(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 728 337**

(51) Int. CI.:

G06F 21/55 (2013.01)
G06F 21/57 (2013.01)
H04L 29/06 (2006.01)
G06F 21/31 (2013.01)
G06T 19/00 (2011.01)
A63F 13/75 (2014.01)
A63F 13/71 (2014.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **02.06.2017 PCT/US2017/035679**

(87) Fecha y número de publicación internacional: **18.01.2018 WO18013244**

(96) Fecha de presentación y número de la solicitud europea: **02.06.2017 E 17828119 (2)**

(97) Fecha y número de publicación de la concesión europea: **01.05.2019 EP 3338205**

(54) Título: **Simulación y realidad virtual basada en sistemas de comportamiento cibernético**

(30) Prioridad:

14.07.2016 US 201662362346 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.10.2019

(73) Titular/es:

IRONNET CYBERSECURITY, INC. (100.0%)
8135 Maple Lawn Blvd. Suite 455
Fulton, MD 20759, US

(72) Inventor/es:

GROSSMAN, ROBERT L.;
ALEXANDER, KEITH B.;
HEATH, JAMES E. y
GARRETT, RANDY LYNN

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Simulación y realidad virtual basada en sistemas de comportamiento cibernético

Referencia cruzada a solicitudes relacionadas

Esta solicitud reclama prioridad a la Solicitud Provisional de EE. UU. No. 62/362,346, presentada el 14 de julio de 2016, que se incorpora aquí como referencia.

Campo técnico

Algunas realizaciones de la presente invención se refieren en general a la seguridad cibernética y, en particular, a los sistemas de comportamiento cibernético basados en simulación y realidad virtual y al intercambio de conocimientos entre sistemas de comportamiento cibernético.

Antecedentes

Tradicionalmente, los defensores de red revisan solo fragmentos de información para ayudar a entender lo que realmente está sucediendo en su red. Puede ser extremadamente difícil y de intensa mano de obra para simular toda la red para ver los posibles cursos de acción, las maniobras defensivas y los escenarios de fuerza en la fuerza. Los ejercicios actuales de seguridad cibernética permiten a los defensores jugar unos contra otros, pero los ejercicios no cubren todos los escenarios posibles que podrían ocurrir en la red. Cada día, la cantidad y la complejidad de las nuevas amenazas aumentan, y cada vez es más difícil para los defensores de red mantenerse al día con los sistemas operativos cibernéticos actuales.

En general, las empresas y organizaciones trabajan en temas relacionados con la seguridad cibernética de forma independiente. Cuando comparten información, generalmente es a través de políticas y marcos de trabajo de la industria o del gobierno para facilitar el intercambio de datos relacionados con la seguridad cibernética. Las prácticas tradicionales para compartir información no son suficientes para manejar el volumen o la velocidad de los ataques. No permite a las empresas aprovechar al máximo la mano de obra disponible para defender activamente dentro de una red, ni entre redes que luchan para defender un sector, múltiples sectores o una nación.

Resumen

De acuerdo con la materia divulgada, se proporcionan sistemas, métodos y medios legibles por ordenador no transitorios para proporcionar un sistema de seguridad cibernética para gestionar el comportamiento cibernético asociado con actores cibernéticos de tal manera que el comportamiento cibernético pueda calcularse y predecirse y las interacciones cibernéticas se pueden crear entre los actores cibernéticos. La invención se define en la reivindicación independiente 1.

En algunas realizaciones, el tema divulgado incluye un sistema de seguridad cibernética que incluye un módulo de gestión del espacio de comportamiento cibernético, un motor de interacción, un motor de flujo de trabajo analítico y un motor de visualización. En algunas realizaciones, el módulo de gestión del espacio de comportamiento cibernético está en comunicación con el motor de interacción, el motor de flujo de trabajo analítico y el motor de visualización. En algunas realizaciones, el módulo de gestión del espacio de comportamiento cibernético está configurado para recibir al menos uno de los datos de entrada, los datos de entrada incluyen al menos uno de los datos cibernéticos de entrada, datos del sensor, datos de enriquecimiento y datos de terceros, datos del motor de interacción, y datos del motor de flujo de trabajo analítico. En algunas realizaciones, el módulo de gestión de espacio de comportamiento cibernético está configurado para generar una pluralidad de espacios de comportamiento cibernético basados en al menos uno de los datos de entrada, los datos del motor de interacción y los datos del motor de flujo de trabajo analítico, cada uno de la pluralidad de espacios de comportamiento cibernético que comprenden datos del espacio de comportamiento cibernético. En algunas realizaciones, los datos del espacio de comportamiento cibernético incluyen datos cibernéticos, los datos cibernéticos incluyen al menos uno de los datos cibernéticos de entrada y los datos cibernéticos de entrada transformados, datos de actores cibernéticos asociados con una pluralidad de actores cibernéticos y datos de escenas cibernéticas asociados con una pluralidad de las escenas cibernéticas, los datos del espacio de comportamiento cibernético se definen por una pluralidad de dimensiones, una pluralidad de modos y una pluralidad de escalas. En algunas realizaciones, el motor de interacción está configurado para recibir datos del primer actor cibernético asociado con un primer actor cibernético de la pluralidad de actores cibernéticos, el primer actor cibernético incluye al menos uno de un actor cibernético real y un actor simulado. En algunas realizaciones, el motor de interacción está configurado para procesar los datos recibidos del primer actor cibernético para facilitar al menos una de una primera interacción entre el primer actor cibernético con al menos uno del espacio cibernético, la escena cibernética y un mapa cibernético, el mapa cibernético asociado con al menos uno de la pluralidad de espacios de comportamiento cibernético, y una segunda interacción entre el primer actor cibernético con un segundo actor cibernético de la pluralidad de actores cibernéticos. En algunas realizaciones, el motor de interacción está configurado para transmitir datos asociados con al menos una de la primera interacción y la segunda interacción. En algunas realizaciones, el motor de flujo de trabajo analítico está configurado para analizar los datos del espacio de comportamiento cibernético

asociados con cada uno de la pluralidad de espacios de comportamiento cibernético para calcular los comportamientos cibernéticos, y actualizar al menos uno de los datos cibernéticos, los datos del actor cibernético y los datos de la escena cibernética basados en al menos uno de los datos del espacio de comportamiento cibernético, los comportamientos cibernéticos calculados y una asignación de los comportamientos cibernéticos calculados a al menos uno de los datos cibernéticos, los datos del actor cibernético y los datos de la escena cibernética, la primera interacción y la segunda interacción. En algunas realizaciones, el motor de interacción está configurado para transmitir datos asociados con la actualización de al menos uno de los datos cibernéticos, los datos del actor cibernético y los datos de la escena cibernética. En algunas realizaciones, el motor de visualización está configurado para calcular visualizaciones de al menos uno de los datos asociados con al menos una de la primera interacción y la segunda interacción del motor de interacción, y al menos uno de los espacios de comportamiento cibernético, la pluralidad de Los actores cibernéticos, la pluralidad de escenas cibernéticas, la pluralidad de mapas cibernéticos y los comportamientos cibernéticos calculados, y transmiten las visualizaciones para su visualización.

En algunas realizaciones, el sistema de seguridad cibernética incluye un motor de consulta, en comunicación con el módulo de gestión del espacio de comportamiento cibernético, el motor de consulta configurado para recibir, desde el primer actor cibernético, una consulta sobre al menos uno de la pluralidad de espacios de comportamiento cibernético. En algunas realizaciones, la consulta está asociada con al menos uno de riesgo asociado con una primera entidad cibernética de una pluralidad de entidades cibernéticas, un grupo de entidades cibernéticas de la pluralidad de entidades cibernéticas con un perfil similar a la primera entidad cibernética, construcciones organizativas internas o externas y comportamiento asociado al menos a una de las primeras entidades cibernéticas, cada entidad cibernética en el grupo de entidades cibernéticas, el primer actor cibernético, el segundo actor cibernético y un tercer actor cibernético. En algunas realizaciones, el motor de flujo de trabajo analítico está configurado para computar y actualizar continuamente los riesgos asociados con cada entidad cibernética de la pluralidad de entidades cibernéticas y cada actor cibernético de la pluralidad de actores cibernéticos.

En algunas realizaciones, el sistema de seguridad cibernética incluye un motor de simulación, en comunicación con el módulo de gestión del espacio de comportamiento cibernético, configurado para generar la pluralidad de escenas cibernéticas, cada una de la pluralidad de escenas cibernéticas incluye un subconjunto de datos cibernéticos, escenas cibernéticas y mapas cibernéticos asociados con la pluralidad de espacios de comportamiento cibernéticos. En algunas realizaciones, el motor de simulación está configurado para generar simulaciones, las simulaciones configuradas para operar en al menos uno de los datos del mundo real y datos simulados y proporcionar un curso de acción para al menos una de operaciones, análisis, conocimiento, planificación, capacitación, acción de remediación, y acción de mitigación.

En algunas realizaciones, el motor de flujo de trabajo analítico está configurado para crear un espacio de comportamiento cibernético transformado, en el que para crear el espacio de comportamiento cibernético transformado, el motor de flujo de trabajo analítico está configurado además para transformar los datos del espacio de comportamiento cibernético en datos de tensor y rango inferior tensor de aproximaciones, y utilizar el aprendizaje de máquina para definir los comportamientos cibernéticos y la pluralidad de espacios de comportamiento cibernético asociados con el espacio de comportamiento cibernético transformado.

En algunas realizaciones, el motor de flujo de trabajo analítico está configurado para aplicar al menos una de las reglas y el aprendizaje de máquina al espacio de comportamiento cibernético transformado para definir comportamientos cibernéticos que aumentan o disminuyen el riesgo asociado con al menos uno de un actor cibernético real o un actor simulado, una entidad cibernética, una máquina, una organización y un proceso.

En algunas realizaciones, el sistema de seguridad cibernética está asociado con una primera organización, además, los comportamientos cibernéticos que aumentan o disminuyen el riesgo son observables por los actores cibernéticos asociados con la primera organización y no observables por los actores cibernéticos asociados con una segunda organización. En algunas realizaciones, el sistema de seguridad cibernética incluye un motor de intercambio de comportamiento cibernético, el motor de intercambio de comportamiento cibernético en comunicación con el módulo de gestión del espacio de comportamiento cibernético. En algunas realizaciones, el motor de intercambio de comportamiento cibernético está configurado para transmitir los comportamientos cibernéticos que aumentan o disminuyen el riesgo para un motor de intercambio de comportamiento cibernético asociado con la segunda organización que utiliza al menos uno de un algoritmo de aprendizaje de máquina distribuido que preserva la privacidad y un protocolo de comunicaciones que preserva la privacidad. de tal manera que los comportamientos cibernéticos que aumentan o disminuyen el riesgo se pueden usar para analizar datos en la segunda organización, y los datos del espacio de comportamiento cibernético asociados con la primera organización no son observables por los actores cibernéticos asociados con la segunda organización.

En algunas realizaciones, el sistema de seguridad cibernética procesa los datos del primer actor cibernético para determinar al menos uno de un primer comportamiento cibernético de los comportamientos cibernéticos asociados con el espacio del comportamiento cibernético transformado, y una primera escena cibernética de la pluralidad de escenas cibernéticas asociadas con el espacio de comportamiento cibernético transformado, y mejora las capacidades operativas, la preparación y el entrenamiento asociados con la respuesta al primer comportamiento cibernético y la primera escena cibernética.

En algunas realizaciones, el motor de flujo de trabajo analítico está configurado para procesar al menos uno de datos de paquetes tráfico de red, registros de ordenador, inteligencia de señales, visible, infrarrojo, multiespectral, hiperespectral, radar de apertura sintética, radar indicador de objetivo móvil, datos de inteligencia técnica, e informes de inteligencia.

En algunas realizaciones, cada uno de la pluralidad de espacios de comportamiento cibernético incluye al menos uno de un espacio de comportamiento cibernético en tiempo real, un espacio de comportamiento cibernético histórico y un espacio de comportamiento cibernético simulado. En algunas realizaciones, el comportamiento cibernético incluye al menos uno de reconocimiento inicial, escaneo, compromiso inicial, establecimiento de un punto de apoyo, baliza, comando y control, captura de credenciales, privilegios crecientes, reconocimiento interno, movimiento lateral, mapeo de red, exfiltración de datos, mantenimiento de la persistencia, y conductas relacionadas. En algunas realizaciones, la pluralidad de dimensiones incluye una combinación de direcciones de origen y destino, hora de llegada, volumen, tamaño de paquete y un tipo de protocolo, la pluralidad de modos incluye una combinación de datos de paquetes, tráfico de red, registros de ordenador, inteligencia de señales, visible, infrarrojo, multiespectral, hiperespectral, radar de apertura sintética, radar indicador de objetivo móvil, datos de inteligencia técnica e informes de inteligencia, y la pluralidad de escalas incluye una combinación de datos temporales de múltiples escalas y datos geoespaciales.

En algunas realizaciones, el módulo de gestión del espacio de comportamiento cibernético está configurado para recibir datos del sensor, los datos del sensor incluyen al menos uno de los datos del sensor del actor físico sobre un actor físico y los datos del sensor del sistema físico sobre un sistema físico, y al menos uno de los datos de entrada, los datos de entrada incluyen al menos uno de los datos cibernéticos de entrada, los datos de enriquecimiento y los datos de terceros, los datos del motor de interacción y los datos del motor de flujo de trabajo analítico. En algunas realizaciones, el módulo de gestión de espacio de comportamiento cibernético está configurado para generar una pluralidad de espacios de comportamiento cibernético basados en los datos del sensor y al menos uno de los datos de entrada, los datos del motor de interacción y los datos del motor de flujo de trabajo analítico, cada uno de la pluralidad de espacios de comportamiento cibernético que comprenden datos del espacio de comportamiento cibernético. En algunas realizaciones, los datos del espacio de comportamiento cibernético incluyen datos cibernéticos, los datos cibernéticos incluyen al menos uno de los datos cibernéticos de entrada y los datos cibernéticos de entrada transformados, datos de actores cibernéticos asociados con una pluralidad de actores cibernéticos y datos de escenas cibernéticas asociados con una pluralidad de escenas cibernéticas. En algunas realizaciones, los datos del espacio de comportamiento cibernético se definen por una pluralidad de dimensiones, una pluralidad de modos y una pluralidad de escalas. En algunas realizaciones, el motor de interacción configurado para recibir datos del primer actor cibernético asociado con un primer actor cibernético de la pluralidad de actores cibernéticos, el primer actor cibernético incluye al menos uno de un actor cibernético real y un actor simulado. En algunas realizaciones, el motor de interacción está configurado para procesar los datos recibidos del primer actor cibernético para facilitar al menos una de una primera interacción entre el primer actor cibernético con al menos uno del espacio de comportamiento cibernético, la escena cibernética y un mapa cibernético, el mapa cibernético asociado con al menos uno de la pluralidad de espacios de comportamiento cibernético, y una segunda interacción entre el primer actor cibernético con un segundo actor cibernético de la pluralidad de actores cibernéticos. En algunas realizaciones, el motor de interacción está configurado para transmitir datos asociados con al menos una de la primera interacción y la segunda interacción. En algunas realizaciones, el motor de flujo de trabajo analítico está configurado para analizar los datos del espacio de comportamiento cibernético asociados con cada uno de la pluralidad de espacios de comportamiento cibernético para calcular los comportamientos cibernéticos, y actualizar al menos uno de los datos cibernéticos, los datos del actor cibernético y los datos de la escena cibernética basados en al menos uno de los datos del espacio del comportamiento cibernético, los comportamientos cibernéticos calculados y una asignación de los comportamientos cibernéticos calculados a al menos uno de los datos cibernéticos, los datos del actor cibernético y los datos de escena cibernética, la primera interacción, la segunda interacción y un cómputo de comportamientos físicos sobre al menos uno del sistema físico y el actor físico. En algunas realizaciones, el motor de interacción está configurado para transmitir datos asociados con la actualización de al menos uno de los datos cibernéticos, los datos del actor cibernético y los datos de la escena cibernética. En algunas realizaciones, el motor de visualización está configurado para calcular visualizaciones de al menos uno de los datos asociados con al menos una de la primera interacción y la segunda interacción del motor de interacción, y al menos uno de los espacios de comportamiento cibernético, la pluralidad de actores cibernéticos, la pluralidad de escenas cibernéticas, la pluralidad de mapas cibernéticos y los comportamientos cibernéticos calculados. En algunas realizaciones, el motor de visualización está configurado para transmitir las visualizaciones para su visualización.

