













La cuarta revolución industrial ya es toda una realidad. Ante la evolución de la industria de servicios, se crearon sistemas de producción inteligentes que han traído más eficiencia y un aumento de la productividad, debido al seguimiento y análisis de datos en tiempo real, la virtualización (monitorización remota de los procesos de producción), la descentralización de la toma de decisiones y la modularización. La característica más llamativa de esta Industria 4.0 es la digitalización de la información, así como la demanda de investigación y desarrollo que ofrecen oportunidades para profesionales técnicamente cualificados, con formación multidisciplinar para entender y trabajar con una gran variedad de tecnologías disruptivas.



a Industria 4.0 se considera la cuarta revolución industrial, ya que implica todo un cambio en el modelo de producción hacia una realidad más digital. Según el informe Forces of change: Industry 4.0 de Deloitte, esta revolución combina técnicas avanzadas de producción y operaciones con tecnologías inteligentes que se integrarán en las organizaciones, las personas y los activos.

La base de esta cuarta revolución industrial es la transformación digital. La Edición 2020 del informe Global Conectedness Index que publica DHL señala que España se encuentra en el puesto 27 de los países más conectados, mientras que BBVA Research en su informe DiGiX 2020 nos sitúa en la posición número 35 a la hora de estudiar el grado de digitalización del país. Estos datos indican que todavía falta mucho camino por recorrer.

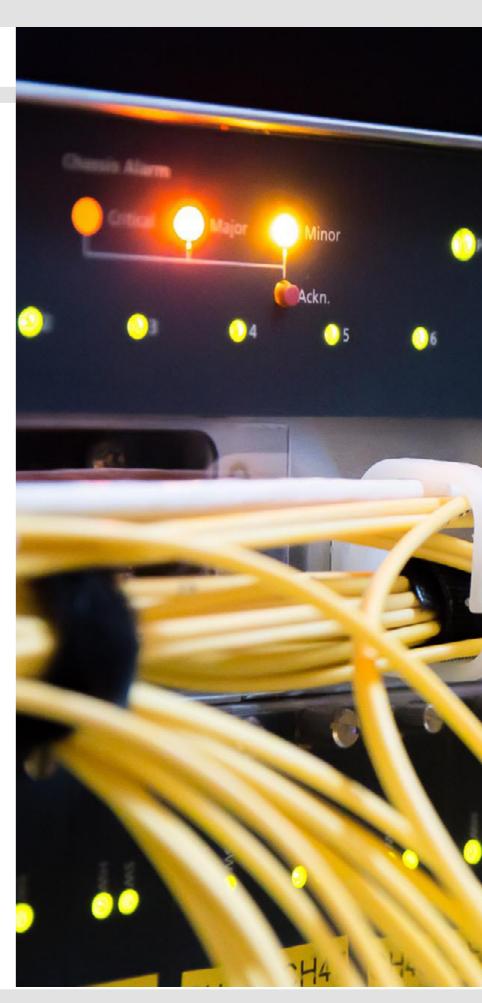
PLAN PARA LA RECUPERACIÓN **DE LA INDUSTRIA**

El impacto de la COVID-19 también fue muy UNA PRIORIDAD grande en el sector industrial español. Es por Deloitte ha realizado una encuesta global a más ello que el <u>Plan de Recuperación, Transforma</u>- de 350 ejecutivos en 11 países de América, Asia ción y Resiliencia que ha puesto en marcha el y Europa, cuyas conclusiones ha destacado el su Gobierno de España para canalizar los fondos informe The Industry 4.0 paradox en el que reproporcionados por Europa con el fin de reparar los daños provocados por la crisis derivada formación digital en el tejido industrial ya es una de la pandemia del coronavirus recoge en su prioridad estratégica para el 94% de los encuesquinta palanca, entre otros aspectos, la moder- tados. A pesar de ello, esto no quiere decir que nización y digitalización del tejido industrial y de esta transformación se vaya a completar de la

la pyme, centrando sus planes para el sector industrial en el componente número 12, titulado Política Industrial España 2030.

El objetivo de este plan es impulsar la modernización y la productividad del ecosistema español de industria-servicios, mediante la digitalización de la cadena de valor, el impulso de la productividad, la competitividad y la mejora de la eficiencia energética de los sectores estratégicos claves en la transición ecológica y la transformación digital. Este informe indica que la industria manufacturera (sin contar el sector energético) representa un 12.3% del Valor Añadido Bruto de la economía española, porcentaje inferior al resto de países que nos rodean. La crisis del coronavirus ha puesto en jaque a la industria española, sector que representa un 83% de la exportación total del país. Así, este plan prevé la puesta en marcha de Proyectos Estratégicos para la Recuperación y la Transformación Económica (PERTEs), los cuales engloban la cadena de valor en un ámbito estratégico.

salta que esta necesidad de abordar una trans-





noche a la mañana, como indican los datos del informe a la hora de hablar de presupuestos destinados a la digitalización: de media las empresas planean invertir en ella el 30% de su presupuesto destinado a TI, mientras que del presupuesto destinado a I+D, solo el 11% iría para trabajar en la digitalización de la compañía.

Everis (ahora NTT Data) habla en su informe Smart Industry 4.0 en España de que la digitalización de la industria se debe tener en cuenta en cuatro áreas: cadena de suministro, fabricación, productos digitales y la propia transformación digital de la empresa. Este estudio resalta que las grandes carencias a la hora de hablar de la cadena de suministro son que no hay una monitorización centralizada y acusan una falta de flujo de información entre proveedores y línea de producción. En cuanto a la fabricación, sería necesario abordar áreas como la secuenciación de la producción, la logística interna y la identificación de los materiales a lo largo de los en una serie de tecnologías que van a apoyar **BLOCKCHAIN** procesos de la planta. A la hora de hablar de los productos digitales, esta necesidad se observa en la inversión planeada para este objetivo: el estudio revela que la mitad de las empresas tenían la previsión de invertir en procesos de creación de productos digitales el año siguiente, mientras que solo un 14% había descartado invertir en el futuro. Asimismo, la industria española está convencida de la necesidad de ir hacia esa digitalización, como indica que solo el 4% había decidido no ponerla en marcha.

La característica más llamativa de esta Industria 4.0 es la digitalización de la información, así como la demanda de investigación y desarrollo que ofrecen oportunidades para profesionales técnicamente cualificados

NUEVAS TECNOLOGÍAS PARA UNA NUEVA REALIDAD INDUSTRIAL

Para hacer realidad esta transformación digital en el sector industrial es necesario apoyarse esta digitalización de procesos. El <u>Informe de</u> La cadena de bloques o Blockchain también es ba que las tecnologías que más se van a utili- ta revolución industrial, ya que permite optizar en el futuro serían la inteligencia artificial, el mizar los procesos industriales, haciendo que no serán solo esas las herramientas que van a En concreto, las áreas en las que más impacto construir el futuro de la industria, ya que otras puede tener esta tecnología, de acuerdo al incomo el Big Data, la ciberseguridad o el cloud forme Tecnologías clave para una Industria 4.0 computing serán fundamentales a la hora de <u>de DigitalES</u>, son la logística y sus procesos asoabordar este cambio. En este sentido, los ana- ciados, la seguridad y la trazabilidad, la reduclistas de Marketsandmarkets han estimado que ción del fraude y el seguimiento en el comercio

el mercado de soluciones para la Industria 4.0 crecerá por encima del 20% anual hasta 2026.

INTELIGENCIA ARTIFICIAL Y ROBÓTICA

Según el estudio La carrera mundial por la IA de IBM, el 82% de las empresas españolas ya está implantando o explorando la incorporación de tecnologías de inteligencia artificial a sus procesos. Esta tecnología permite a las plantas de fabricación escalar en sus modelos de producción sin perjudicar la calidad de los procesos. Los principales ámbitos de uso de la Inteligencia Artificial se podrán observar en la automatización de los procesos industriales, la mejora de las capacidades de la mano de obra y el desarrollo de nuevos productos. Íntimamente ligado a este concepto hallamos la robótica, campo que Gartner espera que crezca en un 19,5% este 2021, hasta llegar a alcanzar los 1.890 miles de millones de dólares.

Tecnologías Disruptivas 2021 de IEBS señala- uno de los elementos que marcarán esta cuar-Blockchain y el Internet de las Cosas (IoT). Pero estos sean más flexibles, eficientes y seguros.



'blockchain' alcanzará los 14.400 millones de en loT va a crecer en un 24% en este 2021. dólares en 2023.

INTERNET OF THINGS

El Internet de las cosas va a ser un factor fundamental en la transformación digital del tejido industrial. Se trata de un ecosistema de sensores, ordenadores integrados y dispositivos inteligentes que se comunican entre sí con el objetivo de recoger y analizar datos del entorno de fabricación. De nuevo el estudio <u>Tecnologías</u> clave para una Industria 4.0 de DigitalES señala que las principales aplicaciones de esta tecnología irían hacia el mantenimiento predictivo, la optimización de la producción, la gestión del inventario, así como la gestión de flotas. Los da-

internacional. <u>IDC</u> estima que el gasto global en tos de <u>IOT Analytics</u> revelan que el gasto global

BIG DATA

Todo lo relacionado con la analítica de datos se La transformación digital no tiene sentido si no va a convertir, si no lo es ya, en una pieza clave se toman las medidas necesarias para proteger de la Industria 4.0. Esta datificación va a impactar en todos los demás elementos tecnológicos que forman parte de esta transformación digital, desde favorecer la automatización hasta optimizar procesos y mejorar la toma de decisiones en base a datos completamente fiables. Los datos se han convertido en el petróleo de hoy, por lo que la gestión y análisis de gran cantidad ción de las ciberamenazas en 2020, el cual revela de estos se ha vuelto clave para poder entender la realidad del negocio. <u>Statista</u> señala las cifras que envuelven a esta tecnología, estimando que

el mercado global del Big Data alcanzará los 103.000 millones de dólares en el año 2027.

CIBERSEGURIDAD

los activos ante el gran abanico de amenazas que se abren al interconectar todos los sistemas de la empresa y la proliferación del Internet de las Cosas. Además, el sector industrial siempre ha sido un blanco muy apetecible para los ciberdelincuentes, como demuestran los datos de Positive Technologies en un estudio sobre la evoluque los ataques a empresas industriales aumentaron un 91% entre 2019 y 2020. Es por ello que la filosofía Zero Trust se está imponiendo en el modelo de ciberseguridad actual, por la cual es necesario desconfiar por defecto de cualquier tipo de acceso a la red para mantenerla segura. **INCIBE-CERT**, en sus predicciones de seguridad industrial 2020-2029 señala varios factores a tener en cuenta, entre los que destacan que crecerá el interés de los ciberdelincuentes por este tipo de entornos, aumentará la superficie de ataque y como consecuencia proliferarán las herramientas para la explotación de vulnerabilidades en entornos industriales.

CLOUD COMPUTING

La nube es uno de los factores clave de toda transformación digital. Según el Enterprise





Cloud Index Report de Nutanix, el 75% del sec- lizar tiradas cortas y permitiendo implementar des como prototipado, mantenimiento y repadel coronavirus ha provocado que aumenten considerablemente sus inversiones en el cloud. Esta tecnología se podrá poner en marcha a través de diferentes modelos, principalmente laaS (Infraestructura como servicio), PaaS (Plataforma como servicio) y SaaS (Software como servicio). <u>INCIBE-CERT</u> señala que la nube híbrida será fundamental para el sector industrial, ya que permite mayor interoperabilidad, escalabilidad, seguridad y una mejor administración y gestión de los activos. En cuanto al crecimiento de este segmento, <u>IDC</u> considera que el gasto global superará el billón de dólares en 2025.

IMPRESIÓN 3D

De acuerdo con un estudio desarrollado por HP y 3dbpm Research, el 75% de los fabricantes españoles espera un fuerte crecimiento de la fabricación aditiva. El mismo estudio revela que el 96% está de acuerdo en que este modelo les va a ayudar a la hora de que sus productos lleguen más rápidamente al mercado y 3 de cada 4 considera que la impresión 3D es útil para ayudar a superar los retos de producción, como la satisfacción de la demanda de nuevos productos y una mayor flexibilidad. Estos datos demuestran que la impresión 3D ha abierto un gran abanico de posibilidades que podrá aprovechar el sector de fabricación, ya que implica un menor coste por pieza, favoreciendo así la posibilidad de rea-

una reducción en las cadenas de suministro y en muchos casos elimina la necesidad de realizar transporte de mercancías físicas y de mantener inventarios, al poder fabricar las piezas necesarias directamente y en poco tiempo.

REALIDAD AUMENTADA

La realidad aumentada permite incorporar elementos visuales a la propia realidad y visualizarlos a través de dispositivos como gafas inteligentes o un smartphone. Para Oasys, esta tecnología

tor industrial y de fabricación señala que la crisis mayor personalización. Además, la fabricación ración, transmisión en video, muestra de datos se vuelve mucho más veloz, ya que es posible en vivo e integración con el resto de sistemas. pasar del diseño a la producción en pocas horas. Además implica una serie de beneficios para el Por otro lado, la impresión 3D implica también sector, como facilitar la formación de nuevos profesionales, previsualizar las funcionalidades de cualquier herramienta facilitando su uso, un etiquetado de los sistemas para identificarlos en cualquier momento y facilitan la accesibilidad. Según Research and Markets, el mercado global de realidad aumentada llegará hasta los 88.400 millones de dólares en 2026.

