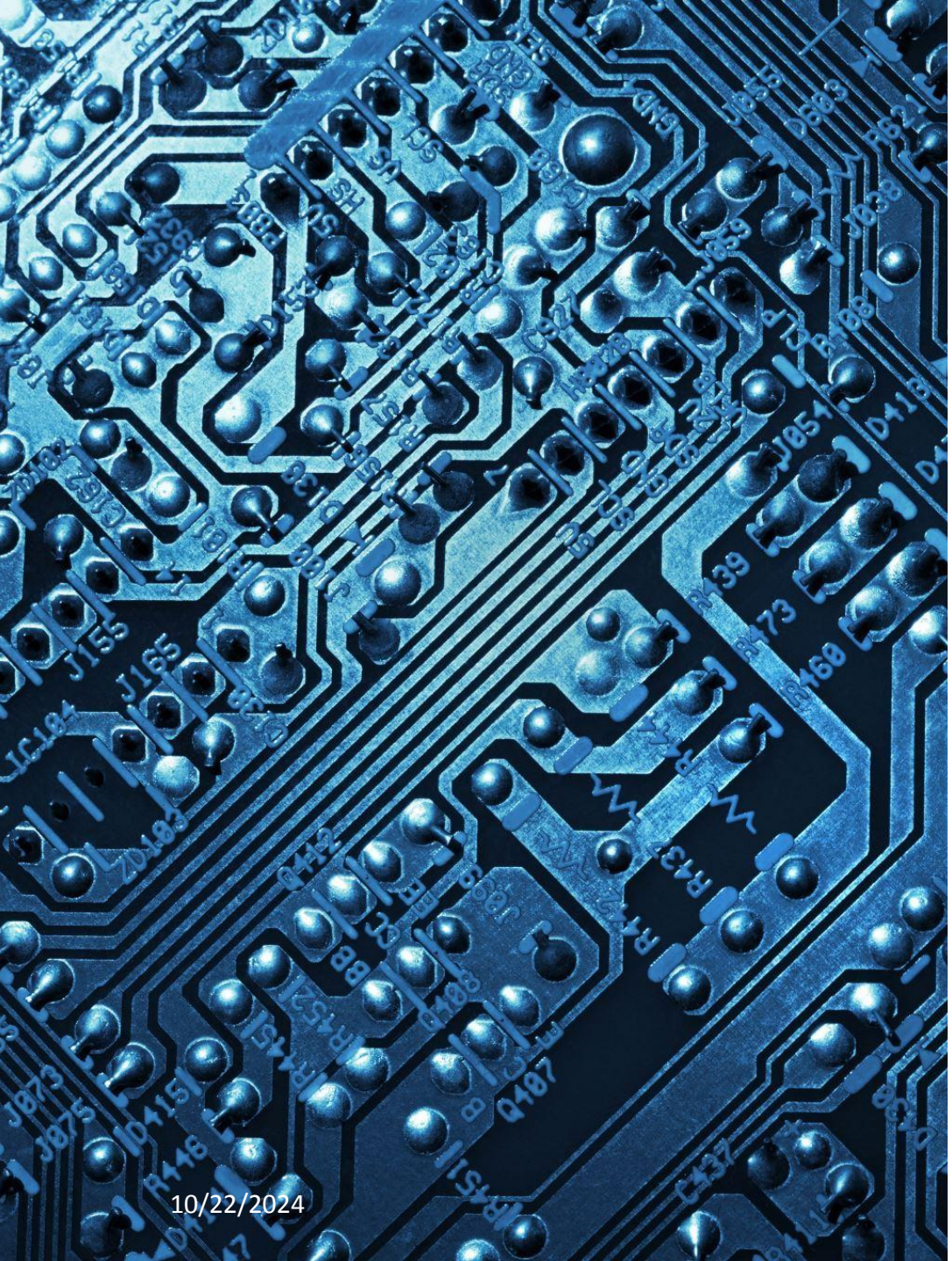
20° Congreso URUMAN + 3° Congreso INGURU

La influencia de la IA en la Ciberseguridad y su afectación en el mundo Operacional

A/P Ethel Kornecki, CISA, CISM,CDPSE
Asistente de la Coord. Académica de Ciberseguridad
Director de Consultoría Krav Maga Hacking Uruguay
kornecki@ort.edu.uy /
ekornecki@kmhcorp.com
093 546 299

