SecuriTIC
Latinoamérica

Información de Valor para Integradores de Seguridad Electrónica y Ciberseguridad

Chat-GPT

¿Enemigo o aliado en ciberseguridad?

VIDEOVIGILANCIA

Hikvision México trabaja para que más mujeres se unan a la industria de la seguridad

CIBERSEGURIDAD

SonicWall entrega el Partner Award 2023 a sus partners más valiosos en Latinoamérica

Abril 2023 Año 10 Número 118 www.securitic.lat

HIKVISION®

Connect, Converge & Collaborate for a Brighter Future

@HikvisionMx
www.hikvision.com/es-la

Hikvision México
sales.mexico@hikvision.com

Índice

Carlos Alberto Soto
carlos@securitic.com.mx
Director General
Editor

Gabriela Pérez
Atención
Corporativa

Alejandro Teodores
webmaster@securitic.com.mx
Diseño Gráfico
Webmaster

Alfredo Escobedo
Telemarketing

Karla Soto
Social Media

Contacto Editorial
y de ventas
carlos@securitic.com.mx

Contacto de Ventas
ventas@securitic.com.mx

www.securitic.lat facebook/SecuriTIC linkedin/securitic twitter/@SecuriTICMX
Visita nuestro aviso de privacidad en: www.securitic.lat

SecuriTIC, revista con periodicidad mensual. Abril de 2023. Editor responsable: Carlos Alberto Soto Benítez. Número del Certificado de Reserva de Derechos al Uso Exclusivo del Título que expide el Instituto Nacional del Derecho de Autor: En Trámite. Número del Certificado de Licitud de Título y Contenido: En Trámite. Domicilio de la publicación: Valle de Ceylán 9-B, Col. El Olivo II, Tlalnepantla, Estado de México, C.P. 54110. Imprenta: Gráfica Romero con domicilio en Calle 3A Oriente, Mz. 7, L 4, colonia Isidro Fabela, Ciudad de México, C.P. 14030. Distribuidor: SEPOMEX. Registro Postal en Trámite.

Chat GPT, ¿enemigo o aliado en ciberseguridad?

A tan solo cuatro meses de su lanzamiento, la herramienta de inteligencia artificial de nombre Chat-GPT ha causado grandes controversias. Desarrollada por la empresa OpenAI, esta tecnología fue diseñada originalmente como un modelo de lenguaje proveído de una gran cantidad de datos de texto, con la capacidad de responder preguntas comprendiendo el contexto.

Uno de los primeros ejemplos que se dieron a conocer fue la forma en que esta plataforma podía generar textos coherentes y con lenguaje natural; y la forma en que podría potenciar el desarrollo de chatbots a fin de que pudieran entregar respuestas más coherentes y precisas.

Sin embargo, enseguida hubo quien puso a prueba las capacidades de Chat-GPT para exponer las capacidades de la herramienta en el desarrollo de malware. En este sentido, ESET hizo una serie de ejercicios y determinaron que el sistema era amigable y utilizaba lenguaje accesible por lo que hace posible el uso o interacción para prácticamente cualquier tipo de usuario.

En el caso de riesgos de ciberseguridad, los expertos ESET expusieron que esta herramienta podría facilitar ciertas tareas a los cibercriminales. Y lo ejemplificaron generando preguntas para desarrollar un supuesto ataque de phishing; y en otro ejercicio, solicitaron ayuda para generar código malicioso. El resultado fue que en ambos casos la plataforma entregó las peticiones, no sin antes advertir de algunas implicaciones legales.

A mediados de marzo de 2023, Open AI lanzó la siguiente versión denominada GPT-4, la cual fue anunciada con mejores capacidades de razonamiento y, un punto muy importante, 82% menos probabilidades de responder a solicitudes de contenido no permitido.

En este sentido, Arturo Torres, Estratega de Inteligencia de Amenazas para FortiGuard Labs de Fortinet América Latina y el Caribe, explicó que ante la llegada de herramientas que hacen uso intensivo de inteligencia artificial como ChatGPT o GPT-4 se puede esperar que las ciberamenazas sigan evolucionando y creciendo, lo que convierte a la prevención y educación en los mejores aliados para mantenernos seguros.

Por su parte, Manuel Acosta, Director General para Hillstone Networks México, añadió que contar con la ayuda de un sistema de inteligencia artificial como ChatGPT no significa que el desarrollo de código malicioso haya llegado al punto de ser indetectable.

El ejecutivo reiteró que es importante tener en cuenta que cualquier herramienta, incluyendo ChatGPT, puede ser utilizada tanto para fines legítimos como ilegítimos. La responsabilidad recae en los usuarios de la herramienta para utilizarla de manera ética y legal; y en los desarrolladores para implementar medidas de seguridad y control de calidad para evitar el uso malintencionado.

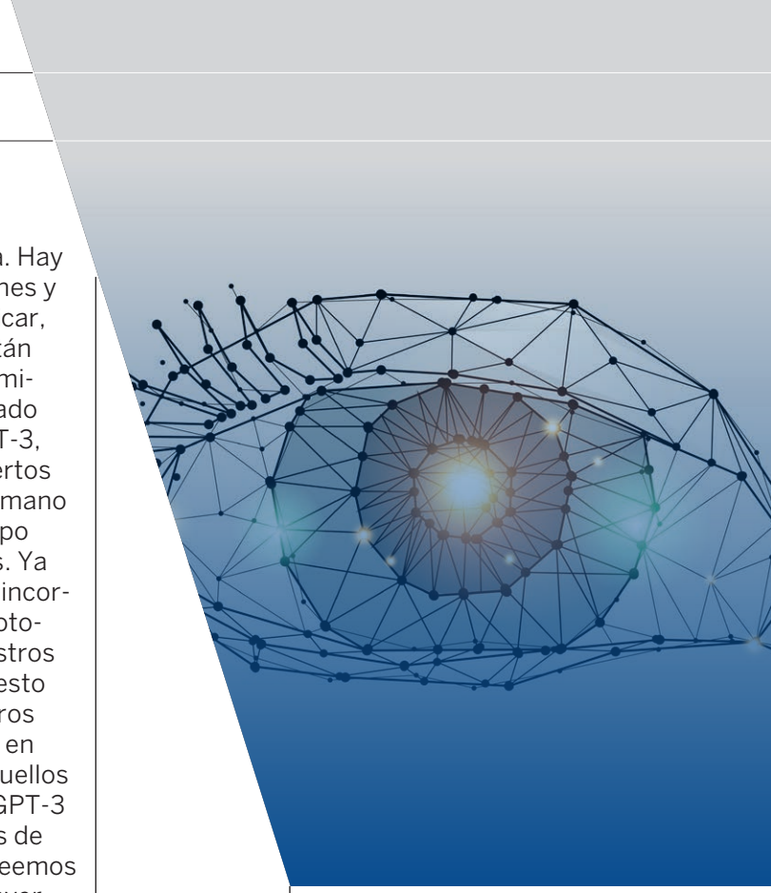
EL OTRO LADO DE LA MONEDA

Si bien es cierto que existe la forma en que ChatGPT o GPT-4 sean utilizadas por ciberdelincuentes, existe otra manera de ver los beneficios que ésta tecnología podía aportar al mundo de la ciberseguridad.

Tal es el caso de Sophos, que ha decidido sacarle provecho a ChatGPT para para simplificar la búsqueda de actividad maliciosa en conjuntos de datos de software de seguridad, filtrar con mayor precisión el spam y acelerar el análisis de los ataques binarios “Living Off the Land” (LOLBin).

Al respecto la empresa compartió que los investigadores de Sophos X-Ops, incluido el científico principal de datos de SophosAI,

“Es posible que dicha herramienta pueda ser utilizada por cibercriminales para llevar a cabo actividades ilegales como generar correos electrónicos falsos o mensajes de texto persuasivos para intentar engañar a las personas y hacerlas caer en una trampa. Además, los cibercriminales podrían utilizar ChatGPT para mejorar su capacidad de crear algoritmos de phishing y otros ataques de ingeniería social que sean más sofisticados y difíciles de detectar”, destacó Acosta.



Younghoo Lee, han estado trabajando en tres proyectos prototipo que demuestran el potencial de GPT-3 como asistente de defensores de la ciberseguridad. Los tres utilizan una técnica llamada "aprendizaje de pocos disparos" para entrenar el modelo de IA con solo unas pocas muestras de datos, reduciendo la necesidad de recopilar un gran volumen de datos preclasificados.

En la primera aplicación el fabricante puso a prueba este método de aprendizaje de pocos disparos utilizando una interfaz de consulta de lenguaje natural para el tamizado de actividades maliciosas en software de seguridad de telemetría; específicamente, Sophos probó el modelo contra su producto de detección y respuesta de endpoints. Con esta interfaz, los defensores pueden filtrar a través de la telemetría con comandos básicos en inglés, eliminando la necesidad de que los defensores entiendan SQL o la estructura subyacente de una base de datos.

En segunda instancia, la firma probó un nuevo filtro de spam utilizando ChatGPT y descubrió que, en comparación con otros modelos de aprendizaje automático para el filtrado de spam, el filtro que utiliza GPT-3 era significativamente más preciso.

Y en el tercer proyecto, los investigadores de Sophos pudieron crear un programa para simplificar el proceso de ingeniería inversa de las líneas de comando de LOLBins. Dicha ingeniería inversa es notoriamente difícil, pero también crítica para comprender el comportamiento de LOLBins y poner fin a esos tipos de ataques en el futuro.

"Una de las crecientes preocupaciones dentro de los centros de operaciones de seguridad es la gran cantidad de 'ruido' que entra. Hay demasiadas notificaciones y detecciones para clasificar, y muchas empresas están lidiando con recursos limitados. Hemos demostrado que, con algo como GPT-3, podemos simplificar ciertos procesos intensivos en mano de obra y devolver tiempo valioso a los defensores. Ya estamos trabajando en incorporar algunos de los prototipos anteriores en nuestros productos, y hemos puesto los resultados de nuestros esfuerzos a disposición en nuestro GitHub para aquellos interesados en probar GPT-3 en sus propios entornos de análisis. En el futuro, creemos que el GPT-3 puede convertirse en un copiloto estándar para los expertos en seguridad", dijo Sean Gallagher, investigador principal de amenazas de Sophos.

Por otro lado, Microsoft anunció recientemente el lanzamiento de Security Copilot, que utiliza los beneficios de GPT-4 directamente en el desarrollo de una herramienta de ciberseguridad. De acuerdo con la compañía, Security Copilot combinará la amplia huella de inteligencia de amenazas de Microsoft con la experiencia líder en la industria para mejorar el trabajo de los profesionales de seguridad a través de un asistente de inteligencia artificial fácil de usar.

Además, dicha solución aprenderá y mejorará de manera continua para garantizar que los equipos de seguridad operen con los últimos conocimientos sobre los atacantes, sus tácticas, técnicas y procedimientos. El producto brindará acceso continuo a los modelos OpenAI más avanzados para admitir tareas y aplicaciones de seguridad exigentes. Su visibilidad de las amenazas se basa tanto en los datos de seguridad de la organización del cliente como en la amplia huella de análisis de amenazas de Microsoft.