En algunas realizaciones, el sistema de seguridad cibernética que está configurado para recibir datos del sensor incluye un motor de consulta, en comunicación con el módulo de gestión del espacio de comportamiento cibernético. En algunas realizaciones, el motor de consulta está configurado para recibir, desde el primer actor cibernético, una consulta sobre al menos uno de la pluralidad de espacios de comportamiento cibernético. En algunas realizaciones, la consulta está asociada con al menos uno de riesgo asociado con una primera entidad cibernética de una pluralidad de entidades cibernéticas, un grupo de entidades cibernéticas de la pluralidad de entidades cibernéticas con un perfil similar a la primera entidad cibernética, construcciones organizativas internas o externas y comportamiento asociado al menos a una de las primeras entidades cibernéticas, cada entidad cibernética en el grupo de entidades cibernéticas, el primer actor cibernético, el segundo actor cibernético y un tercer actor cibernético. En algunas realizaciones, el

motor de flujo de trabajo analítico está configurado para calcular y actualizar continuamente los riesgos asociados con cada entidad cibernética de la pluralidad de entidades cibernéticas y cada actor cibernético de la pluralidad de actores cibernéticos.

En algunas realizaciones, el sistema de seguridad cibernética que está configurado para recibir datos del sensor incluye un motor de simulación, en comunicación con el módulo de gestión de espacio de comportamiento cibernético, el motor de simulación. En algunas realizaciones, el motor de simulación está configurado para generar la pluralidad de escenas cibernéticas, cada una de la pluralidad de escenas cibernéticas incluye un subconjunto de los datos cibernéticos, las escenas cibernéticas y los mapas cibernéticos asociados con la pluralidad de espacios cibernéticos. En algunas realizaciones, el motor de simulación está configurado para generar simulaciones. En algunas realizaciones, las simulaciones están configuradas para operar en al menos uno de los datos del mundo real y los datos simulados, y proporcionan un curso de acción para al menos uno de operaciones, análisis, conocimiento, planificación, capacitación, una acción de remediación y una acción de mitigación.

En algunas realizaciones, el motor de flujo de trabajo analítico asociado con el sistema de seguridad cibernética que está configurado para recibir datos del sensor está configurado para crear un espacio de comportamiento cibernético transformado. En algunas realizaciones, en el que, para crear el espacio de comportamiento cibernético transformado, el motor de flujo de trabajo analítico está configurado para transformar los datos del espacio de comportamiento cibernético en datos de tensor y aproximaciones de tensor de rango inferior, y usar el aprendizaje de máquina para definir los comportamientos cibernéticos y la pluralidad de espacios de comportamiento cibernético asociado con el espacio de comportamiento cibernético transformado.

En algunas realizaciones, el motor de flujo de trabajo analítico asociado con el sistema de seguridad cibernética que está configurado para recibir datos del sensor está configurado para aplicar al menos una de las reglas y el aprendizaje de máquina al espacio de comportamiento cibernético transformado para definir comportamientos cibernéticos que aumentan o disminuyen el riesgo. asociado con al menos uno de un actor real cibernético o un actor simulado, una entidad cibernética, una máquina, una organización y un proceso.

En algunas realizaciones, el sistema de seguridad cibernética que está configurado para recibir datos del sensor está asociado con una primera organización, además en el que los comportamientos cibernéticos que aumentan o disminuyen el riesgo son observables por los actores cibernéticos asociados con la primera organización y no pueden ser observados por los actores cibernéticos asociados con una segunda organización. En algunas realizaciones, el sistema de seguridad cibernética incluye un motor de intercambio de comportamiento cibernético, el motor de intercambio de comportamiento cibernético en comunicación con el módulo de gestión del espacio de comportamiento cibernético. En algunas realizaciones, el motor de intercambio de comportamiento cibernético está configurado para transmitir los comportamientos cibernéticos que aumentan o disminuyen el riesgo para un motor de intercambio de comportamiento cibernético asociado con la segunda organización que utiliza al menos uno de un algoritmo de aprendizaje de máquina distribuido que preserva la privacidad y un protocolo de comunicaciones que preserva la privacidad. de tal manera que los comportamientos cibernéticos que aumentan o disminuyen el riesgo se pueden usar para analizar datos en la segunda organización, y los datos del espacio de comportamiento cibernético asociados con la primera organización no son observables por los actores cibernéticos asociados con la segunda organización.

En algunas realizaciones, los datos del primer actor cibernético asociados con el sistema de seguridad cibernética que está configurado para recibir datos del sensor se procesan para determinar al menos uno de los primeros comportamientos cibernéticos de los comportamientos cibernéticos asociados con el espacio del comportamiento cibernético transformado, y primera escena cibernética de la pluralidad de escenas cibernéticas asociadas con el espacio de comportamiento cibernético transformado; y mejorar las capacidades operativas, la preparación y la capacitación asociadas con la respuesta al primer comportamiento cibernético y la primera escena cibernética.

En algunas realizaciones, el motor de flujo de trabajo analítico está configurado para procesar al menos uno de los datos de los sensores de tecnología operacional (OT), registros de tecnología operacional, datos de paquetes, tráfico de red, registros de ordenador, inteligencia de señales, visible, infrarrojo, multiespectral, hiperespectral, radar de apertura sintética, radar indicador de objetivo móvil, datos de inteligencia técnica e informes de inteligencia.

En algunas realizaciones, cada uno de la pluralidad de espacios de comportamiento cibernético asociados con el sistema de seguridad cibernética que está configurado para recibir datos del sensor incluye al menos uno de un espacio de comportamiento cibernético en tiempo real, un espacio de comportamiento cibernético histórico y un espacio de comportamiento ciberespacio simulado. En algunas realizaciones, el comportamiento cibernético incluye al menos uno de reconocimiento inicial, escaneo, compromiso inicial, establecimiento de un punto de apoyo, baliza, comando y control, captura de credenciales, privilegios crecientes, reconocimiento interno, movimiento lateral, mapeo de red, exfiltración de datos, mantenimiento de la persistencia, y comportamientos relacionados.

En algunas realizaciones, la pluralidad de dimensiones asociadas con el sistema de seguridad cibernética que está configurado para recibir datos del sensor incluye una combinación de direcciones de origen y destino, hora de llegada, volumen, tamaño de paquete y un tipo de protocolo, la pluralidad de modos incluye una combinación de datos de paquete, tráfico de red, registros de ordenador, inteligencia de señales, visible, infrarrojo, multiespectral,

hiperespectral, radar de apertura sintética, radar indicador de objetivo móvil, datos de inteligencia técnica e informes de inteligencia, y la pluralidad de escalas incluye una combinación de datos temporales multiescala y datos geoespaciales.

Estas y otras capacidades de la materia divulgada se entenderán más completamente después de una revisión de las siguientes figuras, descripción detallada y reivindicaciones. Debe entenderse que la fraseología y la terminología empleadas en este documento son para fines de descripción y no deben considerarse limitativas.

Breve descripción de las figuras

Varios objetivos, características y ventajas de la materia divulgada pueden apreciarse más completamente con referencia a las siguientes descripciones detalladas de la materia divulgada cuando se considera en relación con los siguientes dibujos, en los que números de referencia similares identifican elementos similares. Debe entenderse que la fraseología y la terminología empleadas en este documento son para fines de descripción y no deben considerarse limitativas.

La fig. 1 es un diagrama de sistema que muestra un sistema de seguridad cibernética, de acuerdo con algunas realizaciones de la presente divulgación.

La fig. 2A es un diagrama que muestra técnicas de modelado multiescala utilizando ventanas de diferentes tamaños, de acuerdo con algunas realizaciones de la presente divulgación.

La fig. 2B es un diagrama que muestra el modelado multiescala utilizado para modelar datos en la CBS y para representaciones tensoriales de la CBS, de acuerdo con algunas realizaciones de la presente divulgación.

La fig. 3 es un diagrama que muestra la función de las aproximaciones y tensores de rango inferior en la creación de un espacio de comportamiento cibernético (CBS), de acuerdo con algunas realizaciones de la presente divulgación.

La fig. 4 es un diagrama de sistema que muestra un motor de interacción que gestiona un entorno de CBS interactivo, de acuerdo con algunas realizaciones de la presente divulgación.

La fig. 5 es un diagrama de sistema que muestra un motor de simulación que gestiona un conjunto de CBS, de acuerdo con algunas realizaciones de la presente divulgación.

La fig. 6 es un diagrama de sistema que muestra el funcionamiento de múltiples intercambios de comportamiento cibernético (CBX) para compartir información de forma segura dentro o entre empresas de una manera controlada, de acuerdo con algunas realizaciones de la presente divulgación.

La fig. 7 es un diagrama de sistema que muestra un sistema de seguridad cibernética que interactúa con un entorno de tecnología operacional, de acuerdo con algunas realizaciones de la presente divulgación.

Descripción detallada

En algunas realizaciones, se utilizan simulaciones y un sistema de realidad virtual para mejorar las capacidades operativas y la capacitación de los defensores cibernéticos, compartiendo información relacionada con el comportamiento entre ellos, incluida la información relacionada con el comportamiento observada, información relacionada con el comportamiento calculada mediante el uso de flujos de trabajo analíticos e información relacionada con el comportamiento generada cuando múltiples actores cibernéticos reales o virtuales, de una o más organizaciones, participan en escenarios, simulaciones y entornos de realidad virtual.

En algunas realizaciones, la información relacionada con el comportamiento se intercambia de forma segura y preservada de la privacidad mediante el uso de intercambios cibernéticos de comportamiento, de modo que dos o más organizaciones pueden intercambiar información como parte de escenas, simulaciones y entornos de realidad virtual para mejorar la capacitación y mejorar la defensa. de una organización, o para mejorar la defensa de múltiples organizaciones que comparten información.

Espacios de comportamiento cibernéticos

Algunas realizaciones del sistema de seguridad cibernética se basan en un espacio de comportamiento cibernético (también denominado aquí como CBS), que, en una de sus implementaciones, incluye al menos uno de los siguientes cinco elementos: 1) multidimensional, multi-modal, datos multiescala; 2) actores cibernéticos; 3) escenas; 4) asignación de comportamientos cibernéticos a 1), 2) o 3); y 5) asignación de comportamientos físicos a 1), 2), o 3). Cada uno de estos cinco elementos se describe con más detalle a continuación.

Los datos multidimensionales, multimodales y multiescala pueden incluir, entre otros, datos sobre: entidades, actores, redes, espacios físicos, espacios virtuales, sus comportamientos y sus interacciones. Multi-dimensional puede referirse

a los atributos de datos que se derivan, extraen o calculan. Los ejemplos de atributos de datos para datos cibernéticos incluyen, entre otros, direcciones de origen y destino, hora de llegada, volumen, tamaño del paquete y tipo de protocolo. Los datos multimodales se refieren a los datos derivados de múltiples tipos de sensores o dominios, incluidos los dominios cibernéticos. Los ejemplos de datos multimodales incluyen, entre otros: datos de paquetes, tráfico de red, registros de ordenadores, inteligencia de señales, visible, infrarrojo, multiespectral, hiperespectral, radar de apertura sintética, radar indicador de objetivo móvil, datos de inteligencia técnica, e informes de inteligencia. Multiescala se refiere a los datos que pueden utilizarse en modelos con diferentes resoluciones. Los datos temporales, los datos geoespaciales, los datos de la organización y los datos de la red pueden formar parte de los modelos multiescala. Por ejemplo, los datos temporales de varias escalas se refieren al tiempo que se puede modelar, por ejemplo, en unidades de años, meses, semanas, días, horas, minutos, segundos, milisegundos. Los datos geoespaciales multiescala, por ejemplo, pueden incluir datos a diferentes escalas, como nivel de casa, nivel de bloque, nivel de bloque múltiple, ciudad y región.

Un actor cibernético puede referirse a actores individuales o una colección de actores cibernéticos. Un actor cibernético también puede ser un individuo real o un actor virtual, y puede interactuar con espacios cibernéticos de comportamiento en tiempo real, históricos y simulados. Como se describe con más detalle a continuación, los espacios de comportamiento cibernético pueden incluir uno o más actores cibernéticos. En algunas realizaciones, los espacios de comportamiento cibernético no incluyen ningún otro actor cibernético o actor cibernético simulado.

Una escena cibernética puede referirse a una combinación de actores, entidades, redes y espacios físicos o virtuales. En algunas realizaciones, una escena no contiene ningún actor, o puede que no contenga ninguna entidad, red o espacio físico o virtual. Un ejemplo de una escena es: un actor cibernético que filtra (o extrae) datos de una entidad comprometida, la exfiltración de los datos se identifica mediante un modelo de comportamiento y un defensor cibernético que aísla a la entidad comprometida de la red.

Una asignación de comportamientos cibernéticos puede ser a 1), 2) o 3), como se describió anteriormente, o a estructuras, componentes o combinaciones de los mismos. Cada uno de 1) datos multidimensionales, multimodales y multiescala; 2) actores cibernéticos; y 3) las escenas pueden ser en sí mismas complejas y generalmente tienen una estructura jerárquica con elementos, subelementos; y colecciones o colecciones de colecciones, etc. Las asignaciones de comportamientos cibernéticos pueden ser elementos, relaciones entre elementos, arreglos entre elementos o estructuras construidas a partir de elementos, subelementos y sus relaciones, de manera similar para subelementos, etc. o colecciones, relaciones entre colecciones, arreglos entre colecciones, o estructuras construidas a partir de colecciones, colecciones de colecciones y sus relaciones, de manera similar para colecciones de colecciones, etc. Los comportamientos cibernéticos, incluyen, pero no se limitan a, reconocimiento inicial, escaneo, compromiso inicial, establecimiento de puntos de apoyo, baliza, comando y control, captura de credenciales, privilegios crecientes, reconocimiento interno, movimiento lateral, mapeo de red, exfiltración de datos, mantenimiento de persistencia y comportamientos relacionados. Por ejemplo, a algunos grupos de puntos definidos por las características creadas a partir de los datos se les puede asignar “comportamiento exfil”, mientras que a otros grupos se les puede asignar “comportamiento de reconocimiento”. Exfil (exfiltración de datos) se refiere generalmente a la copia, transferencia o recuperación no autorizadas de datos desde un ordenador o dispositivo de almacenamiento. El comportamiento de reconocimiento se refiere generalmente a aprender sobre una red y los dispositivos que contiene para facilitar su compromiso. En algunas realizaciones, los comportamientos se pueden asignar de la siguiente manera: suponga que cada punto en un primer conjunto de datos está etiquetado con uno de los comportamientos cibernéticos enumerados anteriormente o con una etiqueta, como NA, lo que indica que el comportamiento asociado con ese punto no está relacionado con ninguno de los comportamientos enumerados anteriormente. También asuma que se usa un algoritmo para agrupar los puntos en grupos. Cada grupo puede ser etiquetado con una etiqueta que sea más relevante para ese grupo que cualquiera de las otras etiquetas que aparecen en ese grupo. Ahora, dado un segundo conjunto de datos, cada uno de los puntos se puede asignar al grupo que está más estrechamente relacionado con el punto de datos y luego se puede etiquetar con la etiqueta correspondiente a ese grupo. Los comportamientos pueden asignarse a los puntos en el primer conjunto de datos de múltiples maneras, incluyendo, entre otros, el uso de métodos de aprendizaje de máquina o métodos estadísticos que analizan datos históricos. transmisión de datos, o datos interactivos; usar reglas y motores de reglas para definir el comportamiento; utilizando expertos para definir el comportamiento; o utilizando alguna combinación de estos métodos.

Una asignación de comportamientos físicos puede ser a 1), 2) o 3), como se describió anteriormente, o a estructuras, componentes o combinaciones de ellos. Al igual que con el comportamiento cibernético, la asignación del comportamiento físico puede ser a elementos, subelementos, etc. de 1), 2) y 3) y sus arreglos y relaciones y estructuras construidas a partir de ellos, o colecciones, colecciones de colecciones, etc. de 1), 2) y 3) y sus arreglos, relaciones y estructuras construidas a partir de ellos. Los comportamientos físicos incluyen, entre otros, inicios de sesión, ubicaciones geoespaciales de individuos tanto internos como externos a una empresa o sitio de trabajo, movimientos de humanos, dispositivos físicos y máquinas, e interacciones entre humanos, dispositivos físicos y máquinas. Los ejemplos incluyen: lugares de trabajo, vías de acceso, vehículos, centros de datos, entornos que contienen dispositivos físicos y máquinas, plantas físicas y sus componentes, como líneas de transmisión y plantas de generación.