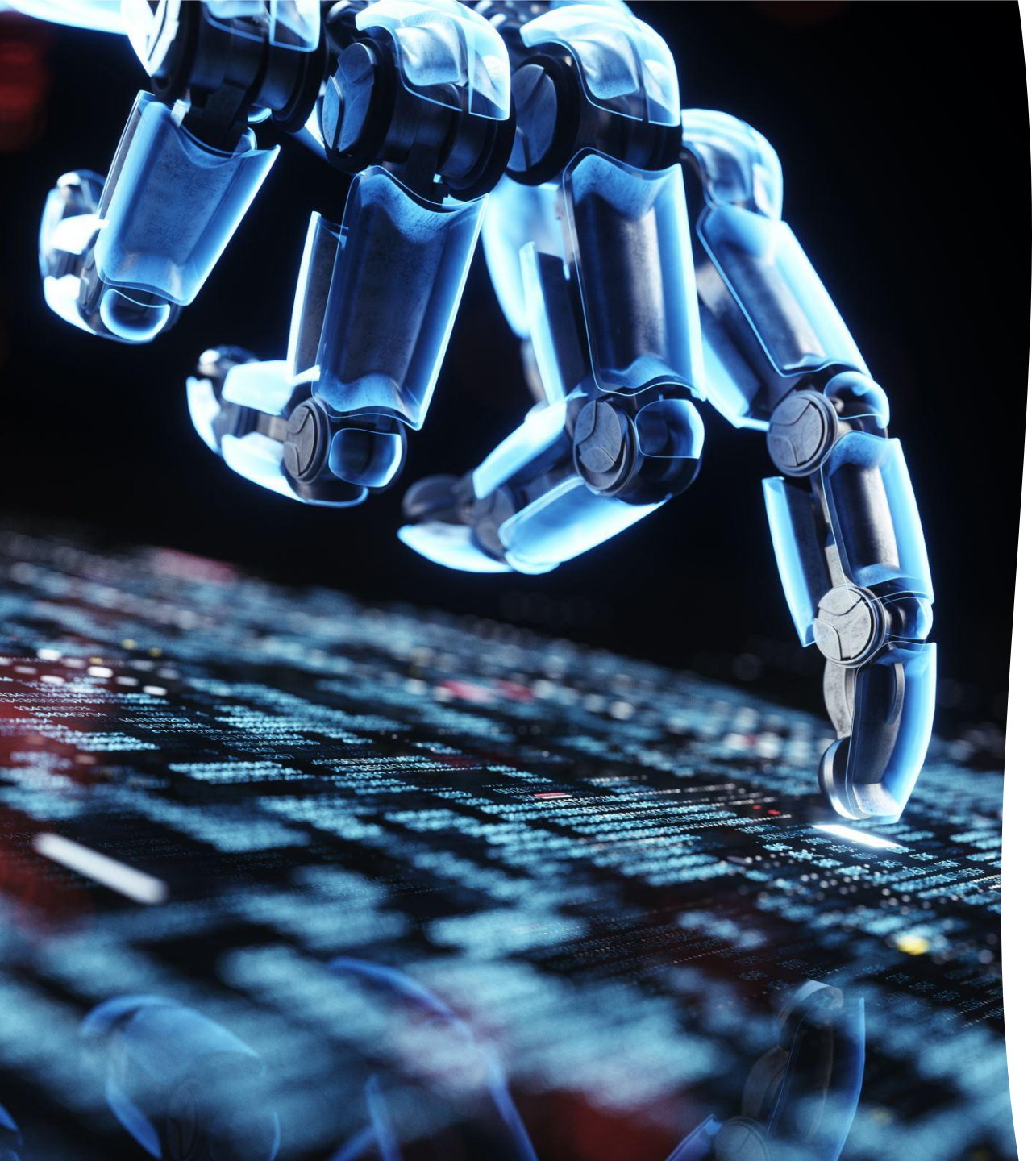


- La ciberseguridad en el ámbito de la Tecnología Operativa (OT) está atravesando un periodo de cambio sin precedentes, especialmente impulsado por la integración de la Inteligencia Artificial (IA).

- Esta transformación está captando la atención global en diversas industrias, ya que la IA juega un papel crucial en la defensa contra las ciberamenazas que afectan a infraestructuras críticas.

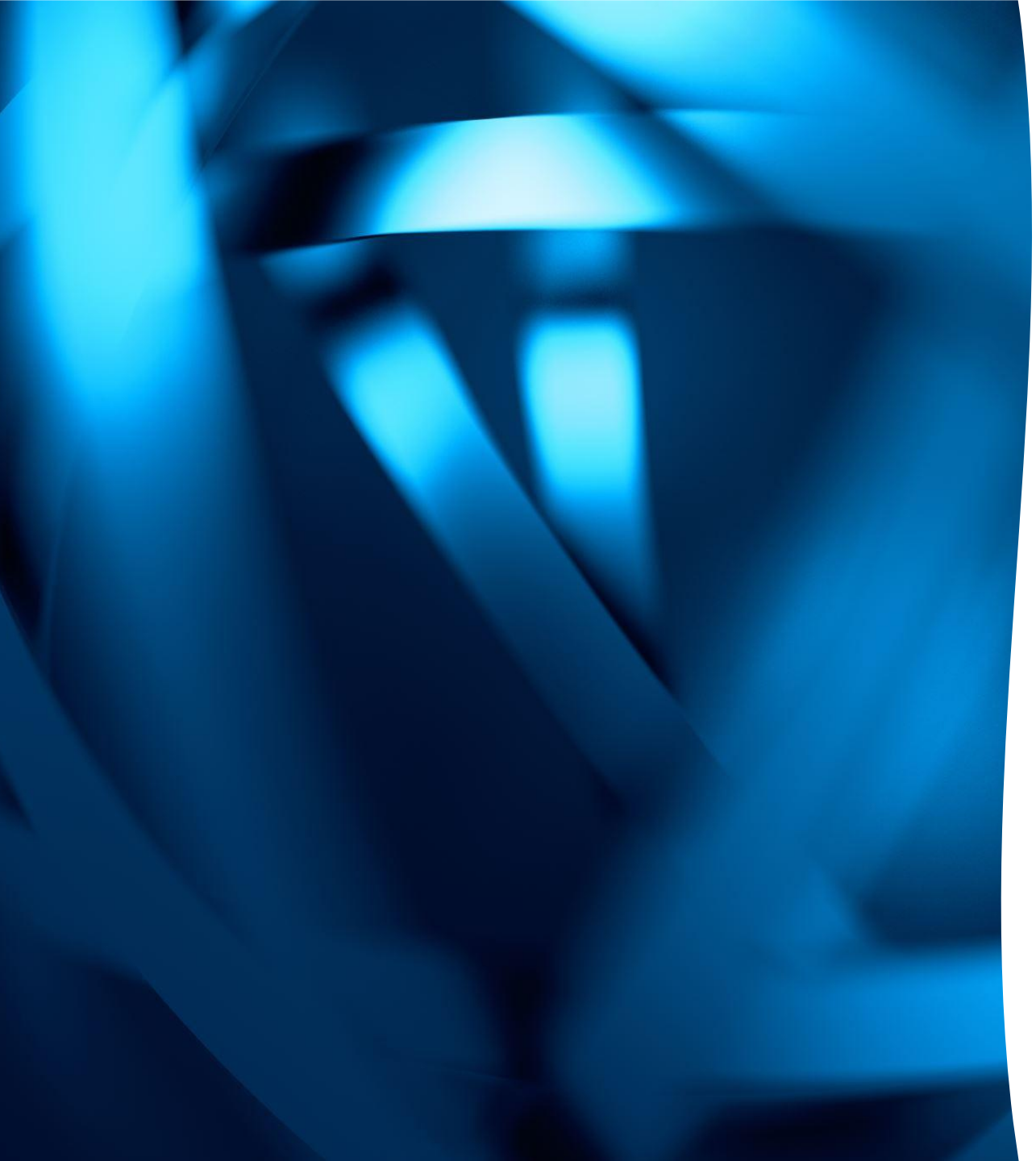
¿Qué es la Ciberseguridad Industrial ?

