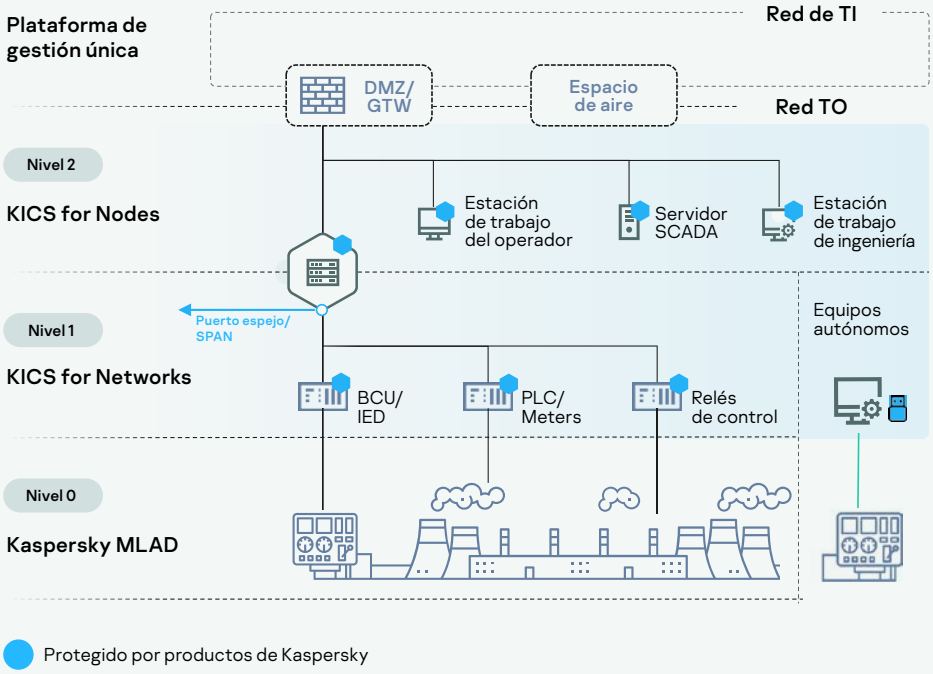
KICS for Networks está diseñado para el análisis, la detección y la respuesta del tráfico de red de TO.

La plataforma de gestión única aporta una interfaz EDR avanzada y una rápida escalabilidad a numerosas ubicaciones.

Funciones adicionales

La solución proporciona numerosas funciones adicionales. La tecnología de **sondeo activo** de la red permite recoger de forma rápida y precisa la topología de la red y la configuración de los activos. La **función de auditoría de endpoints** ayuda a garantizar el cumplimiento de la política de seguridad, incluida la seguridad de la configuración actual, y a controlar los puntos débiles. El método de entrega del **escáner portátil** de KICS for Nodes ayuda a establecer las mejores prácticas de las auditorías de seguridad de los equipos autónomos en el espacio de aire. **El Aprendizaje Automático para la Detección de Anomalías** es un sistema de detección temprana de anomalías en lo más profundo del proceso tecnológico.

Arquitectura de la solución



Características

Detección de activos
Identificación e inventario de activos de TO pasivos

Inspección exhaustiva de paquetes
Análisis en tiempo casi real de la telemetría de procesos técnicos

Control de integridad de la red
Detecta los hosts y flujos de red no autorizados

Sistema de detección de intrusiones
Envía alertas sobre actividades maliciosas en la red

Control de comandos
Inspecciona los comandos en los protocolos industriales

Integración externa
La integración flexible de la API añade capacidades de detección y prevención

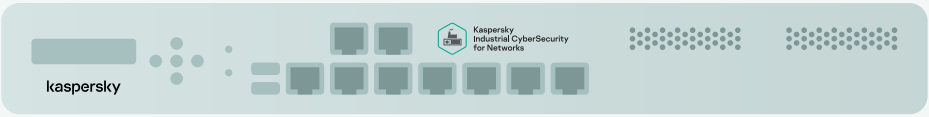
Tecnología Machine learning for anomaly detection (MLAD)
Detecta anomalías físicas o cibernéticas a través de la telemetría y extracción de datos históricos en tiempo real (red neuronal recurrente)

