# ALERTA TECNOLÓGICA

## Sistemas de Bioseguridad

## Sector Industria 4.0

78660557-59
78624395 Ext. 110

consultas@ocpi.cu

www.ocpi.cu

III Trimestre
2021

Título: Sistema de ciberseguridad con capacidad diferenciada para hacer frente a ciberataques complejos.

| Publicación | País de Origen | Solicitante | Fecha de prioridad |
|---|---|---|---|
| EP3151153 | USA | BOEING | 2015-10-01 |

Resumen:

La invención se refiere a un sistema de protección cibernética mejorado con capacidad diferenciada para hacer frente a ataques cibernéticos complejos en industrias complejas y altamente conectadas. La arquitectura del sistema está orientada a objetivos y separa los objetivos y preocupaciones de seguridad por capas a las que se asignan funciones específicas para abordar solo esos objetivos. Las funciones operan simultáneamente dentro de las capas y brindan información sobre sus respectivas capas. Las capas están interconectadas con módulos de conexión utilizando una interfaz bidireccional para establecer una apariencia de retroalimentación dentro de todo el sistema. Se utilizan algoritmos de sistemas adaptativos complejos (CAS) para identificar las posibles amenazas al sistema.

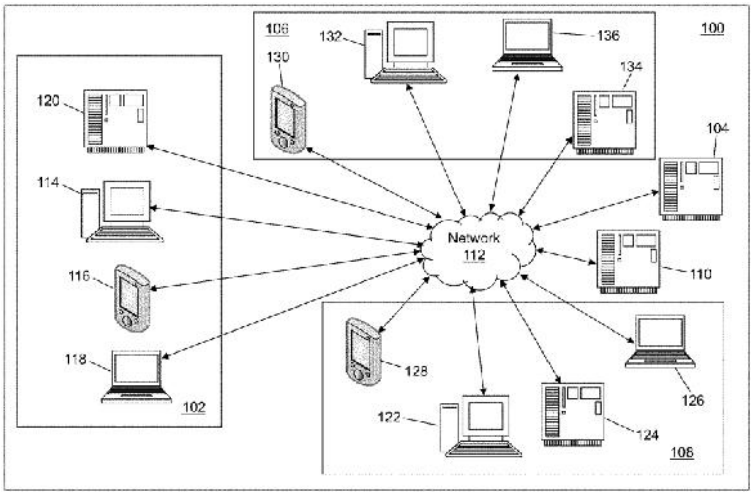
Título: Sistema de ciberseguridad.

| Publicación | País de Origen | Solicitante | Fecha de prioridad |
|---|---|---|---|
| US10965706 | USA | SAS INSTITUTE | 2016-02-25 |

Resumen:

La presente invención está relacionada con un dispositivo informático que determina un identificador de grupo de pares y complementa los registros de netflow con el identificador del grupo de pares. Se recibe un objeto de bloque de eventos de autenticación que fue enviado a una primera ventana de origen. El objeto de bloque incluye un identificador de usuario, una dirección IP y un identificador de grupo de pares. Los miembros del grupo de pares son identificados en base a un comportamiento de actividad de red esperado. El identificador de usuario y el identificador de grupo de pares se almacenan en asociación con la dirección IP en un caché. Se recibe el objeto de bloque enviado a la primera ventana de origen que incluye una dirección IP de paquete de netflow. Se analizan los datos de Netflow

desde el objeto de bloque de eventos de netflow a un registro de netflow. Cuando la dirección IP almacenada coincide con la IP del paquete de netflow, el registro de netflow se complementa con el identificador de usuario y el identificador del grupo de pares. El registro de netflow se envía a datos de resumen.