- La ciberseguridad industrial, también conocida como ciberseguridad OT (Tecnologías de Operación), es una rama de la ciberseguridad que se focaliza en la protección de los sistemas y procesos que se utilizan en la producción, fabricación y otros tipos de actividades industriales frente a las amenazas cibernéticas.



A medida que la IA se convierte en una herramienta clave, surgen preguntas importantes

- ¿Cuál es su rol en la creación de estrategias de ciberseguridad?
- ¿Cómo colabora con los operadores humanos?
- ¿Qué desafíos plantea en términos de seguridad de los datos y confianza?
- ¿Cuáles son las vulnerabilidades y consideraciones éticas que conlleva?
- ¿Cómo está cambiando el panorama de la lucha contra los actores de amenazas?



Cuál es su rol en l creación de estrategias de ciberseguridad?

La IA está revolucionando la forma en que se diseñan las estrategias de ciberseguridad en OT.

Su capacidad para analizar grandes volúmenes de datos en tiempo real permite identificar patrones y detectar anomalías mucho más rápido que los métodos tradicionales.

La IA ayuda a prever ataques potenciales, optimizar las respuestas a incidentes y mejorar la toma de decisiones en la protección de infraestructuras críticas.

¿Cómo colabora con los operadores humanos?

- Automatizando tareas rutinarias y liberando tiempo para que los expertos se concentren en problemas más complejos.
- La colaboración humano-IA también plantea desafíos, como la necesidad de garantizar que las decisiones automatizadas sean transparentes y comprensibles para los operadores.
- La IA no reemplaza a los humanos, sino que potencia sus capacidades, haciendo la defensa más eficiente y efectiva.

¿Qué desafíos plantea en términos de seguridad de los datos y confianza?

- La implementación de IA en OT introduce nuevas preocupaciones sobre la seguridad de los datos, ya que los sistemas de IA dependen de grandes cantidades de información para funcionar correctamente.
- Es crucial asegurar que estos datos estén protegidos contra accesos no autorizados y manipulaciones maliciosas.
- La confianza en las decisiones generadas por la IA debe ser gestionada cuidadosamente, ya que cualquier error o sesgo en los algoritmos podría tener consecuencias significativas.

¿Cuáles son las vulnerabilidades y consideraciones éticas que conlleva?

- La IA puede ser explotada por actores maliciosos para lanzar ataques sofisticados. Por ejemplo, podría ser utilizada para automatizar ataques cibernéticos o explotar vulnerabilidades en sistemas de OT.
- Existen consideraciones éticas sobre el uso de IA en la ciberseguridad, especialmente en lo que respecta a la privacidad de los datos, la transparencia de las decisiones y el impacto potencial en el empleo en sectores relacionados.

¿Cómo está cambiando el panorama de la lucha contra los actores de amenazas?

- La IA está transformando el campo de batalla digital, permitiendo una defensa más proactiva y adaptativa contra las amenazas.
- Sin embargo, los actores maliciosos también están comenzando a utilizar IA para mejorar sus tácticas, lo que significa que la lucha contra el cibercrimen se está volviendo cada vez más sofisticada.
- Las organizaciones deben mantenerse a la vanguardia, invirtiendo en tecnologías avanzadas de IA y actualizando constantemente sus estrategias de seguridad para enfrentar este panorama en constante evolución.

¿Es la inteligencia artificial amiga o enemiga de los expertos en ciberseguridad?

La IA es un arma de doble filo cuando se trata de enfrentarse al panorama de la ciberseguridad de las OT.

Si bien capacita a las organizaciones para detectar y responder proactivamente a las amenazas y sigue ampliando los límites de la automatización en la tecnología en la que se confía para proteger datos, dispositivos y redes esenciales, su susceptibilidad a los ataques adversarios y el potencial de uso indebido por parte de actores maliciosos pueden convertirla en una nueva superficie de ataque, lo que supone un riesgo significativo para los sistemas de infraestructuras críticas y tecnología operativa.

El papel de los operadores humanos en la ciberdefensa OT basada en IA

- Las organizaciones deben priorizar la formación y capacitación continua de su personal.
- Los operadores humanos, al interpretar los conocimientos generados por la IA, pueden tomar decisiones más informadas, mientras que la IA se encarga de automatizar tareas rutinarias y proporciona inteligencia de amenazas en tiempo real.

El papel de los operadores humanos en la ciberdefensa OT basada en IA

Esta sinergia permite que los operadores humanos se concentren en tareas más estratégicas y de alto impacto, mejorando así las capacidades defensivas de la organización.

