(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 736 099**

(51) Int. CI.:

G06F 11/00 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.10.2015 PCT/US2015/056082**

(87) Fecha y número de publicación internacional: **07.07.2016 WO16109005**

(96) Fecha de presentación y número de la solicitud europea: **16.10.2015 E 15875868 (0)**

(97) Fecha y número de publicación de la concesión europea: **29.05.2019 EP 3095034**

(54) Título: **Sistema de ciberseguridad**

(30) Prioridad:

21.10.2014 US 201462066769 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.12.2019

(73) Titular/es:

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

(72) Inventor/es:

GROSSMAN, ROBERT, L.;
HEATH, JAMES, E.;
RICHARDSON, RUSSELL, D. y
ALEXANDER, KEITH, B.

(74) Agente/Representante:

SÁEZ MAESO, Ana

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Sistema de ciberseguridad

Antecedentes

Tradicionalmente, los sistemas de ciberseguridad tienen una capacidad limitada para dar cuenta de las diferencias de dispositivos en redes grandes y para realizar el procesamiento en tiempo real. En una red grande, habrá muchos dispositivos y sus comportamientos serán muy diferentes. El enfoque convencional es desarrollar un modelo de comportamiento único para la red o para cada tipo de dispositivo en la red (estación de trabajo, servidor, conmutador, enrutador, etc. en la red). El problema con este enfoque es que este tipo de enfoque no captura las diferencias entre dispositivos individuales. Otra limitación de los sistemas tradicionales de ciberseguridad es que los modelos de comportamiento convencionales se construyen manualmente una vez que se han acumulado suficientes datos, se han investigado con análisis de datos exploratorios y analizados. Los sistemas tradicionales a menudo requieren: una persona para construir modelos manualmente, información del estado anterior sobre entidades de interés y análisis distribuidos/por lotes que pueden procesar los datos en pases múltiples y requieren datos distribuidos o basados en disco. Como tal, los datos en tiempo real no se aprovechan eficientemente, en todo caso.

El documento US 8,015,133 B1 se relaciona con un sistema de modelado implementado por ordenador y un método para analizar y predecir las intrusiones en la red de ordenadores.

El documento US 2012/0072983 A1 se relaciona con un sistema y un método para la fusión de ciberdatos con privacidad mejorada mediante la agregación y el análisis de comportamiento temporal.

Resumen

Aunque se conocen ciertas técnicas para el modelado predictivo, el enfoque descrito en este documento se puede usar para integrar un modelado analítico segmentado con un tipo de microsegmentación de centro de datos que permite al sistema tomar el evento de mitigación adecuado para cada microsegmento. En otras palabras, de acuerdo con algunas realizaciones, una gran red de empresas se divide primero en un gran número de microsegmentos de centros de datos homogéneos basados en el comportamiento de las entidades en los microsegmentos, los usuarios que interactúan con las entidades y los paquetes y flujos en los microsegmentos. En particular, se crean grandes cantidades de segmentos en la empresa en la que se colocan sensores que pueden recopilar datos para uno o más de dichos segmentos. Luego se construyen modelos para cada segmento, y cada segmento se monitoriza con un sensor y un motor de puntuación, y se toman las medidas de mitigación apropiadas para ese microsegmento en particular. En otras palabras, el uso del modelado basado en eventos y los modelos múltiples se integran con los motores de puntuación en tiempo real y la microsegmentación del centro de datos, lo que permite la aplicación efectiva de eventos de mitigación apropiados para cada microsegmento.

Aunque la separación de la construcción de modelos analíticos (un caso especial de los cuales son modelos de comportamiento) y la puntuación de modelos analíticos usando dos aplicaciones diferentes es una técnica estándar en la monitorización de sistemas en tiempo real y la generación de alertas, el uso de múltiples sensores y motores de puntuación múltiples que se comunican a través de un ESB de alto rendimiento; la capacidad de actualizar un modelo de formato de intercambio de modelo (MIF), como Formato Portátil para Análisis (PFA), utilizando un mensaje enviado a través del ESB; la recopilación de evidencia evento por evento de múltiples motores de puntuación, cada uno de los cuales se comunica mediante un mensaje de inteligencia de amenazas (TIM) a un motor analítico en tiempo real (RTAE) a través del ESB; y el procesamiento de estos TIM por parte del RTAE para enviar eventos de mitigación apropiados (TIM de mitigación) sobre el ESB son avances significativos individualmente sobre el uso de un solo motor de puntuación que procesa un solo corriente de datos que solo puede reemplazar un documento de formato de intercambio de modelo con uno nuevo.