Con estos ejemplos, queda confirmado que el uso de Chat-GPT o GPT4 pueden ser vistos desde dos perspectivas distintas, en beneficio de los ciberdelincuentes o ayudando a las empresas de ciberseguridad a desarrollar nuevas tecnologías para hacer frente a los ataques.

En este sentido, Manuel Acosta, Director General para Hillstone Networks México, reiteró que aun cuando usuarios malintencionados hagan uso de herramientas como ChatGPT o GPT-4 para desarrollar ataques maliciosos, lo cierto es que actualmente existen herramientas que pueden hacer frente a los desafíos más sofisticados, tal es el caso de Hillstone iSource XDR.

En conclusión, ChatGPT o GPT-4 puede ser utilizado como facilitador de los ciberdelincuentes o como aliado en el desarrollo de soluciones de ciberseguridad. Y conforme la tecnología siga avanzando veremos cómo la lucha por la ciberseguridad se va haciendo cada vez más compleja.

Milestone anuncia el lanzamiento de XProtect 2023 R1 con mejoras en la experiencia de usuario

Milestone Systems presenta la última versión de su VMS, el XProtect 2023 R1, esta actualización mejora las innovaciones anteriores del XProtect para ofrecer una experiencia de usuario más integrada, potente y fácil de usar. Con una tecnología de video integral y de alta calidad, la compañía satisface la creciente demanda del mercado por soluciones de video basada en datos.

La actualización R1 para XProtect mejora a partir de las necesidades básicas de los usuarios de software de gestión de video (VMS), brindando soluciones confiables, potentes y fáciles de manejar en una plataforma abierta, que ofrecen flexibilidad y seguridad para cumplir todos los requerimientos de la gestión de video totalmente integrada y basada en datos. Con varias mejoras a la experiencia del usuario y el desempeño del sistema, incluidas herramientas de colaboración para operadores y eficiencias en las verificaciones previas a la instalación, la actualización 2023 R1 es una mejora de software altamente recomendada para todos los usuarios de XProtect.

MEJORAS PARA LOS OPERADORES

La actualización de software 2023 R1 ofrece importantes mejoras en la experiencia del usuario, colaboración con operadores y conciencia situacional. La experiencia de usuario ahora incluye renovaciones UX en las interfases Smart Client y Web Client, con una interfaz moderna e intuitiva y mejor navegación, los usuarios pueden acceder con facilidad al video y gestionar sus datos sin ninguna dificultad y mayor eficiencia. Las herramientas de colaboración para operadores han tenido mejoras superiores con funciones como compartir marcadores, fondo Picture in Picture y capturas de pantalla nativas en el Mobile Client. Estas herramientas mejoran la eficiencia y la comunicación de los operadores, permitiéndoles compartir registros con facilidad y colaborar en el análisis de datos de video. Además, el 2023 R1 incluye más funciones de conciencia situacional con mapas inteligentes en los clientes Mobile. Esta función ofrece a los operadores una visión panorámica en forma de mapa de las cámaras y dispositivos, lo cual permite agilizar los tiempos de respuesta.

FACILIDAD PARA COMPARTIR DATOS DE VIDEO

La función de fondo Picture in Picture permite que los operarios mantengan la atención en una cámara en particular mientras realizan otras tareas, garantizando la conciencia situacional permanente. Además de eso, las capturas de pantalla nativas en los Mobile Client brindan a los operarios una forma fácil de obtener y compartir capturas de video, mejorando la colaboración y la comunicación entre miembros del equipo.

INSTALACIONES VELOCES Y EFICIENTES

La actualización de software incluye una mejor experiencia de instalación, como la disponibilidad de una verificación de prerrequisitos del sistema, copias de seguridad de bases de datos SQL y tiempos de instalación más veloces. Estas mejoras garantizan que la instalación y la configuración del VMS sea más eficiente, lo que a su vez reduce el tiempo y el esfuerzo requerido para tener el sistema encendido y funcionando.

NUEVOS WEBHOOKS EN XPROTECT

Con XProtect 2023 R1, las normas en Management Client ahora soportan la acción de los accesorios webhooks. Esto permite que los usuarios creen un ítem webhook en Management Client con la URL desde cualquier servicio de terceros y posteriormente, configuren una regla en XProtect para activarlo cuando se presente un evento. Con los webhooks, los administradores pueden integrarse con plataformas sin código como Zapier o IFTTT. Nunca ha sido tan sencillo transformar los eventos que se presentan en XProtect en mensajes de texto, llamadas, nuevos tickets, mensajes al equipo o incluso luces parpadeantes.

RESUMEN DE LA ACTUALIZACIÓN 2023 R1

La actualización 2023 R1 para el VMS XProtect proporciona una mejor experiencia de usuario, colaboración entre operarios, conciencia situacional y eficiencias en la instalación. Con funciones como renovaciones UX, compartir marcadores, fondo Picture in Picture, capturas de pantalla nativas y mapas inteligentes (Smart Maps), esta actualización brinda una mejoría importante en la eficiencia, la productividad y la efectividad general. Además de eso, las mejoras en la experiencia de instalación garantizan mayor facilidad y agilidad que nunca en el uso inicial de XProtect. Milestone Systems sigue liderando la industria en soluciones de gestión de video basadas en datos que trabajan en plataformas abiertas, lo cual pone en manos de los usuarios las herramientas que necesitan para gestionar y analizar sus datos de video con rentabilidad, facilidad y eficiencia.

Hanwha Techwin cambia su nombre a Hanwha Vision

Hanwha Techwin anunció que cambiará su nombre a Hanwha Vision, en la misma medida que la empresa amplía su oferta como proveedor de soluciones de visión global.

A través de esta expansión, Hanwha Vision irá más allá de sus productos de videovigilancia para proporcionar soluciones de visión de próxima generación que integren inteligencia artificial (IA) y tecnologías en la nube que ofrezcan perspectivas sobre las operaciones comerciales de los clientes, al tiempo que impulsan la innovación del mercado global.

"Al basarnos en nuestra competitividad principal a través de la innovación, continuaremos aliviando los puntos de dolor de nuestros clientes al tiempo que agregamos un nuevo valor con soluciones de visión avanzadas", dijo Soon-hong Ahn, Presidente y CEO de Hanwha Vision.

"A medida que ampliemos nuestro negocio desde la supervisión de la vigilancia y el análisis posterior a un evento, proporcionaremos información personalizada gracias al análisis de big data y soluciones procesables que no solo previenen incidentes, sino que también responden a ellos en tiempo real. Nuestras soluciones de nueva visión global serán decisivas para impulsar las estrategias operativas de los clientes", añadió Ahn.

En línea con este desarrollo empresarial, Hanwha Vision lanzará gradualmente el cambio de marca de sus filiales y subsidiarias en el extranjero, en función de las condiciones de cada mercado.

Hikvision México trabaja para que más mujeres se unan a la industria de la seguridad

A lo largo de la historia, han existido paradigmas que han limitado la incorporación o permanencia del talento femenino en la fuerza laboral. Sin embargo, las mujeres han logrado avances notables en muchas profesiones, al incrementar sus conocimientos y al mantenerse actualizadas para desarrollar nuevas competencias.

En el estudio Mujeres de la Alta Dirección en México 2023. Liderazgo femenino resiliente a largo plazo, de la Consultora KPMG, se menciona que "los retos que se presentan para las mujeres son diversos, específicamente por la falta de personalización y perspectiva de género en el diseño de las políticas de gestión de talento, las cuales deberían garantizar que existan las condiciones y oportunidades para que las mujeres se puedan desarrollar exitosamente en las distintas etapas de su vida; ser consideradas para promociones y aumentos de la misma forma en la que se considera a los hombres, y tener igualdad en los paquetes de compensación".

Con el creciente desarrollo tecnológico, unido al acelerado ritmo de la generación de información y la omnipresencia de las comunicaciones en el entorno social, hacen que nuestra sociedad esté en constante cambio con nuevas necesidades y valores.

"Actualmente observamos a más y más mujeres competentes, interesadas y preparadas para ocupar diversos cargos en empresas públicas y privadas, con la capacidad de resolver problemas y situaciones del trabajo de forma autónoma", comenta Fran Sánchez, Marcom Director de Hikvision México. "Fomentar y retener el talento femenino es imprescindible si queremos aprovechar todo el potencial humano. Es por ello que lanzamos Mujeres Hikvision, un programa de capacitación dirigido a todas las colaboradoras de nuestro canal de integración y distribución, quienes indudablemente aportan habilidades y talentos a las empresas donde laboran. Este es un proyecto que apenas inicia, pero queremos continuarlo hasta cerrar la brecha de género en la industria".

CAPACITACIÓN DESDE DOS FRENTES

El entrenamiento consto de dos cursos básicos que se llevaron a cabo en las oficinas de Hikvision en CDMX; donde las participantes conocieron las soluciones de seguridad de la empresa para sus productos y servicios. Adicionalmente se abordaron temas de Proyectos, desde un enfoque en gestión y venta de proyectos de integración, pero también desde una orientación en negocios de instalación.

Más de 30 participantes se dieron cita para conocer en detalle el enfoque en seguridad de los productos y soluciones de Hikvision; mujeres con diferentes cargos en la industria, desde aquellas gestionando y comercializando proyectos de integración, hasta las que están directamente relacionadas al negocio de la instalación.

"Este tipo de actividades nos emocionan mucho. Queremos abrir paso a la incursión femenina en diversos sectores e industrias como la de la seguridad. Por ello, buscamos que este proyecto de preparación y capacitación sea permanente, como una manera de fomentar una mayor inclusión e inspirar a las mujeres jóvenes a unirse a la industria de seguridad, la cual queremos sea más equitativa en México y abierta a la diversidad. Invitamos a todas las integradoras y mujeres interesadas en esta industria a seguir las redes sociales de Hikvision México, en las que estaremos anunciando próximas actividades que den continuidad a esta iniciativa", menciona, por su parte, Paulina Lord-méndez, Digital Marketing Manager de Hikvision México. "Este también fue un ejercicio de escucha para nosotros como empresa. Queremos conocerlas, entenderlas y saber cuáles son sus necesidades y retos en esta industria, para así crear mejores oportunidades que les permitan competir laboralmente y ocupar un lugar dentro de este sector".

HID e iPassport desarrollan nueva solución de verificación de identidades para el sector transporte

HID junto con iPassport firmaron recientemente un memorando de entendimiento para trabajar de manera conjunta en una nueva solución de verificación de identidad para la industria de transporte.

Transitar por un aeropuerto representa pasar por una serie de puntos de control y procesos, el check-in, la entrega de equipajes, los puestos de seguridad, las tiendas de zona franca, el acceso a las salas VIP, el abordaje, etc. Esto sumado a las demoras, cancelaciones de vuelos, confusiones con las maletas y la continua presión sobre el personal de aeropuertos, ha hecho la travesía del pasajero más compleja que nunca.

Las aerolíneas necesitan una verificación de identidad ágil y confiable para brindar a los pasajeros un viaje seguro y sin inconvenientes.