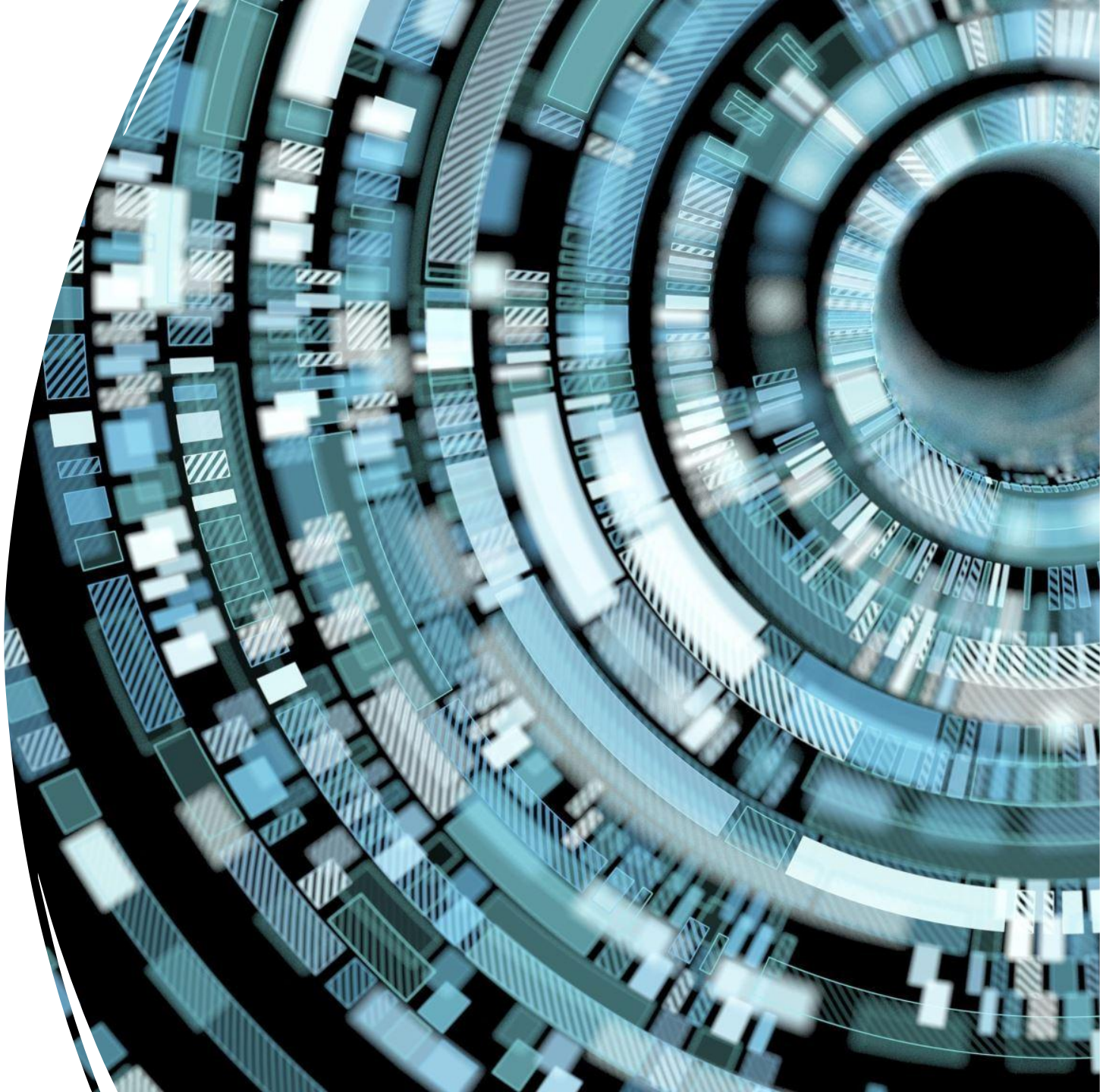
Además, parte de nuestra responsabilidad en esta simbiosis es desarrollar una comprensión profunda de la IA y estar preparados para responder a las preguntas que surgen en torno a esta tecnología en constante evolución

Evaluando Confidencialidad Integridad y Disponibilidad con el uso de la IA

¿Qué significa el desarrollo de la IA para la confidencialidad de los datos?

•El desarrollo e implementación de la Inteligencia Artificial (IA) en la ciberseguridad para entornos de Tecnología Operativa (OT) puede abordarse de dos maneras principales:

- Mediante el desarrollo interno de soluciones específicas
- Personalizando plataformas de IA populares y ya existentes en el mercado.



Desarrollo Interno de IA en Ciberseguridad OT:

- Cuando una organización decide desarrollar internamente su IA, tiene el control total sobre cómo se diseñan y configuran las soluciones.
- Esto permite una personalización completa para abordar las necesidades específicas de la infraestructura OT.
- Además, el desarrollo interno facilita una integración más estrecha con los sistemas y procesos ya existentes, y asegura que toda la gestión de datos se realice bajo las políticas de seguridad y confidencialidad de la propia organización.
- Sin embargo, este enfoque requiere una inversión significativa en tiempo, recursos y talento especializado.

Personalización de Plataformas Externas de IA:

- Otra opción es utilizar plataformas de IA disponibles comercialmente y adaptarlas a las necesidades específicas de la ciberseguridad OT.
- Estas plataformas, desarrolladas por empresas tecnológicas líderes, suelen ofrecer funcionalidades avanzadas y actualizaciones continuas.
- Aunque esta opción puede ser más rápida y menos costosa que el desarrollo interno, conlleva ciertos riesgos, especialmente en lo que respecta al manejo y la protección de datos sensibles.