> Además, otras tecnologías como la simulación, los sistemas de Integración vertical y horizontal, el gemelo digital o los drones también van a colaborar a la hora de hacer realidad la va a permitir desarrollar distintas funcionalida- transformación digital en el sector industrial.





DEMANDA DE PROFESIONALES CUALIFICADOS

La implementación de todas estas novedades va a requerir de profesionales cualificados que sean capaces de manejar todos estos nuevos procesos, y que cuenten con una formación multidisciplinar para entender y trabajar con toda esta gran variedad de nuevas tecnologías. Según los datos del Informe de Tecnologías Disruptivas 2021 de IEBS, solo el 3,2% de los profesionales cualificados son expertos en estas nuevas tecnologías, lo que implica grandes oportunidades laborales en estos sectores. De hecho, el informe de IEBS también señala que 9 de cada 10 profesionales encuestados tiene la intención de formarse en alguna de estas tecnologías para mejorar su recorrido profesional. Sin duda, tanto las necesidades en el sector industrial como las tecnologías para solventarlas ya están sobre la mesa, ahora lo necesario es contar con profesionales técnicamente cualificados que sean capaces de hacer realidad esta transformación digital en el sector industrial.



MÁS INFORMACIÓN

- Informe Forces of change:
 Industry 4.0 de Deloitte
- Informe Global Conectedness Index de DHL
- Informe DiGiX 2020 de BBVA Research
- Plan de Recuperación, Transformación y Resiliencia del Gobierno de España
- Política Industrial España 2030 del Gobierno de España
- Informe The Industry 4.0 paradox de Deloitte
- Informe Smart Industry 4.0 en España de Everis
 (ahora NTT Data)
- Informe de Tecnologías Disruptivas 2021 de IEBS
- Informe sobre la evolución del mercado de tecnología para Industria 4.0 de Marketsandmarkets
- Estudio La carrera mundial por la IA de IBM
- Datos sobre ingresos mundiales del software de automatización de procesos robóticos (RPA) de Gartner

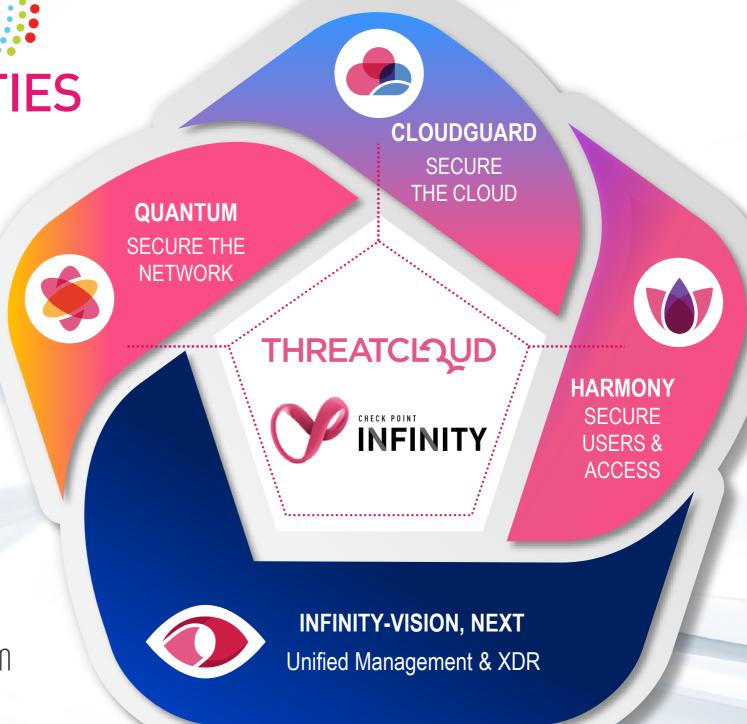
- Informe Tecnologías clave para una Industria
 4.0 de DigitalES
- Datos sobre gasto global en Blockchain de IDC
- Datos sobre inversión en IoT de IOT Analytics
- Previsión de ingresos en el mercado global de Big Data de 2011 a 2027 de Statista
- Estudio sobre la evolución de las ciberamenazas en 2020 de Positive Technologies
- Predicciones de seguridad industrial 2020-2029 de INCIBE-CERT
- Enterprise Cloud Index Report de Nutanix
- Tecnología cloud en entornos industriales de INCIBE-CERT
- Datos de gasto global en cloud computing de IDC
- Estudio sobre fabricación aditiva de HP y

 3dbpm Research
- Realidad aumentada en la industria. Funciones y beneficios. Oasys
- Global Augmented Reality Market Report 2021
 de Research and Markets



NEW WORLD
NEW OPPORTUNITIES

2021



MÁS INFORMACIÓN:

www.checkpoint.com/es
info_iberia@checkpoint.com

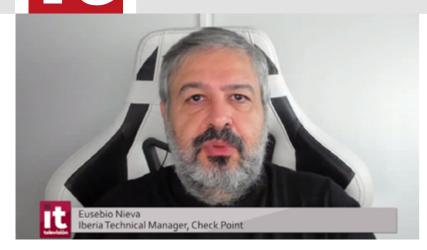


Los retos de la Industria 4.0

La cuarta revolución industrial, también llamada Industria 4.0, ha supuesto un gran avance para el sector, que gracias a las nuevas tecnologías y a la conectividad va a ser capaz de recoger datos con los que realizar una gran optimización de procesos e implantar soluciones y herramientas que mejoren sus rendimientos a todos los niveles. Pero el sector no debe olvidar un aspecto fundamental: la seguridad. Esta conectividad amplía enormemente el perímetro de la red, y con él las amenazas a las que se enfrenta.

a relevancia de las tecnologías IoT, así como las ventajas que ofrecen en nuestro día a día, es una realidad. Sin embargo también presentan varios inconvenientes que hay que tener en cuenta. La información que manejan estos dispositivos es cada vez más sensible o relevante, por lo que mantenerlos seguros resulta de vital importancia. Además, el crecimiento exponencial del número de estos dispositivos supone un incremento en el número de nuevas vulnerabilidades que les afectan. Por ello, ¿cuáles son los principales retos a los que se debe enfrentar el sector de la industria y la fabricación en esta cuarta revolución industrial? Para analizar el papel de la seguridad como elemento habilitador para que la industria 4.0 sea operativa; cuáles son los principales aspectos referentes a la ciberseguridad que hay que tener en cuenta en los entornos IoT e industria 4.0; cuáles son los principales tipos de ataque a los que se enfrenta este sector; cuáles son las principales medidas de prevención y cuáles son las principa-





"Nadie se debería plantear exponer datos internos o de sus usuarios, sin dotarlos del apropiado nivel de seguridad"

EUSEBIO NIEVA

les áreas de mejora, hemos contado en esta Mesa Redonda IT con la participación de Eusebio Nieva, Iberia Technical Manager de Check Point; Carlos Tortosa, Director de Grandes Cuentas de Eset; Pedro Viana, Presales Manager Iberia de Kaspersky; Enrique Martín, Head of Business Development & Innovation Iberia de Samsung; Borja Pérez, Iberia Country Manager de Stormshield; y Jesús Gayoso, System Engineer de Trend Micro.

SEGURIDAD COMO HABILITADOR DE LA INDUSTRA 4.0

Cualquier tipo de negocio que esté conectado a internet tiene que pasar obligatoriamente por

un filtro de seguridad. Para Eusebio Nieva a día de hoy ya nadie debería plantearse hacer negocios en internet sin seguridad por la gran cantidad de amenazas que existen, la dinamicidad de esas amenazas y porque precisamente la seguridad es un habilitador para que esos negocios se puedan realizar de manera correcta. "De la misma forma que ningún banco se plantea tener oficinas sin tener cierto nivel de seguridad, nadie se debería plantear exponer datos internos o de sus usuarios, servicios internos y servicios de sus usuarios en internet sin dotarlos del apropiado nivel de seguridad".

De la misma forma opina Pedro Viana cuando indica que la ciberseguridad en la industria 4.0 es habilitadora. Para el portavoz en la industria 4.0 siempre estaremos hablando de información, hiperconvergencia y seguridad, no solamente a nivel de dispositivo, sino que como indica también "es necesario garantizar que esa información que está almacenada para la toma de decisiones y también para el correcto funcionamiento del proceso productivo esté lo más garantizada posible".

También de acuerdo se muestra Borja Pérez, ASPECTOS A TENER EN CUENTA EN CUANTO A señalando que hasta ahora la disponibilidad ha sido fundamental en el diseño de las redes OT. A la hora de hablar de ciberseguridad en la indus-"Ha habido ciertos momentos donde los responsables de procesos, los responsables de redes operacionales veían con cierto resquemor la ciberseguridad, porque veían un punto de posibles



"El especialista en ciberseguridad debería participar desde el diseño de la arquitectura hasta situaciones donde nos encontramos con plantas industriales realmente con recursos muy limitados"

CARLOS TORTOSA

posible o es muy probable que se puedan tener problemas de disponibilidad".

CIBERSEGURIDAD

tria 4.0 hay que tener en cuenta ciertos aspectos importantes, tanto al hablar de su funcionamiento como en sus comunicaciones.

Teniendo en cuenta que cualquier tecnología ha fallos de disponibilidad. Esto está cambiando. Ya de considerar en el propio diseño los aspectos funla percepción es que sin esa ciberseguridad es damentales de la ciberseguridad, Carlos Tortosa



"Es necesario que la información almacenada para la toma de decisiones y el correcto funcionamiento del proceso productivo esté lo más garantizada posible"

PEDRO VIANA

indica que se han de aplicar también estos criterios cuando hablamos de entornos industriales. "Es necesario proteger las conexiones internas, tanto para evitar posibles ataques externos como para evitar que los dispositivos dentro de la planta industrial sean la puerta de entrada de los atacantes para después acceder a dispositivos con información privilegiada, con una mayor capacidad de almacenamiento, para poder llegar a la información que el atacante está buscando. También se ha de adecuadamente, tanto a nivel de sistemas como proteger en la medida de lo posible la apertura a nivel de comunicaciones.

de procesos que sean sospechosos y que puedan convertirse finalmente en una amenaza real".

Para Enrique Martín, desde el punto de vista del dispositivo hay una serie de consideraciones importantes. "Al fin y al cabo el dispositivo almacena información, desde la información que pueda tener un directivo en un smartphone hasta un elemento conectado que tenga la cadena de producción que tenga cierta información. Al final cada uno tiene distinta información pero seguramente en gran parte de ellos es importante que esa información esté securizada, cifrada y que sea complicado acceder a ella". También es necesario tener en cuenta la seguridad de las comunicaciones a través de mecanismos de cifrado y de securización. Además, dado que lo normal es que las empresas cada vez se dirijan más hacia el cloud, es importante la autenticación. Por último, es necesario que el software esté actualizado.

Por su parte, Jesús Gayoso indica que lo primordial es tener visibilidad para tener un control de qué es lo que está pasando en la planta, cómo está llevándose a cabo ese proceso de producción. "Hay que tener un control de la ejecución de los procesos de un servidor o de un HMI o de un controlador en cuanto a qué se puede ejecutar en esa máquina". A nivel de comunicaciones es muy importante tener segmentación y tener un control del protocolo. Es muy importante tener control de que se estén ejecutando los procesos



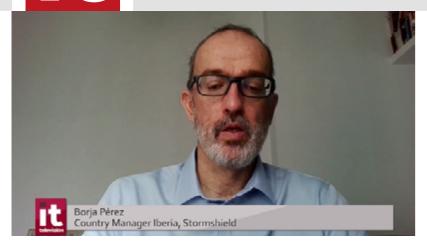
"En un mundo en el que cada día aparecen nuevas funcionalidades, es fundamental tener capacidad de evolucionar"

ENRIQUE MARTÍN

PRINCIPALES TIPOS DE ATAQUE

No cabe duda de que el auge de los dispositivos IoT y su interconexión les convierte en un objetivo perfecto y diario para los ciberdelincuentes. ¿Cuáles son los principales tipos de ataque a los que se enfrenta este sector? ¿Tienen particularidades respecto a otros sectores?

En la opinión de Pedro Viana, los principales tipos de ataques dentro de la vertiente del IoT casi siempre suelen ser ataques de fuerza bruta contra dispositivos que están directamente conectados a internet, que no tienen ningún tipo de supervisión o de protección a nivel perimetral. "Por supuesto son software y dispositivos que tienen una capacidad muy limitada, consecuentemente el proceso de actualización de ese firmware o de ese sistema operativo no sigue un patrón o no si-



"Ha habido momentos donde los responsables de redes operacionales, veían con resquemor la ciberseguridad, porque veían un punto de posibles fallos de disponibilidad"

gue un ritmo adecuado". Además, los ciberdelincuentes a través de estos ataques pueden utilizar estos dispositivos para realizar ataques a otras corporaciones, o para tener acceso a cualquier red dentro de la infraestructura.