De acuerdo con la materia objeto divulgada, se proporcionan sistemas, métodos y medios legibles por ordenador no transitorios para proporcionar un sistema de ciberseguridad para procesar eventos para producir puntajes, alertas y acciones de mitigación.

En algunas realizaciones, la materia objeto divulgada incluye un sistema de ciberseguridad para procesar eventos para producir puntuaciones, alertas y acciones de mitigación. En algunas realizaciones, el sistema incluye una pluralidad de sensores, cada uno de los cuales está configurado para recibir datos del sensor de la red, procesar los datos del sensor para formar eventos y transmitir los eventos. En algunas realizaciones, el sistema incluye una plataforma analítica distribuida, la plataforma analítica distribuida configurada para recibir los eventos de la pluralidad de sensores, procesa los eventos para formar flujos de trabajo analíticos, cada uno de los flujos de trabajo analíticos asociados con uno o más segmentos lógicos, y transmite los flujos de trabajo analíticos y los mensajes de plataforma analítica distribuida. En algunas realizaciones, el sistema incluye una pluralidad de motores de puntuación, cada uno de los cuales está configurado para recibir los flujos de trabajo analíticos desde la plataforma analítica distribuida, recibe los eventos de al menos uno de la pluralidad de sensores, procesa los eventos recibidos utilizando los flujos de trabajo analíticos para producir mensajes del motor de puntuación y transmitir los mensajes del motor de puntuación.

En algunas realizaciones, el sistema incluye un motor analítico en tiempo real, el motor analítico en tiempo real configurado para recibir los flujos de trabajo analíticos de la plataforma analítica distribuida, recibir el flujo de trabajo analítico y las reglas de procesamiento de eventos, recibir los mensajes del motor de puntuación de la pluralidad de motores de puntuación, recibir los mensajes de la plataforma analítica distribuida de la plataforma analítica distribuida, y procesar los mensajes del motor de puntuación y los mensajes de la plataforma analítica distribuida utilizando los flujos de trabajo analíticos de la plataforma analítica distribuida y las reglas de procesamiento de eventos y flujo de trabajo analítico para formar un mensaje de inteligencia de amenazas. En algunas realizaciones, el mensaje de inteligencia de amenazas comprende al menos uno de un mensaje de difusión, el motor analítico en tiempo real configurado para transmitir el mensaje de difusión, un mensaje de mitigación, el motor analítico en tiempo real configurado para transmitir el mensaje de mitigación a un motor de plano de control para realizar una acción de mitigación asociada con un primer segmento lógico de uno o más segmentos lógicos cuando el procesamiento por el motor analítico en tiempo real indica que la acción de mitigación limita el impacto de la actividad anómala y un mensaje de actualización del modelo, el motor analítico en tiempo real configurado para transmitir el mensaje de actualización del modelo para actualizar uno o más flujos de trabajo analíticos cuando el procesamiento por el motor analítico en tiempo real indica que el mensaje de actualización del modelo mejora al menos uno de una tasa de detección de la actividad anómala y una reducción en una tasa de falsos positivos. En algunas realizaciones, cada uno de los uno o más segmentos lógicos asocia un modelo analítico, un conjunto de modelos analíticos o un flujo de trabajo analítico; una o más fuentes de entradas sobre la actividad dentro del segmento lógico; y un conjunto de acciones para mitigar un impacto de la actividad anómala que ocurre dentro del segmento lógico.

En algunas formas de realización, la pluralidad de sensores, la pluralidad de motores de puntuación, la plataforma analítica distribuida, el motor analítico en tiempo real y el motor del plano de control están conectados mediante una red fuera de banda.

En algunas realizaciones, la pluralidad de sensores, la pluralidad de motores de puntuación, la plataforma analítica distribuida, el motor analítico en tiempo real y el motor del plano de control se comunican mediante el envío de mensajes asociados a través de un bus de sistema empresarial.

En algunas realizaciones, la pluralidad de sensores, la pluralidad de motores de puntuación, la plataforma analítica distribuida, el motor analítico en tiempo real y el motor del plano de control están conectados mediante una red fuera de banda y se comunican mediante el envío de mensajes asociados a través de un bus del sistema empresarial.