En algunas realizaciones, solo un subconjunto de los cinco elementos descritos anteriormente está presente en un espacio de comportamiento cibernético.

La fig. 1 muestra un sistema 100 de seguridad cibernética, de acuerdo con algunas realizaciones de la presente divulgación. El sistema 100 de seguridad cibernética incluye el motor 106 de interacción, el motor 107 de consulta de comportamiento cibernético, el motor 108 de visualización, el motor 109 de monitoreo/informes, el administrador 113 CBS, el motor 114 de flujo de trabajo analítico, el motor 115 de simulación, el intercambio 117 de comportamiento cibernético (CBX) y los flujos 118 de trabajo analíticos. La fig. 1 también muestra datos 101 cibernéticos, datos 102 de sensores, datos 103 de enriquecimiento, datos 104 de terceros, actores 105 cibernéticos reales y virtuales, un espacio 110 cibernético (CBS) inicial y actualizado, CBS 111 simulada, CBS 112 interactiva, y observadores y controladores 116.

Los datos 101 cibernéticos pueden incluir datos cibernéticos multidimensionales, de múltiples dominios y multiescala, incluyen, entre otros, datos sobre entidades cibernéticas, actores cibernéticos, paquetes y flujos de redes, sus comportamientos y sus interacciones. En algunas realizaciones, los datos 101 cibernéticos se gestionan mediante un sistema de gestión de datos (no mostrado). Un sistema de gestión de datos puede ser una base de datos relacional, una interfaz para un sistema de gestión de la configuración o cualquier otro sistema informático que tenga una interfaz de usuario y un mecanismo de almacenamiento integrados.

Los datos 102 del sensor pueden incluir datos reales o simulados para el entorno físico, incluidos, entre otros, los siguientes: visible, infrarrojo, multiespectral, hiperespectral, radar de apertura sintética (SAR), indicador de objetivo móvil (MTI), cámaras de seguridad, acústicas, biométricas, y lectores de tarjetas. Los diferentes tipos de datos 102 de sensores también se denominan en este documento datos multimodales.

Los datos 103 de enriquecimiento incluyen información que proporciona un contexto adicional a los datos cibernéticos y los datos del sensor, incluidos, entre otros, el protocolo de configuración dinámica del host (DHCP), el sistema de nombres de dominio (DNS), la gestión de activos, la gestión de configuración, los archivos de registro e información de recursos humanos.

Los datos 104 de terceros son fuentes adicionales de datos que pueden correlacionarse con los tipos de datos anteriores, incluidos, entre otros para: los avances de gestión de amenazas, los dominios de reputación y las listas negras.

Una colección de flujos 118 de trabajo analíticos que procesan datos históricos, transmisión de datos, datos simulados y datos de interacciones para identificar comportamientos cibernéticos. Los comportamientos cibernéticos incluyen, pero no se limitan a: reconocimiento inicial, escaneo, compromiso inicial, establecimiento de baliza, baliza, comando y control, captura de credenciales, privilegios crecientes, reconocimiento interno, movimiento lateral, mapeo de red, exfiltración de datos, mantenimiento de la persistencia, y conductas relacionadas. En algunas realizaciones, el comportamiento cibernético se define mediante métodos de aprendizaje de máquina o métodos estadísticos que analizan datos históricos. En algunas realizaciones, las reglas se utilizan, ya sea manualmente codificadas por expertos o gestionadas por un motor de reglas, para definir el comportamiento. En algunas realizaciones, se usa una combinación de estos y otros métodos.

Los actores 105 cibernéticos, pueden ser individuos reales o virtuales, con la capacidad de interactuar con espacios cibernéticos del comportamiento en tiempo real, históricos y simulados que contienen escenas que involucran cero o más actores cibernéticos y cero o más actores cibernéticos simulados.

Un motor 106 de interacción permite a los actores 105 cibernéticos reales y virtuales interconectar y modificar el sistema de comportamiento cibernético.

Un motor 107 de consulta de comportamiento cibernético permite que los actores reales, los actores virtuales y otros componentes del sistema consulten los comportamientos cibernéticos de CBS, tales como, entre otros, los comportamientos de exfill, baliza o explotación, ya sea en general o aquellos comportamientos cibernéticos que están restringidos a otras restricciones, como, por ejemplo, restricciones a ciertas horas del día, ciertos segmentos de red y ciertos puertos. En algunas realizaciones, el motor de consulta de comportamiento cibernético también puede recuperar ciertos subconjuntos de datos de la CBS, como todos los datos asociados con segmentos de tiempo específicos, segmentos de red específicos, puertos específicos, usuarios específicos, dispositivos específicos o combinaciones booleanas de estos y cualesquiera. Otros atributos o características de los datos en la CBS. En algunas realizaciones, el motor de consulta de comportamiento cibernético también puede desglosar a lo largo de las dimensiones, como, por ejemplo, tiempo, segmentos de red y categorías de usuarios. Por ejemplo, un desglose de usuarios puede proceder de todos los usuarios, a todos los empleados, a todos los empleados con una división, ya todos los empleados dentro de un departamento en la división.

Un motor 108 de visualización proporciona representaciones 2-D y 3-D de la CBS, sus procesos, componentes y salidas.

El motor 109 de supervisión/informe proporciona el estado histórico y en tiempo real de la CBS y sus procesos y componentes.

El CBS inicial 110 proporciona un estado de inicio para el CBS simulado. El CBS 110 actualizado es el CBS resultante después de los datos y otras actualizaciones del sistema.

El CBS 111 simulado representa el CBS generado por el motor 115 de simulación, así como otras actualizaciones proporcionadas por el administrador de CBS 113.

El CBS 112 interactivo representa el CBS generado por el motor 106 de interacción, así como otras actualizaciones proporcionadas por el administrador de la CBS.

Un CBS 118 general se denomina en el presente documento como uno cualquiera o combinación de un CBS 110 inicial, un CBS 110 actualizado, un CBS 111 simulado, un CBS 112 interactivo o cualquier otro CBS generado por uno de los componentes del sistema.

El administrador 113 de CBS (al que también se hace referencia aquí como un módulo de gestión del espacio de comportamiento cibernético) gestiona los datos 119, incluyen, entre otros, los datos 101 cibernéticos, los datos 102 del sensor, los datos 103 de enriquecimiento y los datos 104. de terceros. el administrador 113 también proporciona mecanismos de control y actualización para la CBS asociada con el sistema, incluida la gestión de la CBS simulada inicial, la CBS asociada con el entorno simulado, la CBS asociada con los entornos interactivos, la CBS asociada con el entorno real, otra CBS y varias combinaciones de estos. El administrador 113 de CBS está en comunicación con cada uno de los otros componentes dentro del sistema 100 de seguridad cibernética. El administrador de CBS procesa los datos y encamina los datos procesados y no procesados entre los componentes. Como se describe aquí, El administrador 113 de CBS genera espacios de comportamiento cibernético basados en los datos de entrada. En algunas realizaciones, los espacios de trabajo cibernéticos se generan o actualizan mediante flujos 118 de trabajo analíticos ejecutados por el motor 114 de flujo de trabajo analítico aplicado a al menos uno de CBS, datos de entrada y datos de otros componentes del sistema, como se describe con más detalle a continuación.

El motor 114 de flujo de trabajo analítico gestiona los tipos y combinaciones de analíticas que operan en la CBS, incluidos los flujos de trabajo analíticos para los tensores asociados con la CBS, y los flujos de trabajo analíticos para las aproximaciones de rango inferior de los tensores asociados con la CBS. En algunas realizaciones, el motor 114 de flujo de trabajo analítico analiza los datos del espacio de comportamiento cibernético asociados con los espacios de comportamiento cibernético para calcular los comportamientos cibernéticos, y actualiza al menos uno de los datos cibernéticos, los datos del actor cibernético y los datos de la escena cibernética basados en al menos uno de los datos del espacio de comportamiento cibernético, los comportamientos cibernéticos calculados y una asignación de los comportamientos cibernéticos calculados a al menos uno de los datos cibernéticos, los datos de los actores cibernéticos y los datos de la escena cibernética, y las interacciones entre los actores cibernéticos con otros actores cibernéticos y con los actores cibernéticos y con el espacio de comportamiento cibernético. Por ejemplo, si un actor que normalmente no se conecta con ninguna base de datos, inicia sesión en una estación de trabajo en la que nunca ha iniciado sesión e intenta conectarse a varias bases de datos y falla, un primer flujo de trabajo analítico que examina el comportamiento normal de ese actor puede asignar una alta puntuación basada en su uso de una nueva máquina y para contactar servicios con los que normalmente no se comunica, como las bases de datos. Un segundo flujo de trabajo analítico puede asignar una puntuación alta en función del número de inicios de sesión fallidos, mientras que un tercer flujo de trabajo analítico puede asignar una puntuación alta en base a una base de datos especialmente sensible a la que intentó conectarse, incluso si el inicio de sesión no falló. Finalmente, un cuarto flujo de trabajo analítico, basado en un análisis de los puntajes de los tres flujos de trabajo analíticos, puede asignar una etiqueta de “probable mal actor” al actor y podría asignar una etiqueta de “intento de acceso no autorizado” a los puntos en el conjunto de datos asociado con los inicios de sesión fallidos en las bases de datos, y podría asignar una etiqueta de “intento de movimiento lateral” a la escena que consiste en parte del actor probablemente malo, sus estaciones de trabajo asociadas, las distintas bases de datos y las conexiones asociadas.

El motor 115 de simulación proporciona los mecanismos para inicializar y actualizar el CBS simulado, basado en simulaciones, basado en algoritmos, así como entradas del mundo real y de actores cibernéticos virtuales y reales.

Los observadores y controladores 116 gestionan el estado general de la CBS para garantizar que se logren los objetivos.

El intercambio 117 de comportamiento cibernético proporciona el mecanismo para compartir datos de forma segura y mediar interacciones con otras CBS internas o externas a una empresa.

En algunas realizaciones, los datos para el espacio 110, 111, 112, 118 de comportamiento cibernético provienen de los datos 119, que incluyen los datos 101 cibernéticos, los datos 102 del sensor, los datos 103 de enriquecimiento y los datos 104 de terceros. El comportamiento cibernético de la CBS se define por los flujos 118 de trabajo analíticos gestionados por el motor 114 de flujo de trabajo analítico. Los actores 105 cibernéticos reales y virtuales proporcionan los actores cibernéticos requeridos por la CBS, y las escenas requeridas por la CBS son generadas por el motor 115 de simulación, el motor 106 de interacción, el motor 114 de flujo de trabajo analítico, o una combinación de los motores 106 114 115.

En algunas realizaciones, los datos 101 cibernéticos, los datos 102 del sensor, los datos 102 de enriquecimiento o el tercero 103 pueden distribuirse, ya sea dentro de una única ubicación, o a través de dos o más ubicaciones distribuidas geográficamente. En el caso de que los datos se distribuyan, en algunas realizaciones se utilizan redes, incluidas redes de alto rendimiento, buses de servicio empresarial u otra tecnología para transportar los datos. De manera similar, se pueden distribuir componentes del sistema, incluidos, entre otros, el motor 114 de flujo de trabajo analítico, el motor 115 de simulación, el motor 106 de interacción y el motor 108 de visualización.

La CBS se puede enriquecer con mapas. Los mapas en este contexto pueden verse como una visualización que está vinculada a un espacio de información, un espacio físico, un espacio de red, un espacio cibernético, un espacio social y un espacio organizativo, o una combinación de estos diferentes tipos de espacio que contienen datos e información. Un espacio organizativo muestra las relaciones entre un conjunto de entidades. Un ejemplo es una estructura organizativa para una empresa u otra organización. Los espacios de organización interna pueden referirse a “interno” dentro de la organización, mientras que “externo” puede referirse a relaciones con otras entidades. Por ejemplo, un CBS se puede enriquecer con mapas sobre: las ubicaciones físicas de las instalaciones asociadas con una organización; sobre la topología de red que describe cómo las diferentes entidades de red y otros dispositivos están conectados entre sí; sobre el espacio organizacional, describiendo a los individuos y su estructura de reporte; y sobre la estructura de información que describe cómo se organizan los datos.

En algunas realizaciones, una escena se refiere a una secuencia de comportamientos de actores 105 cibernéticos reales o virtuales que pueden depender de: i) datos cibernéticos, sensores, de enriquecimiento, de terceros u otros; ii) interacciones de dos o más de los actores cibernéticos reales o virtuales en las escenas; o iii) una o más acciones de terceros (es decir, acciones de actores reales o virtuales que no están en escena); o, iv) una o más interacciones de terceros con los actores reales o virtuales en la escena. Las escenas se pueden combinar para crear escenarios de entrenamiento. En algunas realizaciones, los actores de la misma organización pueden distribuirse geográficamente y comunicarse a través de una red. En otros casos, los actores reales y virtuales de diferentes organizaciones, que pueden estar distribuidos geográficamente, pueden utilizar el intercambio 117 de comportamiento cibernético para comunicarse.

Las escenas pueden atraer a varios defensores de diferentes ubicaciones geográficas utilizando el intercambio 117 de comportamiento cibernético para participar en la simulación para comprender un problema común de manera sincronizada. Las escenas y escenarios interactivos pueden, en algunas realizaciones, implicar cambios realizados por acciones que los defensores activos están tomando y que los adversarios están tomando. Como ejemplo, en una escena, un actor cibernético puede participar en el reconocimiento de la red desde una máquina comprometida que es lo suficientemente silenciosa como para ocultarse en el ruido de fondo de un segmento de la red, mientras que varios defensores de múltiples ubicaciones geográficas que actúan individualmente o en equipos tratan de localizar el actor cibernético y la máquina comprometida por los comportamientos observados en el segmento de red.

La CBS se puede crear de múltiples maneras, incluyendo, entre otras, la actualización de una CBS existente para crear una CBS 110 actualizada basada en datos nuevos, simular comportamientos para crear una CBS 111 simulada y hacer que actores reales o virtuales se involucren en entornos interactivos para crear CBS con comportamiento 112 interactivo. Los comportamientos se pueden definir de múltiples maneras, incluyendo lo siguiente: i) los métodos de aprendizaje de máquina e inteligencia artificial (AI) se pueden usar para aprender el comportamiento de datos históricos o simulados; ii) El sistema CBS, en algunas realizaciones, tiene una interfaz de programación de aplicaciones (API) para que los comportamientos se puedan generar utilizando reglas, códigos que impliquen primitivas de comportamiento o utilizando entornos más complejos para generar comportamientos específicos del usuario; iii) Los comportamientos se pueden aprender utilizando el procesamiento de lenguaje natural para extraer comportamientos de texto en documentos, de texto almacenado en redes internas, de texto extraído de Internet y de texto extraído de sistemas de redes sociales; y iv) el comportamiento puede extraerse procesando los datos producidos cuando individuos reales se involucran en comportamientos específicos o ad hoc.

Datos multiescala y representaciones tensoriales

Como el volumen de datos, el número de dimensiones, el número de segmentos del modelo y el número de modalidades de los datos, algunas realizaciones de la presente divulgación representan los datos 119 como tensores. Un tensor es una matriz de múltiples índices de números. El orden de un tensor es el número de sus modos o dimensiones. Los tensores se pueden pensar en generalizaciones de vectores (tensores de orden uno) y matrices (tensores de orden dos), e incluyen vectores y matrices como casos especiales. Los elementos de los tensores son números que pueden derivarse, extraerse o calcularse y pueden representar datos multimodales. Un ejemplo de un tensor de orden tres, es una matriz numérica con cinco índices, donde los elementos representan el volumen de tráfico desde la IP de origen a la IP de destino asociada con un protocolo particular durante un día. Supongamos en este ejemplo, que los protocolos observados se agrupan en 25 tipos, numerados 1, 2, ..., 25. Aquí las tres dimensiones son: IP de origen, IP de destino y tipo de protocolo. Los ejemplos de atributos de datos multimodales que se pueden usar para crear tensores incluyen, entre otros, datos de paquetes, tráfico de red, registros de ordenadores, inteligencia de señales, visible, infrarrojo, multiespectral, hiperespectral, radar de apertura sintética y radar indicador de objetivo móvil.