Título: Sistema de ciberseguridad multicapa para restringir el acceso a los datos.

| Publicación | País de Origen | Solicitante | Fecha de prioridad |
|---|---|---|---|
| US20200074098 | USA | HONEYWELL INTERNATIONAL | 2018-08-30 |

Resumen:

En esta invención se divulgan sistemas y métodos para restringir acceso a datos mediante un sistema de ciberseguridad multicapa. Un primer sistema informático, ejecutando un primer conjunto de instrucciones escritas en un primer lenguaje de programación para operar una primera capa, recibe una solicitud de acceso a datos de un dispositivo solicitante, determina si un primer conjunto de claves coincide con la solicitud de acceso a datos y rechaza la solicitud de acceso a datos si el primer juego de claves no coincide. Si el primer juego de llaves coincide, un segundo sistema informático, ejecutando un segundo conjunto de instrucciones escritas en un segundo idioma de programación, recibe la solicitud de acceso a datos de la primera capa de seguridad, determina si un segundo conjunto de claves coincide

con la solicitud de acceso a los datos, y la rechaza si el segundo juego de claves no coincide. Si el segundo conjunto de claves coincide, se concede la solicitud del acceso a los datos.

Título: Sistema de inteligencia artificial de ciberseguridad.

| Publicación | País de Origen | Solicitante | Fecha de prioridad |
|---|---|---|---|
| WO2018/049437 | Sudáfrica | PAMA THANDISIZWE EZWENILETHU | 2016-09-08 |

Resumen:

Se presenta un sistema de ciberseguridad que incluye un sistema de inteligencia artificial (IA) dentro de una red informática distribuida, el AIS configurado para gestionar y neutralizar las amenazas de ciberseguridad mediante el registro de datos relacionados con las amenazas de ciberseguridad existentes (que incluye amenazas, vulnerabilidades y mutaciones de las mismas) y contramedidas efectivas contra tales amenazas conocidas y vulnerabilidades, para escanear la red en busca de nuevas amenazas y vulnerabilidades, de forma iterativa para desarrollar y aplicar contramedidas a la nueva amenaza o vulnerabilidad hasta que se encuentre una contramedida efectiva, y para registrar el resumen de la amenaza o vulnerabilidad y la contramedida efectiva.

Título: Un método para administrar un dispositivo de Internet de las cosas.

| Publicación | País de Origen | Solicitante | Fecha de prioridad |
|---|---|---|---|
| CN109067753 | China | CHINA APPLIED TECHNOLOGY | 2018-08-15 |

Resumen:

La presente invención se refiere a un método para gestionar un dispositivo de Internet de las cosas. La invención comprende los siguientes pasos: recopilación de datos del dispositivo de Internet de las cosas de una pluralidad de fuentes de datos por una capa de análisis de un sistema de seguridad de red, y extrayendo una configuración línea de base del elemento de análisis del dispositivo de Internet de las cosas a partir de los datos recopilados; recuperar un análisis del elemento de referencia de configuración del dispositivo de Internet de las cosas desde una capa de análisis del sistema de seguridad de la red por un capa de ejecución del sistema de seguridad de la red, o empujar la línea de base del elemento de análisis de configuración del dispositivo de Internet de las cosas a una capa de adaptación de la seguridad de la red sistema; generar una política de seguridad del dispositivo de Internet de las cosas a través de una capa de ejecución de la seguridad de la red. El tráfico de red de los dispositivos de Internet de las cosas de la red privada se controla a través de una capa de ejecución del sistema de seguridad de la red para ajustarse a la seguridad política.