Jesús Gayoso señala que es muy importante disponer de dispositivos IPS, de sondas de red que tengan análisis de comportamiento y ver las anomalías que ese están produciendo a nivel de red en cuanto a ejecución de protocolos, a una explotación de una vulnerabilidad y una propagación

en la misma red. "Yo me he llegado a encontrar en varias plantas Windows NT o Windows 2000, que ya es todavía más obsoleto. Es bastante más difícil de proteger un sistema legacy llegado a ese punto, porque ni siguiera la arquitectura del sistema operativo es la misma que en la que trabajamos a día de hoy", comenta a la hora de hablar de la importancia de contar con sistemas actualizados. El portavoz incide en que es muy importante tener visibilidad a nivel de red, porque en cuanto exista un compromiso en una de las máquinas, en cuanto vaya a haber una propagación, se va a detectar y a partir de ahí se va a poder actuar en consecuencia.

Por su parte, Eusebio Nieva subraya que cualquiera de estas empresas es susceptible de sufrir un ataque a través de los métodos tradicionales y además por métodos más específicos en cualquier entorno industrial. "Tienen un espectro de BORJA PÉREZ vulnerabilidades mucho mayor precisamente porque tienen una peculiaridad. Y además, como se están moviendo muy deprisa hacia una transformación digital en la cual los dispositivos están cambiando, la forma de utilizarlos, la conectividad, dónde residen los servicios...". En su opinión todo esto está exponiendo de manera mucho más importante a estas empresas precisamente porque tienen las mismas amenazas que cualquier empresa tradicional y además un riesgo adicional por sus propias características. Por ello tienen que abordar la seguridad desde esos dos puntos de vista.



"La mayoría tienen poca visibilidad, poca concienciación, mucha heterogeneidad en cuanto a sistemas, no tienen un control de la red, no están segmentadas las redes..."

JESÚS GAYOSO

En el resumen que hace Carlos Tortosa parte de la base de "los ataques de fuerza bruta, de la denegación de servicio, control y mando de los dispositivos, y que esto se convierte en una puerta de acceso para poder ir a parar a cualquier otro dispositivo dentro de la red". Para él lo que se puede hacer es proteger usuarios, proteger accesos, tener visibilidad de los procesos y poner en marcha procesos de actualización. En cuanto a la concienciación, recalca que hay que tener clarísimo que desde la base de la educación de los niños más pequeños hasta situaciones como estas donde el entorno industrial tiene mucha complejidad y tiene una serie de puertas abiertas donde



el atacante puede elegir por dónde quiere entrar, es necesario concienciar al usuario e intentar que se tomen las medidas oportunas.

MEDIDAS DE PREVENCIÓN

Como se ha ido comentando, la prevención es fundamental en el entorno de la industria 4.0, pero, ¿cuáles son las principales medidas de prevención? ¿Estas medidas tienen que tener algún aspecto diferencial respecto a otros entornos?

En este sentido, Enrique Martín destaca que es necesario disponer de equipamiento y tecnolo-

gía actualizada. "En un mundo en el que cada día aparecen nuevas funcionalidades es fundamental tener el software y los sistemas con capacidad de evolucionar". Esos equipos almacenan cada vez más información, por lo que hay que tener capacidad de poder cifrarla y tenerla securizada.

Al hablar del tema de las actualizaciones, Bor- mantenimiento, para hacer actualizaciones, etc., ja Pérez apunta que no es algo tan sencillo. "Las medidas tienen que ser distintas porque lo que momento muy determinado del año. prima en la industria es la disponibilidad". Es importante entender cuáles son los procesos industriales y cuándo se puede parar una planta, por



ya que suele ser una ventana muy estrecha en un

Para Carlos Tortosa no hay que olvidar el factor conocimiento. "Hay que poner en valor también el valor del profesional, en este caso el especialista en ciberseguridad, que debería participar desde el diseño de la arquitectura hasta en situaciones donde nos encontramos con plantas industriales realmente con recursos muy limitados, obsoletos y demás, y que además buscan una interconexión".

Por su parte, Pedro Viana hace hincapié en la curva de madurez del cliente. "Hay clientes que todavía están en un proceso de transferencia de conocimiento de ciberseguridad de la parte de IT, que está más que consolidado, traspasar eso a la parte de OT". Además de la prevención, es necesario señalar la importancia de la reacción, que la industria sepa qué hacer cuando ocurre un incidente.

Áreas de mejora

Es evidente que aún queda mucho por hacer. ¿Cuáles son las principales áreas de mejora que se deben abordar para cerrar ese gap existente? ¿Sigue siendo necesaria en estos entornos la sensibilización y la concienciación?

Como indica Borja Pérez, la sensibilización y la concienciación son claves. "Lo que vemos es que se ha avanzado un montón, en poco tiempo hay un aumento de la concienciación importante". Se ven más consultorías y más auditorías de red para saber qué se está haciendo bien o qué se debe

mejorar, pero aún queda camino рог гесоггег.

Según Jesús Gayoso, "la mayoría de entornos pecan de lo mismo, tienen poca visibilidad, poca concienciación, mucha heterogeneidad en cuanto a sistemas, no tienen un control de la red, no están segmentadas las redes...". Son todos estos los factores que se deben abordar, a través de por ejemplo análisis de telemetría multivector.

Eusebio Nieva se muestra de acuerdo al señalar que aún queda mucho por avanzar en algunos aspectos. Pero gracias a las nuevas

normativas y a los ataques que cada vez más se están produciendo "cada día hay más concienciación, cada día hay más percepción de que la seguridad tiene que ser tomada como algo fundamental".

Para finalizar, Enrique Martín comenta que "ha tenido que venir la pandemia para que todos nos sensibilicemos con la seguridad". El portavoz comenta que sigue siendo necesario seguir concienciando y seguir trabajando, porque aún quedan empresas que no son conscientes de la importancia que tiene la seguridad en su negocio.





Mesa redonda IT- Industria 4.0

ÓSCAR LAGE, HEAD OF CYBER SECURITY & BLOCKCHAIN @ TECNALIA RESEARCH & INNOVATION

"La gran asignatura pendiente es poder compartir y explotar de forma segura el dato industrial"

La relevancia de las tecnologías IoT, así como las ventajas que ofrecen en nuestro día a día, es una realidad. Sin embargo, también presentan varios inconvenientes a tener en cuenta. Con Óscar Lage, Head of Cyber Security & Blockchain @ TECNALIA Research & Innovation, repasamos algunos de ellos.

La información que manejan estos dis- Nos podemos encontrar con diferentes nivenos encontramos hoy en día?

(IIoT), hablando de la Industria 4.0, es capaz de dola a cloud, y explotando dicha información capturar una grandísima cantidad de información con técnicas de inteligencia artificial. de los procesos industriales, pero a día de hoy Pero la gran asignatura pendiente es poder mucha de esa información todavía no está sien- compartir y explotar de forma segura el dato indo almacenada y explotada. En muchos casos, la dustrial con terceros de cara a poder exprimir el falta de explotación de dicha información se debe potencial de la Inteligencia Artificial en la Industria. precisamente al miedo a que dicha información Las empresas conocen el potencial de este tipo de sensible para el negocio pueda ser filtrada a otras acciones, pero, a pesar de ello, todavía no existe empresas competidoras.

positivos es cada vez más sensible o re- les de madurez digital en la empresa industrial, ■ levante, por lo que mantenerlos seguros desde la que ya ha adoptado loT pero que no resulta de vital importancia. ¿En qué estadio está almacenando ni explotando dicha información, hasta las empresas que están captu-La loT industrial, o Industrial Internet of Things rando toda la información disponible, subién-

un marco de confianza para compartir los datos





LOS RETOS DE LA INDUSTRIA 4.0 / ENTREVISTA

con terceros. Esperamos que los últimos avances que está realizando la comunidad científica en técnicas como criptografía homomórfica o computación multiparte, permitan generar la confianza necesaria para la creación de los tan ansiados espacios de datos industriales promovidos por iniciativas como GAIA-X o IDSA.

La tendencia de crecimiento de los dispositivos IoT es exponencial y se estima que en 2025 estos sean más de 21.000 millones. El crecimiento de estos dispositivos supone también un incremento en el número de nuevas vulnerabilidades que les afectan. ¿Cuáles son en su opinión? La principal problemática de IoT en general es precisamente el no contemplar la ciberseguridad desde el diseño. Es muy habitual diseñar, pilotar, y comenzar la explotación de un proyecto industrial, sin que nadie se haya preguntado por los requisitos y necesidades de ciberseguridad del proyecto. Debemos de implantar una cultura de seguridad desde el diseño tanto en los fabricande despliegue de infraestructura.

A pesar de que poco a poco la seguridad va cobrando una mayor relevancia en el ámbito industrial, todavía hoy en día su protagonismo es insuficiente. Muchísimos dispositivos industriales han sido diseñados únicamente bajo requisitos funcionales, incluso en muchos casos la digitalización de un equipamiento industrial se ha focalizado en "digitalizar" los protocolos analógicos con los que

"La gran asignatura pendiente es poder compartir y explotar de forma segura el dato industrial con terceros de cara a poder exprimir el potencial de la Inteligencia Artificial en la Industria"

funcionaban estos dispositivos, pasando a Ether- sido diseñados para convivir con la infraestructunet comunicaciones de tipo serie diseñadas en los ra TI (Tecnologías de la Información), por lo que ochenta sin tener en cuenta las implicaciones de un simple escaneo de puertos, que es muy habiciberseguridad. La Industria 4.0 ha traído la conexión de estos sistemas industriales de forma masiva, y como resultado podemos ver en rastreadores como shodan.io cómo cada vez hay más dispositivos IoT conectados directamente a internet, con protocolos no seguros y/o sin configurar ningún tipo de ciberseguridad en sus despliegues.

El auge de los dispositivos IoT y su gran interconexión les convierte en el objetivo perfecto para los ciberdelincuentes. ¿Cuáles son los principales vectores de ataque?

Podríamos decir que en la última década la tes de equipamiento IoT, como en los proyectos tendencia ha sido maximizar la conectividad de dichos dispositivos para la explotación de datos, sin preocuparse por la seguridad, o sin un conocimiento sobre los riesgos de estas conductas. Esto desafortunadamente va cambiando por culpa de los sustos que las empresas industriales están sufriendo en los últimos años debido en parte a estas conductas.

tual en una red TI, puede suponer una parada en la red industrial.

Los protocolos de las redes industriales, además, pueden no incorporar ningún tipo de ciberseguridad. En el mejor de los casos estos dispositivos admiten las versiones más novedosas de esos protocolos industriales que incorporan protecciones específicas de ciberseguridad, pero desafortunadamente es habitual que éstas no se hayan activado para maximizar la "compatibilidad" con equipamiento legado existente en la red, o simplemente para "facilitar" el despliegue.

En muchos casos estas redes de operaciones, además, no están segmentadas ni cuentan con elementos de protección suficientes, con lo que es habitual que cualquier malware pueda propagarse de forma rápida por toda la infraestructura.

Por si fuera poco, es habitual que los dispositivos industriales estén operados por ordenadores que no han sido actualizados en muchos meses o años, y, por lo tanto, pueden existir diferentes vul-Esta situación se ve agravada debido a que la nerabilidades conocidas para su sistema operatimayoría de los dispositivos industriales no han vo que no han sido parcheadas. Estas situaciones



LOS RETOS DE LA INDUSTRIA 4.0 / ENTREVISTA

a veces son provocadas por falta de actualizaciones del fabricante, y en otros muchos casos por parte del propio operador de la infraestructura cuyo objetivo principal es maximizar la disponibilidad de la red y que ve en estas actualizaciones un riesgo de disponibilidad. Todo ello nos lleva a un riesgo menos inmediato, pero con efectos desastrosos, como es operar una red con dispositivos industriales que muestran decenas de vulnerabilidades conocidas.

Esta situación, en muchos casos, se está aprovechando por operadores de botnets que comprometen cada vez más dispositivos IoT conectados para ponerlos a su servicio.

Los nuevos procesos en la Industria 4.0 solo pueden materializarse aprovechando las oportunidades que brindan las nuevas tecnologías. Se introducen las arquitecturas en la nube, IA, Big Data o la virtualización. ¿Qué nivel de implantación tienen ya estas tecnologías y cómo complican la seguridad?

Existe hoy en día una gran adopción en las grandes mucho mayor que en la época pre-COVID. y medianas empresas, que están viendo el potencial de la explotación del dato, así como la flexibilidad que les ofrece la nube o la virtualización. El peligro de la adopción de estas tecnologías es que, en muchos casos, tal y como advertíamos, es una adopción centrada exclusivamente en el ámbito funcional, sin tener en cuenta la ciberseguridad.