En algunas realizaciones, el sistema descrito aquí comprende además un módulo de actores de ingesta, el módulo de actores de ingesta configurado para recibir datos de aplicaciones de terceros de al menos una de una aplicación de terceros y un dispositivo de terceros, y transmitir los datos de aplicación de terceros para su posterior procesamiento por al menos uno de la pluralidad de motores de puntuación, la plataforma analítica distribuida y el motor analítico en tiempo real.

En algunas realizaciones, la pluralidad de sensores, la pluralidad de motores de puntuación, la plataforma analítica distribuida, el motor analítico en tiempo real, el motor del plano de control y el módulo de actores de ingesta están conectados mediante una red fuera de banda.

En algunas realizaciones, la pluralidad de sensores, la pluralidad de motores de puntuación, la plataforma analítica distribuida, el motor analítico en tiempo real, el motor del plano de control y el módulo de actores de ingesta se comunican mediante el envío de mensajes asociados a través de un bus de sistema empresarial.

En algunas formas de realización, el motor de puntuación está además configurado para recibir los mensajes de actualización del modelo y procesar los mensajes de actualización al mismo tiempo que el procesamiento de los eventos.

En algunas realizaciones, para formar al menos uno de los mensajes de difusión, el mensaje de mitigación y el mensaje de actualización del modelo, el motor analítico en tiempo real está configurado además para recibir una primera salida en un primer momento de al menos uno de la pluralidad de motores de puntuación, la plataforma analítica distribuida y la pluralidad de sensores; recuperar la primera información de estado correspondiente a la primera salida; actualizar la primera información de estado con los primeros datos de salida; procesar la primera información de estado actualizada mediante un flujo de trabajo analítico asociado con el motor analítico en tiempo real para formar la información de primer estado procesada actualizada; almacenar la primera información de estado actualizada procesada en el motor analítico en tiempo real; recibir una segunda salida en un segundo momento de al menos uno de la pluralidad de motores de puntuación, la plataforma analítica distribuida y la pluralidad de sensores; recuperar la segunda información de estado correspondiente a la segunda salida; actualizar la segunda información de estado con segundos datos de salida; procesar la segunda información de estado actualizada mediante el flujo de trabajo analítico asociado con el motor analítico en tiempo real para formar la segunda información de estado actualizada procesada; formar el al menos uno del mensaje de difusión, el mensaje de mitigación y el mensaje de actualización del modelo en función de la segunda información de estado actualizada procesada; y almacenar la segunda información de estado actualizada procesada en el motor analítico en tiempo real.

En algunas realizaciones, el motor analítico en tiempo real está además configurado para recibir una salida interina en un tercer momento desde al menos uno de la pluralidad de motores de puntuación, la plataforma analítica distribuida y la pluralidad de sensores, en donde la tercera vez es posterior a la primera vez y antes de la segunda vez; recuperar información de estado interino correspondiente a la salida interina; actualizar la información de estado interino con datos de salida interinos; procesar la información de estado interina provisional actualizada mediante el flujo de trabajo analítico asociado con el motor analítico en tiempo real para formar información de estado interina actualizada procesada; y almacenar la información de estado interina actualizada procesada en el motor analítico en tiempo real.

En algunas realizaciones, los flujos de trabajo analíticos comprenden un documento de Formato de Intercambio de Modelo, en el que el documento de Formato de Intercambio de Modelo admite una composición de modelos analíticos; una segmentación de modelos analíticos; un conjunto de modelos analíticos; una composición de modelos analíticos con reglas; una composición de modelos analíticos con etapas de preprocesamiento y posprocesamiento, en la que las etapas de preprocesamiento y posprocesamiento incluyen transformaciones de datos y agregaciones de datos; y los flujos de trabajo analíticos, cada uno de los flujos de trabajo comprende al menos uno de los modelos analíticos, reglas, transformaciones de datos, agregaciones de datos y composiciones de los modelos analíticos, las reglas, las transformaciones de datos, las agregaciones de datos, las segmentaciones y las agrupaciones.

En algunas realizaciones, el motor analítico en tiempo real está además configurado para transmitir un modelo de comportamiento actualizado a uno o más de la pluralidad de motores de puntuación cuando los cambios en uno o más de los flujos de trabajo analíticos superan un umbral.