Título: Sistema y método de seguridad de red basado en big data.

| Publicación | País de Origen | Solicitante | Fecha de prioridad |
|---|---|---|---|
| CN107733887 | China | SICHUAN DIANKE INTERNET & INDUSTRY TECHNOLOGY RESEARCH INSTITUTE | 2017-10-11 |

Resumen:

La invención se refiere a un sistema de seguridad de red y método basado en big data. El problema técnico de que la seguridad es baja se resuelve. Un esquema técnico comprende el hecho de que un servidor y los lados del usuario están conectados a través de ajuste de interruptores; los interruptores de usuario

comprenden las primeras unidades IP de anclaje que se utilizan para generar direcciones IP virtuales de cambio de usuario basadas en direcciones IP en tiempo real de cambio de usuario de acuerdo con las tablas de guía de mapeo de direcciones IP; un conmutador de servidor comprende una segunda unidad de IP de anclaje utilizado para generar direcciones IP virtuales de conmutador de servidor basado en el servidor que cambia direcciones IP en tiempo real de acuerdo con las tablas de guía de mapeo de direcciones IP; y el usuario cambia y el conmutador del servidor realiza un salto de dirección IP de acuerdo con las tablas de la guía de mapeo de direcciones IP y establecido como el hecho de comunicarse solo con el extremo opuesto de direcciones IP en tiempo real. Mediante la adopción de esta técnica, el problema está bien resuelto. El sistema y el método se pueden aplicar a la seguridad de la red.

Título: Sistema de seguridad de red y método de seguridad de red.

| Publicación | País de Origen | Solicitante | Fecha de prioridad |
|---|---|---|---|
| EP3672307 | Taiwan | INDUSTRIAL TECHNOLOGY RESEARCH INSTITUTE | 2018-12-22 |

Resumen:

En la siguiente invención se presenta un sistema de seguridad de red que incluye: varios subnodos y un dispositivo de autenticación de identidad, el cual está configurado para generar una inicial clave de subred dinámica, y agrupar los subnodos en una o más subredes según la clave de subred dinámica inicial y al menos un parámetro característico preconfigurado. Para cada subred de una o más subredes, el dispositivo de autenticación de identidad selecciona respectivamente un dispositivo virtual autenticador para gestionar cada uno de los subnodos de cada una de las subredes. Cuando un nuevo subnodo miembro se une a una subred de una o más subredes, cada uno de los subnodos existía en una subred y cada autenticador virtual de una subred ingresa una clave de subred dinámica de la

versión actual en un algoritmo hash para actualizar la clave de subred dinámica de la versión actual para realizar un proceso de actualización de consenso.

Título: Sistema de seguridad de red visual.

| Publicación | País de Origen | Solicitante | Fecha de prioridad |
|---|---|---|---|
| CN108924169 | China | WUHAN SIPULING TECHNOLOGY | 2018-09-17 |

Resumen:

La invención da a conocer un sistema de seguridad de red visual, que comprende un cortafuegos, un módulo de análisis de acceso, un módulo de retrato de comportamiento, un módulo de análisis de rastreo de fuentes, un módulo de control de flujo y un módulo de visualización, en el que el flujo de usuarios, los comportamientos de la red y los ataques son controlados de forma exhaustiva a través del análisis del flujo de usuario, juicio de los comportamientos de la red y análisis de atacar venas y caminos, y la diversa información es resumida, correlacionada y mostrada para ayudar eficazmente a un empresa para monitorear mejor el flujo de la red y el comportamiento de la red.

Título: Sistema de comportamiento cibernético basado en simulación y realidad virtual.

| Publicación | País de Origen | Solicitante | Fecha de prioridad |
|---|---|---|---|
| EP3338205 | USA | IRON NET CYBER SECURITY IRONNET CYBERSECURITY IRONNET CYBERSECURITY | 2016-07-14 |

Resumen:

Se presenta un sistema de ciberseguridad para gestionar el comportamiento cibernético asociado con los ciberactores de modo que el comportamiento cibernético se puedan calcular y predecir y las interacciones cibernéticas entre los actores cibernéticos se puedan crear. El sistema incluye un módulo de gestión del

espacio de comportamiento cibernético configurado para recibir datos de entrada y datos del motor de interacción y el motor de flujo de trabajo analítico, y para generar varios espacios ciberconductuales basados en los datos recibidos. El sistema incluye una interacción motor configurado para procesar datos de actores cibernéticos para facilitar interacciones con el espacio ciberconductual, una escena cibernética, un mapa cibernético y otro actor cibernético. El sistema incluye además un motor de flujo de trabajo analítico configurado para analizar el cyber espacio de comportamiento y actualizar los datos cibernéticos en función de los datos analizados y los datos del motor de interacción. El sistema incluye también un motor de visualización configurado para calcular visualizaciones y transmitir las visualizaciones para su visualización.