En la mayoría de los casos en los que no se tiene en cuenta la ciberseguridad en el despliegue

de un proyecto de transformación digital, nos encontramos como consecuencia decenas o centenares de equipamientos industriales de una empresa visibles a través de internet, con los riesgos que ello supone.

La situación provocada por la COVID-19 ha originado un incremento importante del número de ataques a empresas, y los modelos Industria 4.0, no han sido ajenos a ello. ¿Cuáles has sido los sectores más afectados y de qué manera? Indudablemente el foco durante la pandemia se ha centrado en la industria farmacéutica debido al gran valor de sus activos, las vacunas COVID-19. A nivel general lo que se ha visto es un gran incremento del phishing y ransomware, aprovechando el teletrabajo de muchos de los profesionales del sector industrial. No obstante, la industria, en general, no ha sido un ámbito en el que el teletrabajo haya sido masivo debido a las restricciones físicas y la naturaleza del sector, por lo que tampoco diría que estos ataques hayan tenido una efectividad

¿Hacia dónde debe evolucionar la Industria 4.0 y cuáles son los aspectos más críticos de mejora desde el punto de vista de la Ciberseguridad? La industria debe adoptar la seguridad por diseño tanto en la fabricación de equipamiento industrial como en los despliegues de infraestructura. Es donde creo que se debería poner el foco durante los próximos años.



Precisamente si queremos maximizar la resiliencia de la industria, uno de los tres pilares fundamentales del nuevo paradigma de la Industria 5.0, debemos adoptar tanto patrones de Security by Design, como medidas de seguridad en la cadena de suministro.

Por otro lado, debemos de hacer un especial hincapié en los robots industriales, que ya están saliendo de las jaulas en las que los hemos contemplado durante los últimos años por motivos de seguridad física (safety). Estos robots van a trabajar y cooperar directamente con humanos en entornos de coworking, lo que supone un riesgo aun mayor ya que estos dispositivos en caso de fallo podrán causar daños personales a los trabaiadores. ■

OSCAR LAGE

es Responsable de Ciberseguridad de Tecnalia, conferenciante, profesor y líder del primer laboratorio industrial de blockchain de Europa.





Ciberseguridad orientada al futuro



Kaspersky Industrial CyberSecurity



Avanzar en la digitalización de una forma segura, el mayor reto para la Industria 4.0

DAVID GALDRÁN. **Security Engineer Team** Leader, Major Accounts, **Check Point Software**



ste año 2021 la industria ha "comenzado la vuelta a la normalidad" tras un 2020 en el que, debido a la pandemia, muchas plantas y empresas se han visto obligadas a parar su producción. La situación ha sido complicada para todo el sector y, aun ahora, están comenzando a levantar cabeza. Desde el punto de vista de la ciberseguridad, la situación vivida los últimos meses ha causado que los proyectos asociados a la misma se hayan visto paralizados durante todo el 2020 para relanzarse en 2021 lo que, aunque en un principio ha retasado un poco las cosas, actualmente está suponiendo un avance en ese proceso de digitalización e hiperconectividad que va de la mano del paradigma Industria 4.0.

A pesar de los distintos avances y puestas a punto de este sector, aún quedan bastantes puntos a desarrollar en todo lo relacionado con la ciberseguridad, que sigue sin formar parte de su ADN corporativo. Todos ellos son tremendamente relevantes para realizar una digitalización y tran-

Aunque se está haciendo un esfuerzo titánico en la creación de grupos de trabajo y se ha avanzado mucho en la innovación de planes de ciberseguridad industrial, nos seguimos encontrando, aunque cada vez menos, con escollos debidos a la falta de concienciación en el campo de la ciberseguridad OT.

Industria 4.0 es sinónimo de Transformación DE CIBERSEGURIDAD INDUSTRIAL Digital de la cadena de producción, lo que implica que las amenazas más comunes que afectan PARA LA INDUSTRIA 4.0. a este sector tienen relación con el equipamiento productivo, ya que no está pensado para que la comunicación IP tenga que enviar información a sistemas que, a veces, se encuentran en zonas con conexión a internet (eso sino se comunica el equipo directamente con un activo que esté presente en internet o similar...). Por ello, en muchas ocasiones se ha dado visibilidad a la cadena de producción en el exterior lo que ha hecho que amenazas como el ransomware estén cada vez más presentes en el mundo industrial. Derivado de esta nuesición al modelo Industria 4.0 de forma segura. va situación, se puede dar el caso de que algún como por ejemplo las utilities, que hoy en día aún

ciberdelincuente llegue a secuestrar una cadena de producción y pedir dinero a cambio de la liberación, o el robo de la propiedad intelectual como, por ejemplo, la fórmula de un químico para hacer un producto igual a menor precio.

LA AUSENCIA DE UNA ÚNICA NORMA **ES UNO DE LOS PRINCIPALES PROBLEMAS**

Por el lado contrario, nos encontramos con que los sectores de la Industria 4.0 más protegidos son las denominadas Infraestructuras Críticas. Seguramente, debido a la presión que ha ejercido la administración y la Unión Europea para el establecimiento de un plan de ciberseguridad, los operadores críticos ya cuentan con un uno para el ámbito industrial y están actualmente implantando medidas de control. Está claro que aquellos sectores que cuentan con operadores críticos entre sus filas son los más avanzados. En cambio, hay otros,



LOS RETOS DE LA INDUSTRIA 4.0 / OPINIÓN

están diseñando un plan de ciberseguridad industrial a la vez que avanza la digitalización. Lo que hay que tener claro es que, dentro del mismo sector, nos podemos encontrar con empresas con un nivel de madurez muy alto, mientras otras apenas han comenzado su transformación.

La ausencia de una única norma de ciberseguridad que se pueda llegar a aplicar a toda la industria no ayuda en esta tarea. Esta falta de estandarización es la que está haciendo que,

presencia "mundial" tengan que definir su propia norma como una mezcla de ambas.

somware y robo de información a las empresas de la Industria 4.0 van a crecer exponencialmente acompañados de la evolución y avance de la transformación digital de sus distintos sectores. Los problemas que puede conllevar el no instalar las medidas necesarias de protección de softwa- rrentes amenazas.

determinadas secciones industriales que tienen re en los sistemas OT pueden ir mucho más allá de lo que las empresas puedan llegar a imaginar. La medida de solventar un ataque siempre va a A lo largo del próximo 2022 los ataques de ran- estar ahí, pero la mejor estrategia, sin duda, pasa por implementar un plan de prevención para evitar cualquier tipo de riesgo antes de que suceda. Para ello, es imprescindible avanzar en la digitalización de una forma segura con el objetivo de evitar estar expuestos a las cada vez más recu-

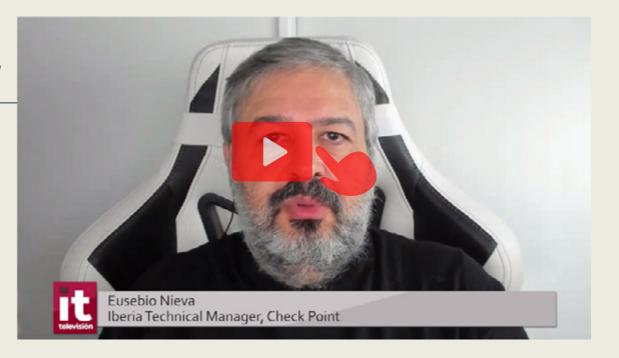
EUSEBIO NIEVA, IBERIA TECHNICAL MANAGER DE CHECK POINT

Adaptar la seguridad a los peligros de hoy

Desde que el uso de los dispositivos IoT en el mundo de la industria 4.0 se ha extendido y su despliegue cada vez es mayor, este sector se ha convertido en un objetivo para los ciberdelincuentes. Por ello es necesario contar con un plan de acción en materia de seguridad.

En el sector industrial existen muchas compañías a las que aún les falta mucho camino por recorrer a la hora de abordar la seguridad de sus activos tecnológicos. Para Eusebio Nieva, Iberia Technical Manager de Check Point, hay que contar siempre con una seguridad adaptada a los peligros que pueden venir, con enfoques novedosos como pueda ser el Zero Trust.

Entre los principales retos a los que se enfrenta la seguridad en entornos industriales, hay que tener en cuenta primero a nivel interno que se trata de un sector resistente al cambio y con una metodología muy establecida, por lo que abordar esa transformación digital y envolverla de una capa de seguridad no debe interferir con el propio funcionamiento de la compañía. Por otra parte, no hay que



olvidar todas las amenazas que pudieran provenir de una conexión con el exterior. Por todo ello, lo fundamental es establecer una estrategia flexible que marque cómo se ha de abordar la securización de este nuevo paradigma.



La ciberseguridad en las empresas 4.0 no es una opción, sino una herramienta esencial para garantizar el éxito

CARLOS TORTOSA Director de Grandes Cuentas de ESET



conectado a través de Internet y el mundo empresarial no es una excepción. Esta interconexión necesaria surgida en los últimos años, por ejemplo, ha motivado que las instalaciones tipo SCADA, DSS o PLC, que tienen en su arquitectura una amplia intervención del propio fabricante del dispositivo, tuvieran que conectarse con el resto de la red para recopilar información necesaria a nivel organizativo.

tipo "caja negra" donde no existía ninguna opción de acceder de manera remota al dispositivo de control industrial asumieran el riesgo de estar conectadas a redes de amplio rango de acceso a Internet y, por lo tanto, expuestas a los mismos riesgos que el resto de dispositivos con acceso a cualquier tipo de aplicativo que requiera de acceso externo.

Ante este panorama tan dependiente de Internet no todas las áreas industriales han tenido opción de afrontar el riesgo con la misma eficacia, y como consecuencia se han ido abriendo

ivimos en un mundo cada vez más inter- claras brechas de seguridad en entornos donde, incluso con intención de hacerlo, resulta sumamente complicado poder aplicar soluciones de seguridad.

Precisamente, llegado a este punto cabe preguntarse cuáles son las principales vulnerabilidades que podrían afectar al mando y control de los propios dispositivos, es decir que un atacante tenga capacidad de acceder a estos y modificar el comportamiento, bloquear el acceso Esta situación ha supuesto que instalaciones a promover actuaciones fuera de toda norma, como podría ser el acceso a dispositivos IoT que tengan que ver con infraestructuras críticas. De hecho, mucho se ha hablado de un popotabilizadoras de agua y el efecto que este podría tener o el control de plantas de generación eléctrica, ahora que está tan de moda el posible "apagón general".

> ner es que este acceso permita a los atacantes lleestos loT posibilitando así que con una "puerta" supuestamente más segura.

trasera" el riesgo se trasladara a equipos supuestamente bien protegidos dentro de la red corporativa y que el IoT fuera únicamente el vehículo de acceso a otros dispositivos.

Por otro lado, se hace inevitable al hablar de la industria 4.0 destacar el avance tecnológico que supondrá el 5G para ella, puesto que conllevará que el acceso a la información sea mucho más rápido fiable y aplicado y esto supondrá una mejora tanto en los procesos como en los productos que serán más rentables, eficientes y seguros.

Si bien es cierto que la mejora será importante, se debe tener en cuenta, también, un importante escollo con el que la industria se va a encontrar y sible ataque que podría producirse en plantas es la actualización de los sistemas que funcionan en los entornos industriales ya que estos suelen resultar sumamente complejos y en ocasiones prácticamente inasumibles, es decir, que en muchas instalaciones industriales será todo un reto Igualmente, otro de los riesgos que pueden te- acondicionar la infraestructura para que estos dispositivos puedan funcionar de manera convegar a otro tipo de dispositivo interconectado con niente con tecnología 5G, que es más eficiente y



LOS RETOS DE LA INDUSTRIA 4.0 / OPINIÓN

Sin embargo, una vez salvado este inconveniente, evidentemente este avance tecnológico es muy positivo para el entorno empresarial.

Por último, es importante subrayar que lo primero que deben considerar las empresas a la hora de diseñar una estrategia de ciberseguridad es tener en cuenta todos los aspectos que puedan suponer un posible inconveniente a

largo plazo. También es importante la informa- ño, que permita actualizaciones del sistema, así ción relativa al consumo de energía, niveles de como el despliegue de parches o el mando descontrol general de las plantas de producción... cliente tenga implementado en el resto de la red. Y es igualmente esencial saber qué dispositivos Es decir, que se tenga en cuenta que el ciclo de rarse que estos dispositivos tengan aplicada una bilidad de aplicar mejoras a nivel de ciberseguripolítica de ciberseguridad desde el propio dise- dad tan necesarias hoy en día.

productividad, la interacción con el sistema de de el centro de control de ciberseguridad que el requieren de interconexión con otros y asegu- vida de la instalación ha de contemplar la posi-

CARLOS TORTOSA, DIRECTOR DE GRANDES CUENTAS DE ESET

"Hay que pensar en la protección desde el diseño"

Los entornos industriales de tipo SCADA se han visto abocados a tener que interconectarse con el resto de dispositivos de una red corporativa, a pesar de que no estaban diseñados para ello. Esto ha supuesto una serie de vulnerabilidades que se han convertido en todo un reto para la seguridad.