En algunas realizaciones, los eventos comprenden al menos uno de los datos sobre flujos de red, datos sobre paquetes, datos sobre entidades, datos sobre usuarios, datos sobre estaciones de trabajo y servidores, datos sobre enrutadores y conmutadores, datos sobre entidades de red externas y datos sobre dispositivos internos y externos que interactúan con la red.

En algunas realizaciones, uno o más de la pluralidad de sensores y la pluralidad de motores de puntuación se integran en una sola aplicación.

En algunas realizaciones, el motor analítico en tiempo real está integrado con uno o más de la pluralidad de motores de puntuación.

En algunas realizaciones, la acción de mitigación comprende al menos uno de: cerrar al menos un puerto, modificar al menos un paquete de datos, controlar la transmisión de paquetes o flujos, bloquear una subred, bloquear uno o más Protocolos de Internet (IP)) o rangos de IP, y bloquear una o más IP internas o externas.

En algunas realizaciones, la acción de mitigación comprende al menos una de: desconectar al menos uno de un servidor y una estación de trabajo, crear al menos uno de un nuevo servidor virtualizado y una nueva estación de trabajo virtualizada de una imagen protegida, y bloquear una acción asociada con al menos uno del servidor y la estación de trabajo.

En algunas formas de realización, la actividad anómala comprende al menos uno de reconocimiento, explotación, intrusión, compromiso, amenaza interna y ataque.

En algunas realizaciones, la acción de mitigación comprende al menos una de modificar al menos un paquete de datos, controlar la transmisión de paquetes o flujos, y eliminar la autorización y los privilegios de acceso para una entidad asociada con la actividad anómala, en donde eliminar la autorización y los privilegios de acceso comprenden al menos bloquear el acceso a la red, bloquear el acceso a los dispositivos de la red, bloquear el acceso a los servidores, bloquear el acceso a las estaciones de trabajo y bloquear el acceso a otros dispositivos informáticos.

En algunas realizaciones, la actividad anómala está asociada con al menos uno de un actor interno malo y de un actor externo malo.

En algunas realizaciones, el sistema comprende además un motor de visualización, el motor de visualización que incluye un monitor, el motor de visualización configurado para recibir estadísticas e imágenes gráficas asociadas con el procesamiento de mensajes del motor de puntuación por el motor analítico en tiempo real; y mostrar las estadísticas e imágenes gráficas en el monitor.

En algunas realizaciones, se divulga una red de ciberseguridad que incluye una pluralidad de los sistemas de ciberseguridad descritos en el presente documento, en donde cada uno de la pluralidad de sistemas de ciberseguridad está configurado para intercambiar un mensaje de inteligencia de amenazas seleccionado con uno o más de los otros sistemas de ciberseguridad en el que el mensaje de inteligencia de amenazas seleccionado está cifrado para proporcionar un mecanismo de seguridad para transferir información, en donde la información en el mensaje de inteligencia de amenazas seleccionada no expone información interna sensible sobre el sistema de ciberseguridad de transmisión.

En algunas realizaciones, el sistema de ciberseguridad está configurado además para intercambiar un mensaje de inteligencia de amenazas externo con un sistema de terceros compatible, en el que el mensaje de inteligencia de amenazas externas está cifrado para proporcionar un mecanismo seguro para transferir información, la información en el mensaje de inteligencia de amenazas externa no expone información interna sensible sobre el sistema que transmite el mensaje de inteligencia de amenazas externas, y el mensaje de inteligencia de amenazas externas está formateado con un formato de intercambio de modelos común.

En algunas realizaciones, la plataforma analítica distribuida está además configurada para recibir los mensajes del motor de puntuación, y procesar los mensajes del motor de puntuación para formar mensajes de inteligencia de amenaza.

En algunas realizaciones, el mensaje de difusión comprende al menos uno de un mensaje de información, un mensaje de evento cibernético y un mensaje de alerta.

En algunas realizaciones, cada uno de la pluralidad de segmentos lógicos está asociado con al menos uno de una división de la red, una división del tráfico en la red, una división de usuarios en la red, una división de dispositivos en la red, una división basada en datos de terceros, y datos asociados con al menos una de las divisiones de la red, el tráfico en la red, los usuarios en la red, los dispositivos en la red y los datos de terceros.

En algunas realizaciones, al menos una primera división se solapa con al menos una segunda división.

