ALERTA TECNOLÓGICA

CIBERSEGURIDAD

Sector Industria 4.0

78660557-59
78624395 Ext. 110

consultas@ocpi.cu

www.ocpi.cu

III Trimestre 2024

Título: Sistema de inteligencia y remediación de amenazas de ciberseguridad.

Publicación	País de Origen	Solicitante	Fecha de publicación
US 2024/0223587 A1	USA	Cytellix Corp	2024-07-04

Resumen:

Se proporciona un sistema de ciberseguridad para obtener información automatizada sobre ciberseguridad, recomendaciones de reparación y prestación de servicios. El sistema de ciberseguridad puede generar información sobre amenazas y/o generar recomendaciones de reparación utilizando modelos de aprendizaje automático y datos de ciberseguridad obtenidos de redes de destino, socios y similares. Para proporcionar servicios de ciberseguridad, el sistema de ciberseguridad puede recopilar metadatos sobre las conexiones de red y los casos de uso deseados para uno o más servicios. Una vez que se han recopilado los metadatos, el sistema de evaluación de ciberseguridad proporciona automáticamente los servicios seleccionados en función de los datos proporcionados, como la duración del tiempo elegido, las métricas del servicio y similares.

Título: Un aparato y método para mejorar la ciberseguridad de una entidad.

Publicación	País de Origen	Solicitante	Fecha de publicación
US 2024/0265114 A1	USA	Bobaguard Llp	2024-08-08

Resumen:

Se proporciona un aparato y método para mejorar la ciberseguridad de una entidad, en donde el aparato incluye al menos un procesador y una memoria que contiene instrucciones que configuran al menos un procesador para recibir datos de entidad que incluyen datos relacionados con la ciberseguridad de una entidad, comparar los datos de entidad con una métrica de ciberseguridad, generar un programa de mejora de la ciberseguridad como una función de la comparación, en donde el programa de mejora de la ciberseguridad incluye una simulación de ciberataque e implementar el programa de mejora de la ciberseguridad para la entidad basándose en los datos de la entidad.

Título: Gestión de ciberseguridad basada en la nube de grupos de redes jerárquicas.

Publicación	País de Origen	Solicitante	Fecha de publicación
US 12003524 B2	USA	Cytellix Corp	2024-06-04

Resumen:

Se proporciona un sistema de evaluación de la ciberseguridad para supervisar, evaluar y abordar el estado de la ciberseguridad de una jerarquía de redes objetivo. El sistema de evaluación de la ciberseguridad puede escanear redes objetivo individuales y producir datos sobre el estado actual y las propiedades de los dispositivos en las redes objetivo. El sistema de evaluación de la ciberseguridad puede generar interfaces de usuario para presentar información de ciberseguridad con respecto a redes objetivo individuales e información de ciberseguridad compuesta con respecto a una jerarquía de redes objetivo o algún subconjunto de las mismas. El sistema de evaluación de la ciberseguridad puede generar configuraciones de acceso que especifican a qué información de ciberseguridad de la jerarquía pueden acceder las redes objetivo individuales de la jerarquía.

Título: Generación de un modelo de riesgo de ciberseguridad utilizando datos dispersos.

Publicación	País de Origen	Solicitante	Fecha de publicación
US 11956254 B1	USA	Arceo Labs Inc	2024-04-09

Resumen:

Se describe la generación de un modelo de riesgo de ciberseguridad utilizando datos dispersos, que incluye: la obtención de señales asociadas con un riesgo de ciberseguridad, en donde las señales obtenidas incluyen señales tecnográficas y señales derivadas de consultas obtenidas a partir de consultas; la generación de pseudo señales basadas al menos en parte en factores a priori relacionados con el riesgo de ciberseguridad; y la combinación de las pseudo señales y las señales obtenidas en un modelo bayesiano que indica el riesgo de ciberseguridad.

Título: Técnicas para detectar riesgos de ciberseguridad en entornos informáticos mediante modelos de inteligencia artificial.

Publicación	País de Origen	Solicitante	Fecha de publicación
US 12003529 B1	USA	Wiz Inc	2024-06-04

Resumen:

Se presenta un sistema y un método para detectar un riesgo de ciberseguridad de una inteligencia artificial (IA). El método incluye: inspeccionar un entorno informático en busca de un modelo de IA implementado en el mismo; generar una representación del modelo de IA en una base de datos de seguridad, incluyendo la base de datos de seguridad una representación del entorno informático; inspeccionar el modelo de IA en busca de un riesgo de ciberseguridad; generar una representación del riesgo de ciberseguridad en la base de datos de seguridad, estando conectada la representación del riesgo de ciberseguridad a la representación del modelo de IA en respuesta a la detección del riesgo de ciberseguridad; e iniciar una acción de mitigación basada en el riesgo de ciberseguridad.

Título: Control remoto de la ciberseguridad.

Publicación	País de Origen	Solicitante	Fecha de publicación
WO 2024/121283 A1	Francia	Electricite De France	2024-06-13

Resumen:

La invención propone un método para asegurar un sistema de información que comprende sistemas comunicantes distribuidos en un mismo territorio y conectados a un mismo sistema de comunicación centralizado. El método se implementa mediante sistemas comunicantes que han recibido una señal codificada a través de primeros receptores. El método comprende, para cada sistema comunicante: - obtener un código resultante de la decodificación de la señal codificada recibida por el primer receptor, - verificar el código obtenido mediante una estrategia de reconocimiento, obteniendo así un resultado de verificación, y - cuando el resultado de verificación indica éxito, autorizar el procesamiento, por parte del dispositivo, de una señal procedente de un segundo receptor a través de un canal de comunicación, y en caso contrario no autorizar dicho procesamiento.