Evaluación de Confidencialidad y Protección de Datos:

- Las organizaciones deben realizar una evaluación exhaustiva de cómo se manejará la confidencialidad y el intercambio de datos.
- Es crucial asegurarse de que la plataforma cumple con los estándares de seguridad más altos y que existen garantías contractuales para la protección de la información sensible.
- Entender dónde y cómo se almacenan los datos, quién tiene acceso a ellos, y cómo se protege la información contra accesos no autorizados o brechas de seguridad.
- Considerar las implicaciones legales y de cumplimiento normativo, especialmente si los datos cruzan fronteras internacionales o están sujetos a regulaciones específicas.

¿Podemos confiar realmente en los sistemas de IA?

El sector de las infraestructuras críticas muestra reservas a la hora de adoptar sistemas de IA, y dado el papel esencial que juega la ciberseguridad en las OT, esta precaución es justificada.

La IA puede desarrollarse mediante pruebas exhaustivas, procesos de validación rigurosos y una comunicación clara sobre sus capacidades y limitaciones.

¿Podemos confiar realmente en los sistemas de IA?

A medida que la IA continúe demostrando su efectividad, es probable que la confianza en su aplicación en la ciberdefensa crezca.

Es esencial identificar cuidadosamente los contextos en los que la IA puede ser más eficaz, maximizando sus beneficios mientras se mantiene un control total sobre los sistemas y equipos de producción críticos, lo cual es crucial para garantizar un alto tiempo de actividad.

sea una formidable superficie de ataque?

- Aunque la IA fortalece la seguridad, también puede representar una nueva superficie de ataque.

- Los adversarios podrían intentar alterar los modelos de IA o los datos utilizados para su entrenamiento con el fin de engañar a los sistemas de seguridad.

¿Estamos entrenando a la IA para que sea una formidable superficie de ataque?

- Existe un riesgo real de que las predicciones generadas por la IA sean manipuladas deliberadamente para provocar fallos críticos en los procesos de toma de decisiones.

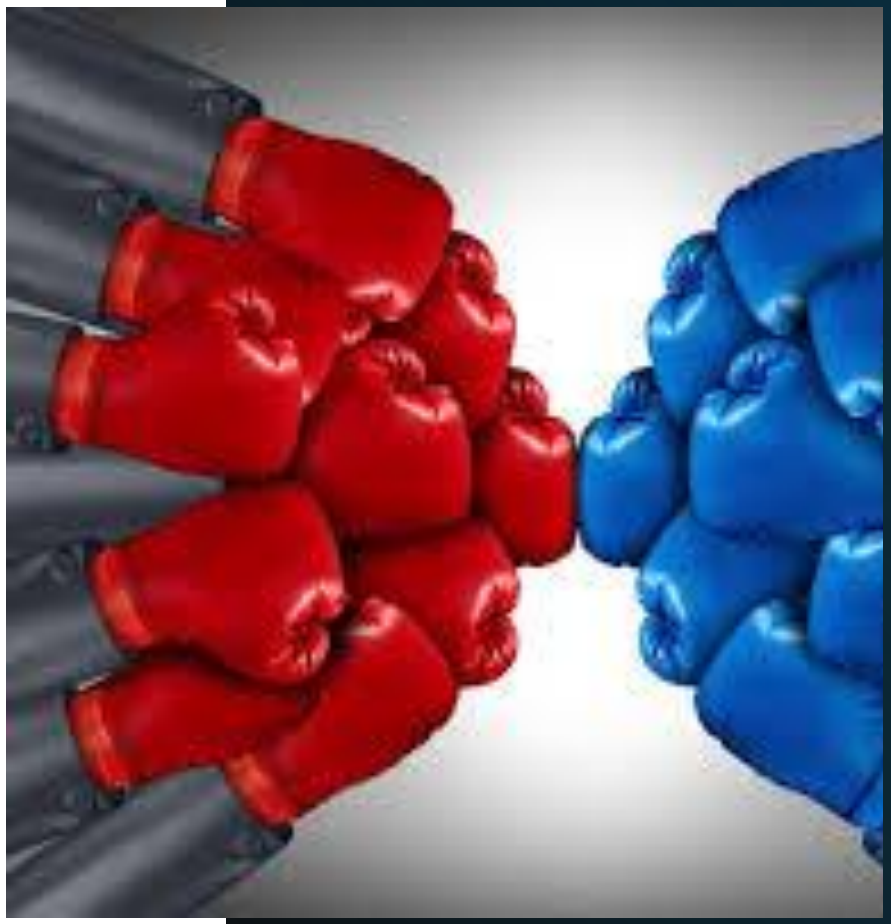
- Esto destaca la importancia de mantener una supervisión constante y de implementar defensas robustas alrededor de los sistemas de IA para protegerlos contra posibles explotaciones.

La IA y los equipos de Red y Blue Team

¿Cómo afectará la IA a los simulacros cibernéticos Red Team/Blue Team?

- La Inteligencia Artificial (IA) está preparada para transformar radicalmente las cibersimulaciones realizadas por los equipos rojos y azules, potenciando tanto las capacidades ofensivas como defensivas.