Título: Detección de ataques de torrents.

| Publicación | País de Origen | Solicitante | Fecha de prioridad |
|---|---|---|---|
| US10623416 | USA | IBM | 2018-01-31 |

Resumen:

Un sistema de ciberseguridad genera firmas de características para respectivos dispositivos de varios dispositivos acoplados comunicativamente. El sistema de ciberseguridad predice firmas características futuras para los respectivos dispositivos. El sistema de ciberseguridad determina una primera probabilidad de una primera firma característica futura que se produce para un primer dispositivo. El sistema de ciberseguridad determina una segunda probabilidad de la primera firma característica futura que se produce teniendo en cuenta el deterioro del rendimiento del primer dispositivo. El sistema de ciberseguridad mitiga un ciberataque identificado basado en la primera y la segunda probabilidad.

Título: Sistema de seguridad cibernética para dispositivos en red.

| Publicación | País de Origen | Solicitante | Fecha de prioridad |
|---|---|---|---|
| EP3704618 | USA | CYBERSWARM | 2017-10-31 |

Resumen:

Un sistema de seguridad puede incluir un relé normalmente abierto entre una conexión de red externa y al menos una conexión de red interna, un controlador de red y un microcontrolador. El controlador de red puede configurarse para monitorear la actividad maliciosa en una red externa accesible a través de la conexión de red externa. El microcontrolador puede configurarse para hacer que el relé normalmente abierto se cierre temporalmente en respuesta a que el controlador de red no detecte la actividad maliciosa durante un período de tiempo predeterminado y haga que el relé normalmente abierto permanezca abierto y genere una alerta en respuesta a la red controlador que detecta la actividad maliciosa.

Título: Sistema y método de ciberseguridad integrados para proporcionar acceso restringido de clientes a un sitio web.

| Publicación | País de Origen | Solicitante | Fecha de prioridad |
|---|---|---|---|
| US20180337907 | USA | SOFTEX | 2017-05-16 |

Resumen:

Se presentan sistemas integrados de ciberseguridad y método para proporcionar acceso del cliente a un sitio web. Los métodos implican recibir información de configuración del sitio web para el acceso del cliente; recibir datos de inscripción de clientes para el acceso de clientes; recibir datos de entrada del cliente de un cliente; definiendo confirmación integrada del cliente; y proporcionar el sitio web con la información de identificación del cliente basada en la confirmación integrada del cliente. La definición implica autenticar datos de entrada del cliente comparándolos con los datos de inscripción del cliente; autorizando al cliente autenticado por determinar la información de autorización del cliente asociada con los datos de inscripción de clientes basados en la información de configuración del sitio web; identificación del cliente autenticado determinando la información de identificación

del cliente asociada con los datos de inscripción del cliente; y proporcionando el sitio web con la información de identificación del cliente basada en la confirmación integrada del cliente. El sitio web está aislado de los datos de inscripción del cliente, los datos de entrada del cliente y la definición de la confirmación integrada del cliente.

Título: Sistema y método para predecir y mitigar configuraciones incorrectas del sistema de ciberseguridad.

| Publicación | País de Origen | Solicitante | Fecha de prioridad |
|---|---|---|---|
| US10826931 | USA | FIREEYE | 2020-11-03 |

Resumen:

La invención se refiere a un método computarizado para reconfigurar uno o más sistemas de detección de malware, cada uno de los cuales realiza ciberseguridad Se describen los análisis de los datos entrantes. El método implica recibir meta información, incluyendo métricas asociado con un sistema de detección de malware. Basado en la meta información, se determina si el sistema de detección de malware funciona a un nivel de desempeño óptimo. De lo contrario, se determinan los resultados producidos al realizar análisis de comportamiento que predicen la operatividad del sistema de detección de malware y los resultados se proporcionan como retroalimentación al sistema de detección de malware para actualizar uno o más valores de los parámetros de configuración de los mismos.