En algunas realizaciones de la presente divulgación, los tensores se procesan utilizando flujos de trabajo que se describen en gráficos acíclicos, en los que los nodos representan cálculos, y los bordes dirigidos representan flujos de datos de un nodo (la fuente del borde) a otro nodo (el objetivo del borde). Los nodos pueden tener múltiples entradas y salidas de tensor, y algunas entradas y salidas pueden usar segmentos o proyecciones de las entradas y salidas de tensor. Los flujos de trabajo que se describen en los gráficos acíclicos son ejemplos de los flujos de trabajo analíticos gestionados por el motor 114 de flujo de trabajo analítico. En particular, los flujos de trabajo analíticos como estos se pueden utilizar para procesar los datos en la CBS para extraer comportamientos de interés utilizando el aprendizaje de máquina, utilizando técnicas estadísticas, utilizando reglas, o utilizando cualquiera de los otros métodos descritos en esta divulgación. Los métodos basados en el tensor también se utilizan para crear el CBS 111 simulado por el motor 115 de simulación.

Para cualquiera de las variables en los datos, el análisis se puede realizar a diferentes escalas o niveles de granularidad, utilizando varios métodos diferentes. El modelado multiescala se refiere a un tipo de modelado en el que múltiples modelos a diferentes escalas se utilizan simultáneamente para describir un sistema, con los diferentes modelos utilizan datos en diferentes escalas de resolución. Por ejemplo, con el análisis temporal multiescala, una ventana 205 de salto, como se describe con más detalle con respecto a la FIG. 2, se puede usar para reemplazar todas las mediciones en la ventana con una sola medición, por ejemplo, una media, una media recortada, una mediana o alguna otra estadística o característica que se calcula a partir de los datos de la ventana. Como se describe en el presente documento, una ventana se refiere a un subconjunto contiguo de un atributo de datos o característica x, como los datos en el intervalo [x, x+w]. Windows puede saltar moviéndose de forma no superpuesta, por ejemplo, desde [x, x+w], [x+w, x+2w], o pueden deslizarse en una cantidad s, donde s < w, por ejemplo, desde [x, x+w], [x+s, x+s+w], [x+2s, x+2s+w]. Al usar ventanas de diferentes tamaños, como las ventanas que crecen en tamaño multiplicativamente, se generan CBS en diferentes escalas de resolución. El análisis multiescala es aplicable tanto al original como a las características derivadas de los datos originales. El análisis temporal multiescala de los datos y comportamientos asociados con CBS también se puede usar para ralentizar o reproducir en un comportamiento más rápido que en tiempo real asociado con CBS.

La fig. 2 es un diagrama que muestra el cálculo de representaciones multiescala de los datos 119, de acuerdo con algunas realizaciones de la presente divulgación. La FIG. 2a muestra técnicas de modelado multiescala utilizando ventanas de diferentes tamaños, de acuerdo con algunas realizaciones, y la FIG. 2b muestra cómo se puede usar el modelado multiescala para modelar datos en la CBS 118 y para las representaciones de tensor 203 de la CBS, de acuerdo con algunas realizaciones. De esta manera, los datos 119 se pueden usar para calcular el CBS 118 que involucra el modelado multiescala, que a su vez se puede representar utilizando los tensores 203 que involucran el modelado multiescala. Los datos y tensores de CBS se pueden analizar mediante el motor 114 de flujo de trabajo analítico para crear modelos de comportamiento, y los modelos de comportamiento y los datos asociados pueden estar disponibles para consultas.

Como se muestra en la FIG. 2, una secuencia de ventanas saltadoras 205 de tamaño creciente, con cada ventana dos veces el tamaño de su predecesora puede usarse para crear una representación multiescala de los datos. Las ventanas de mayor tamaño o escala se pueden generar de otras maneras, como hacer que cada ventana sea 10x, 100x o 100x más grande que la anterior, por ejemplo. Las representaciones tensoriales de los datos 206 y las representaciones tensoras de las representaciones multiescala de los datos 203 pueden ser analizadas por el sistema de la manera que se describe a continuación. Algunas ventajas de usar representaciones de tensor como se describe aquí incluyen habilitar 1) realidad virtual (VR) temporal multiescala y reproducción de datos históricos, incluida la reproducción que es más rápida que en tiempo real; 2) reproducción VR temporal de escala múltiple de datos simulados, incluida la capacidad de reproducción más rápida que en tiempo real; 3) VR temporal multiescala de datos históricos y simulados integrados.

Como un ejemplo simple de tensor y de análisis multiescala, un tensor de 5 vías con IP de origen de dimensiones, IP de destino, puerto de origen, puerto de destino y tiempo t puede construirse para escalas de tiempo w de 1 ms, 10 ms, 100 ms, 1 segundo, 10 segundos, 100 segundos, 1000 segundos, 10.000 segundos y 100.000 segundos, donde cada elemento del tensor indica el número de paquetes desde la IP de origen y el puerto de origen hasta la IP de destino y el puerto de destino durante el tiempo período de t a t + w. Si las visualizaciones e interacciones se actualizan una vez por cada 100 ms (es decir, a 10 × por segundo), el uso de tensores asociados con ventanas de 1 segundo o más produce visualizaciones más rápidas que en tiempo real (en otras palabras, el tiempo se acelera). Por ejemplo, si las ventanas tienen un tamaño de 10 segundos y las escenas en entornos CBS interactivos o las interacciones entre actores reales y/o virtuales se actualizan 10 × por segundo, entonces cada segundo de interacción entre actores reales o virtuales, según lo mide el reloj de pared, corresponde a 100 segundos de actividad si la actividad se desarrollara en tiempo real. Es decir, las interacciones virtuales en los entornos CBS interactivos son más rápidas que en tiempo real.

Algunas realizaciones del sistema utilizan métodos para reducir los datos en la CBS y sus representaciones tensoriales a una estructura dimensional inferior, como las aproximaciones de rango inferior a los tensores que representan los datos o los datos procesados en la CBS. Una forma de definir el rango del tensor es descomponer un tensor de orden k como una suma de productos externos de k vectores de las dimensiones apropiadas, como se muestra en el

siguiente ejemplo. En este caso, el número de sumandos es el rango. Estas aproximaciones de rango inferior a los tensores originales se pueden calcular de diferentes maneras, incluidas, entre otras, la CANDECOMP/PARAFAC (CP) o la descomposición de Tucker de un tensor. En algunas realizaciones del sistema, los modelos de comportamiento están asociados con características de estas aproximaciones de rango inferior a los tensores originales.

Como ejemplo simple, considere un tensor de orden 3 $T_{x1, x2, x3,}$ donde el primer componente del tensor es de dimensión n_1, el segundo componente del tensor es de dimensión n_2 y el tercer componente del tensor es de dimensión n_3. El tensor $T_{x1, x2, x3,}$ se puede escribir como una suma:

$$T_{x1, x2, x3} = \Sigma\, a_i \circ b_i \circ c_i,$$

donde la suma es para i = 1 a r, a_i, b_i y c_i son vectores de dimensiones n_1, n_2 y n_3 respectivamente, y ∘ indica los productos externos de los vectores. Aquí r es el rango de la aproximación del tensor dimensional inferior. Observe que el tensor $T_{x1, x2, x3}$ tiene $n_1\, n_2\, n_3$ grados de libertad, mientras que la aproximación del tensor r del rango dimensional más bajo tiene r $(n_1 + n_2 + n_3)$ grados de libertad, que es mucho menor que $n_1\, n_2\, n_3$ para r pequeña y dimensiones grandes n_i. Esto se debe a que, por ejemplo, hay n_1 grados de libertad para a_1, n_2 grados de libertad para b_1, y n_3 grados de libertad para c_1, por lo tanto $(n_1 + n_2 + n_3)$ grados de libertad para el producto externo de $a_1 \circ b_1 \circ c_1$. Como hay r tales productos externos en la suma en el lado derecho de la ecuación anterior, la observación sigue. Esta descomposición puede ser calculada utilizando varios algoritmos, que incluyen el algoritmo CANDECOMP/PARAFAC.

En algunas realizaciones, los métodos de aprendizaje de máquina se aplican a los datos de los sensores mediante el motor 114 de flujo de trabajo analítico para crear datos 210 de comportamiento procesados, incluyen modelos de comportamiento, comportamiento de grupo y segmento, y matrices de riesgo de entidades. Los datos creados pueden luego ser consultados por un parámetro especificado por el usuario, como el comportamiento, el riesgo o las consultas ad hoc. En algunas realizaciones, las reglas y los métodos de aprendizaje de máquina se aplican a las matrices de riesgo de la entidad, de modo que el riesgo de las entidades se basa en reglas y análisis que incluyen los resultados de las diversas reglas, modelos y flujos de trabajo que se colocan en el sistema. Estas matrices de riesgo de entidad actualizadas, que se pueden actualizar utilizando lotes, transmisión por secuencias, actualizaciones basadas en eventos, se pueden consultar mediante un parámetro especificado por el usuario, como el comportamiento, el riesgo o las consultas ad hoc.

La Figura 3 es un diagrama que muestra aproximaciones de rango inferior a los tensores en la creación de CBS, de acuerdo con algunas realizaciones de la presente divulgación. En algunas realizaciones de la presente descripción, las aproximaciones de rango inferior se calculan a partir de los tensores 203 asociados con el CBS 118 utilizando el motor 114 de flujo de trabajo analítico para aplicar el flujo de trabajo analítico para calcular las aproximaciones de tensores de rango inferior 303 a los tensores 203. Estas aproximaciones de tensores de rango inferior 303 se utilizan a su vez para definir el nuevo CBS 304 transformado. De esta manera, los datos 119 se utilizan para crear el CBS 304 con propiedades estadísticas que pueden ser más útiles para ciertas aplicaciones, ya que se puede eliminar un “ruido” dimensional superior utilizando estas aproximaciones 303 de tensor de rango inferior. El motor 117 de consulta de comportamiento cibernético puede consultar el CBS 304, y el motor 106 de interacción puede admitir entornos interactivos basados en el CBS 304. Además, el intercambio 117 de comportamiento cibernético puede compartir información del CBS 304 con el CBS asociado con otras organizaciones.

En algunas realizaciones, el motor 114 de flujo de trabajo analítico calcula múltiples modelos analíticos utilizando métodos basados en tensor sobre cada entidad y/o actor y utiliza estos múltiples modelos analíticos para crear puntuaciones de riesgo para cada entidad y/o actor. En algunas realizaciones, estas puntuaciones de riesgo se actualizan a medida que se procesan nuevos datos que son relevantes para la entidad o el actor. Un actor puede referirse a un individuo o colección de individuos u organización o colección de organizaciones. Por ejemplo, los actores pueden incluir individuos o grupos de individuos, conocidos o desconocidos, que atacan o defienden un sistema. Las entidades pueden referirse a cualquier elemento que esté asociado con datos, incluidos dispositivos de red, estaciones de trabajo, servidores, dispositivos móviles y sensores. En general, las entidades también pueden incluir individuos, grupos y organizaciones que están asociadas con datos. Dependiendo del contexto, las entidades físicas asociadas con los datos pueden distinguirse de las personas y las organizaciones asociadas con los datos (actores).

Entornos de CBS interactivos

La Fig. 4 es un diagrama de sistema que muestra un motor 106 de interacción que gestiona un entorno 401 de CBS interactivo, de acuerdo con algunas realizaciones de la presente divulgación. El motor 106 de interacción crea CBS interactivo, permitiendo que dos o más actores 105 cibernéticos reales o virtuales actualicen de forma asíncrona uno o más de los CBS gestionados por el entorno 401 de CBS interactivo con acciones o interacciones específicas, o con secuencias de acciones o interacciones definidas por comportamientos cibernéticos. Múltiples actores cibernéticos reales o virtuales participan en interacciones cibernéticas en entornos virtuales utilizando el motor 106 de interacción para actualizar los entornos 401 de CBS interactivos, y de esta manera, crear entornos de realidad virtual.

El motor 106 de interacción usa almacenes de datos 101 cibernéticos históricos para proporcionar una base para la creación del entorno 401 de CBS interactivo. Los datos 102 del sensor proporcionan información sobre el entorno físico. Los datos 103 de enriquecimiento proporcionan un contexto adicional. El motor 106 de interacción crea un entorno que consiste en un conjunto de CBS que integra estas fuentes de información.

El entorno 401 de CBS interactivo proporciona un sistema distribuido para visualización, análisis, colaboración, planificación, entrenamiento, ejercicios y juegos de guerra. Numerosos actores 105 pueden competir o colaborar en el entorno 401 de CBS interactivo. Los actores 105 pueden organizarse en equipos u otros grupos. Los actores 105 pueden representar a sus propias u otras organizaciones. Los actores 105 pueden tener una amplia gama de objetivos que pueden competir con otros actores 105.

Las entidades 403 simuladas pueden representar una versión sintética de un actor 105, pero también pueden representar una amplia gama de otras entidades dentro del entorno 401 de CBS interactivo. Algunas entidades 403 simuladas pueden representar adversarios. Otras entidades 403 simuladas pueden complementar y apoyar a los actores 105 simulando actores 105 para proporcionar funciones adicionales. Las entidades 403 simuladas pueden usarse para aumentar la escala de las actividades dentro del entorno 401 de CBS interactivo. Las entidades 403 simuladas pueden representar equipos en el entorno 401 de CBS interactivo que funciona de manera autónoma o responde a los actores 105 u otras entidades 403 simuladas.

Los observadores-controladores 402 monitorean las interacciones entre los actores 105, las entidades 403 simuladas y el entorno 401 de CBS interactivo. Los observadores-controladores 402 pueden ayudar en el análisis de un conjunto de interacciones dentro del entorno 401 de CBS interactivo. Los observadores-controladores 402 puede intervenir en las interacciones entre los actores 105, entidades 403 simuladas dentro del entorno 401 de CBS interactivo para asegurar que se cumplan los objetivos del análisis, el ejercicio de capacitación o el escenario.

El motor 106 de interacción produce un conjunto de resultados 404. En algunas realizaciones, el motor 106 de interacción puede generar resultados provisionales, así como resultados finales. Los resultados pueden consistir en visualizaciones, gráficos e informes sobre las actividades del actor 105 y las entidades 403 simuladas, así como los resultados generales del análisis, el ejercicio de capacitación o el escenario.

En algunas realizaciones, el motor 106 de interacción permite que múltiples defensores, representados como actores 105 o entidades 403 simuladas de diferentes ubicaciones geográficas, participen en la simulación para comprender un conjunto de problemas común de manera sincronizada. Esta capacidad está respaldada por la capacidad de la CBS 401 para integrar mapas geográficos en la CBS 401. Del mismo modo, múltiples defensores de diferentes compañías y diferentes sectores pueden integrarse en un entorno de realidad virtual para comprender un conjunto de problemas comunes de manera sincronizada. Esta capacidad es compatible con la capacidad del CBS 401 para integrar mapas organizativos en el CBS 401.

La fig. 5 es un diagrama de sistema que muestra un motor 115 de simulación que gestiona un conjunto de CBS, de acuerdo con algunas realizaciones de la presente divulgación. El motor 115 de simulación crea un comportamiento cibernético simulado, utilizando uno o más de los métodos descritos anteriormente. En particular, en algunas realizaciones, los datos 101 cibernéticos, los datos 102 del sensor y los datos 103 del enriquecimiento se utilizan para crear un CBS 501 inicial y para proporcionar la información estadística requerida por el motor 115 de simulación. Esta capacidad de simulación permite al defensor de la red llevar la red a la vida, y simular diversos procesos, eventos y acciones para determinar los posibles resultados. El contexto de simulación permite a los defensores de red comprender el impacto de una serie de herramientas diferentes para determinar cuáles son las mejores opciones y acciones para defender activamente una red.

El paquete integrado de CBS 502 generado por el motor 115 de simulación se compara y contrasta entre sí para optimizar las acciones de defensa de la red. En particular, los modelos de comportamiento generados por el motor 114 de flujo de trabajo analítico pueden usarse para crear comportamientos cibernéticos específicos de interés para actores 503 particulares en escenarios y escenarios particulares, y para actualizar la simulación. El motor 115 de simulación también se puede utilizar para probar dinámicamente las configuraciones de red para encontrar puntos débiles.

El motor 115 de simulación también se puede utilizar para probar y certificar defensores de la red, y para capacitar a varias compañías dentro de un sector utilizando programas de simulación y el monitoreo y los informes 504.

Finalmente, el motor 115 de simulación se puede usar para explorar dinámicamente en tiempo más rápido que en tiempo real la importancia relativa de los eventos en curso para priorizar acciones para los defensores de la red. En particular, se pueden usar simulaciones a pequeña escala o “micro” para apoyar acciones de defensa de red simples para varios niveles de defensores entrenados.