Gestión de vulnerabilidades
Base de datos actualizable de vulnerabilidades en equipos industriales, impulsada por Kaspersky ICS CERT

Kaspersky Industrial CyberSecurity for Networks

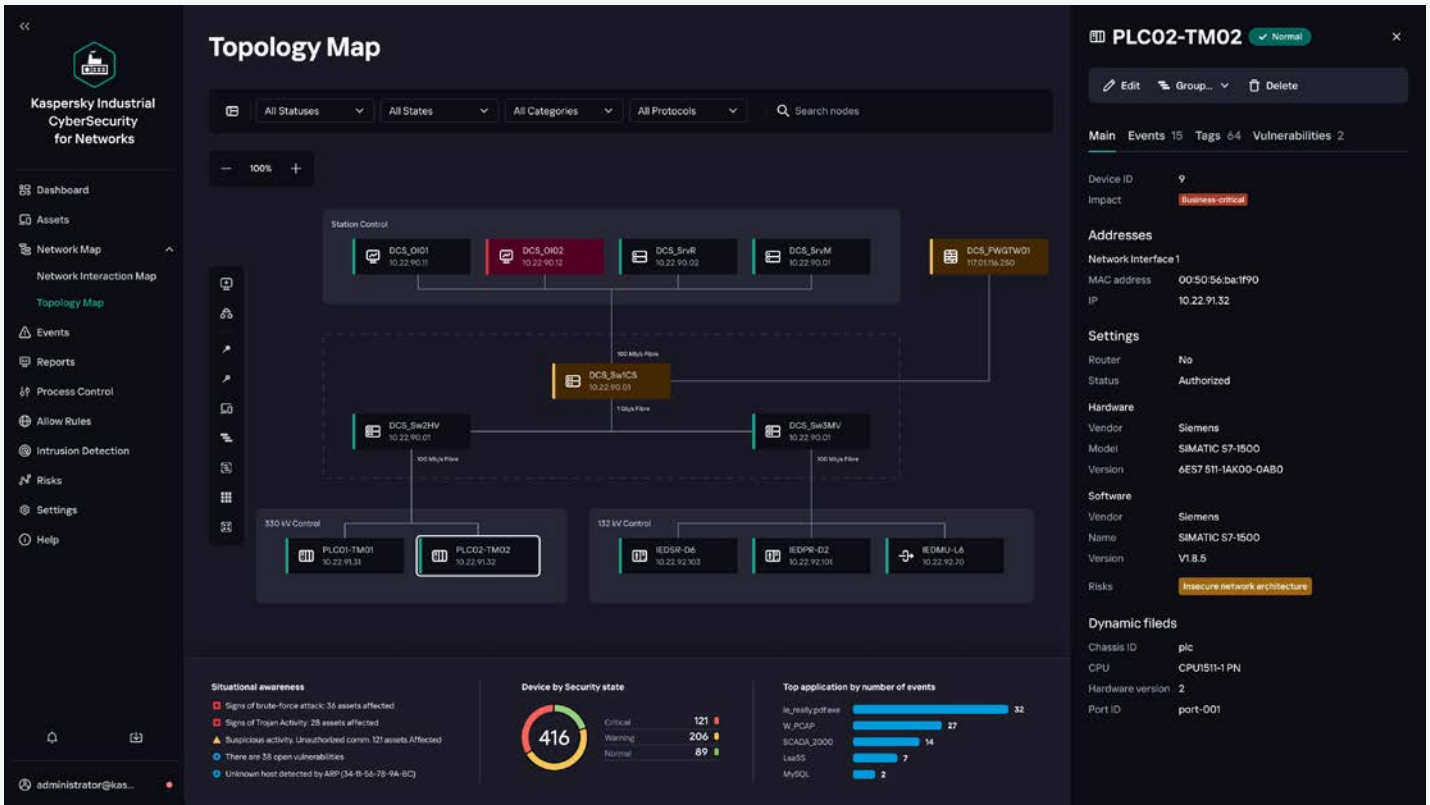
Análisis, detección y respuesta del tráfico de la red de TO. Visibilidad clara de los riesgos con la supervisión pasiva del tráfico, el sondeo activo y los sensores de endpoints.