La necesidad de interconectar dispositivos que no estaban preparados ha abierto la puerta a que algún atacante pueda acceder a los mismos. Carlos Tortosa, Director de Grandes Cuentas de Eset, señala dos peligros fundamentales: que un acceso exterior pueda obtener el control de estos dispositivos, con lo que todo ello pudiera conllevar por ejemplo a la hora de hablar de infraestructuras críticas, o que a través de esta vía de entrada pueda irrumpir en otras partes de la red corporativa.

Por ello la compañía recomienda que a partir del propio diseño o definición de la estructura se tenga en cuenta que tiene que ser protegida. Asimis-



mo, es necesario tener en cuenta la necesidad de actualización de esos sistemas, por lo que habrá que hacerlos accesibles a través de algún entorno tipo consola de administración que permita este acceso a la hora de actualizar el sistema sin necesidad de parar el proceso productivo.



Avanzando hacia la industria 4.0 con seguridad

ALFONSO RAMÍREZ director general Kaspersky Iberia



seguridad en sus redes de TI y OT (tecnología operativa) de manera diferente. De hecho, la mayoría de las empresas ya cuentan con medidas maduras de detección de infracciones y respuesta a incidentes en su infraestructura corporativa, pero cuando se trata de la tecnología operativa este enfogue suele encontrarse bastante desfasado.

Sin embargo, la creciente tendencia de Industria 4.0, también llamada industria inteligente o cuarta revolución industrial, busca transformar a la empresa en una organización inteligente para conseguir los mejores resultados de negocio.

Términos como fabricación aditiva, robótica colaborativa, herramientas de planificación de la producción, visión artificial, realidad virtual, gamificación, simulación de procesos, inteligencia operacional o IoT, entre otras, suponen que las empresas industriales sean cada vez más "digitales", incrementen constantemente su inversión en tecnología inteligente y, en consecuencia, se desdibuje la frontera tradicional entre los entornos de TI y OT, por lo que las ciberamenazas pue-

istóricamente, las empresas industriales den llegar con mayor frecuencia a los sistemas de todo el mundo han abordado la ciber- de control industrial. De hecho, según un reciente informe de Kaspersky ICS CERT, en el primer semestre de 2021 el porcentaje de ordenadores industriales en los que se detectaron objetos maliciosos alcanzó el 33,8%.

INTERNET, CORREO ELECTRÓNICO Y **DISPOSITIVOS EXTRAÍBLES:** ORIGEN DE LAS AMENAZAS

Las amenazas provenientes de Internet crecieron en este semestre un 1,5% y fueron detectados en somware introducido involuntariamente en el 18,2% de los equipos industriales. Las amenazas que llegan a través de conexiones de medios extraíbles se bloquearon en el 5,2% de los ordenadores ICS, lo que supone un descenso del 0,2 % respecto con demasiada frecuencia, es evidente que un del semestre anterior y confirma la tendencia a la hacker motivado también puede penetrar en baja iniciada en el segundo semestre de 2019.

del correo electrónico se bloquearon en el 3,4% de los ordenadores industriales, lo que supone un descenso del 0,6% respecto al semestre anterior. Los países del sur de Europa errores humanos y la mejor manera de afron-(Italia, España, Grecia y Portugal) destacan en tarlos es la formación. Ya existen en el mercado

el Top 15 como los más afectados por este tipo de ataques. En concreto en nuestro país se bloqueó un 5,7% de este tipo de amenazas provenientes de adjuntos al correo electrónico.

Vistas las cifras, el riesgo de infección es claro. De hecho, no siempre es necesario que la empresa industrial sea el objetivo, también existe el riesgo de infección accidental por malware convencional: una simple unidad flash o un mensaje de correo electrónico de tipo phishing con un troyano bancario o ranel entorno ICS puede afectar seriamente a la actividad principal de una empresa. Incluso si las infecciones accidentales no se producen las redes de OT y causar daños considerables Por último, los archivos adjuntos maliciosos a la producción o en equipos de gran valor, o bien robar información valiosa.

> Tampoco se puede olvidar que más del 80% de los ciber-incidentes en las empresas se deben a



LOS RETOS DE LA INDUSTRIA 4.0 / OPINIÓN

soluciones de formación gamificada online que utilizan las técnicas más modernas de aprendizaje y abordan todos los niveles de la estructura empresarial. Este tipo de soluciones brinda a las organizaciones una serie de resultados muy alentadores, ya que consiguen hasta un 90% de reducción en el número total de incidentes y un anomalías para identificar acciones maliciosas 50% de reducción en el impacto económico de en el nivel PLC. los incidentes.

puedan avanzar seguras en la digitalización es mizar el factor humano.

importante que tengan en cuenta unas medidas básicas de ciberseguridad:

- para prevenir las infecciones accidentales y dificultar las intrusiones motivadas.
- Supervisión de la red de OT y detección de
- Programas de formación para los emplea-Por ello, para que las empresas industriales dos con el fin de reducir los accidentes y mini-

Servicios de expertos dedicados a investigar la infraestructura, llevar a cabo análisis Protección de los endpoints industriales de expertos o mitigar el impacto de un incidente. ■



- Ciberseguridad orientada al futuro
- Kaspersky Industrial Cybersecurity

PEDRO VIANA, PRESALES MANAGER IBERIA DE KASPERSKY

"La visibilidad es la clave"

A pesar de que el nivel de la ciberseguridad en el sector industrial español está mejorando, aún queda mucho camino por recorrer. Amenazas como los ataques dirigidos o el ransomware pueden poner en jaque a las infraestructuras críticas del país. La monitorización es fundamental para poder reaccionar a tiempo ante cualquier tipo de problema.

Aún queda mucho margen de mejora a la hora de analizar la ciberseguridad en el sector industrial. Así lo señala Pedro Viana, Presales Manager Iberia de Kaspersky, que menciona varios verticales que están recibiendo un mayor número de amenazas dentro del sector industrial: la inmótica, la cadena de suministro,

Oil&Gas, energía y la industria automovilística. Entre los riesgos que más pueden afectar al sector industrial destacan los ataques dirigidos, las URLs maliciosas y los scripts, el compromiso de los sistemas para el minado de criptomonedas y el ransomware, amenaza que cada vez va a más. Por ello, para la compañía de

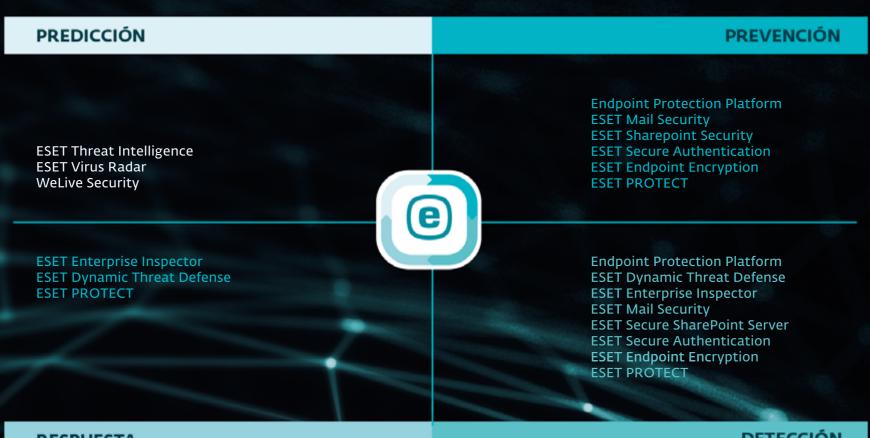


seguridad la monitorización de los sistemas es clave para poder generar una respuesta de la forma más adecuada posible en caso de incidente, de tal forma que no tenga impacto en el proceso productivo.



BLINDA TU EMPRESA CON LA COMODIDAD DE LA NUBE

Gestiona toda la ciberseguridad de tu empresa estés donde estés.





RESPUESTA DETECCIÓN

CYBERSECURITY EXPERTS ON YOUR SIDE



La seguridad móvil un factor clave para la nueva Industria 4.0



ENRIQUE MARTÍN, Head of Business Development & Innovation Iberia

no de los principales objetivos de los industria 4.0. En nuestro caso, el ecosistema instaladores) gracias a la familia de equipos rueconomía. Para ello, la Unión Europea está de- nectividad 5G y Wifi 6E. La productividad en el turas extremas. cidida a digitalizar la industria para proporcionar productos y procesos de mayor valor, con los dispositivos móviles disponen de la poten- dad. Somos el único fabricante de dispositivos el fin de ser más competitivos. Para llevar a cabo esta transformación, será muy necesario apoyarse en las nuevas tecnologías de conectividad, como 5G, y en aquellos dispositivos que nos permiten ganar productividad y eficiencia en todo tipo de escenarios. Pero lo más impor- experiencia similar a la de un PC) y a las funcio- ceso incorporamos la plataforma de seguridad tante, será la seguridad, que habilitará redes y nes multitarea en los plegables serie Z (con la Knox en el hardware y el sistema operativo, puntos de acceso a la información fiables, en opción de utilizar S Pen para tomar notas) po- para asegurar la integridad del dispositivo en un nuevo mundo hiperconectado que sentará las bases de la Industria 4.0.

porcionar la tecnología y los dispositivos ne- con trabajos en movilidad (personal en tien- siempre en su dispositivo, y en las aplicaciones cesarios para abordar con éxito la transfor- das, sucursales, restaurantes, fabricas, agricul- o datos que se encuentre en él. Además, Knox mación de procesos y de los negocios en la tura, construcción, salud, logística, seguridad, es una plataforma abierta, lo que supone que

puesto de trabajo es otro de nuestros focos, cia y funcionalidades necesarias para que sea- que adopta una estrategia tan amplia e intemos efectivos y eficientes en nuestro trabajo, gral para garantizar la seguridad de la informite usar un terminal móvil como un portátil, cación de los componentes de hardware en transformando la interfaz de usuario en una nuestras propias fábricas, y durante ese prodemos gestionar procesos y realizar tareas en todo momento. Así, desde su iniciación hasta En Samsung estamos preparados para pro- la eficiencia más allá de la oficina a empleados consumidores o empresas-pueden confiar

Fondos Europeos de Recuperación es Galaxy cada vez es mayor, con las máximas gerizados para profesionales que trabajan en que los países miembros refuercen su prestaciones y las ultimas innovaciones en co- entornos exigentes, con humedad y tempera-

> Y, por supuesto, otro factor clave: la seguripor ejemplo, gracias a Samsung DeX (que per- mación. Empezamos con el diseño y la fabricualquier lugar y momento. También llevamos la ejecución de tareas, nuestros clientes –sean



LOS RETOS DE LA INDUSTRIA 4.0 / OPINIÓN

y flexibles.

das las series Z, S, Note, A, XCover y Tab, ahora otros actores de la industria avalan nuestra gital con éxito.

todas las mejoras y capacidades están a dispo- recibirán al menos cuatro años de actualiza- estrategia de seguridad móvil. En definitiva, sición de la industria, para que puedan utilizar- ciones. Por último, nuestros dispositivos son ponemos nuestra experiencia, innovación y lo en sus soluciones y estas sean más seguras los únicos que están probados y certificados capacidad de respuesta al servicio de la Induspor el CCN, aptos para ser utilizados en des- tria 4.0 y de la movilidad. De esta manera ayu-También ofrecemos un grado de compromi- pliegues ENS Alto, y colaboramos con el INCIBE damos a que las empresas puedan desarrollar so con la seguridad, ya que la mayoría de los en España para mejorar la seguridad de nues- todo su potencial con seguridad y garantías, lo productos Galaxy lanzados desde 2019, inclui- tras empresas, lo que demuestra que también que les facilitará afrontar la transformación di-

ENRIQUE MARTÍN, HEAD OF BUSINESS DEVELOPMENT & INNOVATION IBERIA DE SAMSUNG

"Hay que apostar por la innovación y la seguridad"

El perímetro se ha convertido en algo muy difícil de controlar, debido a la gran cantidad de dispositivos y otros elementos que han comenzado a conectarse entre sí en esta nueva revolución industrial. Por ello es necesario concienciar a las compañías de que la ciberseguridad de este nuevo entorno 4.0 es muy importante.

La digitalización y la movilidad permiten acceder a información en cualquier lugar y en cualquier momento, además de poder aportar información a los procesos industriales. Para Enrique Martín, Head of Business Development & Innovation Iberia de Samsung, esta

es una de las grandes ventajas que permite la movilidad dentro del entorno industrial, haciendo que los procesos cada vez sean más automatizados y más inteligentes, de manera que la empresa sea mucho más eficiente y productiva. El 5G va a traer mejoras tanto en conec-



tividad, como en velocidad, calidad y retardo. La seguridad de este nuevo entorno debe incidir mucho en el dispositivo, tanto a la hora de proteger lo que contiene como las conexiones que va a realizar, a través de métodos de autenticación robusta. Además, no hay que olvidar la importancia de tener la

capacidad de actualizar y tener el software actualizado en todos los sistemas de la compañía.