En algunas realizaciones, el sistema usa un conjunto de claves de cifrado para verificar que los participantes en la simulación están autorizados para participar en la simulación. De esta manera, hay una forma verificable y segura de

reunir equipos, incluso equipos distribuidos dentro de un sector industrial o de múltiples sectores industriales, utilizando el intercambio 117 de comportamiento cibernético , por ejemplo, como se muestra en la FIG. 1.

Las actualizaciones 505 proporcionan un mecanismo para los cambios en los datos cibernéticos, los datos del sensor y los datos de enriquecimiento que se producen durante el período de tiempo de la simulación, pero no afectan a la simulación que se incorporará a la CBS. Por ejemplo, los cambios en los datos del terreno podrían no cambiar la simulación, pero deberían aparecer en la CBS. Los cambios en los datos cibernéticos, los datos de sensores y los datos de enriquecimiento que cambian la simulación se incorporan como parte de la operación del sistema de simulación.

La guía 506 interactiva proporciona un mecanismo para alterar la CBS fuera del curso normal de la operación de simulación. Este mecanismo se puede usar para que los usuarios/administradores guíen el curso de la simulación para eliminar áreas no interesantes o no productivas.

Las restricciones 507 basadas en la condición proporcionan un mecanismo para minimizar los resultados inexactos al evitar que la simulación exceda los límites. Las simulaciones generalmente tienen condiciones más allá de las cuales se vuelven inexactas o inválidas. Por ejemplo, las simulaciones de vuelo pueden ser inválidas por encima de ciertas velocidades aéreas, altitudes o para actitudes inusuales.

Intercambios de comportamiento cibernético

La información de dos o más sistemas se puede compartir a través de intercambios de comportamiento cibernéticos. La Fig. 6 es un diagrama de sistema que muestra el funcionamiento de múltiples intercambios de comportamiento cibernético (CBX) para compartir información de manera segura dentro o entre las empresas 620 630 de una manera controlada, de acuerdo con algunas realizaciones de la presente divulgación.

En algunas realizaciones, se identifican CBS que contienen información 601 compartida. Algunos CBS 602 dentro de una empresa no se pueden compartir, debido a las políticas de intercambio de información de las organizaciones participantes.

Un CBS 603 modificado, creado, por ejemplo, por proyección, enmascaramiento de datos, transformación de datos, utilizando un número fijo de componentes principales, reducción a una aproximación de rango inferior, utilizando aprendizaje de máquina preservando la privacidad, o cifrado homomórfico, o se puede crear un método similar que contenga un subconjunto, un conjunto transformado o un conjunto de información cifrada para compartir en el formato correcto para la máquina o el consumo humano. En algunas realizaciones, el componente del sistema proyecta, enmascara, o de otra manera transforma 612 los datos para crear un CBS 603 modificado.

En algunas realizaciones, si queda alguna información comercial privada o sensible, entonces las transformaciones que preservan la privacidad, como agregar ruido a los datos, o cifrar los datos utilizando cifrado homomórfico se utilizan en 604 para transformar los datos en un CBS 605 que se puede intercambiar.

Se aplican todas las restricciones adicionales al intercambio 606 de información que son requeridas por la seguridad de la información y otras políticas de las organizaciones participantes.

En algunas realizaciones, el CBS 605 compartible resultante se envía al CBX 607 para su transmisión segura a otras empresas 630 habilitadas para el CBX, que incluye, posiblemente, a terceros de confianza. En algunas realizaciones, si cada una de las empresas que le envían datos confía en la empresa 630 habilitada para CBX, no es necesario que la información se comparta con otras organizaciones directamente, sino solo de manera indirecta cuando el tercero de confianza devuelve los resultados después de transformaciones que preservan la privacidad y se aplican agregaciones a los datos enviados.

En algunas realizaciones, el CBS 605 que puede intercambiar se cifra para crear un CBS 608 seguro que se transmite de manera segura a otras empresas habilitadas para CBX para consumo humano o de máquina.

El CBS 605 que puede intercambiar o el CBS 608 cifrado son recibidos por una o más empresas 630 habilitadas para CBX a través de un CBX 609 asociado con esa empresa.

Las empresas que cooperan actualizan la CBS relevante para crear la CBS 610 actualizada. La determinación de qué CBS es relevante para las actualizaciones se puede hacer de múltiples maneras, que incluyen, entre otras: el uso de claves únicas para entidades, actores, comportamientos, datos para determinar cuál debe actualizarse; el uso de etiquetas, atributos, características y comportamientos para determinar cuáles deben actualizarse; o, utilizando reglas o métodos de aprendizaje de máquina para seleccionar qué CBS se debe actualizar.

En algunas realizaciones, algunos CBS 611 no se actualizan, según las políticas, reglas o regulaciones de seguridad e intercambio de información de las empresas pertinentes.

En algunas realizaciones, el CBS se intercambió de acuerdo con el proceso descrito en la FIG. 6 puede ser tan simple como un registro de datos con formato único o una colección de registros de datos con formato o tan complejo como una colección de datos cibernéticos, actores cibernéticos y escenas cibernéticas que representan un oficio en particular para obtener acceso a un entorno protegido, privilegios crecientes, moviéndose lateralmente, y atacando al sistema.

Entrenamiento virtual y defensa

En algunas realizaciones, se utilizan simulaciones y un sistema de realidad virtual para mejorar las capacidades operativas o la capacitación de los defensores cibernéticos al compartir información relacionada con el comportamiento entre sí, tanto la información relacionada con el comportamiento observado como la información relacionada con el comportamiento que se genera cuando participan múltiples actores cibernéticos virtuales o reales. En escenarios, simulaciones y entornos de realidad virtual. El hecho de compartir de este modo los comportamientos cibernéticos observados o simulados entre todos los elementos operativos, dentro o entre empresas geográficamente dispersas, permite un “ejército” inmediato de ciberdelitos frente a un solo elemento de defensores. Este “ejército” de actores cibernéticos o avatares virtuales, tanto reales como simulados, permite a los defensores cibernéticos participar y colaborar en escenarios, simulaciones y entornos de realidad virtual. Esta colaboración en tiempo real se habilita mediante la simulación de múltiples cursos de acción (COA), estrategias defensivas, impactos de acciones e incorporando esta información en un entorno virtual compartido para visualizaciones mejoradas que respaldan un entendimiento operativo rápido y más comprensivo y un proceso de decisión.

En algunas realizaciones, el intercambio de información relacionada con el comportamiento puede ser de actores reales y virtuales o avatares de dos o más organizaciones. En algunas realizaciones, las simulaciones y los entornos de realidad virtual también pueden ser de dos o más organizaciones. De esta manera, los defensores cibernéticos de dos o más organizaciones pueden participar y colaborar en escenarios, simulaciones y entornos de realidad virtual.

En algunas realizaciones, el motor 115 de simulación se usa para generar múltiples CBS 111 simulados que se utilizan en el entorno 401 de CBS interactivo para proporcionar cursos de acción (COA) para los defensores de red (en el caso de que algunos de los actores 105 sean defensores de la red). Los datos para crear los entornos de CBS interactivos pueden incluir, entre otros, datos 101 cibernéticos, datos 102 de sensores y varios tipos de datos 103 de enriquecimiento. Los actores 105 y los observadores/controladores 402 pueden usar el motor 401 de interacción para crear escenarios de capacitación, desarrolle COA, repita escenarios y tome diferentes acciones para tratar de mejorar los resultados. Estos escenarios en el entorno interactivo pueden incluir entidades 403 simuladas.

En algunas realizaciones de la presente divulgación, el motor 115 de simulación se usa para generar múltiples CBS simulados que involucran a actores virtuales cibernéticos simulados que se involucran en comportamientos, tales como, entre otros, el reconocimiento inicial, el escaneo, el compromiso inicial, el establecimiento de un punto de apoyo. baliza, comando y control, captura de credenciales, escalado de privilegios, reconocimiento interno, movimiento lateral, mapeo de red, exfiltración de datos, mantenimiento de la persistencia y comportamientos relacionados; y el motor 106 de interacción se utiliza para que los actores defensores de red puedan tomar acciones en el entorno de CBS interactivo, lo que incluye, entre otros, impedir que un dispositivo se comunique, bloquear puertos para detener una exfiltración, eliminar usuarios o eliminar privilegios de usuarios y liquidar procesos. Para virtual, real, o combinaciones de los dos, el CBS se puede utilizar para promulgar escenarios hipotéticos dentro de un entorno virtual o para aumentar un entorno real. De manera similar, los defensores de red pueden practicar la defensa de la red contra actores cibernéticos virtuales o reales en un entorno CBS interactivo.

En algunas realizaciones, el motor 115 de simulación se usa para generar múltiples CBS simulados que involucran a actores cibernéticos virtuales simulados que se involucran en comportamientos, tales como, entre otros, reconocimiento inicial, escaneo, compromiso inicial, establecimiento de un punto de apoyo, baliza, comando y control, captura de credenciales, escalado de privilegios, reconocimiento interno, movimiento lateral, mapeo de redes, exfiltración de datos, mantenimiento de la persistencia y comportamientos relacionados; y el motor 106 de interacción se utiliza para que los actores defensores de red puedan realizar acciones en el entorno de CBS interactivo, que incluyen, entre otros, bloquear o redirigir la comunicación de un dispositivo, bloquear puertos para detener una exfiltración, eliminar o redirigir usuarios o quitando privilegios de usuarios, y liquidando procesos. De este modo, los defensores de red pueden practicar técnicas de mitigación cibernética en un entorno virtual. Cuando existe una actividad cibernética real de naturaleza maliciosa en la CBS, los defensores de red pueden comprender rápidamente los efectos potenciales de sus acciones de mitigación, antes de que estas acciones se realicen realmente. Los defensores de red pueden practicar la defensa en red contra los actores cibernéticos virtuales en un entorno de CBS interactivo mientras se está llevando a cabo un ataque cibernético real para reducir el riesgo y aumentar la probabilidad de que la defensa y otras acciones realizadas puedan lograr el resultado deseado. En algunas realizaciones, estas simulaciones se pueden ejecutar más rápido que en tiempo real, lo que permite a los defensores de red trabajar más rápidamente en escenarios y acciones que conducen a mejores resultados de forma más rápida y eficiente. Para virtual, real, o combinaciones de los dos, El CBS se puede utilizar para promulgar escenarios hipotéticos dentro de un entorno virtual o para aumentar un entorno real. De manera similar, los defensores de red pueden practicar la defensa de la red contra actores cibernéticos virtuales o reales en un entorno de CBS interactivo.

En algunas realizaciones, los actores pueden acercar o alejar la imagen utilizando la estructura multiescala y los mapas que forman parte de la CBS; centran su visión en ciertas clases de entidades, sistemas, flujos o procesos; o, anote el entorno interactivo de CBS con notas, imágenes y paneles de control. De esta manera, los actores pueden obtener una mejor comprensión del entorno.

En algunas realizaciones, los actores cibernéticos reales pueden comunicarse entre sí dentro del entorno de CBS interactivo para coordinar mejor sus acciones de defensa.

En algunas realizaciones, el motor 115 de simulación se usa para generar múltiples CBS simulados que involucran a actores cibernéticos virtuales simulados que se involucran en comportamientos, tales como, pero no limitados a, reconocimiento inicial, escaneo, compromiso inicial, establecer un punto de apoyo, baliza, comando y control, captura de credenciales, escalado de privilegios, reconocimiento interno, movimiento lateral, mapeo de redes, exfiltración de datos, mantenimiento de la persistencia y comportamientos relacionados. utilizando estas múltiples simulaciones de CBS, los cálculos de riesgo de las entidades en un CBS se pueden calcular de varias maneras diferentes, que incluyen, entre otros, el uso de métodos de Monte Carlo o métodos Bayesianos. De esta manera, se puede asignar un puntaje de riesgo a todas las entidades en una CBS. De manera similar, estos métodos también pueden usarse para calcular una puntuación de diversidad.

En algunas realizaciones, el motor 114 de flujo de trabajo analítico se usa para calcular aproximaciones de tensor de dimensiones inferiores de los datos en CBS. El motor 115 de simulación se usa luego con estas aproximaciones de tensor de dimensión inferior para generar múltiples CBS simulados que involucran a actores cibernéticos virtuales simulados que se involucran en comportamientos, tales como, entre otros, reconocimiento inicial, escaneo, compromiso inicial, establecimiento de un punto de apoyo, baliza, comando y control, captura de credenciales, escalado de privilegios, reconocimiento interno, movimiento lateral, mapeo de redes, exfiltración de datos, mantenimiento de la persistencia y comportamientos relacionados. utilizando estas múltiples simulaciones de CBS, los cálculos de riesgo de las entidades en un CBS se pueden calcular de varias maneras diferentes, incluyendo, pero no limitándose a, el uso de métodos de Monte Carlo o métodos Bayesianos. De esta manera, Se puede asignar un puntaje de riesgo a todas las entidades en un CBS. De manera similar, estos métodos también pueden usarse para calcular una puntuación de diversidad.

El puntaje de diversidad es una cuantificación del grado y la cantidad de variedad dentro de una organización o entre organizaciones. La variedad se puede aumentar al tener diferentes proveedores de equipos, como enrutadores, cortafuegos y ordenadores. La variedad también se puede aumentar a través de diferentes configuraciones de red y topologías. La diversidad es importante para evaluar la vulnerabilidad de una organización o de varias organizaciones a los ataques. Por ejemplo, si una organización tiene una puntuación de diversidad baja, un tipo de ataque podría interrumpir una gran parte de la organización. En contraste, una organización con un alto puntaje de diversidad solo tendría una pequeña cantidad de la organización interrumpida por el mismo ataque. De manera similar, en múltiples organizaciones, los altos puntajes de diversidad significarían que no todas las organizaciones se verían afectadas en el mismo grado por el mismo tipo de ataque.

Las puntuaciones de diversidad pueden almacenarse como tensores. Los tensores pueden capturar de manera única una multiplicidad de aspectos que contribuyen al puntaje de diversidad. El puntaje de diversidad se puede calcular aplicando operadores a tensores o colecciones de tensores previamente calculados. El motor 115 de simulación se puede utilizar para derivar y explorar múltiples configuraciones dentro o entre organizaciones. Los resultados de las simulaciones se pueden almacenar en tensores o colecciones de tensores que luego se utilizan para calcular una puntuación de diversidad.

Las puntuaciones de riesgo, similares a las puntuaciones de diversidad, son una cuantificación del grado y la cantidad de riesgo de un ataque dentro de una organización o entre organizaciones. Como se discutió anteriormente, el puntaje de diversidad es un contribuyente significativo al puntaje de riesgo. Las puntuaciones de riesgo también se pueden almacenar como tensores. El puntaje de riesgo se puede calcular aplicando operadores a tensores o colecciones de tensores previamente calculados. Las simulaciones también se pueden usar para derivar y explorar riesgos dentro o entre organizaciones. Los resultados de las simulaciones se pueden almacenar en tensores o colecciones de tensores que luego se utilizan para calcular una puntuación de riesgo.

En algunas realizaciones, las puntuaciones de diversidad y las puntuaciones de riesgo se actualizan a medida que se actualizan los datos cibernéticos, los datos del sensor, los datos de enriquecimiento y/o los datos de terceros al administrador 102 de CBS, que crea una nueva CBS simulada actualizada, que a su vez se utiliza para calcular los puntajes de riesgo actualizados para todas las entidades en la CBS.

La diversidad resultante y los tensores de riesgo también pueden compartirse de manera segura en múltiples ubicaciones geográficamente dispersas utilizando CBX 117 para compartir información y actualizar los entornos 401 de CBS compartidos.

En algunas realizaciones, primero se crea una colección de CBS, cada una con un nivel diferente de diversidad de las entidades en la CBS y sus características, que incluyen, entre otros, sus sistemas operativos, sus configuraciones,

sus bibliotecas de software. y utilidades de software, sus aplicaciones de software y sus interfaces. Para cada CBS de este tipo, el motor 115 de simulación se utiliza para generar múltiples CBS simulados que involucran a actores cibernéticos virtuales simulados que se involucran en comportamientos, tales como, entre otros, el reconocimiento inicial, el escaneo, el compromiso inicial, el establecimiento de un punto de apoyo, baliza, comando y control., captura de credenciales, escalado de privilegios, reconocimiento interno, movimiento lateral, mapeo de redes, exfiltración de datos, mantenimiento de la persistencia y comportamientos relacionados. utilizando estas simulaciones múltiples de CBS, los cálculos de riesgo de las entidades para un nivel dado de diversidad se calculan utilizando, por ejemplo, métodos de Monte Carlo o métodos bayesianos. De esta manera, los defensores de red pueden entender la relación entre la diversidad y los puntajes de riesgo de las entidades en una CBS y se pueden utilizar para reducir los puntajes de riesgo de las entidades en una CBS.