En algunas realizaciones, al menos una primera división se solapa con al menos una segunda división y la pluralidad de sensores, la pluralidad de motores de puntuación, la plataforma analítica distribuida, la máquina analítica en tiempo real, la máquina del plano de control y el módulo de actores de ingesta se comunica mediante el envío de mensajes asociados a través de un bus de sistema empresarial.

En algunas realizaciones, la materia objeto divulgada incluye un sistema de ciberseguridad para procesar eventos para producir puntuaciones, alertas y acciones de mitigación. En algunas realizaciones, el sistema incluye una pluralidad de sensores, cada uno de los cuales está configurado para recibir datos del sensor de la red, procesar los datos del sensor para formar eventos y transmitir los eventos. En algunas realizaciones, el sistema incluye una plataforma analítica distribuida, la plataforma analítica distribuida configurada para recibir los eventos de la pluralidad de sensores, procesa los eventos para formar flujos de trabajo analíticos, cada uno de los flujos de trabajo analíticos asociados con uno o más segmentos lógicos, y transmite los flujos de trabajo analíticos y los mensajes de plataforma analítica distribuida. En algunas realizaciones, el sistema incluye un motor de puntuación, el motor de puntuación configurado para recibir los flujos de trabajo analíticos de la plataforma analítica distribuida, recibir los eventos de al menos uno de la pluralidad de sensores, procesar los eventos utilizando los flujos de trabajo analíticos para producir mensajes del motor de puntuación, y transmitir los mensajes del motor de puntuación. En algunas realizaciones, el sistema incluye un motor analítico en tiempo real, el motor analítico en tiempo real configurado para recibir los flujos de trabajo analíticos de la plataforma analítica distribuida, recibir el flujo de trabajo analítico y las reglas de procesamiento de eventos, recibir los mensajes del motor de puntuación de la pluralidad de motores de puntuación, recibir los mensajes de la plataforma analítica distribuida de la plataforma analítica distribuida y procesar los mensajes del motor de puntuación y mensajes de la plataforma analítica distribuida que utilizan los flujos de trabajo analíticos de la plataforma analítica distribuida y el flujo de trabajo analítico y las reglas de procesamiento de eventos para formar un mensaje de inteligencia de amenazas. En algunas realizaciones, el mensaje de inteligencia de amenazas comprende al menos uno de un mensaje de difusión, el motor analítico en tiempo real configurado para transmitir el mensaje de difusión, un mensaje de mitigación, el motor analítico en tiempo real configurado para transmitir el mensaje de mitigación a un motor de plano de control para realizar una acción de mitigación asociada con un primer segmento lógico de uno o más segmentos cuando el procesamiento por el motor analítico en tiempo real indica que la acción de mitigación limita el impacto de una actividad anómala, y un mensaje de actualización del modelo, el motor analítico en tiempo real configurado para transmitir el mensaje de actualización del modelo para actualizar uno o más flujos de trabajo analíticos cuando el procesamiento realizado por el motor analítico en tiempo real indica que el mensaje de actualización del modelo mejora al menos uno de una tasa de detección de la actividad anómala y una reducción de una tasa de falsos positivos. En algunas realizaciones, cada uno de los uno o más segmentos lógicos asocia un modelo analítico, un conjunto de modelos analíticos o un flujo de trabajo analítico; una o más fuentes de entradas sobre la actividad dentro del segmento lógico; y un conjunto de acciones para mitigar un impacto de la actividad anómala que ocurre dentro del segmento lógico.

Estas y otras capacidades de la materia objeto 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

Diversos objetivos, características y ventajas de la materia objeto divulgada pueden apreciarse más completamente con referencia a la siguiente descripción detallada de la materia objeto divulgada cuando se considera en relación con los siguientes dibujos, en los que números de referencia similares identifican elementos similares.

La figura 1 es un diagrama de sistema que muestra un marco de ciberseguridad, de acuerdo con algunas realizaciones de la presente divulgación.

La figura 2 es un diagrama de sistema que muestra un marco de ciberseguridad implementado en tres redes, de acuerdo con algunas realizaciones de la presente divulgación.

La figura 3 es un diagrama de sistema que muestra las tomas de red insertadas en diferentes partes de una red empresarial, de acuerdo con algunas realizaciones de la presente divulgación.

La figura 4 es un diagrama de bloques que muestra un motor de puntuación de acuerdo con algunas realizaciones de la presente divulgación.