Hacia un mundo OT eficiente y seguro: la ciberseguridad industrial a examen

BORJA PÉREZ, Iberia Country Manager de Stormshield



y movilidad están sufriendo importantes episo- también a OT, como ha ocurrido recientemente en caso de ataque, este se extienda por toda la dios de ransomware, con un impacto directo en a varios actores industriales (Trigano, Tata Steel u sus cuestiones operativas. El ansia de ciberde- Honda, entre otros). lincuentes por infiltrarse y aprovechar las conexiones entre OT e IT para obtener acceso a las **SEGMENTAR PARA PROTEGER** capas inferiores industriales, es una cuestión crucial que toda industria debe abordar.

En la ciberseguridad de los sistemas industriales existen tres puntos débiles que deben ser abordados con la máxima celeridad. Así, la gestión de un extenso conjunto de recursos industriales (a través de una arquitectura distribuida), con fábricas cada vez más interconectadas, supone un importante riesgo de propagación de ataques. Lo mismo ocurre con la creciente permeabilidad entre los sistemas industriales y los sistemas de rrera entre IT y OT, lo que supone segmentar los y por estar directamente conectada al sistema ininformación, al abrir nuevas superficies de ataque; o con el cibergobierno, un reto para los de- red de la oficina y el sistema industrial, el siste- dad, que evidencian la necesidad de proteger los partamentos de IT y OT. El ERP (en el lado de IT) y ma industrial e internet... en definitiva, garantizar datos subidos a la nube, instalando cortafuegos

os ciberataques contra la industria se están el MES (en el lado de OT) están cada vez más indiversificando. Empresas energéticas, ma- terconectados, intercambiando más y más datos, nufactureras, de distribución o transporte por lo que cualquier ataque contra IT afectaría

Para evitar incidentes de este tipo, y garantizar que cualquier ataque se detenga y se contenga en un único lugar, realizar una segmentación dustrial necesita controlar sus comunicaciones para aislar los distintos sistemas (producción, calidad y seguridad) ayudará a minimizar los así incluso en la nube. ataques de rebote.

No obstante, estas medidas de protección digi- ASEGURANDO LO QUE ESTÁ EN LA NUBE tal, que son esenciales y sientan las bases de la Por su creciente importancia, la nube se está conseguridad global, requieren la adopción de tres virtiendo en un nuevo factor a tener en cuenta en pasos esenciales de seguridad: mantener la basistemas de información y las fábricas entre sí, la dustrial, su uso conlleva nuevos retos de seguri-

que haya un nivel básico de seguridad entre las fábricas y todo lo demás. El segundo paso consiste en segmentar la red industrial, para evitar que, planta. La introducción de la segmentación permite asegurar ciertas zonas, frenar el ataque y contenerlo. Por último, la tercera etapa consiste en acercarse lo más posible a los controladores industriales y asegurar las comunicaciones entre ellos. Como ocurre con la IT tradicional, la IT inutilizando los cortafuegos adecuados. Y esto es

la estrategia global de seguridad. En este sentido



LOS RETOS DE LA INDUSTRIA 4.0 / OPINIÓN

en la nube para lograr que las comunicaciones entre el sistema industrial y la nube sean seguras, y salvaguardar su infraestructura, para evitar que cualquier problema pueda ser transmitido al sistema industrial.

Una última cuestión importante es el mantenimiento remoto. ¿Quién dice que no sea más pe- LA MEJOR PROTECCIÓN ligroso el uso negligente de una llave USB que un ataque desde el sistema informático? Cada vez frentan a los mismos riegos que las tradicionales, que alguien se conecta a distancia a la red de la adoptar un enfoque de protección basado en la

pone un punto débil entre el servidor y el mundo exterior. Por tanto, es imperativo que el túnel de comunicación sea seguro: que el usuario pueda autenticarse adecuadamente y que los intercambios estén cifrados.

Dado que las organizaciones industriales se en-

empresa para recuperar datos de un servidor, ex- segmentación de la red, el uso seguro de la nube y el mantenimiento de las mejores prácticas digitales se convierte en la medida más eficaz para contener las ciberamenazas y evitar que el malware se propague dentro de una infraestructura de IT u OT. De igual modo, y para las necesidades específicas del mundo industrial, una oferta compuesta por cortafuegos industriales y un agente de seguridad para endpoint permite abordar la industria del futuro con total tranquilidad cibernética.

BORJA PÉREZ, IBERIA COUNTRY MANAGER DE STORMSHIELD

"Un entorno industrial es más vulnerable que un entorno TI"

Las empresas industriales están evolucionando muy rápidamente hacia la Industria 4.0 por todas las ventajas que les aporta. A pesar de ello, se está dejando un poco de lado la ciberseguridad. Hoy por hoy, estas organizaciones están expuestas a los mismos peligros que las redes IT pero aún les falta concienciación en seguridad.

El sector industrial es un entorno muy heterogéneo, con lo cual es posible encontrar realidades muy diversas. Según Borja Pérez, Iberia Country Manager de Stormshield, en general son redes u organizaciones que han pasado de estar desconectadas a estar completamente conectadas, aumentando la

superficie de ataque en gran medida, por lo que se trata de un entorno más vulnerable que el entorno IT y menos acostumbrado a lidiar con estos riesgos. Las grandes barreras que se dan en este sector son que existe una separación entre el mundo de procesos y el de IT, así como el miedo a que



la introducción de cualquier elemento vaya a tener un impacto en la disponibilidad de la planta. Por ello, a la hora de implantar un sistema de ciberseguridad es necesario primero hacer una auditoría para comprobar la composición de la red y chequear qué procesos deben comunicarse entre sí para poder realizar una segmentación adecuada.



Endpoints de ICS: bajo la lupa de las ciberamenazas

RAÚL NÚÑEZ HERRERO. sales engineer y experto en ciberseguridad, Trend Micro Iberia



terconexión entre el proceso empresarial TI encontradas dentro del entorno ICS. y el proceso OT. Aunque esta interconexión entorno ICS a las amenazas que han estado y pérdida de control del entorno ICS. afectando a las redes de TI durante décadas.

tipo de redes motiva aún más a los atacantes como malware persistente antiguo que perya que pueden adquirir mayor notoriedad o mite hacerse con el control de las máquinas sitos de tiempo de actividad, y aprender el lograr un mayor beneficio económico gracias de una manera silenciosa. a la criticidad de las redes ICS.

los entornos industriales por la creciente in- gracias a la explotación de vulnerabilidades con la red OT.

mejora la visibilidad, la eficiencia y la velo- miento y protección de los endpoints permi- hablando previamente con el personal de cidad de información, también expone al te evitar tiempos de inactividad involuntarios sistemas del entorno OT para que puedan

El malware introducido en una red ICS pue- re en los entornos ICS, indica que los atacan- para proteger correctamente estos sistemas de proporcionar información sobre el entor- tes están empezando a reconocer estos sis- críticos.

a seguridad de los Sistemas de Control no de la red afectada, esta información es temas y atacándolos más activamente. Esto Industrial (ICS) ha pasado a un primer utilizada directamente por el software mali- significa que se debe dar un mayor peso a plano debido a la mayor exposición de cioso para hacerse con persistencia en la red la seguridad antes de interconectar la red TI

Una de las claves principales es que el per-Ante este escenario, la visibilidad, conoci- sonal de seguridad de TI aborde la seguridad comprender y abordar la seguridad con he-Los métodos utilizados en los ataques ac- rramientas focalizadas a las necesidades de La relevancia o importancia que tiene este tuales combinan tanto técnicas modernas dicho entorno. Es necesario abordar la compatibilidad del sistema operativo y los requiproceso y las prácticas operativas para llegar La presencia cada vez mayor de ransomwa- a una estrategia de ciberseguridad adecuada



LOS RETOS DE LA INDUSTRIA 4.0 / OPINIÓN

RECOMENDACIONES

Éstas son algunas recomendaciones para asegurar los endpoints de ICS:

- Aplicar parches con prontitud es vital. Si esto no es posible, considere la posibilidad de aplicar una correcta política de parcheo virtual tanto a nivel de red como a nivel de host gracias a las soluciones de Trend Micro.
- Utilice herramientas de reconocimiento y control de aplicativos para hacer un correcto bastionado de los host.

- Utilice herramientas de detección y respuesta a amenazas que permitan barrer las redes en busca de IoC.
- Restrinja los recursos compartidos de la red y aplique combinaciones sólidas de nombre de usuario y contraseña para evitar el acceso no autorizado a través de la fuerza bruta de credenciales.
- Utilice un IDS o IPS para establecer una línea de base del comportamiento normal de la red y así detectar mejor la actividad sospechosa.



- Escanee los endpoints de ICS en entornos cerrados con herramientas independientes.
- ❖ Aplicar el principio del mínimo privilegio a los administradores y operadores de redes OT.

JESÚS GAYOSO, SYSTEM ENGINEER DE TREND MICRO

"Las redes industriales están más expuestas, y hay que tener mayor control sobre ellas"

Cada día las redes están más interconectadas. Antiguamente hablábamos de plantas industriales completamente aisladas y controladas, a día de hoy cada vez hay más conectividad. Para contar con unos sistemas completamente seguros es necesario tener el control de todos los procesos que se definen en una planta.

Cada vez hay mayor concienciación, pero las plantas industriales deben de acelerar los conceptos básicos como visibilidad, concienciación de los usuarios, segmentación de las redes y control de lo que está ocu-

rriendo en una planta. Jesús Gayoso, System Engineer de Trend Micro, señala que las redes están más expuestas y hay que tener un mayor control sobre ellas, sobre todo a causa de sistemas operativos obsoletos, que



no pueden parchearse, que son más vulnerables y los ataques cada vez son más sofisticados. La industria 4.0 se basa en recoger datos y en que las máquinas puedan tomar decisiones por sí mismas, por lo que hay que tener muy controlado el entorno y la planta industrial. Lo primordial es tener una segmentación y una visibilidad de la red, sobre todo segmentar esas redes críticas en cuanto a nivel de operación y producción.

SAMSUNG

Tu "Todo en uno"

Mitad smartphone. Mitad tablet.
Galaxy Z Fold3 es resistente al agua,
compacto y puede ejecutar varias
aplicaciones a la vez. ¡Ideal para
trabajar sobre la marcha!



Galxy Z Fold3



Soluciones específicas para cada necesidad

nivel de seguridad". Por ello, abordan las necesi- focarse en aquellas tecnologías y capacidades zas impulsada con Inteligencia Artificial. dades de ciberseguridad más inminentes de las que brindarán seguridad sin concesiones baorganizaciones basándose en tres principios bási- sada en estos tres principios básicos. cos. Estos principios son:

- tecciones de usuario preventivas para eliminar res principales: Harmony, CloudGuard y Quanlas amenazas antes de que lleguen a los usuarios. tum, con Infinity-Vision como base.
- Gestión Gold Standard: panel único para gestionar todo el patrimonio de seguridad.
- Solución consolidada: protección preventiva completa contra las amenazas más avanzadas mientras se logra una mejor eficiencia operativa.

SECURE YOUR EVERYTHING CON **CHECK POINT INFINITY**

En esta nueva normalidad, los clientes merecen mantener la productividad mientras permanecen protegidos en todo lo que hacen. Dondequiera que se conecte, a lo que se conecte y como quiera que se conecte: su hogar, sus dispositivos, su privacidad y los datos de

cualquier organización la capacidad de rea- hacer realidad esta visión, en 2021 han recali-

Check Point consolida más de 80 productos * Enfoque de prevención: implementar pro- y tecnologías y los ha organizado en tres pila-

HARMONY, EL MÁS ALTO NIVEL **DE SEGURIDAD PARA USUARIOS REMOTOS**

Check Point Harmony protege a los empleados remotos, los dispositivos y la conectividad a Internet de ataques maliciosos, al tiempo que garantiza un acceso remoto seguro y de confianza cero a cualquier escala y en cualquier aplicación corporativa. Check Point Harmony proporciona conectividad segura y de punto final (SASE), como una solución consolidada y unificada basada en la nube que incluye el acceso remoto más en la nube, tanto públicas como privadas. Ofrefácil y seguro (basado en la adquisición de Odo), su organización deben estar seguros y prote- navegación segura por Internet, punto final y se- serverless y una nueva generación de firewalls

a misión de Check Point es "proporcionar a gidos de cualquier amenaza cibernética. Para guridad móvil y seguridad del correo electrónico. La solución ofrece la cobertura más amplia de lizar su trabajo en Internet con el más alto brado su oferta de productos Infinity para en-vectores de ataque con la prevención de amena-

> Harmony presenta las tecnologías que admiten entornos híbridos seguros de trabajo desde cualquier lugar (WFA). Asegurar a los empleados en el domicilio se ha convertido en una de las principales prioridades de las organizaciones de todo el mundo. La nueva familia de productos Harmony reúne más de siete categorías de productos para proporcionar una protección preventiva completa para los usuarios remotos. Incluye conectividad segura desde cualquier lugar y un entorno de trabajo seguro en cualquier dispositivo, incluidos los dispositivos móviles, personales y administrados por la empresa, tanto cliente como sin cliente.