"Hoy en día, para transitar con seguridad por un aeropuerto se requiere un sistema de verificación de identidad permanente y constante que no sólo mejore la experiencia del pasajero, sino que optimice la eficiencia en todos los procesos. HID tiene grandes expectativas en la colaboración con iPassport para llevar esta nueva solución al mercado", afirmó Vito Fabbrizio, director administrativo de Biometría para las Tecnologías de Acceso Extendido de HID.

Con el enfoque modular de HID, las aerolíneas y operadores aeroportuarios podrán añadir funciones de verificación de identidad de manera rápida y sencilla a los sistemas existentes sin necesidad de "desmontar y cambiar todo" o de costosas migraciones a una plataforma totalmente nueva.

Esta solución modular incluye los siguientes componentes:

- Cámaras de reconocimiento facial
- Lectores de huellas dactilares, documentos de identidad y boletos
- Kits de Desarrollo de Software (SDK)
- Verificación de identidad y servidor biométrico
- Gestión de dispositivos
- Servicios biométricos profesionales

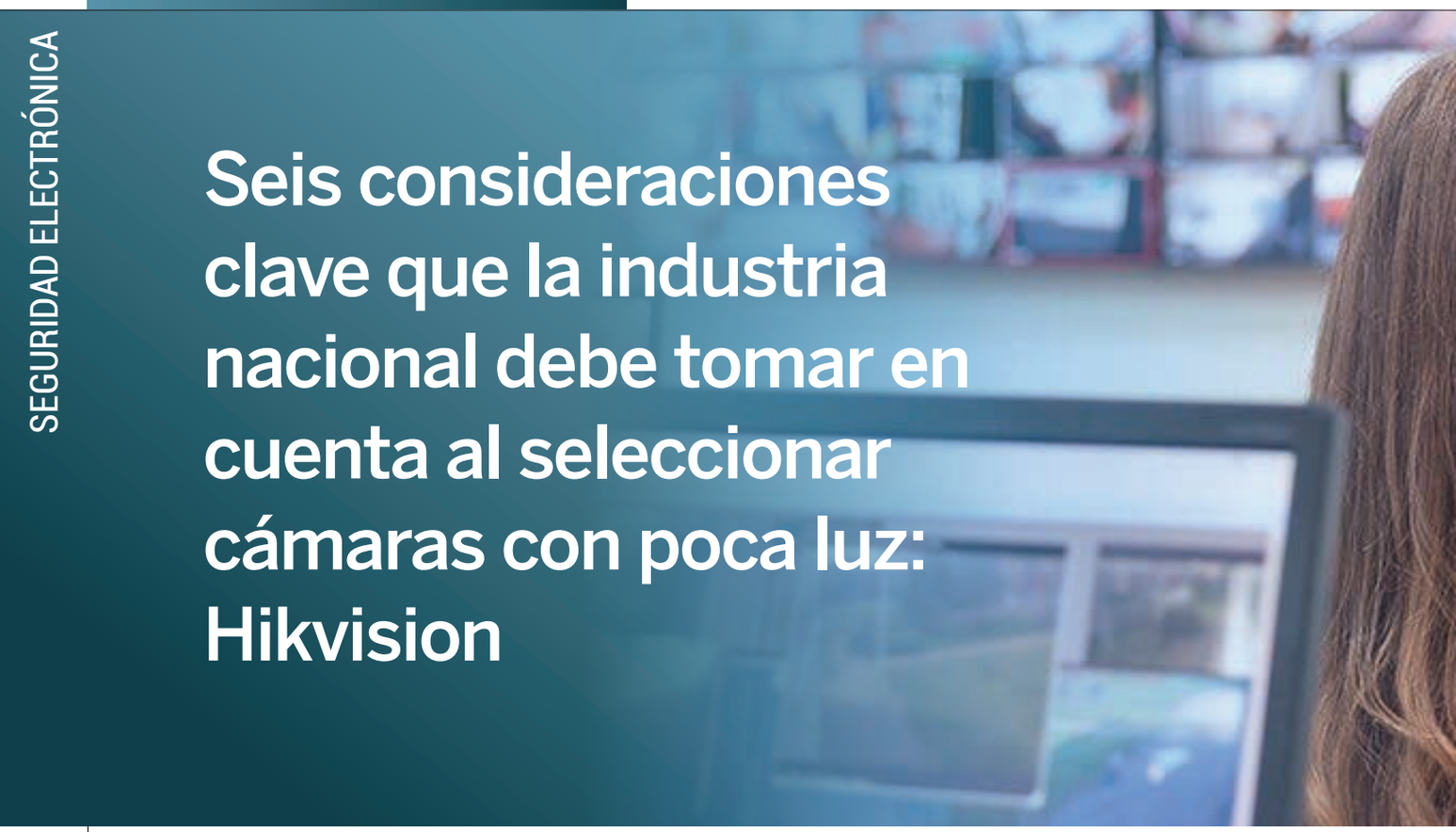
La patentada tecnología de imagen multiespectral (MSI) de HID, combinada con la inteligencia artificial (AI) con criterios éticos dentro de un Sistema de Identificación de Cámaras HID U.ARE.U, hacen posible alcanzar una precisión significativa al cotejar los datos biométricos.

El uso del reconocimiento facial en los aeropuertos está sujeto al consentimiento previo del pasajero en la reserva o en el check-in. Además, la información biométrica solo se guarda y se usa durante el tiempo que el pasajero esté en tránsito dentro del aeropuerto, en conformidad con las leyes aplicables de derecho a la privacidad.

Aparte de las aerolíneas y aeropuertos, otros sectores de la industria de viajes, como cruceros y hotelería, también pueden beneficiarse de:

- IA incorporada con criterios éticos para eliminar errores al momento de cotejar datos
- Detección de ataques de presentación facial (PAD) líderes en la industria para frustrar tentativas de falsificación
- Desempeño superior en condiciones de iluminación deficiente
- Detección automática de rostros, y verificaciones de calidad de captura e imagen, aun con mascarillas
- Procesamiento biométrico con seguridad de punto final en el dispositivo

Seis consideraciones clave que la industria nacional debe tomar en cuenta al seleccionar cámaras con poca luz: Hikvision



Cada vez más, las cámaras con poca luz están ganando terreno en la industria de la seguridad. La necesidad de una videovigilancia nocturna mejor y más eficaz es un factor importante, y los avances tecnológicos y la asequibilidad también son clave.

Las cámaras de seguridad se utilizan ampliamente para proporcionar evidencia clara de amenazas y emergencias de seguridad, las cuales generalmente ocurren de noche, cuando apenas se ven los detalles del objetivo. Justamente son las cámaras con poca luz las que brindan un buen rendimiento de imagen con detalles coloridos en entornos oscuros, ideales para los usuarios de video vigilancia.

"A medida que se desarrolla la tecnología, el rendimiento de las cámaras con poca luz ha mejorado. Por lo que serán asequibles para más y más usuarios", explica Miguel Arrañaga, Director Regional de Ventas de Hikvision. "Seremos testigos del crecimiento continuo del mercado de cámaras con poca luz".

¿Cómo debería elegir el usuario una cámara para condiciones de poca luz que se ajuste a sus necesidades y requisitos? A continuación, se mencionan los siguientes puntos para considerar:

SELECCIÓN DEL TIPO DE CÁMARA: La selección comienza con el tipo de cámara de poca luz que el usuario desea obtener. Actualmente, existen principalmente tres tipos de cámaras con poca luz: cámara IR, que cambia al modo blanco y negro por la noche; cámara con poca luz, que captura color las 24 horas del día, los 7 días de la semana; y cámara de seguridad regular con iluminación suplementaria. Cada uno tiene sus beneficios y se puede aplicar en diferentes aplicaciones.

CONSIDERACIONES DE ILUMINACIÓN COMPLEMENTARIA: El usuario también debe considerar el tipo de iluminación complementaria que desea utilizar: luz blanca, luz IR o híbrida. Nuevamente, esto depende del caso del usuario. La luz blanca se puede implementar en calles, patios y otras áreas abiertas al aire libre donde los usuarios no encuentran la luz molesta. La luz IR, por otro lado, es imperceptible y se puede aplicar en prácticamente todos los escenarios; la desventaja, por supuesto, es que ofrece imágenes en blanco y negro, y es posible que se pierdan detalles de color importantes.

La luz suplementaria híbrida, que combina los beneficios de la luz infrarroja y la luz blanca, puede ser una opción viable. Cuando se requiere que la luz sea encubierta, la luz suplementaria híbrida se puede configurar como modo "escala de Luxes".

CONOCER LA CALIFICACIÓN DE LUX: Esta clasificación de una cámara de se-

guridad se refiere al nivel de iluminación por el cual puede producir una buena imagen. Para su referencia rápida, la iluminancia bajo la luz solar directa mide hasta 100 000 lux; mientras que la iluminación de la oficina puede ser de alrededor de 500 lux y una noche nublada y sin luna de 0,0001 lux. Básicamente, cuanto menos luz, menor es el número de lux.

Una cámara con poca luz con una clasificación de lux de 0,001 lux o inferior puede proporcionar una capacidad de imagen lo suficientemente brillante sin luz adicional incorporada en un entorno urbano convencional con luz ambiental. Con un valor de clasificación de lux más bajo, la cámara con poca luz depende menos de la luz suplementaria con imágenes nocturnas lo suficientemente brillantes. La luz es necesaria para entornos más oscuros y la cámara puede proporcionar imágenes más brillantes con el mismo nivel de luz adicional.

TAMAÑO DEL SENSOR O MEGAPÍXELES: Cuando se trata de sensores de imagen para las mejores cámaras de seguridad con poca luz, el tamaño importa. Muchas personas pensarían que los megapíxeles más altos equivalen directamente a una mejor calidad de imagen, pero entran en juego muchos factores diferentes. Por tanto, con la misma resolución, el sensor de mayor tamaño funciona mejor, ya que puede captar más luz y generar una imagen más brillante.

ELEGIR EL FACTOR DE FORMA CORRECTO: Al elegir una cámara con poca luz, ¿qué factor de forma debería elegir el usuario: bala, domo o PTZ? Según el ejecutivo, depende de la distancia de monitoreo y los entornos. Para el monitoreo de larga distancia de 60 metros y más, se recomienda PTZ. Para el monitoreo de distancia estándar que está dentro de los 60 metros, se recomiendan formas de domo/torre para interiores y se recomienda forma de bala para exteriores.

ANALÍTICA DE VIDEO NECESARIA: El uso de análisis de video en cámaras con poca luz ha ganado popularidad en los últimos años, lo que permite funciones como detección de objetos y movimiento y alertas en tiempo real. La clasificación de personas y vehículos es muy práctica en cámaras con poca luz. Con análisis, los usuarios pueden detectar y recuperar objetivos claros humanos y de vehículos por la noche. Por ello resulta pertinente que el operador comprendiera las limitaciones que plantean las difíciles condiciones de poca luz y planifique en consecuencia.

PROPUESTA DE VALOR: A pesar de su asequibilidad cada vez mayor, algunas cámaras todavía se perciben como caras. Corresponde a los proveedores, entonces, enfatizar que la protección que ofrecen estas cámaras puede ayudar a los usuarios a ahorrar más dinero en el futuro.

Dahua presenta IPC WizMind S con funciones de IA enriquecidas

Dahua está lanzando la última serie IPC WizMind S que ofrece una mayor potencia informática.