La figura 5 es un diagrama de flujo que ilustra un método para procesar y enviar mensajes mediante el motor analítico en tiempo real, de acuerdo con algunas realizaciones de la presente divulgación.

La figura 6A es un diagrama de flujo que muestra el procesamiento de entradas o eventos directamente, de acuerdo con algunas realizaciones de la presente invención.

La figura 6B es un diagrama de flujo que muestra la asociación de uno o más estados persistentes con cada evento, de acuerdo con algunas realizaciones de la presente divulgación.

La figura 6C es un diagrama de flujo que ilustra el preprocesamiento y el postprocesamiento de un modelo analítico, de acuerdo con algunas realizaciones de la presente divulgación.

La figura 7 es un diagrama de sistema que muestra el procesamiento del tráfico de red para producir modelos analíticos, que se importan a motores de puntuación, de acuerdo con algunas realizaciones de la presente divulgación.

La figura 8A es un diagrama de sistema que muestra un conjunto de modelos, de acuerdo con algunas realizaciones de la presente divulgación.

La figura 8B es un diagrama de sistema que muestra una composición o encadenamiento de modelos, de acuerdo con algunas realizaciones de la presente divulgación.

La figura 8C es un diagrama de sistema que muestra modelos segmentados, de acuerdo con algunas realizaciones de la presente divulgación.

La figura 9 es un diagrama de flujo que representa el corriente de datos entre componentes en el marco de la ciberseguridad, de acuerdo con algunas realizaciones de la presente divulgación.

La figura 10 es un diagrama de sistema que ilustra una respuesta a una amenaza externa al marco de ciberseguridad, de acuerdo con algunas realizaciones de la presente divulgación.

La figura 11 es un diagrama de sistema que ilustra una respuesta y una amenaza interna al marco de ciberseguridad, de acuerdo con algunas realizaciones de la presente divulgación.

Descripción detallada

En la siguiente descripción, se exponen numerosos detalles específicos con respecto a los sistemas y métodos de la materia objeto divulgada y el entorno en el que pueden operar tales sistemas y métodos, etc., para proporcionar una comprensión completa de la materia divulgada. Sin embargo, será evidente para un experto en la materia que la materia objeto divulgada puede ponerse en práctica sin tales detalles específicos, y que ciertas características, que son bien conocidas en la técnica, no se describen en detalle para evitar complicaciones innecesarias de la materia objeto divulgada. Además, se entenderá que las realizaciones proporcionadas a continuación son de ejemplo, y que se contempla que existen otros sistemas y métodos que están dentro del alcance de la materia divulgada.

Algunas realizaciones de la presente divulgación se refieren a la creación de un marco de ciberseguridad. El marco de ciberseguridad realiza acciones de detección y mitigación casi en tiempo real en una empresa distribuida, mientras simplifica la monitorización, análisis y despliegue.

Los procesos descritos en este documento en algunas realizaciones utilizan el ESB fuera de banda y la red fuera de banda, que permiten procesar la gran cantidad de datos de flujo de red, archivos de paquetes (PCAP), datos de registro del sistema, datos de amenaza externa, y otros datos de interés por la plataforma analítica distribuida; puntuación casi en tiempo real; procesamiento en tiempo casi real de los mensajes de inteligencia de amenazas (TIM), eventos de mitigación y actualizaciones de modelos por parte de los diversos componentes del sistema; y visualización casi en tiempo real analítica, monitorización y actualizaciones a las consolas de control.

Las acciones representativas en el ciberentorno incluyen: el análisis de datos ciberanalíticos, modelos de comportamiento de construcción, puntuación de modelos de comportamiento, actualización de modelos de comportamiento, envío de alertas, evaluación de alertas, comando de envío, acciones de control y mitigación, visualización en tiempo real y marco de operación y colaboración.

Arquitectura del sistema

La figura 1 es un diagrama de sistema que muestra un marco de ciberseguridad, de acuerdo con algunas realizaciones de la presente divulgación. La figura 1 muestra el sensor 102 (también denominado aquí cibersensor), los actores 104 de ingesta, la plataforma 106 analítica distribuida, el motor 108 de puntuación, el motor analítico en tiempo real (RTAE) 110, el motor 112 de visualización, el motor 114 de plano de control y el bus de servicio empresarial distribuido (ESB) 116. En algunas realizaciones de la presente divulgación, el sensor 102 y el motor 108 de puntuación se combinan en una sola aplicación integrada. La figura 1 también muestra componentes adicionales del sistema, incluidos los puntos 120 finales, el plano 122 de datos, los servidores y las estaciones de trabajo 126, el personal de ciberoperaciones (ops) y los ciberanalistas 128, aplicaciones de terceros, aplicaciones de terceros, fuentes y dispositivos 130, y cortafuegos, conmutadores y enrutadores 132.