CLOUDGUARD, NUBE SEGURA DE FORMA AUTOMÁTICA

CloudGuard establece el estándar de oro para proteger las cargas de trabajo críticas ce gestión de la postura en la nube, seguridad



LOS RETOS DE LA INDUSTRIA 4.0 / SOLUCIONES TECNOLÓGICAS

de aplicaciones web con tecnología de inteligencia artificial contextual que protege las API, las aplicaciones web y los servidores web alojados y on-premise. CloudGuard proporciona seguridad consolidada y prevención de amenazas en todos los entornos, activos y cargas de trabajo de la nube. Alineado con la naturaleza ágil del desarrollo y la implementación en la nube, CloudGuard ofrece una solución tanto para los profesionales de la seguridad en la nube como para las DevOps en la nube, desde la fase inicial de DevSecOps, pasando por la seguridad de la red en la nube Además, lanzan una nueva serie de dispositivos hasta la seguridad de las aplicaciones en la nube (WAAP), así como la protección de contenedores y medianas empresas: Quantum SPARK. y funciones sin servidor.

> **QUANTUM, SEGURIDAD DE LA RED EMPRESARIAL PARA EL** PERÍMETRO Y EL DATACENTER

En 2021, continúan aprovechando Maestro, su solución de rendimiento escalable. Acelerarán la innovación en el firewall del centro de datos con la introducción de un gateway de firewall con un rendimiento de firewall de 200 Gbps y una latencia de menos de 3 microsegundos.

Quantum refleja la solución de seguridad de red más completa para la organización, perímetro y

centro de datos, que abarca IoT Nano-Security hasta superredes Terabit, y ofrece los más altos niveles de seguridad y rendimiento para administrar entornos de centros de datos.

Las puertas de enlace de seguridad de Check Point Quantum brindan seguridad más allá de cualquier firewall de próxima generación (NGFW) y están diseñadas para administrar los requisitos de políticas más complejos. Con más de 60 servicios de seguridad, estos gateways son los mejores para prevenir la quinta generación de ciberataques. para sucursales y oficinas dirigidos a las pequeñas

INFINITY VISION, GESTIÓN UNIFICADA Y XDR

Alcance una gestión de seguridad unificada y un 100% de prevención de brechas de seguridad. Administre todo su patrimonio de seguridad con Check Point Infinity Portal, una gestión de seguridad como servicio (SMaaS) basada en la nube. Entregue políticas, supervisión e inteligencia unificadas desde un solo punto. Exponga, investigue y bloquee los ataques más rápido, con una precisión del 99,9% con las capacidades SOC y XDR utilizadas por Check Point Research.





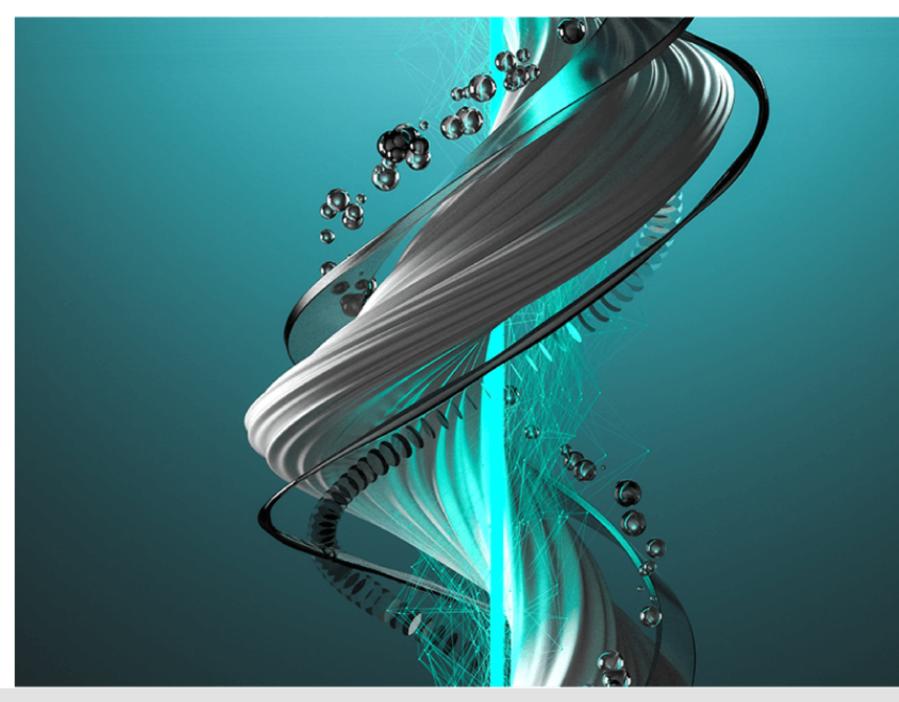
- Guide for delivering IoT Security
- **Check Point IoT Protect Solution Brief**
- **IoT Security for Networks and Devices**
- IoT Security for Enterprise, Industrial and Healthcare
 - CloudGuard for Cloud Native Security



La propuesta de seguridad de ESET apuesta por ofrecer soluciones específicas para necesidades específicas

Una solución para cada necesidad

- ❖ ESET PROTECT ADVANCED, es una solución para un nivel de ciberseguridad empresarial más avanzado con administración basada en la nube. Proporciona protección a su red de equipos y servidores de archivos contra ransomware, amenazas avanzadas y amenazas zero-day. Asegure sus datos con el cifrado completo del disco y administre todo desde la consola en la nube ESET PROTECT. Está orientado a la protección de servidores, ordenadores de sobremesa, portátiles y dispositivos móviles.
- ❖ ESET PROTECT COMPLETE es una solución de protección completa para empresa que además mantiene seguras las aplicaciones de Microsoft 365 con administración basada en la nube. Proporciona protección para su red de equipos, servidores, correo electrónico no deseado, de las aplicaciones de la empresa en la nube, contra todo tipo de amenazas: ransomware, avanzadas, día cero y malware, también protege sus datos con el cifrado de disco completo y todo administrado desde la consola de administración en la nube ESET PROTECT. Está diseñado para la protección de aplicaciones, al-





LOS RETOS DE LA INDUSTRIA 4.0 / SOLUCIONES TECNOLÓGICAS

dispositivos móviles.

- nube ESET PROTECT. Orientado a la protección sa, portátiles y dispositivos móviles. del servidor de correo electrónico, el vector de ataque más común.
- ción de protección avanzada para el correo, ciones de Microsoft 365. Proporciona protecsharepoint y almacenamiento de Microsoft ción para su red de equipos, servidores, correo 365. Su combinación de filtrado spam, anti- electrónico no deseado, contra todo tipo de malware, antiphishing, escaneo y detección de páginas fraudulentas ayuda a proteger la comunicación, las aplicaciones y almacenamiento de la empresa en la nube además puede desde la consola local ESET PROTECT. Protege inspeccionar los objetos que están en cuarentena. Protege la comunicación de la empresa y nes de Microsoft 365, servidores de archivo, el almacenamiento en la nube para las aplica- servidores de correo, ordenadores de sobreciones de Microsoft 365.
- 365, servidores de archivo, servidores de co- lución para grandes empresas que incorpora rreo, ordenadores de sobremesa, portátiles y una potente capa de protección EDR: identificación de comportamientos anómalos, fugas de información, análisis de riesgos... Proporcio-**ESET PROTECT MAIL PLUS**, solución que na máxima protección para su red de equipos protege las comunicaciones por correo elec- y servidores de archivo contra ransomware, trónico con espacio seguro basado en la nube. amenazas persistentes avanzadas (APT), ame-Protege su empresa de los ataques de red y nazas día cero y malware sin archivo. Protege ofrece protección directamente a través del sus datos con el cifrado de disco completo y servidor antes de llegar a las cuentas de co- además incrementa su seguridad con la prorreo de los usuarios, filtra los mensajes de co- tección EDR más avanzada por su detección rreo no deseado con casi el 100% de precisión y respuestas de amenazas en equipos. Todo además de brindar seguridad frente a las ame- gestionado fácilmente desde la consola de adnazas persistentes avanzadas y amenazas día ministración local ESET PROTECT. Protege sercero. Todo administrado desde la consola en la vidores de archivo, ordenadores de sobreme-
- **SET PROTECT COMPLETE ON-PREM**, una solución de protección completa para empre-* ESET CLOUD OFFICE SECURITY, una solu- sa que, además, mantiene seguras las aplicaamenazas: ransomware, avanzadas, día cero y malware, también protege sus datos con el cifrado de disco completo y todo administrado aplicaciones, almacenamiento y comunicaciomesa, portátiles y dispositivos móviles.

La propuesta de seguridad de ESET apuesta por ofrecer soluciones específicas para necesidades específicas





Compártelo en redes

- Tendencias en Ciberseguridad 2021
- Informe sectorial sobre los gobiernos 2021
- Protección de end point
- **Dynamic Threat Defense**





Trend Micro Vision One™



Movilidad segura en Industria 4.0

La movilidad es uno de los elementos destacados en el avance de la Industria 4.0. Pero como ocurre en todos los segmentos del negocio, esta movilidad debe ser segura y eficiente.

os entornos industriales también necesitan mite de fuerza para proteger la pantalla principal dispositivo mientras se consultan las notas de dispositivos para trabajar en movilidad, y, sobre todo, para hacerlo de forma segura. La propuesta de Samsung en este terreno para más cosas a la vez como, por ejemplo, unirse presentación y redactar un mensaje de texto por los dispositivos, pero no se detiene ahí.

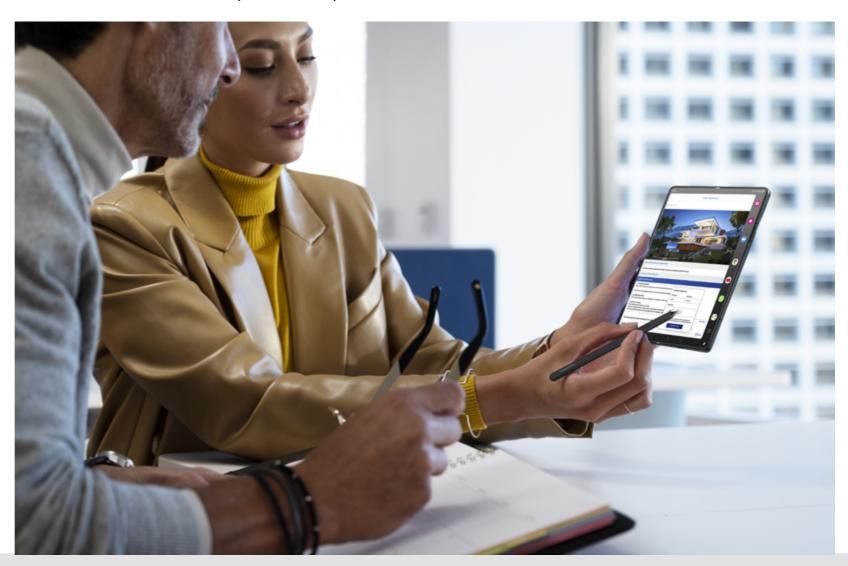
Galaxy Z Fold3. Posee una pantalla Infinity Flex de 7,6 pulgadas, y cuenta con una mayor área visible para que los usuarios obtengan un fondo ininterrumpido para ver sus aplicaciones favoritas. Con la nueva tecnología de pantalla Eco, la pantalla es un 29% más brillante y consume menos energía. Gracias a la tasa de refresco adaptable Super Smooth de 120 Hz, se puede experimentar un deslizamiento por la pantalla aún más suave y una rápida interacción con el dispositivo, tanto en la pantalla principal como en la de la cubierta frontal.

Por primera vez en la serie Galaxy Z, Samsung incorpora la funcionalidad de S Pen. Ahora es más sencillo tomar notas durante una videollamada o revisar una lista de tareas mientras se leen correos electrónicos. Los usuarios de Z Fold3 pueden escoger entre dos opciones: S Pen Fold Edition y S Pen Pro. Ambos cuentan con una punta retráctil especialmente diseñada con un lí-

de Z Fold3 5G; con una latencia aún más baja.

a una videollamada en la pantalla superior del mientras se consulta el calendario; todo desde

la reunión en la inferior. Con la función Mul-El modo Flex de Z Fold3 5G permite hacer ti-Active Window es más fácil organizar una





LOS RETOS DE LA INDUSTRIA 4.0 / SOLUCIONES TECNOLÓGICAS

la pantalla grande del dispositivo. Además, en Z Fold3 5G, los usuarios pueden crear un acceso directo y volver a abrir las aplicaciones más tarde en la misma posición, gracias a App Pair. También pueden utilizar la nueva barra de tareas para cambiar rápidamente de aplicación sin tener que volver a la pantalla de inicio.

❖ Galaxy Tab S7 FE. Con un diseño minimalista y ligero, Galaxy Tab S7 FE luce un cuerpo metálico elegante de 6,3 mm y 608 g de peso, lo que lo convierte en un dispositivo fácil de llevar a cualquier parte. Además, cuenta con compatible con carga súper rápida de 45W.