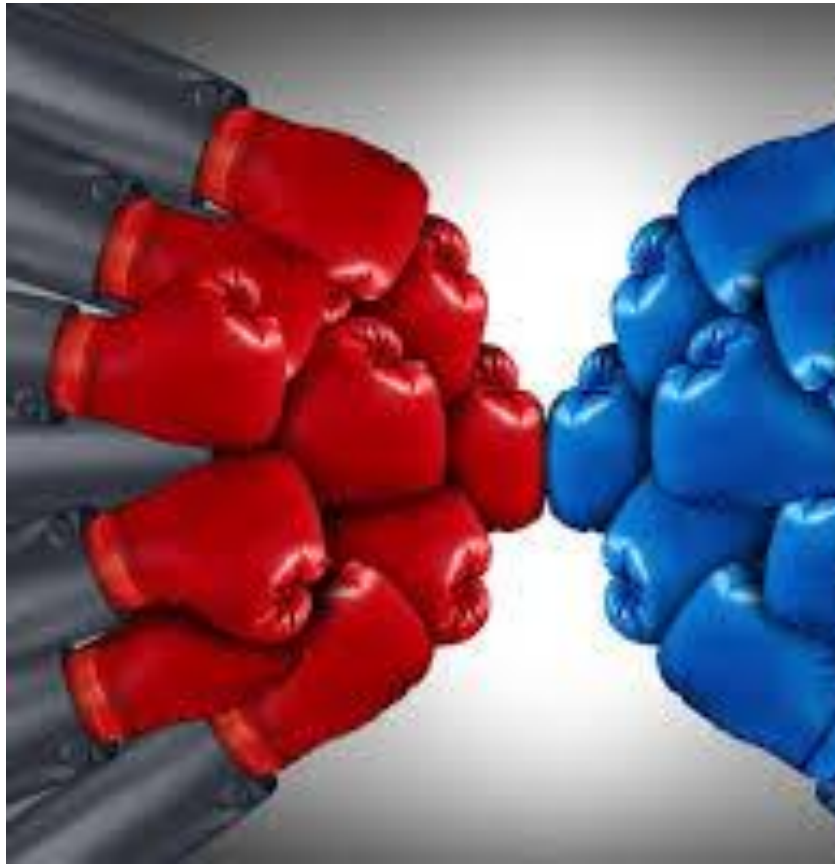
- **Para los equipos rojos**, las simulaciones de ataques impulsadas por IA pueden hacer que los escenarios de amenazas sean aún más sofisticados y dinámicos, emulando con precisión las tácticas en constante evolución de los atacantes reales.



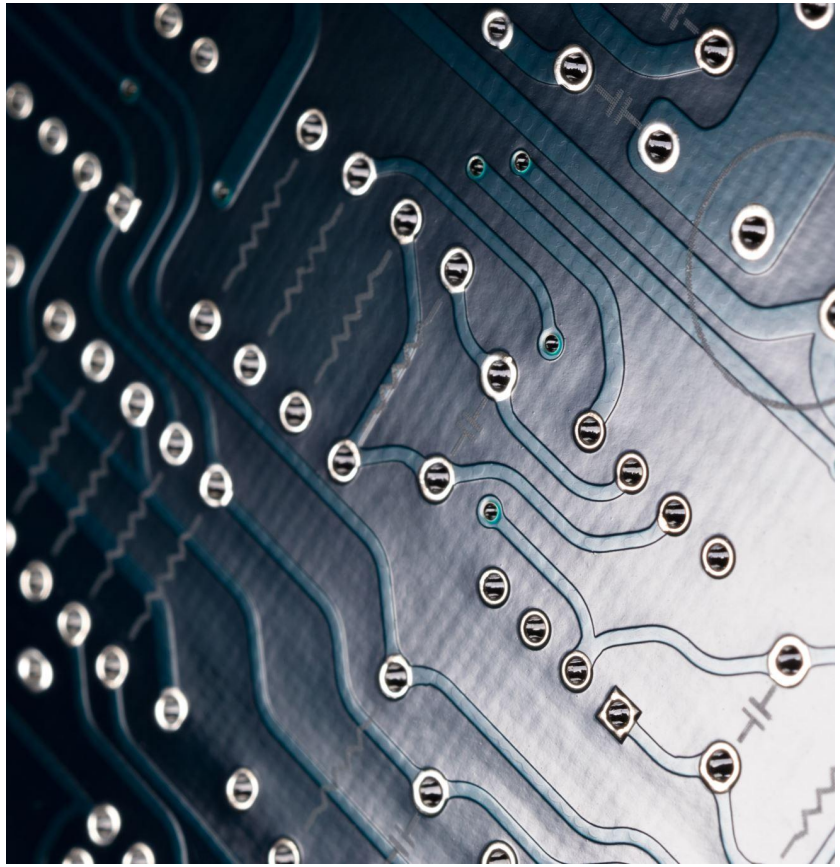
¿Cómo afectará la IA a los simulacros cibernéticos Red Team/Blue Team?

- **Para los equipos azules**, logra reforzar significativamente la detección de amenazas y la respuesta a incidentes al identificar rápidamente patrones inusuales, vulnerabilidades emergentes y anomalías en el comportamiento del sistema, lo que mejora las defensas y ayuda a automatizar tareas rutinarias que anteriormente consumían mucho tiempo.
- Puede extraer información crítica mediante el análisis profundo de grandes volúmenes de datos, permitiendo una toma de decisiones más eficiente, medidas de seguridad proactivas y una mejor anticipación de futuras amenazas.

- **En resumen, la integración de IA no solo optimiza la eficiencia operativa, sino que también eleva el nivel de ciberseguridad, preparando a las organizaciones para enfrentar un panorama de amenazas en constante cambio.**



- La integración de **TI y OT**, junto con la adopción de la **Inteligencia Artificial (IA)** para la detección y respuesta a amenazas, marca un avance significativo en la seguridad de un entorno industrial cada vez más digitalizado.
- La **IA** puede ser un multiplicador de fuerzas que permite a los equipos de seguridad no sólo responder más rápido que los ciberatacantes, sino también anticipar y actuar de antemano, detectando desvíos en patrones que serían imperceptibles para una persona.
- La tecnología y las herramientas de ciberseguridad de **IA** están en las primeras etapas de adopción, con un mercado global que se espera crezca en US$19 mil millones entre 2021 y 2025.