Manteniendo la tecnología acumulada de la serie IPC WizMind 5, la serie IPC WizMind S lleva la experiencia del usuario a un nivel completamente nuevo en términos de excelencia en imagen cumpliendo los requerimientos de varios escenarios de aplicación. Además, está equipado con múltiples funciones inteligentes, ofrece una adaptabilidad creíble e incluso viene en un empaque sin plástico, lo que permite un mejor rendimiento de la imagen, promueve la sostenibilidad ambiental y brinda a los clientes globales una visión más inteligente y una protección más fuerte.

EXCELENTE EFECTO DE IMAGEN

La serie IPC WizMind logra una calidad de imagen óptima a través de una variedad de tecnologías de mejora de imágenes que cumplen con los desafíos complejos de los escenarios de seguridad.

La imagen impulsada por IA, como su nombre indica, se crea a través de IA y proporciona una claridad de imagen completa de varios entornos. El brillo general de las filmaciones en condiciones de poca luz es más equilibrado y los objetivos clave se pueden enfocar de manera inteligente a través de un algoritmo de aprendizaje profundo para eliminar el ruido y restaurar los detalles. Además, esta serie está equipada con tecnología WDR que ajusta automáticamente la sobreexposición o la sub exposición e incluso hace que los objetos en movimiento en la imagen sean claros y reconocibles. También cuenta con tecnología de exposición por división de tiempo para instantáneas más claras cuando se utilizan funciones inteligentes (por ejemplo, metadatos de video).

Deeplight, que es un efecto de imagen de baja iluminación mejorado de Starlight y Starlight+, utiliza un algoritmo de aprendizaje profundo para procesar imágenes, lo que reduce el ruido de la imagen y logra imágenes óptimas con mayor claridad y mejores detalles de color por la noche.

Otra característica única de la serie IPC WizMind S es la corrección de distorsión de imagen que adopta un algoritmo de corrección de distorsión para capturar secuencias de video más naturales y realistas. En comparación con productos anteriores, la activación de esta función reduce significativamente la pérdida en el campo de visión de la escena.

MÚLTIPLES FUNCIONES INTELIGENTES

La nueva serie IPC WizMind S ofrece varias funciones inteligentes, como metadatos de video, que detectan objetivos humanos, vehiculares y no motorizados, tomas instantáneas y análisis de atributos precisos. También está equipado con Detección de sonido inteligente que distingue entre diferentes sonidos, como gritos y rotura de cristales. También está disponible una funcionalidad mejorada de mapa de calor (que se puede usar junto con el conteo de personas). Otras funciones inteligentes incluyen: Detección de rostros, Detección inteligente de objetos abandonados o perdidos; Protección perimetral mejorada para reconocer mejor las actividades específicas de objetivos humanos y de vehículos, como intrusión, cruce de línea, objetivos que se mueven rápidamente, estacionamiento, merodeo y reunión; y más funcionalidades para diferentes aplicaciones.

ADAPTABILIDAD CREÍBLE

En situaciones donde el monitoreo continuo las 24 horas del día, los 7 días de la semana es esencial, o donde hay una fuente de alimentación poco confiable, la serie IPC WizMind S brinda flexibilidad operativa en el campo con respaldo de energía dual. Esto permite el cambio automático a otra fuente de alimentación

(sin reiniciar el dispositivo IPC) si falla una de las fuentes de alimentación, lo que garantiza el funcionamiento continuo de la cámara.

Los modelos H de esta serie también están equipados con: control preciso de apertura de lente P-iris, que proporciona un control de entrada de luz más preciso; micrófonos duales para una mayor distancia de captación de sonido; revestimiento anticorrosión para uso en zonas costeras; y un calentador que permite el funcionamiento en ambientes con temperaturas tan bajas como -40oC.

EMBALAJE LIBRE DE PLÁSTICO

En cuanto al medioambiente, los productos WizMind S se suministran en embalajes respetuosos con el medioambiente, que utilizan materiales biodegradables y libres de plástico para empaquetar de forma segura las cámaras y los accesorios, incluidas las inserciones de cartón, la superficie de la caja sin plástico, las bolsas de PLA y un revestimiento de la caja protectora no tóxico. También se ha sometido a una prueba de caída alta para garantizar su estabilidad y durabilidad.

La serie WizMind S es adecuada para escenarios de aplicación como estadios deportivos, centros de transporte, entornos urbanos concurridos y locales comerciales, así como grandes sitios remotos que necesitan vigilancia continua. Por lo tanto, si se necesitan cámaras que brinden un rendimiento óptimo en términos de claridad de imagen superior, funciones de monitoreo inteligente, detección y reconocimiento precisos, adaptabilidad creíble y empaque ecológico, entonces la serie IPC WizMind S es la opción ideal.

Concientización, la estrategia de ALAS para potenciar el negocio de seguridad en la región

En entrevista exclusiva con Carlos Martinez, presidente de ALAS Internacional Comité México, en el marco del Encuentro Tecnológico ALAS México 2023, compartió que uno de los objetivos centrales en la estrategia de la asociación que preside es brindar capacitación y transmitir buenas prácticas a fin de impulsar la profesionalización del mercado de seguridad.

Carlos Martinez, presidente de ALAS Internacional Comité México

A primera vista el tema de capacitación no debería ser considerado como un pilar exclusivo de alguna estrategia, sin embargo, la visión del presidente de ALAS va más allá de solo ampliar el conocimiento de los asociados, es decir, el foco de esta iniciativa está en las empresas, los usuarios finales que son los que necesitan asesoría respecto a cómo resolver ciertas necesidades de seguridad.

"Cada mercado vertical tiene diferentes necesidades y seguramente el conocimiento de las soluciones es limitado, ahí es donde ALAS se vuelve relevante. Nosotros como asociación especializada en seguridad podemos compartir con las organizaciones cuáles son las principales tendencias en sus mercados, cuáles son los avances tecnológicos más innovadores y qué tipo de conocimiento deben de tener los especialistas a la hora de buscar proveedores", explicó Martínez.

"En suma, ayudarlos con el conocimiento que hemos reunido entre todos los especialistas que pertenecemos a la asociación. De esta manera, las empresas o usuarios finales tendrán mayor conocimiento de cómo abordar la solución de sus requerimientos", añadió.

Este plan, resulta en un doble beneficio, por un lado las empresas u organizaciones pueden confiar en una institución especializada en temas de seguridad para resolver sus necesidades; por el otro, entre más empresas tengan conocimiento de las tendencias tecnológicas disponibles en el mercado más oportunidades de negocio se abrirán para la cadena de valor, es decir, el beneficio se derramará entre fabricantes, mayoristas e integradores involucrados en proveer la solución.

Esta iniciativa, desde la visión del presidente de ALAS Internacional Comité México, forma parte precisamente de las tareas que se ha propuesto llevar a cabo durante el periodo que dure su mandato.

"En América Latina la cultura de la seguridad es un tema en el que hay mucho trabajo por hacer. En otras partes del mundo como la región europea o Estados Unidos, las empresas saben de la importancia de tener o utilizar tecnologías de seguridad y esto se ve reflejado en el potencial de negocio que tiene cada región. Y eso es precisamente lo que buscamos en ALAS, impulsar el negocio de seguridad concientizando a las empresas latinoamericanas de los beneficios que pueden proporcionarles las nuevas tecnologías", concluyó Carlos Martínez.

Dahua aporta tecnología para preservar al gibón de Hainan

Muchas especies de la Tierra están actualmente amenazadas por problemas medioambientales y actividades humanas. Para ayudar a sobrevivir a las especies en peligro, la tecnología se utiliza cada vez más como una forma innovadora de promover la sostenibilidad y la conservación de la biodiversidad.

Los gibones de Hainan (Nomascus hainanus) viven en la Reserva Natural Nacional de Bawangling, en la isla china de Hainan. Están catalogados como "en peligro crítico" por la Unión Internacional para la Conservación de la Naturaleza (UICN), y en los años 80 quedaban menos de 10 ejemplares. Con los años de protección, el número de gibones de Hainan ha crecido hasta 37 individuos en 5 poblaciones. Dahua se unió al proyecto de protección del gibón de Hainan en 2021, utilizando tecnología de vídeo inteligente para mejorar la eficacia de la vigilancia de la reserva y ayudar en la protección de la biodiversidad local.

VIGILAR A LOS GIBONES SOLÍA SER UN RETO

Como animales arborícolas de toda la vida, los gibones de Hainan son difíciles de ver en los bosques densos. "Al principio, huían en cuanto me veían. Después de mucho tiempo, poco a poco podemos 'comunicarnos', sobre todo los cachorros recién nacidos. Nos acercamos y saludamos todos los días. Al cabo de unos años, nos llevamos bien, e incluso viene directamente a nosotros", explica el Sr. Zhang, del personal de vigilancia.

Observar a los gibones es gratificante, pero el proceso suele ser agotador. Se mueven rápido, a veces demasiado rápido para que el ojo humano pueda seguirlos. Para seguir el ritmo de los gibones, los monitores a menudo se saltan comidas y sufren problemas estomacales. El mal tiempo, como la lluvia, los truenos e incluso los tifones, puede empeorar las cosas.

OJOS" INTELIGENTES GRACIAS A LA TECNOLOGÍA DE VÍDEO

La introducción de la tecnología cambió todo eso. A los gibones que deambulaban por la selva tropical les salieron un día unos "ojos" nuevos. Son cámaras inteligentes que pueden identificar rápidamente a los gibones y tomar fotos, lo que permite a los monitores observar de cerca a estas criaturas sin molestarlas. Y detrás hay un "cerebro" inteligente.

Con la ayuda de cámaras inteligentes, los gibones aparecen en vídeo con más claridad que antes a simple vista.

"El gibón en sí es difícil de ver en los árboles, y se muestran muy vigilantes cuando se les acerca la gente. El objetivo de la cámara resolvió perfectamente este problema", explica Zhang.

Dahua ha integrado en la cámara inteligente un algoritmo de movimiento altamente sensible. El algoritmo se entrena continuamente a través de la plataforma de IA de Dahua para identificar con precisión y recoger imágenes de gibones en rápido movimiento basándose en el color del pelo, los movimientos, los hábitos, etc. del gibón, con el fin de proporcionar una base científica para el estudio de individuos, poblaciones, edad, sexo, tendencias de desarrollo y cambios dinámicos en los hábitats de los gibones de Hainan.

ACCIONES DE DAHUA PARA LA PROTECCIÓN DE LA BIODIVERSIDAD

Dahua utiliza continuamente tecnologías digitales e inteligentes para promover la sostenibilidad y la protección de la biodiversidad a escala mundial.

En el parque Schwarze Berge (Montañas Negras), situado en Alemania, se ha adoptado una serie completa de cámaras innovadoras de Dahua equipadas con tecnologías clave, como imágenes térmicas y a todo color, para ayudar al parque a supervisar el entorno vital y el estado de salud de los animales salvajes en cualquier momento sin molestarlos. Además, contribuye a mejorar la eficacia operativa y de gestión del parque.