Detecta anomalías e intrusiones dentro de las redes ICS en sus primeras etapas y garantiza que se tomen las medidas necesarias para evitar cualquier impacto negativo en los procesos industriales.



Solución agnóstica de los aparatos, que puede integrarse de forma rápida y óptima en las prácticas establecidas de abastecimiento, integración y garantía de nuestros clientes.

Interfaz



KICS for Nodes se ha diseñado específicamente para las rigurosas exigencias de los sistemas de automatización distribuidos: entornos mixtos y complicados, tiempo de funcionamiento prolongado, casos de uso autónomos y conectados, instancias atendidas y sin mantenimiento y prioridad de disponibilidad de control a toda costa

Kaspersky Industrial CyberSecurity 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.

Respuesta, detección y protección de endpoint industrial

Protege cada endpoint de un sistema de automatización moderno, digital, gestionado y distribuido. Revela nuevos niveles de visibilidad de los incidentes en el proceso de análisis de la causa raíz. El agente recoge la telemetría de los endpoints 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.

Ventajas

Bajo impacto
en el dispositivo protegido para un mejor rendimiento del sistema

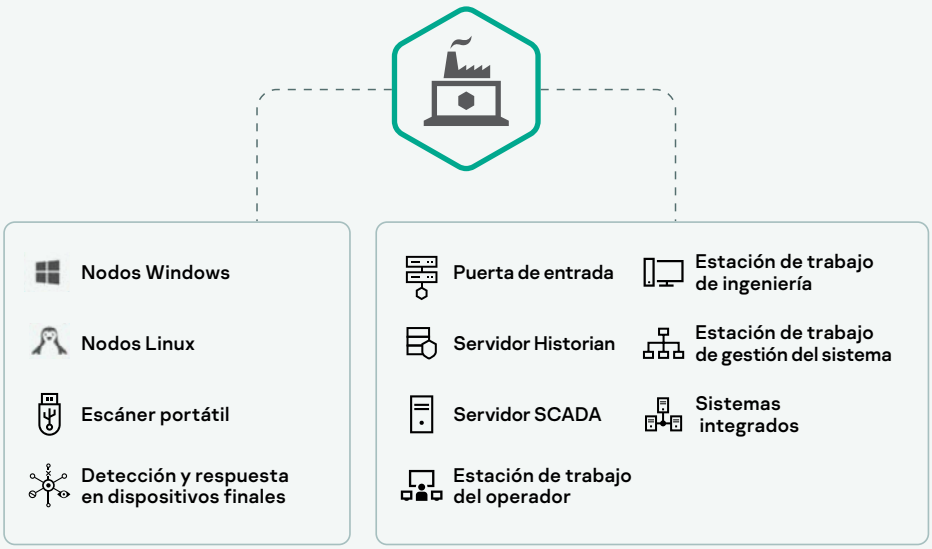
Compatible
con ordenadores de bajo rendimiento de generaciones anteriores, y sistemas de Windows XP SP2 y Windows Server 2003 SP1 y superiores

Ciclo de vida ampliado
hasta 5 años de licencia y soporte técnico extendido

Funcionalidad completa
para todos los sistemas operativos MS Desktop, Server y Windows Embedded

Despliegue modular
Opciones flexibles y ajustes seguros y no intrusivos

Abarca las infraestructuras mixtas
Windows, Linux y variantes portátiles



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. Máximo conocimiento de la situación y visibilidad de TO incluso desde una infraestructura independiente.

Solución sin necesidad de instalación
KICS for Nodes puede activarse en varias unidades flash de escáner portátil adicionales. Esto ayuda a realizar escaneos simultáneos bajo demanda en múltiples máquinas durante las ventanas de mantenimiento, para recolectar los datos de los puntos finales y organizarlos en un práctico informe resumido.