Cada uno de los elementos en la figura 1 se describe con más detalle a continuación. Brevemente, el sensor 102 captura y procesa los datos del plano 122 de datos de la empresa y pasa los datos al ESB 116, donde los datos se enrutan para su procesamiento posterior. El plano 122 de datos transmite datos hacia y desde los diversos dispositivos en la red de la empresa, incluidos los dispositivos 120 de punto final, los servidores y las estaciones de trabajo 126, y los cortafuegos, conmutadores y enrutadores 132. El motor 114 de plano de control recibe datos procesados del ESB 116 y monitoriza, configura y reconfigura los dispositivos de red, incluidos los conmutadores, enrutadores y cortafuegos 132. El motor 108 de puntuación recibe datos del ESB 116 y, para cada evento en la corriente, procesa el evento utilizando uno o más modelos analíticos, para producir salidas, incluidas las puntuaciones, alertas y mensajes, así como información relacionada. Los actores 104 de ingesta capturan y procesan datos de aplicaciones, fuentes y dispositivos de terceros, y envía los datos a ESB 116, donde los datos se enrutan para su posterior procesamiento. La plataforma 106 analítica distribuida (que también se puede denominar una nube analítica) es una plataforma informática distribuida que se puede usar para analizar grandes cantidades de datos y producir diversos resultados analíticos. La plataforma 106 analítica distribuida recibe y envía datos hacia y desde ESB 116, los actores 104 de ingesta, RTAE 110 y el motor 112 de visualización. RTAE 110 recibe datos de ESB 116 y la plataforma 106 analítica distribuida y realiza cálculos casi en tiempo real utilizando memoria distribuida y procesadores especializados, como las GPU, crean visualizaciones casi en tiempo real, y crean decisiones casi en tiempo real sobre las acciones de mitigación al procesar datos de múltiples motores 108 de puntuación y otras fuentes. El motor de visualización, la consola central y el monitor 112 reciben y envían datos hacia y desde ESB 116, RTAE 110 y la plataforma 106 analítica, y proporcionan a los ciberops y analistas 128 una representación visual de los otros elementos descritos en la figura 1. El Motor de visualización, consola central y monitor 112 puede proporcionar consolas centrales configurables por el usuario, proporcionar información en tiempo real y soporte para consultas en tiempo real de RTAE 110, proporcionar y visualizar los resultados del análisis utilizando la plataforma 106 analítica distribuida, y proporcionar capacidad interactiva para consultar entidades, alertas, eventos, datos PCAP, Corriente de datos, gráficos.

Como muestra la figura 2, en algunas realizaciones de la presente divulgación, se puede implementar un marco de ciberseguridad en tres redes. La figura 2 muestra un plano 122 de datos de empresa, un plano 204 de control de empresa y una red 206 de sistema fuera de banda. En algunas realizaciones de la presente divulgación, un bus de servicio de empresa 116 se despliega sobre la red de sistema fuera de banda. La red 206 del sistema fuera de banda conecta el sensor cibernético 102, la plataforma 106 analítica distribuida, el RTAE 110, el motor 108 de puntuación, el motor 114 de plano de control y los agentes 210 de mitigación. En algunas realizaciones, dos o más de los siguientes componentes se comunican con otros componentes en la red fuera de banda a través de ESB 116: el cibersensor 102, plataforma 106 analítica distribuida, RTAE 110, motor 108 de puntuación, motor 114 de plano de control y agentes 210 de mitigación.