En algunas realizaciones, el motor 114 de flujo de trabajo analítico se usa para calcular aproximaciones de tensor de rango inferior de los datos en CBS. A continuación, se crea una colección de CBS en estas aproximaciones de tensor de rango inferior, cada una con un nivel diferente de diversidad de las entidades en la CBS y sus características, incluidos, entre otros, sus sistemas operativos, sus configuraciones, sus bibliotecas de software. y utilidades de software, sus aplicaciones de software y sus interfaces. Para cada CBS de este tipo, el motor de simulación se usa para generar múltiples CBS simulados que involucran a actores cibernéticos virtuales simulados que se involucran en comportamientos, tales como, entre otros, el reconocimiento inicial, el escaneo, el compromiso inicial, el establecimiento de un punto de apoyo, baliza, comando y control, captura de credenciales, escalado de privilegios, reconocimiento interno, Movimiento lateral, mapeo de redes, exfiltración de datos, mantenimiento de la persistencia y comportamientos relacionados. Utilizando estas múltiples simulaciones de CBS, los cálculos de riesgo de entidades para un nivel dado de diversidad se calculan utilizando, por ejemplo, métodos de Monte Carlo o métodos Bayesianos. De esta manera, los defensores de red pueden entender la relación entre la diversidad y los puntajes de riesgo de las entidades en una CBS y se pueden utilizar para reducir los puntajes de riesgo de las entidades en una CBS.

Entornos OT

En algunas realizaciones, el sensor y los datos cibernéticos pueden provenir de datos en un entorno de tecnología operacional (OT). Un entorno OT se refiere a sensores y software de hardware diseñados para monitorear y controlar máquinas físicas y procesos físicos, como en, pero no limitado a, un entorno industrial.

La figura 7 es un diagrama de sistema que muestra un sistema de seguridad cibernética que interactúa con un entorno de tecnología operacional, de acuerdo con algunas realizaciones de la presente divulgación.

Las máquinas 701 físicas son monitoreadas por los sensores 702 OT y los datos pasan a una red 703 OT. Los sensores 702 OT también monitorean a los actores 704 físicos que interactúan y ajustan las máquinas 701 físicas. Los sensores 702 OT recopilan datos sobre el estado, operaciones, interacciones, condiciones internas, condiciones externas, estado interno, rendimiento y datos relacionados sobre máquinas y dispositivos. Los sensores 702 de OT también recopilan datos sobre entornos físicos, incluidas las condiciones y los cambios ambientales, la presencia de seres humanos y datos relacionados. Los sensores OT están conectados a máquinas y dispositivos con cables, conectados a máquinas y dispositivos a través de la red OT, conectados a las máquinas y dispositivos a través de la red de TI o distribuidos a través del entorno físico. Los datos de OT se encapsulan en paquetes de red estándar en una interfaz 705 de red OT/IT, donde están disponibles para ser procesados por un entorno 707 de TI asociado con el entorno 705 de OT. Los diversos componentes de TI en el entorno 707 de TI, incluida la interfaz 705 de red OT/IT puede ser monitoreada o puede producir archivos de registro que crean datos 707 cibernéticos, que a su vez están disponibles para el sistema de seguridad de seguridad cibernética como un ejemplo de los datos 101 cibernéticos en algunas realizaciones. En algunas realizaciones, los datos 706 del sensor, encapsulados en paquetes de red o archivos de registro, están disponibles como una de las entradas 103 al sistema de seguridad cibernética. Los datos 103 del sensor y los datos 101 cibernéticos son procesados por el administrador 113 CBS como se describió anteriormente.

La materia descrita en el presente documento puede implementarse en circuitos electrónicos digitales, o en software de ordenador, firmware o hardware, incluidos los medios estructurales descritos en esta especificación y sus equivalentes estructurales, o en combinaciones de ellos. El objeto descrito en este documento puede implementarse como uno o más productos de programas informáticos, como uno o más programas informáticos incorporados tangiblemente en un soporte de información (por ejemplo, en un dispositivo de almacenamiento legible por máquina), o incorporados en una señal propagada, para su ejecución por, o para controlar el funcionamiento de un aparato de procesamiento de datos (por ejemplo, un procesador programable, un ordenador o varios ordenadores). Un programa de ordenador (también conocido como un programa, software, aplicación de software o código) puede escribirse en cualquier forma de lenguaje de programación, incluidos los lenguajes compilados o interpretados, y se puede implementar en cualquier forma, incluso como un programa independiente o como un módulo, componente, subrutina u otra unidad adecuada para su uso en un entorno informático. Un programa de ordenador no necesariamente corresponde a un archivo. Un programa puede almacenarse en una parte de un archivo que contiene otros programas o datos, en un solo archivo dedicado al programa en cuestión o en múltiples archivos coordinados (por ejemplo, archivos que almacenan uno o más módulos, subprogramas o partes de código). Un programa informático puede implementarse para ejecutarse en un ordenador o en varios ordenadores en un sitio o distribuirse en múltiples sitios e interconectarse mediante una red de comunicación.

Los procesos y flujos lógicos descritos en esta especificación, incluidos los pasos del método del tema descrito en este documento, pueden ser realizados por uno o más procesadores programables que ejecutan uno o más programas de ordenador para realizar las funciones del tema descrito en este documento al operar en los datos de entrada y generando salida. Los procesos y flujos lógicos también pueden ser realizados por, y el aparato del objeto descrito aquí puede implementarse como un circuito lógico de propósito especial, por ejemplo, un FPGA (matriz de puerta programable de campo) o un ASIC (circuito integrado de aplicación específica).

Los procesadores adecuados para la ejecución de un programa informático incluyen, a modo de ejemplo, microprocesadores de propósito general y especial, y uno o más procesadores de cualquier tipo de ordenador digital. En general, un procesador recibirá instrucciones y datos desde una memoria de solo lectura o una memoria de acceso aleatorio o ambos. Los elementos esenciales de un ordenador son un procesador para ejecutar instrucciones y uno o más dispositivos de memoria para almacenar instrucciones y datos. En general, un ordenador también incluirá, o estará acoplada operativamente, para recibir datos de o transferir datos a, o ambos, uno o más dispositivos de almacenamiento masivo para almacenar datos, por ejemplo, discos magnéticos, magnetos ópticos, u ópticos. Los portadores de información adecuados para incorporar las instrucciones y datos del programa de ordenador incluyen todas las formas de memoria no volátil, incluyendo a modo de ejemplo dispositivos de memoria de semiconductores (por ejemplo, EPROM, EEPROM y dispositivos de memoria flash); discos magnéticos (por ejemplo, discos duros internos o discos extraíbles); discos magneto ópticos; y discos ópticos (por ejemplo, discos de CD y DVD). El procesador y la memoria pueden complementarse o incorporarse en circuitos lógicos de propósito especial.

Para proporcionar interacción con un usuario, el objeto descrito aquí se puede implementar en un ordenador, dispositivo portátil, pantalla frontal, gafas, dispositivos retinales que tienen un dispositivo o mecanismo de visualización, por ejemplo, un CRT (tubo de rayos catódicos), dispositivo de proyección láser, pantalla LCD (pantalla de cristal líquido), LED (diodo emisor de luz) u OLED (diodo orgánico emisor de luz), para mostrar información al usuario y un teclado y un dispositivo señalador (por ejemplo, un mouse o un trackBall), mediante el cual el usuario puede proporcionar información a la computadora o dispositivo. También se pueden utilizar otros tipos de dispositivos para proporcionar interacción con un usuario. Por ejemplo, la retroalimentación proporcionada al usuario puede ser cualquier forma de retroalimentación sensorial (por ejemplo, retroalimentación visual, retroalimentación auditiva o retroalimentación táctil), y la entrada del usuario puede recibirse en cualquier forma, incluida la entrada acústica, de voz o táctil.

La materia descrita en este documento puede implementarse en un sistema de computación que incluye un componente de servicio (por ejemplo, un servidor de datos), un componente de middleware (por ejemplo, un servidor de aplicaciones), o un componente de módulo de interfaz (por ejemplo, un dispositivo móvil de ordenador de cliente, dispositivo portátil, con una interfaz gráfica de usuario o un navegador web a través del cual un usuario puede interactuar con una implementación del tema descrito en este documento), o cualquier combinación de dichos componentes de servicio, middleware y módulo de interfaz. Los componentes del sistema pueden estar interconectados por cualquier forma o medio de comunicación de datos digitales, por ejemplo, una red de comunicación. Los ejemplos de redes de comunicación incluyen una red de área local (“LAN”) y una red de área amplia (“WAN”), por ejemplo, Internet.

Debe entenderse que el objeto divulgado no está limitado en su aplicación a los detalles de construcción y a las disposiciones de los componentes expuestos en la siguiente descripción o ilustrados en los dibujos. El objeto divulgado es capaz de otras realizaciones y de ser practicado y llevado a cabo de varias maneras. Además, debe entenderse que la fraseología y la terminología empleadas en este documento son para fines de descripción y no deben considerarse limitativas.

Como tales, los expertos en la técnica apreciarán que la concepción, sobre la que se basa esta divulgación, puede utilizarse fácilmente como base para el diseño de otras estructuras, métodos y sistemas para llevar a cabo los diversos propósitos de la materia divulgada. Es importante, por lo tanto, que se considere que las reivindicaciones incluyen tales construcciones equivalentes en la medida en que no se aparten del espíritu y alcance de la materia divulgada.

Aunque el tema divulgado se ha descrito e ilustrado en las realizaciones ejemplares anteriores, se entiende que la presente divulgación se ha realizado solo a modo de ejemplo, y que pueden realizarse numerosos cambios en los detalles de la implementación del tema divulgado. debe realizarse sin apartarse del espíritu y alcance de la materia divulgada, que está limitada únicamente por las siguientes reivindicaciones.

REIVINDICACIONES

1. Un sistema de seguridad cibernética para administrar el comportamiento cibernético asociado con los actores cibernéticos de manera que el comportamiento cibernético se puede calcular y predecir y se pueden crear interacciones cibernéticas entre los actores cibernéticos, el sistema comprende:

un módulo de gestión del espacio cibernético de comportamiento;

un motor de interacción;

un motor de flujo de trabajo analítico; y

un motor de visualización,

el módulo de gestión del espacio de comportamiento cibernético, en comunicación con el motor de interacción, el motor de flujo de trabajo analítico y el motor de visualización, y configurado para:

recibir al menos uno de:

datos de entrada, los datos de entrada que incluyen al menos uno de los datos cibernéticos de entrada, datos de sensores, datos de enriquecimiento y datos de terceros,

datos del motor de interacción y

datos del motor de flujo de trabajo analítico;

generar una pluralidad de espacios de comportamiento cibernético basados en al menos uno de los datos de entrada, los datos del motor de interacción y los datos del motor de flujo de trabajo analítico, cada uno de la pluralidad de espacios de comportamiento cibernético que comprende datos del espacio de comportamiento cibernético, los datos del espacio de comportamiento del ciberespacio que incluyen:

datos cibernéticos, los datos cibernéticos que incluyen al menos uno de los datos cibernéticos de entrada y datos cibernéticos de entrada transformados, datos de

actores cibernéticos asociados con una pluralidad de actores y

cibernéticos y datos de escenas cibernéticas asociados con una pluralidad de escenas cibernéticas,

los datos del espacio de comportamiento cibernético están definidos por una pluralidad de dimensiones, una pluralidad de modos y una pluralidad de escalas;

el motor de interacción configurado para:

recibir datos del primer actor cibernético asociado con un primer actor cibernético de la pluralidad de actores cibernéticos, el primer actor cibernético incluye al menos uno de un actor cibernético real y un actor simulado,

procesa los datos recibidos del primer actor cibernético para facilitar al menos una de:

una primera interacción entre el primer actor cibernético con al menos una de:

el espacio cibernético del comportamiento,

la escena cibernética y

un mapa cibernético, el mapa cibernético asociado con al menos uno de la pluralidad de espacios cibernéticos del comportamiento, y

una segunda interacción entre el primer actor cibernético con un segundo actor cibernético de la pluralidad de actores cibernéticos, y

transmitir datos asociados con al menos una de la primera interacción y la segunda interacción;

el motor de flujo de trabajo analítico configurado para:

analizar los datos del espacio de comportamiento cibernético asociados con cada uno de la pluralidad de espacios de comportamiento cibernético para calcular los comportamientos cibernéticos, y

actualizar al menos uno de los datos cibernéticos, los datos del actor cibernético y los datos de la escena cibernética basados en al menos uno de:

los datos del espacio de comportamiento cibernético,

los comportamientos cibernéticos calculados y una asignación de los comportamientos cibernéticos calculados a al menos uno de los datos cibernéticos, los datos del actor cibernético y los datos de la escena cibernética,

la primera interacción, y

la segunda interacción, y

transmitir datos asociados con la actualización de al menos uno de los datos cibernéticos, los datos del actor cibernético y los datos de la escena cibernética;

el motor de visualización configurado para:

calcular visualizaciones de al menos uno de:

los datos asociados con al menos una de la primera interacción y la segunda interacción del motor de interacción, y

al menos uno de los espacios de comportamiento cibernético, la pluralidad de actores cibernéticos, la pluralidad de escenas cibernéticas, la pluralidad de mapas cibernéticos y los comportamientos cibernéticos calculados, y

transmitir las visualizaciones para su visualización.

2. El sistema de seguridad cibernética de la reivindicación 1, que comprende, además:

un motor de consulta, en comunicación con el módulo de gestión de espacio de comportamiento cibernético, el motor de consulta configurado para recibir, desde el primer actor cibernético, una consulta sobre al menos uno de la pluralidad de espacios de comportamiento cibernético, la consulta asociada con al menos uno de:

riesgo asociado con una primera entidad cibernética de una pluralidad de entidades cibernéticas;

un grupo de entidades cibernéticas de la pluralidad de entidades cibernéticas con un perfil similar a la primera entidad cibernética;

construcciones organizativas internas o externas; y

comportamiento asociado al menos a una de las primeras entidades cibernéticas, cada entidad cibernética en el grupo de entidades cibernéticas, el primer actor cibernético, el segundo actor cibernético y un tercer actor cibernético; y

en el que el motor de flujo de trabajo analítico está además configurado para computar y actualizar continuamente los riesgos asociados con cada entidad cibernética de la pluralidad de entidades cibernéticas y cada actor cibernético de la pluralidad de actores cibernéticos.

3. El sistema de seguridad cibernética de la reivindicación 1, que comprende además un motor de simulación, en comunicación con el módulo de gestión del espacio de comportamiento cibernético, configurado para generar la pluralidad de escenas cibernéticas, cada una de la pluralidad de escenas cibernéticas incluye un subconjunto de los datos cibernéticos y Mapas cibernéticos asociados a la pluralidad de espacios de comportamiento cibernéticos.

4. El sistema de seguridad cibernética de la reivindicación 3, en el que el motor de simulación está además configurado para generar simulaciones, las simulaciones configuradas para:

operar con al menos uno de datos del mundo real y datos simulados; y

proporcionar un curso de acción para al menos una de operaciones, análisis, información, planificación, capacitación, una acción de remediación y una acción de mitigación.

5. El sistema de seguridad cibernética de la reivindicación 1, en el que el motor de flujo de trabajo analítico está configurado además para:

crear un espacio de comportamiento cibernético transformado, en el que, para crear el espacio de comportamiento cibernético transformado, el motor de flujo de trabajo analítico está configurado además para:

transformar los datos del espacio de comportamiento cibernético en datos de tensor y aproximaciones de tensor de rango inferior; y

utilizar el aprendizaje de máquina para definir comportamientos cibernéticos y la pluralidad de espacios de comportamiento cibernéticos asociados con el espacio de comportamiento cibernético transformado.

6. El sistema de seguridad cibernética de la reivindicación 5, en el que el motor de flujo de trabajo analítico está además configurado para:

aplicar al menos una de las reglas y el aprendizaje de máquina al espacio de comportamiento cibernético transformado para definir los comportamientos cibernéticos que aumentan o disminuyen el riesgo asociado con al menos uno de:

un actor cibernético real o un actor simulado;

una entidad cibernética;

una máquina;

una organización; y

un proceso.