Cumplimiento de la normativa y la política interna
El escáner portátil KICS for Nodes lleva a cabo comprobaciones de conformidad antimalware de los equipos que acceden a un sitio de TO, incluidos los ordenadores de asesores externos. Tiene una huella operativa muy baja y no interfiere con las soluciones de seguridad existentes.

Ventajas

Visión de la situación

Gestión de políticas/ sistemas

Cadena de exterminio y respuesta

Informes y análisis

Integración con SIEM

Integración HMI/MES

Kaspersky Single Management Platform

La plataforma de gestión única es una solución de gestión de la seguridad centralizada para la dirección de la seguridad de toda la infraestructura de TO, con un mapa de todos los activos distribuidos geográficamente enriquecido con eventos, análisis de incidentes y más. Aumenta la eficacia de los equipos de seguridad mixtos de TO y TI. Un lugar donde todos sus controles de seguridad funcionan en buena sintonía, permitiendo una respuesta rápida y precisa.

Servicios expertos

Nuestro conjunto de servicios constituye una parte importante de la cartera de KICS. Ofrecemos un ciclo completo de servicios de seguridad: desde la evaluación de la ciberseguridad hasta la respuesta ante incidentes.

> Su experiencia en el campo de la ciberseguridad ICS, su profesionalidad y la complejidad de su solución en comparación con otros proveedores, nos ha aportado un gran valor y nos ha garantizado un futuro brillante para la estrategia de seguridad de nuestra empresa.
>
> Ondřej Sýkora,
> responsable de C&A,
> Plzeňský Prazdroj

Evaluación de la ciberseguridad industrial

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

> Mediante la práctica y el aprendizaje de los conocimientos del equipo de Kaspersky, hemos aumentado nuestra protección frente a las amenazas a la ciberseguridad.
>
> Yu Tat Ming,
> director general, PacificLight

Threat Intelligence

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

INCIDENT RESPONSE

En el caso de que ocurra un incidente, los expertos de Kaspersky recopilan y analizan los datos y el malware, reconstruyen la línea de tiempo del incidente, determinan las posibles fuentes y la motivación y desarrollan un plan de reparación detallado. El plan incluye recomendaciones para eliminar el malware de los sistemas de los clientes y revertir las acciones maliciosas.

Formación y concienciación

> Kaspersky era la mejor empresa posible para ofrecer formación sobre habilidades profesionales en ciberseguridad industrial para nuestro grupo ICS.
>
> Søren Egede Knudsen,
> Jefe de la Oficina Técnica

Formación en concienciación sobre ciberseguridad industrial

Módulos interactivos de formación presencial o en línea y juegos de ciberseguridad para empleados que trabajan con sistemas informáticos industriales y sus gerentes. Los participantes adquieren una nueva visión del panorama de amenazas y los vectores de ataque dirigidos específicamente a los entornos industriales, pueden analizar casos prácticos y adquieren habilidades de ciberseguridad.

Programas de formación de expertos

Los cursos de formación en Pruebas de Penetración ICS y Forenses Digitales ICS están dirigidos a profesionales de la ciberseguridad. Los participantes adquieren todos los conocimientos avanzados necesarios para llevar a cabo análisis de penetración integrales o análisis forenses digitales en entornos industriales.

Ecosistema de soluciones especializadas

Kaspersky IoT Infrastructure Security

Protege el Internet de las Cosas a nivel de puerta de enlace según el enfoque de Inmunidad Cibernética de Kaspersky

Más información

Kaspersky Antidrone

Protege de drones el espacio aéreo en instalaciones de cualquier tamaño

Más información

Kaspersky Secure Remote Workspace

Infraestructura funcional de cliente ligero con ciberinmunidad

Más información

Kaspersky Security CAD

Modelado digital de sistemas de seguridad de la información para las fases de diseño y funcionamiento

Más información

Kaspersky Machine Learning for Anomaly Detection

Sistema de detección temprana de anomalías en los procesos tecnológicos industriales

Más información

Kaspersky Industrial CyberSecurity

Más información

www.kaspersky.es