Dahua también estableció un sistema de monitorización digital 5G para ayudar a la Reserva Natural de Baima Snow Mountain a monitorizar 62 especies de vida salvaje, lo que proporcionó una observación precisa y una evaluación de investigación de la vida salvaje, los tipos ecológicos y la biodiversidad de la reserva, ayudando así a proteger las especies que viven en la zona y su equilibrio ecológico. El sistema inteligente es capaz de calcular la población animal, analizar sus pautas de actividad, comprender sus hábitos de vida y detectar actividades ilegales en la reserva como la caza furtiva, la tala ilegal y el pastoreo excesivo.

Además, Dahua entró por primera vez en la región antártica donando 15 dispositivos inteligentes a diferentes bases científicas locales. Proporcionar imágenes claras de la flora y la fauna en la región argentina de la Antártida es beneficioso en los estudios de investigación realizados en "El Continente Blanco."

Con su misión de "hacer posible una sociedad más segura y una vida más inteligente", Dahua seguirá creando valor más allá de la seguridad a través de la tecnología y contribuyendo a la comunidad armoniosa de los seres humanos y la naturaleza.

HID identifica 5 temas que ayudarán a maximizar oportunidades en el mercado de seguridad

HID su primer informe sobre el estado de la industria de la seguridad, que recoge las respuestas de 2,700 socios, usuarios finales y empleados del área de seguridad e informática, con una amplia gama de cargos y provenientes de organizaciones de diversos tamaños, en representación de más de 11 sectores.

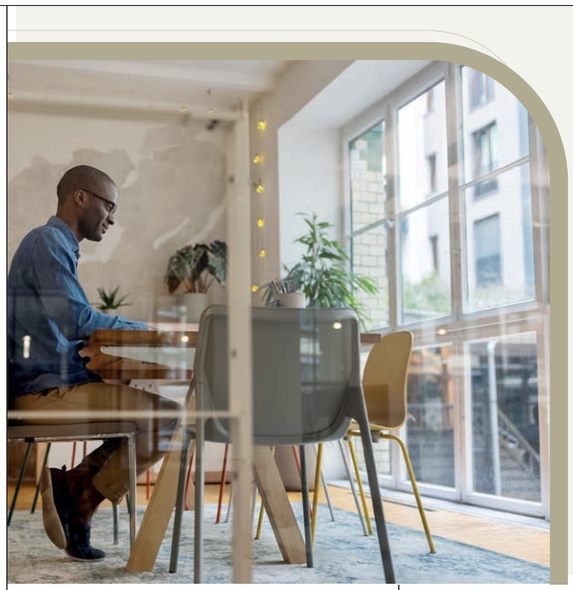
Al analizar lo que está impulsando las últimas innovaciones y la tecnología que les sirve de soporte, la industria de la seguridad tiene la capacidad de generar más valor tanto para sus organizaciones como para las personas que la conforman. La encuesta, realizada en el otoño de 2022, revela los siguientes cinco hilos conductores:

SOSTENIBILIDAD

Los usuarios finales exigen cada vez más a los proveedores transparencia en cuanto a la huella ambiental generada por sus operaciones, abastecimiento de productos y prácticas de investigación y desarrollo. Para atender a esta exigencia, los equipos responsables de la seguridad están aprovechando la nube y el Internet de las cosas, para optimizar los procesos y reducir los recursos. Además, se están desarrollando estratégicamente nuevos productos y soluciones para lograr el consumo prudente de energía, la reducción de residuos y la optimización de recursos.

TRABAJO HÍBRIDO

La mayoría de los encuestados, el 81 % de ellos, afirmó estar ofreciendo un modelo de trabajo híbrido, y



han expuesto que existe la necesidad de soluciones de autenticación de múltiples factores y sin contraseña, así como identificaciones digitales y móviles. Sin embargo, casi la mitad de los encuestados todavía no tienen considerado adoptar una estrategia de 'identificación como servicio' (IDaaS).

IDENTIFICACIONES DIGITALES Y LA AUTENTICACIÓN MÓVIL

Las grandes compañías de bienes raíces comerciales están aprovechando el acceso móvil como parte de sus aplicaciones para mejorar la experiencia de los ocupantes de los edificios.

BIOMETRÍA SIN CONTACTO

La importancia de esta tendencia queda ilustrada en los datos de la encuesta, que muestran que el 59% de los encuestados está usando actualmente, o planea implementar o al menos probar tecnologías biométricas en un futuro cercano.

PROBLEMAS EN LA CADENA DE SUMINISTRO

Más de dos terceras partes de las organizaciones con menos de 1000 empleados indican que se vieron muy afectadas por los problemas en la cadena de suministro en 2022, pero también son las más optimistas y creen que estos problemas se resolverán en 2023.

Bajo esta perspectiva de las necesidades del mercado, HID busca facilitar la comprensión de la necesidades en temas de seguridad, a fin de que los integradores puedan evolucionar de una estrategia meramente transaccional hacia un modelo de servicios.

De esta manera, los esfuerzos al interior de las empresas especializadas se ubicarán en verticales o necesidades con mayores oportunidades de negocio, al mismo tiempo se abrirá el espectro de conocimiento de nuevas tecnologías para hacer frente a las nuevos requerimientos relacionados con la experiencia de usuario.

Estudio muestra por qué y cuándo el trabajo híbrido puede ser el villano de la ciberseguridad

En un reporte publicado por Cisco en enero pasado, la mayoría de los ejecutivos (92 %) informan que sus empleados utilizan múltiples redes para conectarse al entorno de trabajo, como sus hogares, cafeterías, centros comerciales o incluso supermercados.

Juan Marino, Gerente de Ciberseguridad en Cisco América Latina

Crece la adherencia al trabajo desde cualquier lugar o simplemente a distancia o híbrido. Los profesionales están encantados con el modelo porque eliminan la necesidad de estar limitados a cuatro paredes para realizar sus tareas. Las organizaciones ven el modelo como una oportunidad para atraer y retener talento, además de alcanzar nuevos niveles de productividad.

El modelo ganó nuevos contornos con la necesidad de aislamiento impuesta por el COVID-19, cuando nos vimos obligados a adoptar el trabajo remoto sin que las empresas tuvieran el tiempo y el presupuesto para planificar este cambio. Esto provocó que un gran número de trabajadores adoptara equipos personales para realizar las tareas corporativas.

Ahora, con el regreso de las actividades más cerca de la normalidad que vivíamos antes de la pandemia, el trabajo a distancia ha ganado nuevos contornos y denominación. Empezamos a llamarlo trabajo híbrido, un modelo en el que los profesionales se conectan desde cualquier lugar, incluida la red corporativa, para desarrollar sus actividades.

En el estudio presentado en enero pasado por Cisco muestra que esta nueva forma de trabajar ha creado grandes oportunidades, pero también ha traído nuevos desafíos para los equipos de TI, incluida la necesidad de garantizar que las personas tengan las herramientas y el soporte que necesitan para hacer su trabajo desde su lugar. elegir

En esta nueva normalidad, el primer hallazgo del estudio es que algunos empleados utilizan más de 10 redes diferentes para conectarse a los servidores corporativos, lo que confirma la tendencia del trabajo híbrido y refuerza la necesidad de que los equipos de TI limiten los riesgos de seguridad.

El cambio al trabajo híbrido está agregando una nueva capa de riesgo y aumentando los desafíos que enfrentan los profesionales de la ciberseguridad. El informe revela que, dado que las personas trabajan desde múltiples ubicaciones, el uso de dispositivos no registrados para acceder a las plataformas de trabajo es una preocupación importante y un riesgo creciente.

- El 84% de los encuestados dice que sus empleados inician sesión para trabajar desde dispositivos no registrados.
- El 71% dice que sus empleados pasan al menos el 10% de su día trabajando así.
- El 44% dice que sus empleados pasan el 20% de su día o más en un dispositivo no registrado conectado a la red de la empresa.
- El 84% de los encuestados a nivel mundial dice que el trabajo remoto ha aumentado el riesgo de incidentes de ciberseguridad.
- El 84% dice que los dispositivos no registrados podrían causar un incidente de ciberseguridad.

Con empleados libres para trabajar donde quieran, las organizaciones deben garantizar que las redes sean seguras. Sin embargo, dado que estas redes pueden estar en cualquier lugar, desde la cafetería local hasta el supermercado, algo que plantea un gran desafío para los equipos de seguridad.

No por casualidad, seis de cada diez líderes de ciberseguridad encuestados -40% en México- informaron haber sufrido un incidente cibernético en los últimos 12 meses, como malware, phishing y fuga de datos.

La mayoría, 76 % en México, cree que es probable que los incidentes de ciberseguridad interrumpan su negocio en los próximos 12 a 24 meses. Como resultado, se están preparando para protegerse de las amenazas internas y externas, y el 86 % dice que su organización planea aumentar su presupuesto de ciberseguridad en al menos un 10 % durante los próximos 12 meses.

Realizado entre 6,700 profesionales de 27 países entre agosto y septiembre de 2022, el estudio concluye que a pesar del sombrío escenario del impacto del trabajo híbrido en la seguridad empresarial, existe una oportunidad para ser evaluado por empresas y gobiernos. La necesidad de proteger a las personas, los datos y las redes crea una enorme oportunidad para aumentar la asociación público-privada. Los gobiernos de todo el mundo están implementando políticas para frenar el fraude cibernético y fortalecer la protección de datos. Las organizaciones pueden invertir en seguridad robusta, adoptando soluciones que garanticen que los clientes tengan la mejor experiencia posible y que sus empleados aún puedan disfrutar de la libertad de trabajar donde quieran, de forma segura.

SonicWall entrega el Partner Award 2023 a sus partners más valiosos en Latinoamérica

SONICWALL RECONOCIÓ A LOS PARTNERS Y DISTRIBUIDORES DESTACADOS POR SU EXCELENCIA CONTINUA EN LA PROTECCIÓN DE LOS CLIENTES EN UN PANORAMA DE AMENAZAS DESAFIANTE, OTORGANDO EL GALARDÓN SONICWALL PARTNER AWARD 2023.

Los premios honran a las organizaciones asociadas de Sonicwall en todo el mundo que han ido más allá de la entrega de soluciones de ciberseguridad a sus clientes.

"Desde nuestros inicios, los logros de SonicWall siempre han estado vinculados al éxito de sus estimados partners y distribuidores", dijo Bob VanKirk, CEO y presidente de SonicWall. "Estamos encantados de reconocer a nuestros partners SecureFirst de SonicWall que constantemente brindan servicios de seguridad de primera clase a organizaciones de todos los tamaños. Estamos extremadamente agradecidos y honrados por nuestra red global de más de 17,000 canales y distribuidores, y estos premios reconocen su trabajo sobresaliente".

Los partners fueron nominados en varias categorías en cada región destacándose por un rendimiento sobresaliente durante el año pasado.

Sonicwall se complace en anunciar los siguientes ganadores en Latinoamérica:

MEXICO:	
Distributor of the Year LATAM	Dominion
Partner of the Year	SitWifi
Distributor of the year Central LATAM	MAPS
CHILE:	
Distributor of the year South LATAM	Nexsys
PARAGUAY:	
Partner of the Year South LATAM	Parasur

Para conocer a todos los ganadores, visite: https://blog.sonicwall.com/es-mx/2023/03/reconocimiento-a-los-partners-y-distribuidores-con-un-rendimiento-excelente-en-2022

Licencias OnLine impulsa en México los servicios de ciberseguridad integral Sophos MDR

Con base en la actual situación en donde la velocidad de los ataques es cada vez mayor, Licencias OnLine y Sophos están trabajando en conjunto para impulsar su tecnología especializada con el fin de detener las amenazas activas cada vez con mayor velocidad.