Las organizaciones que aborden estos desafíos de manera efectiva no solo asegurarán su supervivencia, sino que también se posicionarán como líderes en la industria.

Las industrias pueden liderar en la protección contra amenazas de ciberseguridad y asegurar sus operaciones en este mundo digital en rápida evolución, fortaleciendo la seguridad y fomentando la eficiencia operativa.

La seguridad en redes **OT** es, por lo tanto, un pilar crucial en la estrategia corporativa moderna, esencial para mantener la integridad y confiabilidad de los procesos industriales vitales.

Presente y futuro del aprendizaje

La Inteligencia Artificial (IA) está transformando la defensa en ciberseguridad de las Tecnologías Operativas (OT), presentando tanto oportunidades como desafíos. Aunque se perfila como un aliado valioso, su integración debe abordarse con una evaluación cuidadosa de sus capacidades y limitaciones.

La sinergia entre operadores humanos e IA es esencial para fortalecer la resiliencia, y a medida que la IA siga demostrando su eficacia, la confianza en su aplicación crecerá de manera natural en los contextos adecuados.

El futuro de la ciberseguridad en los sistemas operativos radica en superar los desafíos éticos, gestionar los ciclos de retroalimentación, y adaptarse continuamente a un entorno digital en constante cambio.

Un 73% de las organizaciones de OT se han visto afectadas por un ataque

En el último año, los ciberataques que comprometen los sistemas de tecnología operativa (OT) han aumentado considerablemente.

2023 :el 49% de las organizaciones encuestadas reportaron intrusiones que afectaron solo a los sistemas OT o a ambos, OT y TI.

2024: ha crecido hasta casi el 73%.

En este sentido, el reciente informe de Fortinet ha revelado que las intrusiones que afectaron exclusivamente a los sistemas OT aumentaron del 17% al 24%.

La región de EMEA (Europa, Oriente Medio y Africa) ha presentado el mayor porcentaje de ataques a sistemas OT con un 33%, seguida por Latinoamérica con un 28%, Norteamérica con un 19% y Asia Pacífico con un 18%.

El Estado de la Tecnología Operativa y la Ciberseguridad 2024 muestra que mientras que las organizaciones de OT están haciendo progresos significativos en reforzar su postura de seguridad, los equipos siguen enfrentándose a importantes retos a la hora de garantizar la seguridad de los entornos TI/OT convergentes.

La adopción de herramientas y capacidades esenciales para mejorar la visibilidad y las protecciones en toda la red será vital para estas organizaciones a la hora de reducir el tiempo medio de detección y respuesta y, en última instancia, reducir el riesgo general de estos entornos

Camino a tomar en la adopción de la IA

Hoja de Ruta

- **Desplegar la segmentación.**

- Reducir las intrusiones requiere un entorno OT reforzado con fuertes controles de políticas de red en todos los puntos de acceso.

- **Establecer controles de visibilidad y compensación para los activos de OT**.

- Las organizaciones deben ser capaces de ver y comprender todo lo que hay en la red de OT.
- Una vez establecida la visibilidad, las organizaciones deben proteger todos los dispositivos que parezcan vulnerables, lo que requiere controles compensatorios de protección creados específicamente para dispositivos OT sensibles.

- **Integrar la OT en las operaciones de seguridad y en la planificación de la respuesta a incidentes**.

- Las organizaciones deberían estar madurando hacia SecOps IT-OT. Para lograrlo, los equipos deben tener en cuenta específicamente la OT en relación con los planes de SecOps y de respuesta a incidentes.

Hoja de Ruta

Adoptar servicios de seguridad e inteligencia sobre amenazas específicos para OT. La seguridad de las OT depende de la concienciación y de los conocimientos analíticos precisos sobre los riesgos inminentes. Las organizaciones deben asegurarse de que sus fuentes de contenido e inteligencia sobre amenazas incluyan información sólida y específica sobre OT en sus feeds y servicios.

Un enfoque de la seguridad basado en plataformas puede ayudar a las organizaciones a consolidar proveedores y simplificar su arquitectura. **Una sólida plataforma de seguridad diseñada específicamente para proteger tanto las redes de TI como los entornos de OT** puede proporcionar integración de soluciones para mejorar la eficacia de la seguridad, al tiempo que permite una gestión centralizada para mejorar la eficiencia.

Como mantener a los equipos protegidos

Realizar evaluaciones de seguridad periódicas de los sistemas OT para identificar y eliminar posibles problemas de ciberseguridad.

Establecer un proceso continuo de evaluación y triaje de vulnerabilidades como base para una gestión eficaz.

Soluciones de seguridad, que ofrecen una asistencia eficiente con una fuente de información procesable.

Actualizar los componentes clave de la red OT de la empresa; aplicar correcciones y parches de seguridad o implementa medidas compensatorias rápidamente. Es crucial para prevenir un incidente grave que podría llegar a costar millones debido a la interrupción del proceso de producción.