Galaxy Tab S7 FE está pensado para hacer más trabajo en menos tiempo. Incluye S Pen en la caja para hacer todo tipo de tareas más rápido, y, con Samsung Notes, se puede convertir las notas escritas a mano en texto. Con ciberataques. Multi Active-Window se pueden abrir hasta tres aplicaciones a la vez, y con Grupo de Apps, aplicaciones

Además, gracias a Samsung DeX y a una funda teclado, el usuario puede utilizar la tablet como un portátil, transformando la interfaz de usuario en una experiencia similar a la de un PC. Y con la opción de Segunda Pantalla, Galaxy Tab S7 FE se puede convertir en una pantalla adicional para el PC y así maximizar la produc- la Pantalla Infinita del terminal como un panel táctividad en un tiempo menor.

Samsung Knox Vault. Desde su presentación en 2013, Samsung Knox ha evolucionado hasta convertirse en una plataforma de gestión de seguridad integral, que protege los dispositivos móviles de millones de usuarios y empresas en todo el mundo frente a las amenazas más sofisticadas. Samsung Knox Vault es la evolución natural de la plataforma de seguridad de Samsung, que proporciona un entorno aislado e integrado en el hardware, para mantener los datos protegidos. Knox Vault aísla la información más crítica del terminal, como claves y certificados digitales, para que no permanezcan vulnerables ante un una potente batería de hasta 13 horas, y es acceso no autorizado. Este nuevo protocolo permite separar los datos confidenciales del sistema operativo, para evitar brechas de seguridad como el malware. Se incluye en todos los dispositivos de la serie Galaxy S21 y en los plegables Galaxy Z, con el fin de protegerlos ante ataques físicos y

Samsung DEX. DeX convierte cualquier lugar se puede guardar e iniciar rápidamente varias en un puesto de trabajo al conectar un smartphone Galaxy compatible, un monitor y un teclado. Proporciona a los usuarios una experiencia de escritorio segura y productiva que permite editar documentos, ver presentaciones en pantalla completa y realizar tareas de ordenador, entre otras funciones, con solo conectar el smartphone a la base. Además, el nuevo dispositivo aprovecha til para controlar el cursor. ■



MÁS INFORMACIÓN

- El 5G abre un mundo de oportunidades de negocio
- ¿De qué está hecho un móvil todoterreno para resistir tanto?
- Firmas legales con S-Pen, el secreto de Samsung **Galaxy Note**
 - Siete pasos para asegurar tu dispositivo móvil



Soluciones de seguridad para la empresa

Stormshield pone sobre la mesa diferentes soluciones tecnológicas para garantizar la seguridad de las empresas según las distintas necesidades que éstas tengan.

❖ SNi20, un firewall a medida para entornos industriales. Perfectamente adaptado a su entorno operativo, el firewall industrial SNi20 ofrece una integración de red única y completa (enrutamiento y NAT) y seguridad avanzada. Asimismo, proporciona una inspección profunda de paquetes (análisis basado en el contexto), permitiéndole proteger sus protocolos de comunicación industrial. El firewall garantiza la confiabilidad operativa de su infraestructura y una continuidad de negocio óptima en todo momento, incluso en caso de avería, gracias al sistema de alta disponibilidad y modo de seguridad de la red operativa. El SNi20 le asegura ciberserenidad industrial.

El cortafuegos industrial SNi20 ha sido diseñado para cumplir con los estándares de certificación más estrictos del mercado. Es por eso que las organizaciones con las necesidades de seguridad más críticas confían en Stormshield: organizaciones de defensa, organismos públicos y gubernamentales e infraestructuras críticas.

❖ SNi40, firewall para sistemas industriales. El cortafuegos industrial SNi40 está especial-





PROTECCIÓN DE INSTALACIONES INDUSTRIALES

De amenazas dirigidas a estaciones de trabajo o provenientes de la red





LOS RETOS DE LA INDUSTRIA 4.0 / SOLUCIONES TECNOLÓGICAS

mente diseñado para proteger PLC (controladores lógicos programables) y ofrece una am- A menudo considerados como los eslabones nes necesarias para los puestos son mínimas plia gama de funciones: segmentación de red, más débiles en la seguridad de TI, los termi- y estables. control de acceso por filtrado de direcciones IP nales incluyen todos los dispositivos que se o MAC, análisis contextual de paquetes, con- conectan a la red central de una empresa: ortrol de mensajes operativos y cumplimiento de denadores de escritorio y portátiles, tabletas, trabajo, bloqueando, por ejemplo, el uso no protocolos (IPS), comunicaciones seguras de teléfonos inteligentes, impresoras y todos los deseado de dispositivos USB. ■ mantenimiento remoto (VPN). Además, este demás dispositivos (inteligentes o no) que se equipo se puede integrar fácilmente en su en- nos requiera conectar a la red interna. Sin emtorno industrial, especialmente en sus armarios de control (sobre rieles DIN), gracias a un sencillo procedimiento de puesta en marcha.

El SNi40 garantiza la continuidad de la actividad gracias, en particular, a su sistema de alta disponibilidad y al modo de seguridad de la red operativa, que mantiene sus sistemas de graves daños. producción funcionando sin interrupción incluso en caso de fallo.

El SNi40 es un cortafuegos industrial certificado al más alto nivel europeo. Ha recibido la certificación y calificación CSPN a nivel elemental, emitida por ANSSI. Por ello, si elige esta solución de Stormshield Network Security, puede estar seguro de que su infraestructura industrial estará cubierta por la mejor protección posible.

bargo, todos estos terminales podrían ser secuestrados y utilizados por los ciberdelincuentes como un punto de entrada para penetrar en su sistema informático con el fin de instalar malware u obtener acceso a sus datos. Desde ellos, pueden saltar a la red OT provocando

SES tiene características que lo hacen especialmente adecuado para el entorno industrial: protege sistemas operativos obsoletos que siguen operando en redes OT como puede ser Windows XP. Por otra parte, SES no está basado en firmas ni necesita conexiones al exterior para su correcto funcionamiento. Por último, hay que destacar sus capacidades de creación de listas blancas, que no son manejables en el

Stormshield Endpoint Solution (SES). mundo IT pero sí en el OT, donde las aplicacio-

SES también controla qué dispositivos y a qué redes puede conectarse cada puesto de







- From 2015 to tomorrow: cyberintrusions in electrical grids
- Sistemas DPI y seguridad de red: la tecnología IPS Stateful DPI en entornos de TO

A menudo considerados como los eslabones más débiles en la seguridad de TI, los terminales incluyen todos los dispositivos que se conectan a la red central de una empresa

Una propuesta más allá de la seguridad tradicional para afrontar desafíos complejos

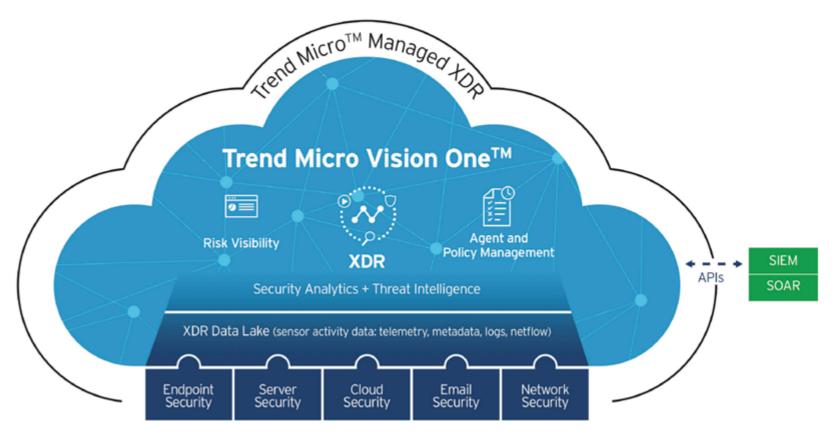
En el ámbito industrial, al igual que en otros, Trend Micro escucha las necesidades tanto de principales fabricantes como de operadores de infraestructuras críticas y luego recopila la mejor propiedad intelectual existente en las empresas asociadas.

los desafíos complejos. Y eso se materializa en vos críticos que dependen de sistemas operativos ta el acceso y preserva los recursos del sistema una propuesta como la de Trend Micro TXOne. antiguos son especialmente vulnerables, ya que con su sencilla y fiable tecnología de listas de con-

* Txone Networks Portable Security v3. Se es probable que sean difíciles o imposibles de fianza. Desplegada, esta solución solo permite la trata de una herramienta de escaneo y limpieza de malware para sistemas con conexión aislada y ordenadores autónomos. Portable Security facilita a los propietarios y operadores de ICS el escaneo de malware y la recopilación de información de activos en ordenadores autónomos y en sistemas aislados. A diferencia del software antivirus tradicional, Portable Security escanea y limpia el malware sin necesidad de instalar software de escaneo, mostrando el estado con una pantalla LED fácil de entender. Durante el escaneo, Portable Security 3 también recopila información sobre los activos, lo que ayuda a mejorar la visibilidad de la OT y a eliminar el shadow OT.

* TXOne StellarEnforce. Es un software de bloqueo de sistemas para dispositivos de misión crítica. Los sistemas de control industrial (ICS), los

I resultado es una respuesta personaliza- activos industriales de IoT y los dispositivos inte- parchear, funcionando con vulnerabilidades que da que va más allá de las herramientas grados esenciales para las operaciones diarias se los atacantes pueden explotar fácilmente. TXOne de seguridad tradicionales para mitigar enfrentan a un riesgo cada vez mayor. Los acti- StellarEnforce bloquea los activos sensibles, limi-





LOS RETOS DE LA INDUSTRIA 4.0 / SOLUCIONES TECNOLÓGICAS

ejecución de aplicaciones aprobadas y necesarias para las operaciones diarias, impidiendo la propagación y ejecución de malware sin depender de los archivos de patrones u otros recursos.

- * TXOne StellarProtect. Hablamos de seguridad de endpoint profesional y de última generación para los ICS. La protección de los endpoints de ICS debe tener en cuenta diferentes prioridades, pues el antivirus tradicional ya no es suficiente. Así, las soluciones elegidas deben garantizar que los procesos de trabajo diarios nunca se vean comprometidos, que los cálculos nunca se ralenticen y que las decisiones de producción nunca se retrasen. TXOne StellarProtect es la primera solución de este tipo: protección de endpoints todoterreno, una solución defensiva diseñada a medida para la tecnología operativa. Su escaneo avanzado de amenazas hace frente a los ataques conocidos mientras que su motor de machine learning de última generación bloquea las amenazas desconocidas, sin necesidad de acceso a Internet. El filtrado ICS de StellarProtect, basado en un inventario de aplicaciones y certificados, elimina la sobrecarga innecesaria para permitir el funcionamiento más ligero posible.
- ❖ TXOne Networks EdgeFire. Se trata de detección eficiente en línea que respalda las operaciones continuas de los lugares de trabajo. EdgeFire, es un firewall de nueva generación que permite la segmentación y segregación de la red para dividirla en diferentes zonas de control, incluso hasta el nivel de célula.

- ❖ TXOne Networks EdgeIPS. IPS industrial de próxima generación que protege los activos de misión crítica. EdgeIPS protege de forma transparente activos individuales y pequeñas zonas de producción, al tiempo que proporciona una visibilidad fiable de OT, filtrado de protocolos de OT y funcionalidad en línea o fuera de línea, todo ello diseñado específicamente para adaptarse a su red sin alterar sus configuraciones preexistentes.
- ❖ TXOne Networks IPSPro. Matriz de IPS industrial inteligente basado en propósito para operaciones a gran escala. El dispositivo de seguridad industrial transparente y multisegmento protege las máquinas críticas y apoya el funcionamiento continuo de la línea de producción. La segmentación de red basada en la intención es la base de una seguridad de red ICS cómoda, conveniente y fiable, eliminando las superficies de ciberataque y reduciendo el impacto de cualquier incidente de seguridad.
- ❖ Trend Micro Deep Security Virtual Patching. Módulo Virtual Patching de la plataforma Deep Security ofrece protección frente a las vulnerabilidades de sistemas críticos hasta que haya disponible un parche que se pueda implementar, o bien como alternativa al parche en el caso de que este nunca se publique. El parcheo virtual funciona implementando capas de políticas y reglas de seguridad que impiden e interceptan que un exploit tome las rutas de red hacia y desde una vulnerabilidad. Una buena solución de parcheo virtual debe ser multicapa. Esto incluye capacida-



des que inspeccionan y bloquean la actividad maliciosa del tráfico crítico para el negocio; detectan y previenen las intrusiones; frustran los ataques a las aplicaciones orientadas a la web; y se despliegan de forma adaptable en entornos físicos, virtuales o en la nube.



- Trend Micro Industrial Network Security
- Lost in Translation When industrial protocol translation goes wrong
- Secure manufacturing on Cloud, Edge and 5G
- Seguridad de endpoint para los ICS con Trend Micro StellarProtec
- TXone Networks
- Industrial Endpoint Security