Haciendo frente a las necesidades de las empresas que muchas veces no disponen de las herramientas, el personal suficiente o los procesos adecuados para gestionar eficazmente sus programas de ciberseguridad y al mismo tiempo protegerse de forma proactiva contra las amenazas emergentes.

La importancia actual de implementar soluciones de ciberseguridad que tengan la capacidad de integrar y simplificar todo el tráfico de información en una sola herramienta respaldada por un equipo de expertos, da a las organizaciones la tranquilidad de saber que sus datos están seguros permanentemente y ante cualquier ataque dirigido contra sus ordenadores, servidores, redes, cargas de trabajo en la nube, cuentas de correo electrónico y más.

Como parte de la oferta de Licencias OnLine y el fabricante especializado, llama la atención Sophos MDR (Managed Detection and Response), que es una solución gestionada por el equipo de expertos Sophos que trabajan para hacer frente a las posibles amenazas. Con el fin de detectar ataques avanzados perpetrados por humanos o máquinas y neutralizar dichas amenazas antes de que afecten a las operaciones empresariales y pongan en peligro sus datos confidenciales.

Nayelli Suárez, Product Manager Sophos en Licencias OnLine México.

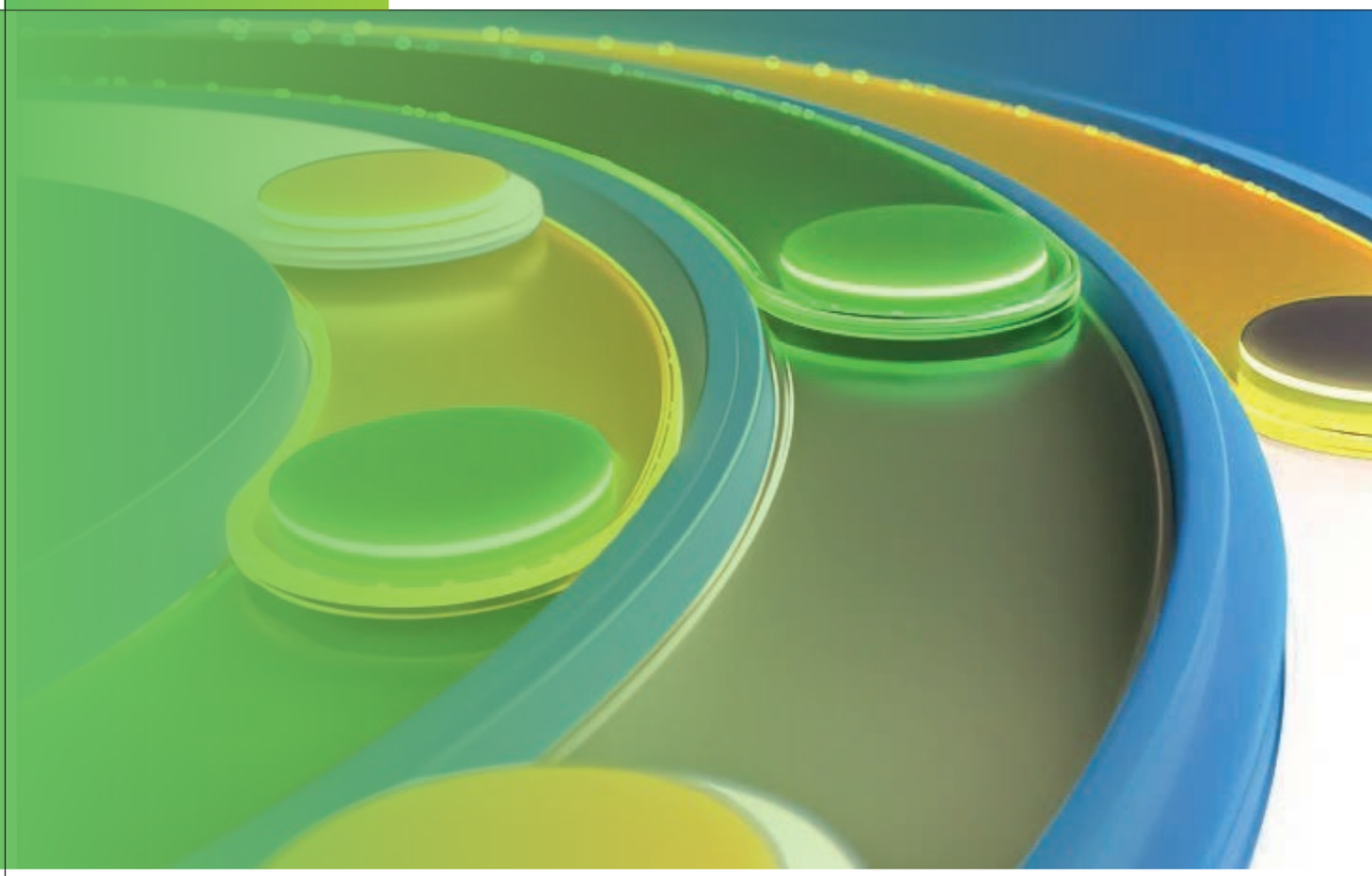
"Lo más atractivo para la oferta de los canales, es que este tipo de soluciones se puede personalizar con varios niveles de servicio y prestarse a través de su tecnología propia y también desde las soluciones tecnologías de ciberseguridad heredadas. MDR es una solución totalmente gestionada por expertos Sophos que detectan y responden a los ciberataques dirigidos contra toda la superficie de ataque" mencionó Nayelli Suárez, Product Manager Sophos en Licencias OnLine México.

Mediante técnicas de investigación patentadas, el equipo de especialistas de Sophos determina la diferencia entre un comportamiento legítimo y las tácticas, técnicas y procedimientos utilizados por los ciberdelincuentes. Que, en conjunto con la Inteligencia Artificial integrada, generan ciencia de datos con Machine Learning, simplificando la tarea de identificar y responder a ataques avanzados y adversarios sofisticados en minutos.

Además, las investigaciones de amenazas se complementan con la telemetría de otros productos de Sophos que protegen el resto de la superficie además del endpoint, para ofrecer una visibilidad completa de las actividades del adversario. Con las capacidades de investigación de amenazas de SophosLabs, que son conocidos por ser líderes en el mundo, ofrecen un análisis exhaustivo del Malware, archivos y URL maliciosos, indicadores de peligro, técnicas y procedimientos de los atacantes.

Es importante destacar que sigue considerando la opción de compatibilidad, ya que los analistas en las organizaciones pueden utilizar las tecnologías previamente instaladas para ciberseguridad y así detectar amenazas y responder a ellas. Actualmente este tipo de solución es compatible con una lista cada vez mayor de proveedores de telemetría de seguridad que se consolida, correlaciona y prioriza automáticamente con información exhaustiva de Sophos Adaptive Cybersecurity Ecosystem (ACE) y la unidad de información sobre amenazas Sophos X-Ops.

"Disponer de este tipo de herramientas en nuestro portafolio de ciberseguridad en México, nos ayuda ofrecer a los canales y clientes finales una solución de rápida activación, la licencia de MDR se puede activar el mismo día en que se realiza el pedido y una vez desplegada la licencia en Sophos Central, despliega los agentes de inmediato. Durante años hemos trabajado con Sophos y es importante mencionar que recientemente obtuvo una calificación de 4.8 sobre 5 estrellas con base en más de 280 opiniones en Gartner Peer Insights" concluyó Nayelli Suárez.



Microsoft lleva el poder de la IA a la ciberdefensa

Microsoft anunció el martes que traerá la próxima generación de inteligencia artificial a la seguridad cibernética con el lanzamiento de Microsoft Security Copilot, para brindar a los defensores una herramienta muy necesaria para detectar y responder de manera rápida a las amenazas y comprender mejor su paisaje en general. Security Copilot combinará la amplia huella de inteligencia de amenazas de Microsoft con la experiencia líder en la industria para mejorar el trabajo de los profesionales de seguridad a través de un asistente de inteligencia artificial fácil de usar.

“Hoy, las probabilidades siguen en contra de los profesionales de la ciberseguridad. Con demasiada frecuencia, libran una batalla asimétrica contra atacantes implacables y sofisticados”, dijo Vasu Jakkal, vicepresidenta corporativa de Microsoft Security. “Con Security Copilot, buscamos cambiar el equilibrio de poder a nuestro favor. Security Copilot es el primer y único producto de seguridad de IA generativa, que permite a los defensores moverse a la velocidad y escala de la IA”.

Security Copilot está diseñado para funcionar de manera fluida con los equipos de seguridad, lo que permite a los defensores ver lo que sucede en su entorno, aprender de la inteligencia existente, correlacionar la actividad de amenazas y tomar decisiones más informadas y eficientes a la velocidad de la máquina.

SIMPLIFICAR LA COMPLEJIDAD Y ACELERAR LAS RESPUESTAS

En un mundo donde hay 1,287 ataques de contraseña por segundo, las herramientas y la infraestructura fragmentadas no han sido suficientes para detener a los atacantes. Y aunque los ataques han aumentado un 67% en los últimos cinco años, la industria de la seguridad no ha podido contratar suficientes profesionales de riesgos cibernéticos para seguir el ritmo. Esto ha llevado a los defensores que se ven

abrumados en la búsqueda de ataques bien disfrazados dentro de un volumen imposiblemente grande de tráfico de red en expansión y otras señales.

Security Copilot simplificará la complejidad y ampliará las capacidades de los equipos de seguridad al resumir y dar sentido a la inteligencia de amenazas, para ayudar a los defensores a ver a través del ruido del tráfico web e identificar actividades maliciosas.

También ayudará a los equipos de seguridad a detectar lo que otros pasan por alto al correlacionar y resumir datos sobre ataques, priorizar incidentes y recomendar el mejor curso de acción para remediar con rapidez diversas amenazas, a tiempo.

Aprender de manera continua para aumentar la experiencia de los equipos de seguridad.

Security Copilot también aprenderá y mejorará de manera continua para garantizar que los equipos de seguridad operen con los últimos conocimientos sobre los atacantes, sus tácticas, técnicas y procedimientos. El producto brindará acceso continuo a los modelos OpenAI más avanzados para admitir tareas y aplicaciones de seguridad exigentes. Su visibilidad de las amenazas se basa tanto en los datos de seguridad de la organización del cliente como en la amplia huella de análisis de amenazas de Microsoft.

Estas capacidades pueden impulsar a los equipos de seguridad de cualquier tamaño con las habilidades y capacidades de organizaciones mucho más grandes. Además, Security Copilot ayuda a abordar la escasez de habilidades en ciberseguridad al cerrar las brechas de conocimiento y mejorar los flujos de trabajo, los perfiles de los actores de amenazas y los informes de incidentes en los equipos.