7. El sistema de seguridad cibernética de la reivindicación 6, en el que el sistema de seguridad cibernética está asociado con una primera organización, además en el que los comportamientos cibernéticos que aumentan o disminuyen el riesgo son observables por los actores cibernéticos asociados con la primera organización y no pueden ser observados por los actores cibernéticos asociados con una segunda organización, el sistema de seguridad cibernética comprende, además:

un motor de intercambio de comportamiento cibernético, el motor de intercambio de comportamiento cibernético en comunicación con el módulo de gestión del espacio de comportamiento cibernético, el motor de intercambio de comportamiento cibernético configurado para:

transmitir los comportamientos cibernéticos que aumentan o disminuyen el riesgo para un motor de intercambio de comportamiento cibernético asociado con la segunda organización que usa al menos uno de un algoritmo de aprendizaje de máquina distribuido de preservación de la privacidad y un protocolo de comunicaciones de preservación de la privacidad de modo que los comportamientos cibernéticos que aumentan o disminuyan el riesgo puedan usarse para analizar datos en la segunda organización, y los datos del espacio de comportamiento cibernético asociados con la primera organización son Inobservable por los actores cibernéticos asociados con la segunda organización.

8. El sistema de seguridad cibernética de la reivindicación 5, en el que los datos del primer actor cibernético se procesan aún más para:

determinar al menos uno de:

un primer comportamiento cibernético de los comportamientos cibernéticos asociados con el espacio de comportamiento cibernético transformado, y

una primera escena cibernética de la pluralidad de escenas cibernéticas asociadas con el espacio de comportamiento cibernético transformado; y

mejorar las capacidades operativas, la preparación y la capacitación asociadas con la respuesta al primer comportamiento cibernético y la primera escena cibernética.

9. El sistema de seguridad cibernética de la reivindicación 1, en el que el motor de flujo de trabajo analítico está además configurado para procesar al menos uno de datos de paquetes, tráfico de red, registros de ordenador, inteligencia de señales, visible, infrarrojo, multiespectral, hiperespectral, radar de apertura sintética, movimiento indicador de objetivo de radar, datos de inteligencia técnica e informes de inteligencia.

10. El sistema de seguridad cibernética de la reivindicación 1, en el que cada uno de la pluralidad de espacios de comportamiento cibernético incluye al menos uno de un espacio de comportamiento cibernético en tiempo real, un espacio de comportamiento cibernético histórico y un espacio de comportamiento cibernético simulado.

11. El sistema de seguridad cibernética de la reivindicación 1, en el que el comportamiento cibernético incluye al menos uno de reconocimiento inicial, escaneo, compromiso inicial, establecimiento de punto de apoyo, baliza, comando y control, captura de credenciales, privilegios crecientes, reconocimiento interno, movimiento lateral, mapeo de red, exfiltración de datos, mantenimiento de la persistencia y comportamientos relacionados.

12. El sistema de seguridad cibernética de la reivindicación 1, en el que:

la pluralidad de dimensiones incluye una combinación de direcciones de origen y destino, hora de llegada, volumen, tamaño de paquete y un tipo de protocolo;

la pluralidad de modos incluye una combinación de datos de paquete, tráfico de red, registros de ordenador, inteligencia de señales, visible, infrarrojo, multiespectral, hiperespectral, radar de apertura sintética, radar indicador de objetivo móvil, datos de inteligencia técnica e informes de inteligencia; y

la pluralidad de escalas incluye una combinación de datos temporales de múltiples escalas y datos geoespaciales.

13. El sistema de seguridad cibernética de cualquiera de las reivindicaciones 1-12, en el que el módulo de gestión del espacio de comportamiento cibernético está configurado además para:

recibir datos del sensor, los datos del sensor incluyen al menos uno de los datos del sensor del actor físico sobre un actor físico y los datos del sensor del sistema físico sobre un sistema físico, los datos del sensor incluyen al menos uno de:

datos de entrada, los datos de entrada incluyen al menos uno de los datos cibernéticos de entrada, datos de enriquecimiento y datos de terceros,

datos del motor de interacción y

datos del motor de flujo de trabajo analítico; y

generar la pluralidad de espacios de comportamiento cibernético basados en los datos del sensor y al menos uno de los datos de entrada, los datos del motor de interacción y

los datos del motor de flujo de trabajo analítico que el motor de flujo de trabajo analítico configuró para:

actualizar al menos uno de los datos cibernéticos, los datos del actor cibernético y los datos de la escena cibernética basándose en al menos uno de los siguientes:

los datos del espacio de comportamiento cibernético,

los comportamientos cibernéticos calculados y una asignación de los comportamientos cibernéticos calculados a al menos uno de los datos cibernéticos, los datos del actor cibernético y

los datos de la escena cibernética,

la primera interacción,

la segunda interacción y

un cálculo de comportamientos físicos sobre al menos uno del sistema físico y el actor físico.

14. El sistema de seguridad cibernética de la reivindicación 13, que comprende además un motor de simulación, en comunicación con el módulo de gestión del espacio de comportamiento cibernético, el motor de simulación configurado para generar la pluralidad de escenas cibernéticas, cada una de la pluralidad de escenas cibernéticas incluye un subconjunto de datos cibernéticos, las escenas cibernéticas y los mapas cibernéticos asociados con la pluralidad de espacios de comportamiento cibernéticos;

y, opcionalmente, en el que el motor de simulación está además configurado para generar simulaciones, las simulaciones configuradas para:

operar en al menos uno de los datos del mundo real y los datos simulados; y

proporcionar un curso de acción para al menos una de operaciones, análisis, información, planificación, capacitación, una acción de remediación y una acción de mitigación.

15. El sistema de seguridad cibernética de la reivindicación 13, en el que el motor de flujo de trabajo analítico está además configurado para procesar al menos uno de los datos de sensores de tecnología operacional (OT), registros de tecnología operacional, datos de paquetes, tráfico de red, registros de ordenadores, inteligencia de señales, visible, infrarrojo, multiespectral, hiperespectral, radar de apertura sintética, radar indicador de objetivo móvil, datos de inteligencia técnica e informes de inteligencia.

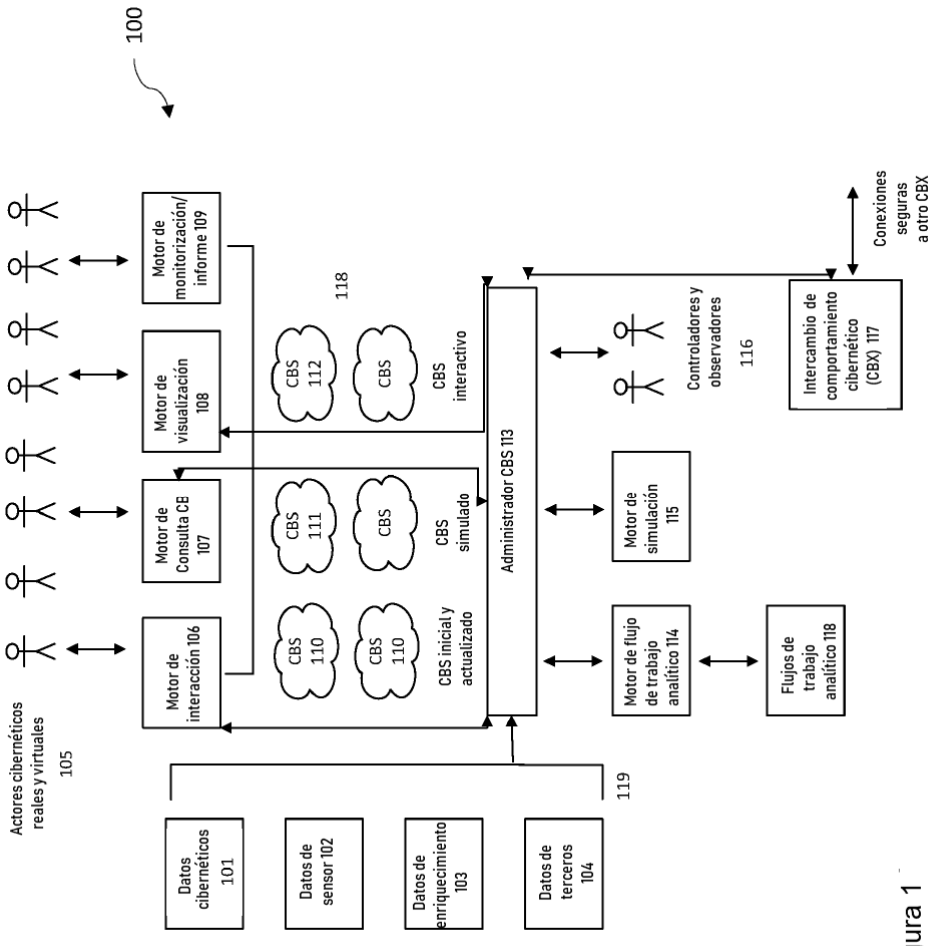
100
Actores cibernéticos reales y virtuales 105
Motor de interacción 106
Motor de Consulta CB 107
Motor de visualización 108
Motor de monitorización/ informe 109
CBS 110
CBS 111
CBS 112
CBS
CBS inicial y actualizado
CBS simulado
CBS interactivo
118
Administrador CBS 113
Motor de flujo de trabajo analítico 114
Motor de simulación 115
Controladores y observadores 116
Intercambio de comportamiento cibernético (CBX) 117
Flujos de trabajo analítico 118
Conexiones seguras a otro CBX
119
Datos cibernéticos 101
Datos de sensor 102
Datos de enriquecimiento 103
Datos de terceros 104

Figura 1

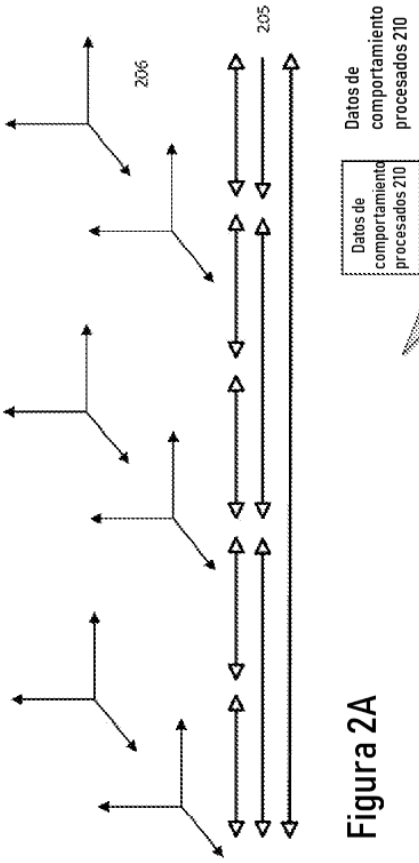

Figura 2A

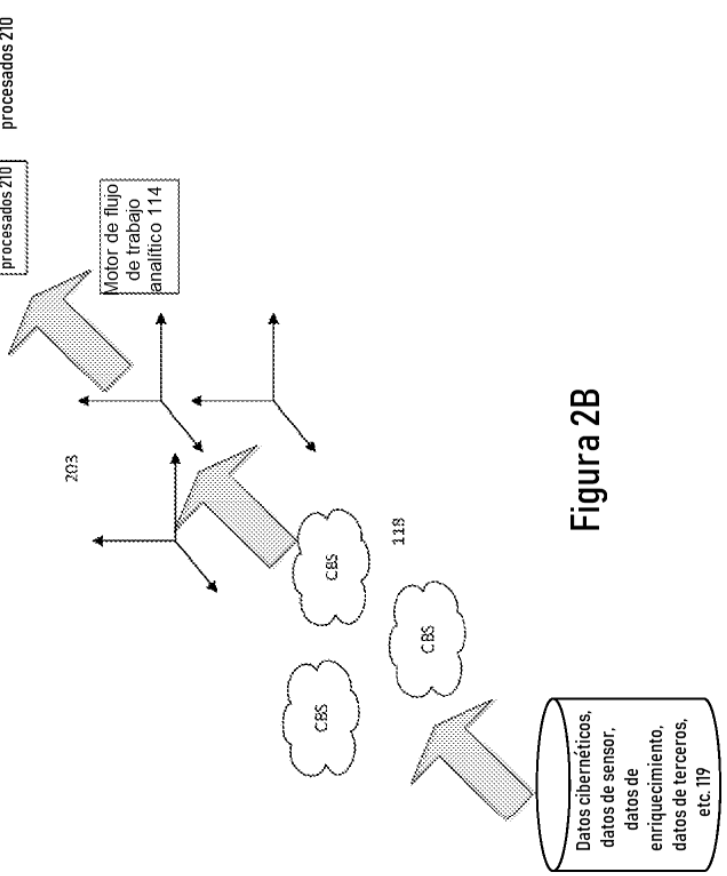

Figura 2B

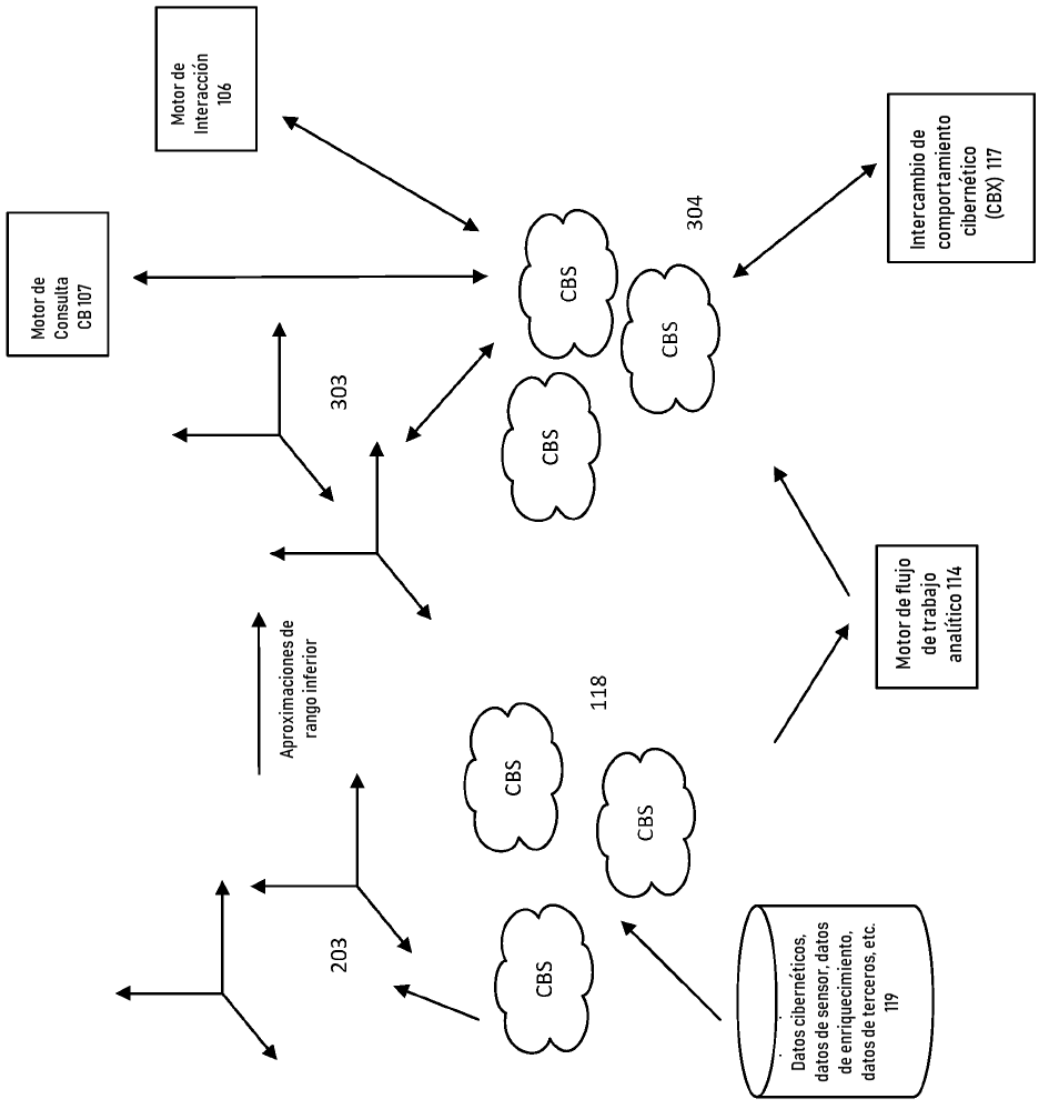
Motor de Interacción 106
Motor de Consulta CB 107
Intercambio de comportamiento cibernético (CBX) 117
Motor de flujo de trabajo analítico 114
Datos cibernéticos, datos de sensor, datos de enriquecimiento, datos de terceros, etc. 119
Aproximaciones de rango inferior
CBS
203
303
304
118