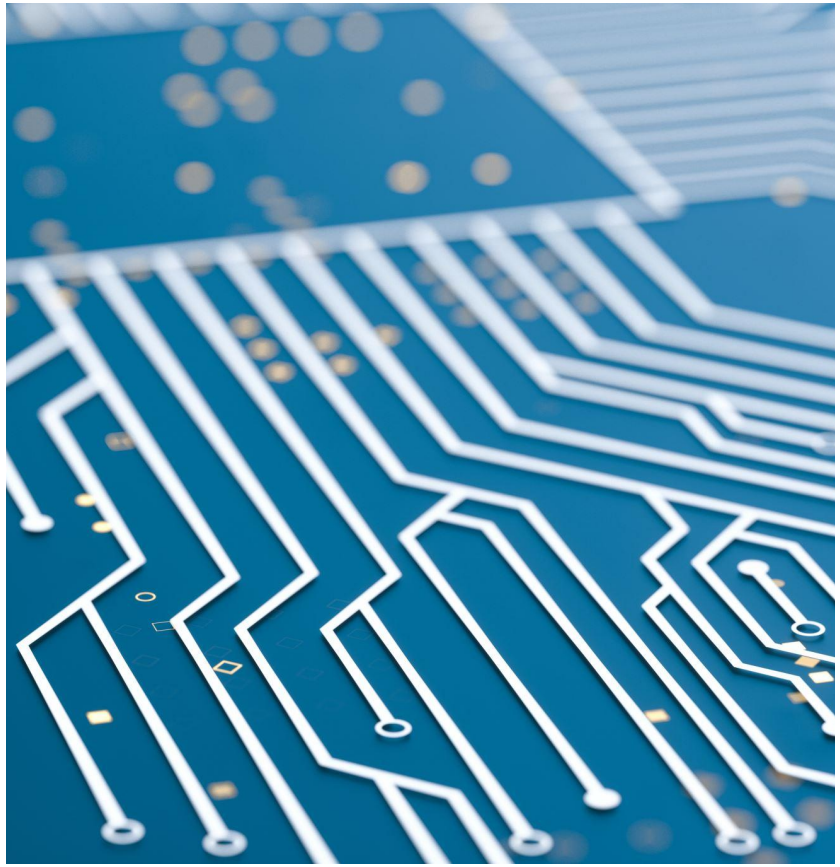
UTILIZAR SOLUCIONES EDR PARA LA DETECCIÓN OPORTUNA DE AMENAZAS SOFISTICADAS, INVESTIGACIÓN Y REPARACIÓN EFICAZ DE INCIDENTES.

MEJORAR LA RESPUESTA ANTE TÉCNICAS MALICIOSAS NUEVAS Y AVANZADAS MEDIANTE LA CREACIÓN Y EL REFUERZO DE LAS CAPACIDADES DE PREVENCIÓN, DETECCIÓN Y RESPUESTA DE TUS EQUIPOS.

FORMAR Y EDUCAR EN SEGURIDAD EN OT A LOS EQUIPOS DE SEGURIDAD DE TI Y EL PERSONAL DE OT.

Retos para la seguridad de los datos

- Con la creciente integración de tecnologías avanzadas como la IA, el IoT , la seguridad de los datos se convierte en una preocupación importante.
- Los dispositivos conectados y los sistemas digitales, aunque mejoran la eficiencia, también exponen las operaciones de fabricación a amenazas de ciberseguridad.
- Proteger los datos sensibles de producción, la propiedad intelectual e incluso los sistemas operativos de los ciberataques será crucial para los fabricantes.



Pronósticos

- Los pronósticos positivos y los negativos establecen un marco de revisión que implica múltiples aristas de análisis para concretar nuevas oportunidades o potenciar nuevas amenazas.

- La inteligencia artificial generativa ha puesto en el escenario las posibilidades que tiene tanto para el bien como para el mal.

- El mal uso de esta tecnología por los adversarios, sugiere un panorama incierto e inexplorado que puede sorprender a la humanidad en el mediano y largo plazo.

Pronósticos 2025 2030

Una encuesta realizada en 2023 entre 350 fabricantes reveló que **más del 70% ya ha implantado alguna forma de IA en sus operaciones**. Las tres áreas principales son la producción, la formación de los empleados y el servicio al cliente.(Rootstock)

Concretamente en producción, la **automatización es el tipo de IA más utilizado en esta fase** (60%), aunque los fabricantes están explorando otros tipos, como la IA predictiva (37%) y la IA generativa (35%)

Los resultados también mostraron que **la IA es fundamental para las estrategias tecnológicas y las hojas de ruta**, y sólo Cloud/SaaS proporciona más retorno de la inversión que la IA.(Rockwell Automation)

A pesar de los beneficios potenciales que los fabricantes están obteniendo con la IA, los **obstáculos** más **importantes para su adopción son la falta de conocimientos internos** (49%), la dificultad de integración (43%) y los elevados costos de implantación (37%).(Fuente: Rootstock)

Pronósticos 2025 2030

A pesar de estos retos, **el 76% afirma estar entusiasmado con el uso de la IA**. Más aún, el 91% está de acuerdo en que la IA es importante para el futuro de la fabricación.(Rootstock)

Los fabricantes prevén aumentar significativamente sus presupuestos de IA en los próximos 12-18 meses, con un 82% de intención de ampliar sus inversiones en IA. Entre estas inversiones, la producción, el control de calidad y la optimización de procesos son las principales áreas para el despliegue de recursos adicionales de IA.(Rockwell Automation)

En total, **se espera que la inversión en IA para la fabricación crezca un 57%** hasta 2026, pasando de 1.100 millones de dólares en 2020 a 16.700 millones en 2026.(Foro Económico Mundial)

Pioneros en fabricacion

•A la cabeza de la transformación de la fabricación impulsada por la IA, **empresas como Siemens, Toyota y Tesla demuestran el notable potencial de la inteligencia artificial**.

•Estos pioneros están aprovechando las tecnologías de IA para revolucionar sus métodos de producción y establecer nuevos estándares de eficiencia y calidad en el sector manufacturero.

20° Congreso URUMAN + 3° Congreso INGURU

Preguntas

A/P Ethel Kornecki, CISA, CISM,CDPSE
Asistente de la Coord. Académica de Ciberseguridad
Director de Consultoria Krav Maga Hacking Uruguay
kornecki@ort.edu.uy / ekornecki@kmhcorp.com
093 546 299