Basado en la plataforma de Microsoft y la inteligencia de amenazas líder en la industria

Microsoft está calificado de manera única para ayudar a los clientes a explorar y adaptar la IA para mejorar sus defensas de ciberseguridad. Microsoft Security realiza un seguimiento activo de más de 50 bandas de ransomware, más de 250 organizaciones de ciberdelincuentes únicas de estados nacionales y recibe 65 billones de señales de amenazas todos los días. La tecnología de Microsoft bloquea más de 25 mil millones de intentos de robo de contraseñas por fuerza bruta cada segundo, y más de 8 mil profesionales de seguridad de Microsoft analizan más señales de seguridad que casi cualquier otra empresa; en promedio, los analistas del Centro de operaciones de seguridad de Microsoft utilizan más de 100 fuentes de datos diferentes.

Adquisiciones como las de RiskIQ y Miburo le dan a Microsoft una amplitud de señal y una inteligencia profunda sobre los actores de amenazas que nadie más tiene. Y Security Copilot también se integra de forma nativa con una lista cada vez mayor de productos de seguridad de Microsoft, como Sentinel y Microsoft Defender, para ayudar a los clientes a crear una experiencia integral en todo su programa de seguridad.

“Avanzar en el estado de la seguridad requiere tanto de personas como de tecnología: el ingenio humano combinado con las herramientas más avanzadas que ayuden a aplicar la experiencia humana a velocidad y escala”, dijo Charlie Bell, vicepresidente ejecutivo de Microsoft Security. “Con Security Copilot construimos un futuro en el que todos los defensores cuentan con las herramientas y tecnologías necesarias para hacer del mundo un lugar más seguro”.

Por Carlos Soto

Check Point Software marca la pauta en ciberseguridad con su iniciativa Mujeres Inspirando Mujeres

Check Point Software llevó a cabo con gran éxito el primer evento de su iniciativa Mujeres Inspirando Mujeres, el cual estuvo orientado a ejecutivas y directivas que trabajan en el mercado de ciberseguridad.

Durante el evento se dio a conocer que todavía hay mucho camino por recorrer en temas de equidad laboral en el sector de ciberseguridad, ya que a nivel mundial solo el 20 por ciento de los puestos está ocupado por mujeres y en el caso de América Latina el porcentaje alcanza los 25 puntos porcentuales. Aunado a esto, se estima que globalmente solo el 30 por ciento de los estudiantes de carreras STEM (Ciencia, Tecnología, Ingeniería y Matemáticas, por sus siglas en inglés) son mujeres.

En esta búsqueda por tener una participación más activa en temas de equidad de género en ciberseguridad, Check Point Software decidió llevar a cabo este evento de concientización y networking que reunió un gran número de mujeres interesadas en conocer las iniciativas de la marca y escuchar un panel de destacadas ejecutivas que compartieron su visión acerca de las problemáticas que vive el mundo en temas igualdad de oportunidades para el crecimiento y desarrollo profesional.

PANEL DE MUJERES REFERENTES EN LA INDUSTRIA

En este panel participó, Erika Mata, directora ejecutiva de Hitachi Vantara, Enaela García, directora y fundadora de CYCSAS, Magda Díaz, directora de ingeniería en procesos de Grupo Financiero Banorte,

Cynthia Salgado, directora de Global Digital Solutions para ENEL México y Verónica García, PMO Manager en NTT.

En su primera intervención Erika Mata comentó que si bien los empleos en ciberseguridad son ocupados en un 20 por ciento por mujeres cuando se habla de puestos directivos la cifra se reduce considerablemente. “Actualmente existen muchas iniciativas de género que están ayudando a cerrar la brecha, pero todavía sucede ‘algo’ que no deja avanzar a las mujeres hacia puestos directivos”, destacó.

En este sentido Enaela García, añadió que en efecto en el mercado de TI a las mujeres les dan pocas oportunidades de llegar a puestos altos, sin embargo, la contraparte es que tampoco existe mucho interés por parte de ellas por estudiar carreras como ingenierías o licenciaturas en temas tecnológicos.

Magda Díaz reconoció que otro reto a trabajar es la brecha salarial y el primer paso en la solución de esta problemática es precisamente que no se niegue su existencia. “El cambio comienza con nosotras, desde cómo nos tratamos. Tenemos que empezar a quitarnos el miedo a crecer, de pensar que existe otra persona mejor preparada que pueda ocupar ese cargo que está disponible”, exhortó.

Por su parte, Cynthia Salgado añadió que además de todo lo señalado, es necesario que como sociedad se rompa el sesgo que se ha sido adoptado desde la infancia en temas de género, ya que muchas de las problemáticas generadas en este sentido provienen precisamente de incentivar el machismo en los roles familiares. En temas de educación, no existen programas donde las mujeres tengan un rol relevante, entonces las niñas crecer consumiendo contenido que no les sirve como referente para su vida adulta.

Verónica García se unió al comentario y aclaró que los padres, deben tener un rol activo en el cuidado de los hijos.

En temas de negocio, la charla se extendió hacia que en el mercado de ciberseguridad la participación de la mujer en puestos directivos es limitado, por lo regular se percibe mayor participación en áreas comerciales, sin embargo, las ponentes instaron a las asistentes a identificar el gran potencial que tienen y usarlo para destacar en el mercado.

Por otro, lado se invitó a fomentar en las niñas el interés por las tecnologías, erradicar estos sesgos ideológicos dónde hay roles preestablecidos para las actividades que pueden desempeñar. Además, se extendió la invitación a crear redes de apoyo entre mujeres para ayudarse unas a otras a crecer.

Por último, se unificó un mensaje respecto a que, como mujeres deben aceptar sus capacidades y confiar en ellas mismas, a reconocer su propia luz, la cual las hará brillar en cualquier segmento del mercado en el que se desempeñen.

Kaspersky desarrolla Academia 360 para capacitar a su ecosistema de canales

Con el objetivo de robustecer el programa de capacitación para el ecosistema de canales, Kaspersky presenta: Academia 360.

Este proyecto está diseñado para ayudar a los socios a mejorar su conocimiento sobre las soluciones clave de la compañía, a fin de que se conviertan en los mejores aliados para la estrategia de ciberseguridad de PyMEs y grandes empresas. Asimismo, busca brindarles herramientas útiles para que fortalezcan sus competencias y se mantengan como un talento competitivo ante el contexto actual y las necesidades del mercado.

En 2022, las tecnologías de Kaspersky registraron 4,000 ataques de ransomware al día en América Latina, y se espera que este panorama siga creciendo. De acuerdo con los expertos, algunos de los riesgos que podrán enfrentar las empresas este año son: extorsión a través de medios de comunicación, reportes de supuestas fugas de datos, compra de accesos a organizaciones previamente comprometidas en la Darkweb, incremento del Malware-as-a-Service y ataques en la nube, así como a la cadena de suministro de TI y telecomunicaciones por medio de proveedores del sector.

"En este escenario, se requiere no solo de un talento especializado que cuente con las capacidades necesarias para gestionar adecuada y oportunamente los incidentes de ciberseguridad; sino también de un ecosistema de canales en donde los socios puedan dar un seguimiento puntual a cada una de las soluciones de seguridad y ayuden a garantizar su eficacia en todos los niveles; desde la protección, la detección y respuesta, así como a la inteligencia contra amenazas", comenta Gustavo Cols, Director de Canales B2B para América Latina de Kaspersky.

Por ello, para sumar a su capacitación y competitividad, desde enero y hasta finales de 2023, Academia 360 ofrecerá una amplia plataforma de webinars sobre temas técnicos y comerciales, impartidos por el equipo de expertos (preventas y ventas) de alto nivel. Cualquier partner de América Latina interesado puede participar; al momento se han registrado más de 650 socios de la región.

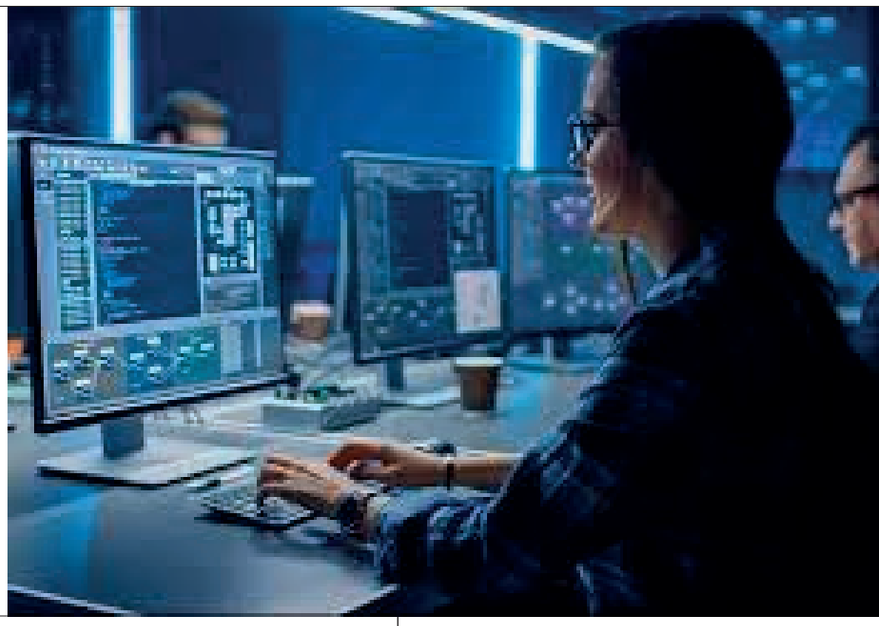
Los participantes recibirán un reconocimiento e incentivos a través del programa de puntos de la plataforma Kaspersky KUDOS, para que, además de capacitarse, puedan obtener certificaciones, entre otros beneficios. Los webinars quedarán alojados en una plataforma en línea para consulta posterior de los socios.

Para Kaspersky la educación y capacitación constante conducirán a una era digital más segura, y con Academia 360 reitera su compromiso de seguir fortaleciendo al ecosistema de ciberseguridad a fin de satisfacer las necesidades de las organizaciones y los usuarios en la materia.

Por Carlos Soto

Hackrocks e Imagen TI promueven nueva plataforma de entrenamiento y prácticas de ciberseguridad

Hackrocks es una plataforma de formación y entrenamiento en ciberseguridad que busca ayudar a revolver de una manera más práctica y lúdica, la falta de expertos en seguridad informática. Con este nuevo modelo de entrenamiento con retos, empresas, universidades y gobierno ahora contarán con un aliado para verificar las capacidades técnicas de los funcionarios encargados de ciberseguridad.



De acuerdo con Javier Nieto, Business Development Manager Europe & Latin America en Hackrocks, el conocimiento en cursos tradicionales solo se confirma con exámenes, sin embargo, la forma en que la empresa aborda la transmisión de conocimiento es a través de cursos en línea que van acompañados de retos, de tal manera que una vez que el usuario haya concluido un tema, sus conocimientos puedan ser evaluados en la práctica.

"En el caso de las universidades, la plataforma puede adaptarse para que, al finalizar el semestre, se pueda tener visibilidad del nivel que tienen los estudiantes, aplicando un concurso tipo Capture The Flag por equipos, incluso permite ubicar un esquema de 'atacantes y defensores' para poner a prueba las habilidades en ambos lados de la ciberseguridad", explicó Nieto.