Título: Uso de desplazamientos de páginas de memoria para detectar ataques cibernéticos.

Publicación	País de Origen	Solicitante	Fecha de publicación
WO 2024/112272 A1	Suecia	Ericsson Telefon Ab L M , Hanifi Khadija	2024-05-30

Resumen:

Se proporcionan técnicas para identificar modificaciones de un flujo de control de un sistema en el que se ejecutan instrucciones de software. Un método es llevado a cabo por una entidad de monitorización del sistema. El método comprende obtener direcciones de memoria procesadas por la ejecución de las instrucciones de software. Las direcciones de memoria se obtienen monitorizando el sistema en tiempo de ejecución. El método comprende identificar cualquier anomalía en las secuencias de desplazamiento de página de memoria mediante el análisis, en tiempo de ejecución, de secuencias de desplazamiento de página de memoria compuestas por desplazamientos de página de memoria extraídos de las direcciones de memoria obtenidas. El método comprende llevar a cabo una acción preventiva y/o protectora para el sistema tras haber identificado la anomalía en al menos una de las secuencias de desplazamiento de página de memoria. La identificación de la anomalía identifica el flujo de control del sistema que ha sido modificado.

Título: Sistema y método de análisis inteligente de seguridad de redes informáticas basado en big data.

Publicación	País de Origen	Solicitante	Fecha de publicación
CN117896137A	China	Guangzhou Pixiaodu Technology Co ltd	2024-04-16

Resumen:

La solicitud divulga un sistema y método de análisis inteligente de seguridad de red informática basado en big data, el método incluye: recopilar y procesar datos de red, realizar análisis de secuencia temporal en los datos de red, identificar comportamientos anormales de red según un resultado de análisis de secuencia temporal, generar datos de comportamiento anormal de red y activar un mecanismo de nivel de alarma anormal; recopilar y procesar datos de información de amenaza de red, extraer reglas de asociación entre los datos de información de amenaza de red y los resultados de análisis de secuencia

temporal e identificar patrones de comportamiento de amenaza potencial de la red para generar datos de patrón de comportamiento de amenaza; construir un diagrama de estructura de topología de red, realizar análisis de asociación en datos de comportamiento anormal y el diagrama de estructura de topología de red, determinar una ruta de ataque de comportamiento de amenaza potencial de la red y generar datos de ruta de comportamiento de amenaza; activar una herramienta de gestión de seguridad para procesar los comportamientos de amenaza según los datos de modo de comportamiento de amenaza y los datos de ruta de comportamiento de amenaza; se realiza el monitoreo y la respuesta oportuna a los comportamientos de amenaza potencial de la red, se mejora el nivel de seguridad de la red y se reducen los riesgos y pérdidas potenciales.

Título: Equipos de operación y mantenimiento de seguridad de redes y su método de trabajo.

Publicación	País de Origen	Solicitante	Fecha de publicación
CN117879948A	China	State Grid Information and Telecommunication Co Ltd	2024-04-12

Resumen:

La invención se refiere a los equipos de operación y mantenimiento de seguridad de red y a un método de trabajo para los mismos. En la invención, el sistema de operación y mantenimiento de seguridad de red se utiliza para llevar a cabo trabajos de mantenimiento de seguridad en el servidor, llevar a cabo la detección de número de puerto, la evaluación de contraseña ssh y el trabajo de gestión de operador en la evaluación de puerto ssh, lograr las funciones de detección y corrección de configuración relevante, evitar elementos débiles, cargar un programa de inicio a través de un eje de tiempo del sistema, ejecutar un archivo de proyecto, lograr la función de escaneo de vulnerabilidad Yun Dun, llevar a cabo adivinación de contraseña y ataque de simulación de programa basado en el archivo de proyecto, obtener un informe de seguridad del sistema más efectivo, reforzar los elementos débiles, llevar a cabo trabajos de monitoreo y gestión en tiempo real en flujos de datos diarios y garantizar aún más la seguridad de la red en la mayor medida posible.

Título: Sistema de detección de información y vídeos falsos con apoyo de inteligencia artificial y solución de ciberseguridad.

Publicación	País de Origen	Solicitante	Fecha de publicación
TR2024002644A2	Turquía	Halim Semih Özcan	2024-04-22

Resumen:

Esta patente ofrece un sistema innovador que detecta información y vídeos falsos y garantiza la ciberseguridad mediante el uso del poder de la inteligencia artificial y el código. El sistema analiza el texto y el contenido visual, determina las características distintivas del contenido falso y envía advertencias a los usuarios. De esta manera, se pueden prevenir con antelación los ataques cibernéticos y las campañas de desinformación y se puede proporcionar un entorno seguro en el entorno cibernético.

Título: Sistema de seguridad cibernética.

Publicación	País de Origen	Solicitante	Fecha de publicación
TR2024006804A2	Turquía	Türk Telekomünikasyon Anonim Şirketi	2024-06-21

Resumen:

La invención se refiere a un sistema de ciberseguridad que analiza las aplicaciones instaladas en el dispositivo móvil del usuario, detecta vulnerabilidades de seguridad y proporciona información. El sistema, a través del módulo de inteligencia artificial que lleva incorporado, sigue las afirmaciones que los sitios de noticias, instituciones oficiales y propietarios de aplicaciones hacen en internet respecto de las aplicaciones en cuestión, detecta noticias de violaciones de seguridad de la información relacionadas con las aplicaciones e informa al usuario.