Figura 3

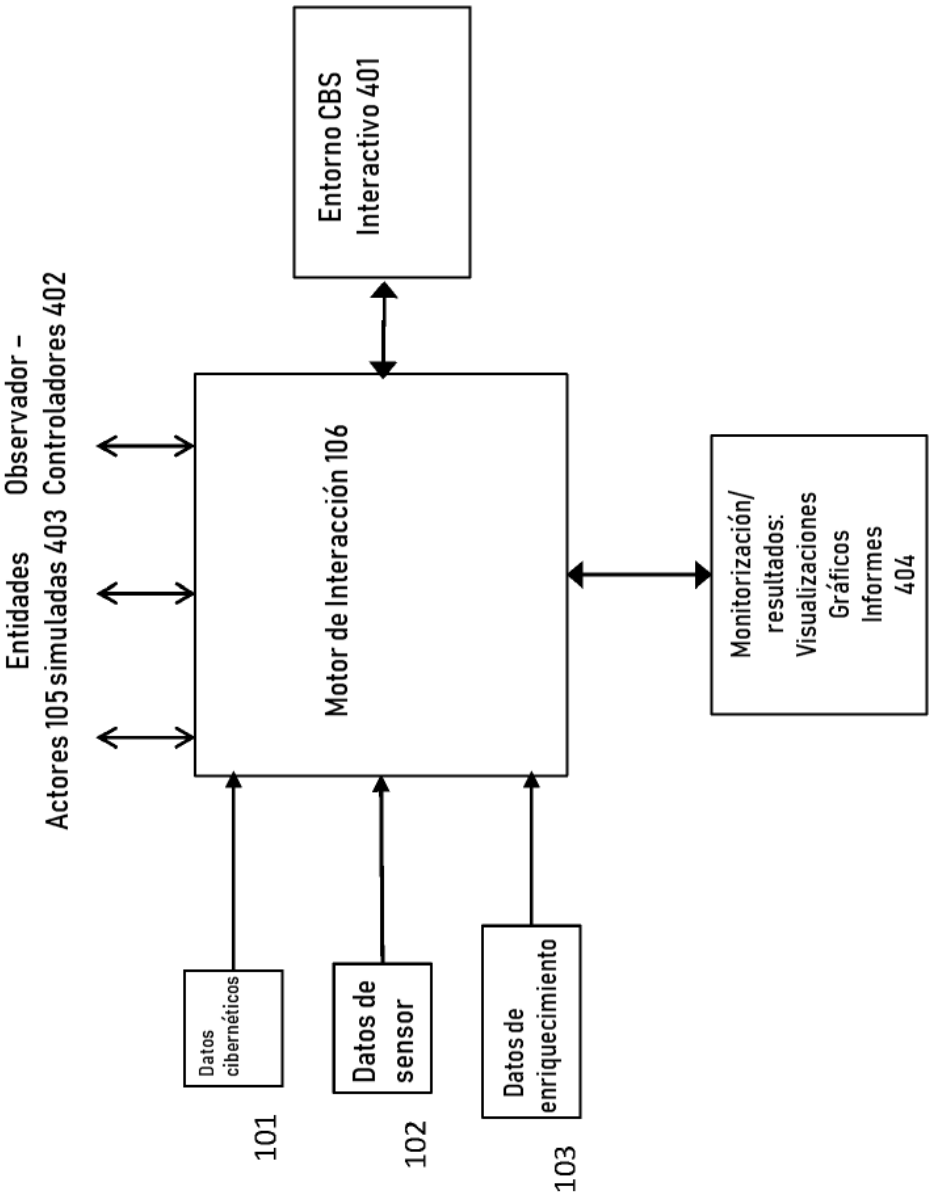
Entorno CBS Interactivo 401
Entidades simuladas 105
Observador - Controladores 402
Actores 403
Motor de Interacción 106
Monitorización/ resultados: Visualizaciones Gráficos Informes 404
Datos cibernéticos
Datos de sensor
Datos de enriquecimiento
101
102
103

Figura 4

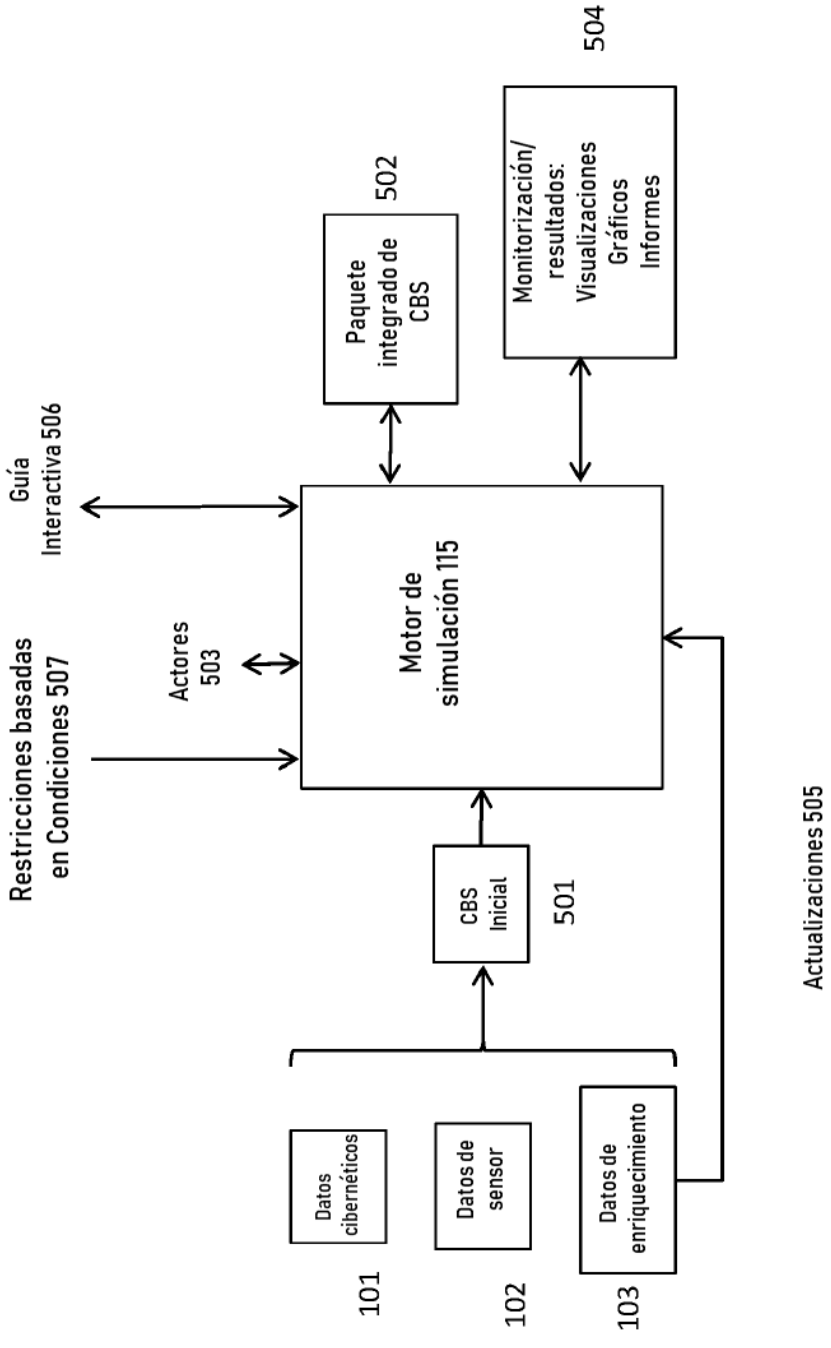
Datos cibernéticos
Datos de sensor
Datos de enriquecimiento
101
102
103
CBS Inicial
501
Motor de simulación 115
Actores 503
Guía Interactiva 506
Restricciones basadas en Condiciones 507
Paquete integrado de CBS
502
Monitorización/ resultados: Visualizaciones Gráficos Informes
504
Actualizaciones 505

Figura 5

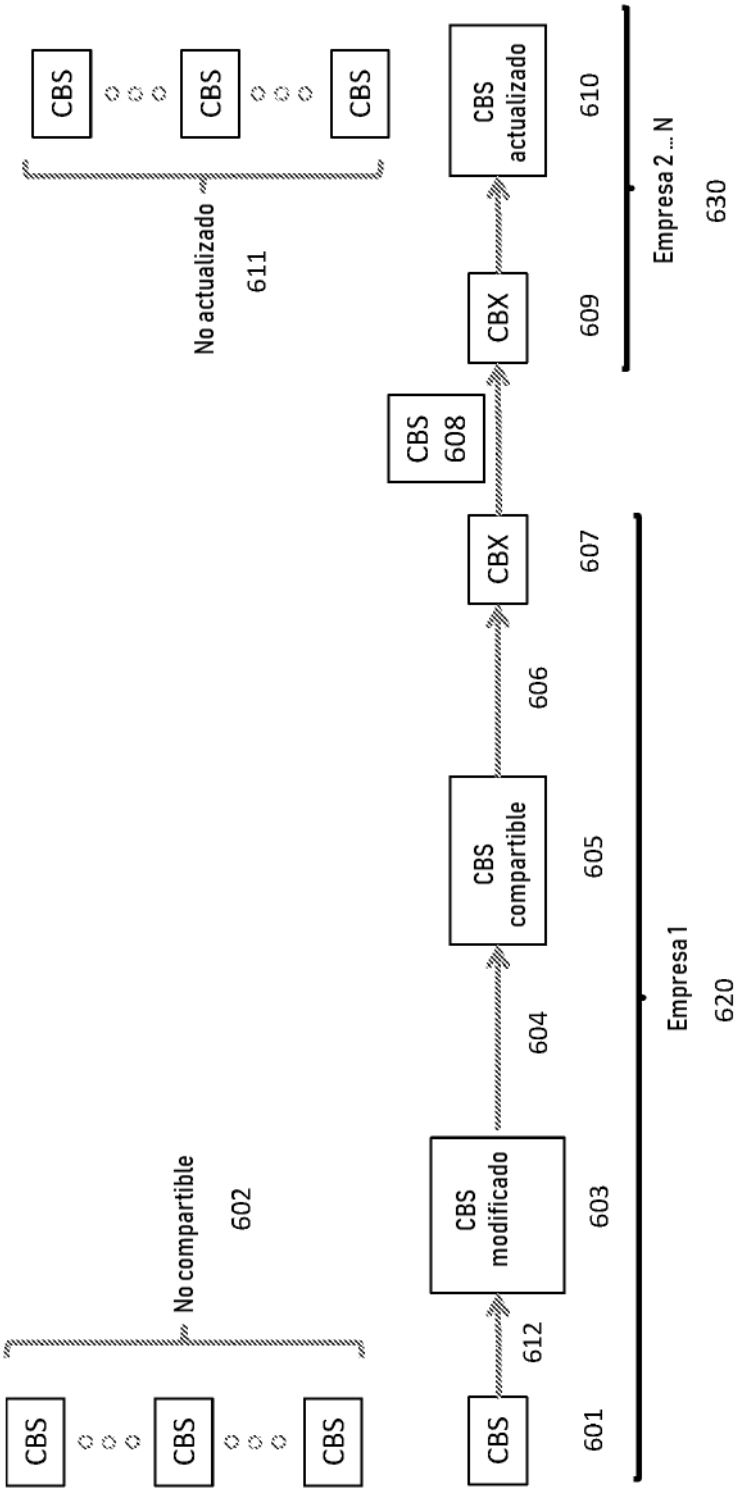
CBS
CBS
CBS
No compartible
602
CBS
modificado
603
612
CBS
601
604
CBS
compartible
605
606
CBX
607
CBS
608
CBX
609
CBS
actualizado
610
Empresa 2 ... N
630
Empresa 1
620
No actualizado
611
CBS
CBS
CBS

Figura 6

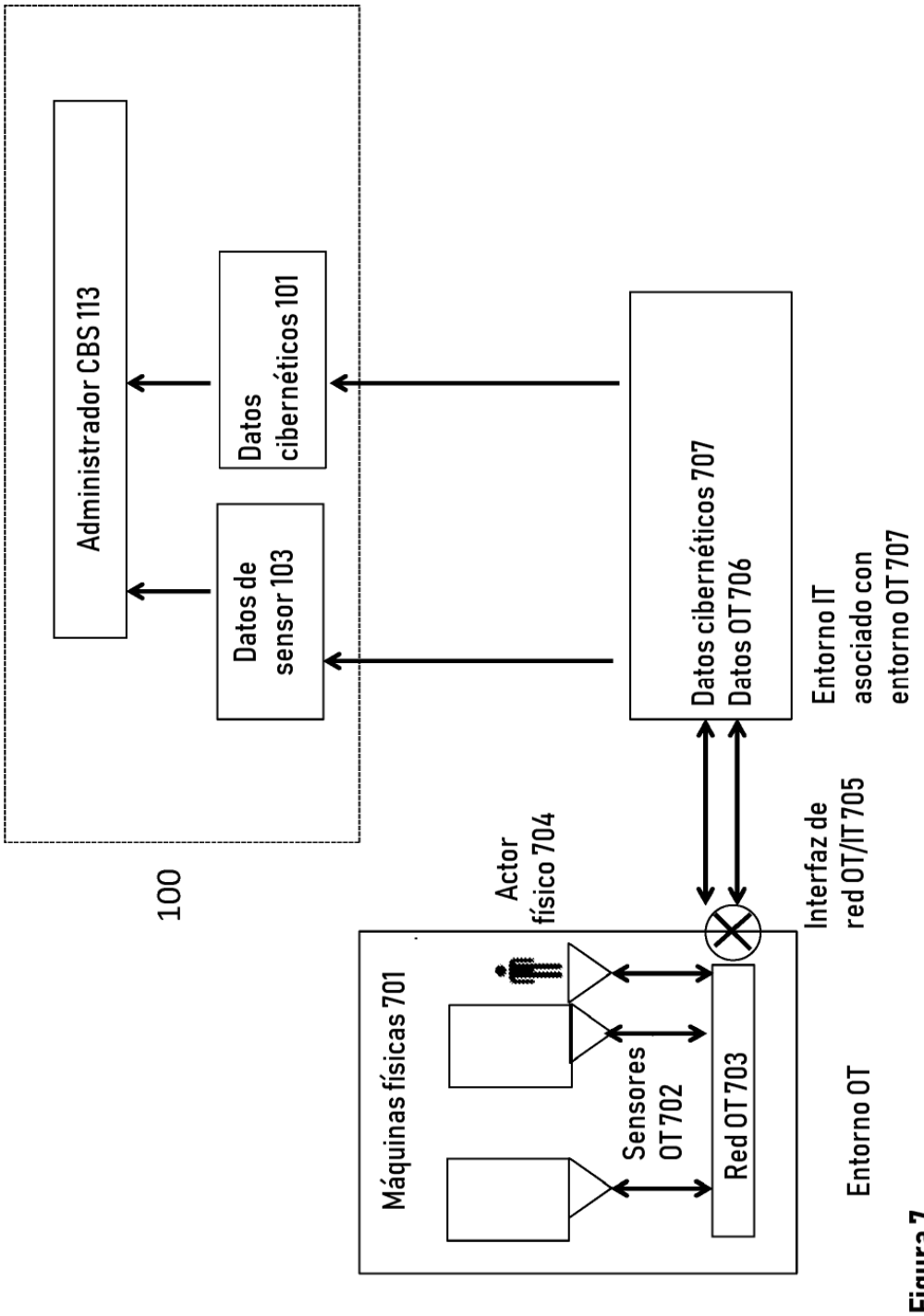
Administrador CBS 113
Datos cibernéticos 101
Datos de sensor 103
100
Datos cibernéticos 707
Datos OT 706
Entorno IT asociado con entorno OT 707
Actor físico 704
Interfaz de red OT/IT 705
Máquinas físicas 701
Sensores OT 702
Red OT 703
Entorno OT

Figura 7