Para el sector empresarial, Hackrocks permite obtener un espacio de formación continua para ejecutivos técnicos y comerciales, que serviría no solo para aumentar las capacidades en ciberseguridad sino para demostrarlas en un formato "gamificado", a fin de reducir la falta de interés que provocan las plataformas comunes.

Por otra parte, la plataforma sirve como herramienta de recursos humanos, es decir, si se abre una vacante en algún puesto de ciberseguridad, presentar numerosos diplomas no es garantía del conocimiento, por lo tanto, se puede realizar una serie de retos con los que el candidato demuestre en la práctica su conocimiento.

Por su parte Luis Díaz, Director de Imagen TI, explicó que la falta de profesionales de ciberseguridad es un reto global y no solo es un tema mercadológico, la realidad es que hay mucho interés en este tipo de temas pero las opciones tradicionales para adquirir el conocimiento no se adaptan a las necesidades del mercado.

"Ha sido todo un reto promover la alta especialización en ciberseguridad, por alguna razón las personas que trabajan en este segmento no están motivadas a elevar su nivel de conocimiento. Ahora, con la opción de Hackrocks, el usuario podrá experimentar una nueva manera de aprender, y los retos serán un detonante del interés para seguir avanzando", comentó Díaz.

"Incluso se puede usar la plataforma para implementar concursos, que motiven a los entusiastas a participar y de esta manera detectar nuevo talento. Estrategia que no solo limita al segmento educativo como universidades, sino entre empresas o entidades de gobierno", añadió.

NEGOCIO EN PUERTA

En la parte de negocio, el director de Imagen TI, instó a los especialistas en ciberseguridad que abran sus expectativas y se acerquen a conocer la plataforma. Una vez conociendo cómo funciona será relaticamente fácil encontrar oportunidades de negocio.

"En los últimos tiempos se han hecho cada vez más visibles ataques a grandes empresas y entidades de gobierno, por lo que una plataforma para evaluar las habilidades de sus especialistas en ciberseguridad sería de gran ayuda para mantener buenos niveles en su personal a cargo", concluyó Díaz.

Fortinet mejora su solución SASE con nuevas capacidades para habilitar el trabajo desde cualquier lugar

Fortinet anunció varias mejores a FortiSASE para permitir flexibilidad de despliegue adicional y nuevas capacidades de acceso seguro a recursos digitales en todas las aplicaciones privadas, SaaS e Internet.

Con la integración existente de FortiGate Secure Edge, los clientes de Fortinet Secure SD-WAN se benefician de la flexibilidad para llevar a cabo procesos de seguridad en las instalaciones (a través de FortiGate) o en la nube (a través de FortiSASE). Las nuevas mejoras a esta integración de FortiGate Secure Edge brindan a los equipos un control y una flexibilidad aún más granulares para elegir cuándo ejecutar la seguridad en las instalaciones o en la nube para optimizar la experiencia del usuario. Esta mejora beneficiará particularmente a las organizaciones con una fuerza laboral híbrida y garantizará seguridad constante sin importar dónde se encuentren los usuarios.

Además, se han realizado mejoras adicionales en los tres casos de uso clave de FortiSASE para asegurar el acceso de los usuarios hacia y desde Internet, aplicaciones alojadas de forma privada y aplicaciones SaaS.

- **Acceso seguro a Internet:** FortiSASE se ha mejorado aún más con un mejor rendimiento y escalabilidad de la infraestructura y soporte de IP pública dedicada. La experiencia mejorada basada en geolocalización permite el acceso a servicios personalizados basados en la ubicación de un usuario.
- **Acceso privado seguro:** FortiSASE ahora ofrece conectividad concentrada y amplificada para SD-WAN seguro para admitir redes híbridas globales aún más grandes con una integración local perfecta, lo que brinda a los usuarios remotos un acceso seguro a las aplicaciones corporativas.
- **Acceso seguro SaaS:** FortiSASE se ha mejorado con las innovaciones del corredor de seguridad de acceso a la nube (CASB) que amplían la cobertura de las aplicaciones y brindan un control más profundo del comportamiento de las aplicaciones SaaS y la capacidad de restringir el control de acceso de los usuarios.

Diseñado para brindar seguridad consistente a los usuarios en cualquier lugar, FortiSASE converge la seguridad brindada en la nube, que incluye Secure Web Gateway (SWG), el acceso a Zero Trust Network Universal (ZTA), CASB de modo dual de próxima generación, Firewall as a Service (FWaaS) y redes (SD-WAN segura). Con la tecnología de un solo sistema operativo (FortiOS), los servicios de seguridad impulsados por IA de FortiGuard y un agente FortiClient unificado, FortiSASE ayuda a mejorar la eficiencia y brinda seguridad constante en cualquier lugar.

Dell Technologies fortalece su portafolio de seguridad con nuevos servicios y soluciones

Dell Technologies anuncia nuevos servicios y soluciones de seguridad para ayudar a las organizaciones a protegerse contra las amenazas, responder a los ataques y asegurar sus dispositivos, sistemas y nubes.

El 72% de los líderes de negocio y profesionales de TI creen que el cambiante mundo laboral expone a sus organizaciones a un mayor riesgo . El ambiente de TI crea nuevas oportunidades para los ciber criminales y requiere que las empresas transformen su enfoque para proteger y recuperar sus datos y sistemas. Las nuevas ofertas de seguridad de Dell Technologies ayudan a enfrentar estos desafíos para que las compañías puedan reducir riesgos y proteger su negocio.

Matt Baker, vicepresidente ejecutivo de Estrategia Corporativa de Dell Technologies.

“La seguridad se encuentra en el ADN de Dell. Está integrada en nuestros diseños, infraestructura, cadena de suministro y productos”, afirmó Matt Baker, vicepresidente ejecutivo de Estrategia Corporativa de Dell Technologies.

“Nuestra creciente cartera de servicios y soluciones de seguridad está ayudando a las organizaciones a enfrentar sus desafíos de seguridad más difíciles y abordar la creciente complejidad de cómo mantenerse seguros en redes, dispositivos y sistemas. Estamos ayudando a los clientes a duplicar la resiliencia en un entorno desafiante”.

MANAGED DETECTION AND RESPONSE (MDR) PRO PLUS AYUDA A PROTEGER LOS AMBIENTES DE TI

Dell amplía las capacidades de su oferta de MDR con Managed Detection and Response Pro Plus, una solución de operaciones de seguridad completamente administrada que ayuda a las organizaciones a prevenir, responder y recuperarse de las amenazas de seguridad.

Con Managed Detection and Response Pro Plus, Dell

Technologies protege los endpoints, la infraestructura, el software, el hardware y las nubes al:

- Brindar detección e investigación de amenazas 24/7, al tiempo que identifica vulnerabilidades y prioriza la aplicación de parches.
- Llevar a cabo simulaciones de filtraciones y ataques para garantizar que los controles de seguridad existentes de una organización, incluida la configuración de la puerta de enlace web o de correo electrónico, estén configurados y funcionen correctamente.
- Realizar pruebas de penetración para encontrar vías vulnerables en el ambiente de una organización con las mismas técnicas que usan los hackers experimentados, marcando actividades potencialmente sospechosas y recomendando mejoras en la postura de seguridad.
- Brindar capacitación sobre seguridad cibernética durante todo el año en módulos concisos y fáciles de aprender para mejorar el conocimiento de los empleados sobre los riesgos y fomentar el uso de mejores prácticas.
- Ofrecer Incident Recovery Care para desplegar rápidamente un equipo de expertos certificados a fin de evaluar un incidente de seguridad y llevar al cliente de vuelta a la operación en caso de que ocurra una filtración.

DELL AUMENTA SU PORTAFOLIO DE GESTIÓN DE AMENAZAS CON CROWDSTRIKE

Además de un enfoque de servicios gestionados, Dell Technologies permite a las organizaciones diseñar, administrar y asegurar sus propios entornos de TI, ofreciendo a los clientes más opciones en software de seguridad cibernética con la adición de CrowdStrike Falcon en el portafolio SafeGuard and Response.

Con CrowdStrike, la plataforma nativa de nube líder en la industria, las organizaciones pueden acceder a un conjunto extendido de defensas que aceleran la investigación y respuesta de amenazas para proteger áreas críticas de riesgo empresarial: terminales y cargas de trabajo en la nube, identidad y datos.

Agregar CrowdStrike a la estrategia corporativa facilita que las organizaciones confíen en Dell para sus necesidades de seguridad en expansión, incluso en su viaje hacia una arquitectura Zero Trust con soluciones escalables y las mejores en su categoría.

DELL OFRECE PROTECCIÓN DE HARDWARE A LAS PCS COMERCIALES DE DELL

Dell fabrica las PCs comerciales más seguras del mercado . Ofreciendo a las organizaciones un impulso adicional de confianza con la integración entre el diseño de sus PCs y la cadena de suministro, Dell lanza una versión basada en la nube de su oferta de Verificación de Componentes Seguros (SCV, por sus siglas en inglés). La solución mejorada brinda a los clientes empresariales una garantía de seguridad adicional para que sus PCs lleguen tal como fueron ordenadas y construidas de fábrica.

La Verificación de Componentes Seguros en la nube ayuda a reducir el riesgo de manipulación del producto en las PCs comerciales. Dell Technologies genera un certificado digital, almacenado en un ambiente de nube seguro, que documenta los componentes clave del equipo en la fábrica. Al momento de la entrega, los equipos de TI pueden revisar las PCs con sus certificados correspondientes para verificar la integridad de los componentes. Esta oferta exclusiva también permite a los equipos de TI verificar una flota completa de PCs en una sola inspección en lugar de tener que validar cada dispositivo de manera local, lo que brinda una capa adicional de seguridad, a la vez que ahorra tiempo.

PRODUCT SUCCESS ACCELERATOR PARA CYBER RECOVERY AYUDA A PROTEGER CONTRA ATAQUES

Para ayudar a las organizaciones a prepararse para un posible evento de ciberseguridad, Dell presenta Product Success Accelerator (PSX) para Cyber Recovery. El nuevo servicio agiliza la implementación y el funcionamiento de una bóveda de recuperación cibernética más segura y aislada para que las organizaciones puedan proteger los datos críticos y mantener la continuidad del negocio.

Uniéndose a la creciente cartera de soluciones y servicios de recuperación cibernética de Dell, PSX para Cyber Recovery es el primer servicio estandarizado basado en resultados disponible dentro de la nueva familia PSX. Las empresas pueden elegir entre tres niveles de asistencia en función de sus necesidades:

- **Listo**, que incluye la planificación de talleres, la instalación y la configuración de una bóveda Dell Cyber Recovery, un manual de ejecución, un plan de éxito y capacitación sobre habilidades de ciberseguridad. ●
- **Optimizar**, que agrega evaluaciones de bóveda trimestrales, recomendaciones para el ambiente, incluyendo actualizaciones, parches, políticas y simulaciones de prueba de restauración asistida.
- **Operar**, que agrega asistencia operativa continua para supervisar e investigar la actividad, iniciar acciones correctivas y brindar soporte en caso de un ataque cibernético.