Título: Sonido reputación.

| Publicación | País de Origen | Solicitante | Fecha de prioridad |
|---|---|---|---|
| US10887334 | USA | BAE SYSTEMS INFORMATION & ELECTRONIC SYSTEMS INTEGRATION | 2018-09-06 |

Resumen:

Un sistema y método de ciberseguridad que utiliza SONIDO reputación, donde un conjunto de reputaciones se asocia con cada actor en una red. Los actores de una red pueden ser usuarios, hosts, aplicaciones y similares. Las reputaciones asociadas se agregan y actualizan como nueva información sobre la actividad de un actor que se informa de acuerdo con un protocolo o política definida y moldeable. La actividad del actor puede ser informada por uno o más sensores de amenazas. El efecto de un una mala conducta particular se puede ajustar para satisfacer las necesidades de la red específica. Cuando la reputación de un mal actor se hunde demasiado bajo, el sistema puede tomar cualquier acción que sea apropiada: se pueden enviar informes, se puede notificar a un operador, el delincuente puede ser desconectado de la red, o similar.

Título: Identificación de dispositivos de red maliciosos.

| Publicación | País de Origen | Solicitante | Fecha de prioridad |
|---|---|---|---|
| EP3593508 | USA | VISA | 2017-03-10 |

Resumen:

Las realizaciones prevén que se determinen puntuaciones de malicia para direcciones IP y / o dominios de red. Por ejemplo, se puede recibir una solicitud para evaluar la actividad maliciosa con respecto a una dirección IP / dominio de red. Varios sistemas de terceros, y en algunos casos dispares, pueden proporcionar información de actividad maliciosa asociada con la dirección IP y / o el dominio de red. Se puede extraer un conjunto de características de la información de actividad maliciosa y se pueden calcular valores estadísticos a partir de los datos extraídos y

agregarlos al conjunto de características. El conjunto de características se puede proporcionar a un modelo de aprendizaje automático como entrada y se puede devolver una puntuación / clasificación de malicia. Se pueden realizar acciones correctivas de acuerdo con las salida del modelo de aprendizaje automático.

Título: Sistema de seguridad de red con análisis de tráfico mejorado basado en bucle de retroalimentación e identificación de dominio de bajo riesgo.

| Publicación | País de Origen | Solicitante | Fecha de prioridad |
|---|---|---|---|
| US20200128038 | USA | AKAMAI TECHNOLOGIES | 2018-10-23 |

Resumen:

Este documento describe, entre otras cosas, los sistemas de seguridad de red que incorporan un circuito de retroalimentación para ajustar automática y dinámicamente el alcance del tráfico de red que está sujeto a inspección. El tráfico peligroso se puede enviar para inspección; el tráfico de riesgo que se ha demostrado que tiene una alta tasa de amenazas puede bloquearse por completo sin una inspección adicional; el tráfico que está causando errores debido a la incompatibilidad del protocolo o que no debe ser inspeccionado por normativas u otras razones se pueden marcar para que pase por alto el sistema de inspección de seguridad. El sistema puede operar dominio por dominio, dirección IP o de otra manera.

Título: Sistemas y métodos para detectar un ciberataque en un dispositivo en una red informática.

| Publicación | País de Origen | Solicitante | Fecha de prioridad |
|---|---|---|---|
| US20190190952 | USA | MERCY HEALTH | 2017-12-20 |

Resumen:

Los sistemas y métodos se describen en este documento para detectar un ciberataque a un dispositivo en la computadora de una organización la red.