En algunas realizaciones, el motor 114 del plano de control puede enviar mensajes de mitigación a los agentes 210 de mitigación a través del plano 204 de control de empresa. Los agentes 210 de mitigación pueden estar integrados en el motor 114 del plano de control, o pueden estar incrustados o integrados con otros componentes del sistema o con otros dispositivos o componentes de la empresa. Por ejemplo, un agente 210 de mitigación se puede integrar con el motor 114 del plano de control y enviar mensajes al plano de control de la empresa para cerrar puertos o bloquear direcciones IP. Los agentes 210 de mitigación envían una acción de mitigación al plano de control, que luego realiza una acción, tal como la modificación de tablas en un enrutador o conmutador. Las acciones de mitigación incluyen modificaciones que resultan en cerrar un puerto, aislar un dispositivo de extremo, servidor o servicio de red, aislar una subred, etc. Otro ejemplo es que un agente 210 de mitigación puede enviar una acción de mitigación a un dispositivo de red en el plano de datos de la empresa que modifica paquetes o cambia la transmisión de paquetes o flujos.

En algunas realizaciones, los sensores 102 (también referidos en este documento como cibersensores) se colocan en el plano 122 de datos de la empresa. Como se describe con más detalle a continuación, los sensores 102 recopilan y procesan datos de red en el plano 122 de datos de la empresa para enviar los datos procesados a la red 206 del

sistema fuera de banda. En algunas realizaciones, el cibersensor 102 se puede conectar directamente al motor 108 de puntuación (por ejemplo, sin estar conectado a través de un ESB 116) o integrarse con el motor 108 de puntuación.

Como se muestra en la figura 2, una red empresarial funciona como el plano 122 de datos y transporta la mayor parte de los datos que pasan por las redes en la empresa. Además, algunas empresas pueden usar un plano 204 de control para comunicar información de control a conmutadores, enrutadores, cortafuegos 132 y otros dispositivos de red. El control 204 y el plano 122 de datos están separados lógicamente y pueden o no compartir la misma red física. En algunas realizaciones de la presente divulgación, también hay una red 206 de sistema fuera de banda que los componentes del sistema usan para la comunicación. En esta divulgación, fuera de banda se refiere a una red física separada del plano 122 de datos empresariales y el plano 204 de control.

En algunas realizaciones de la presente divulgación, la red 206 del sistema fuera de banda tiene mayor capacidad que el plano 122 de datos de la empresa. Por ejemplo, si el plano de datos de la empresa es una red 10G, entonces la red del sistema fuera de banda puede ser una red 40G. Si el plano de datos de la empresa es una red 40G, la red del sistema fuera de banda es una red 100G.

En algunas realizaciones, los componentes descritos anteriormente en la figura 1 están ubicados dentro de la misma red. Por ejemplo, en algunas realizaciones, el plano 122 empresarial y el plano 204 de control están en la misma red que la plataforma 106 analítica distribuida, el motor 108 de puntuación, el motor analítico de tiempo real (RTAE) 110, el motor 112 de visualización y el motor 114 de plano de control.

En algunas realizaciones de la presente divulgación, el sistema de ciberseguridad descrito en este documento, por ejemplo, en la figura 1, puede desplegarse en una pluralidad de ubicaciones físicas o lógicas. Cada uno de los sistemas de ciberseguridad desplegados puede configurarse para intercambiar mensajes seleccionados de inteligencia de amenazas con uno o más de los sistemas de ciberseguridad. En algunas realizaciones, los mensajes seleccionados de inteligencia de amenazas se cifran para proporcionar un mecanismo seguro para transferir información. En algunas realizaciones, la información transferida en el mensaje de inteligencia de amenaza seleccionado no expone información interna sensible sobre el sistema de ciberseguridad de transmisión, como dispositivos internos específicos comprometidos o las IP internas específicas bajo ataque, sino que contiene información sobre tipos de ataques, IP externas, etc.

En algunas realizaciones de la presente divulgación, el sistema de ciberseguridad descrito en este documento puede configurarse para intercambiar un mensaje externo de inteligencia de amenazas con un sistema de terceros compatible. El mensaje externo de inteligencia de amenazas se puede cifrar para proporcionar un mecanismo seguro para transferir información. En algunas realizaciones, la información en el mensaje de inteligencia de amenazas externa no expone información interna sensible sobre terceros, como dispositivos internos específicos comprometidos o las IP internas específicas bajo ataque, sino que contiene información sobre tipos de ataques, IP externas, etc. El mensaje externo de inteligencia de amenazas se puede formatear con un Formato de intercambio de modelos común para modelos de comportamiento que entienden los motores de puntuación, la plataforma analítica distribuida y la máquina analítica en tiempo real.

Las figuras 1 y 2, tomadas juntas, se describen con más detalle a continuación.

Bus 116 de servicio de empresa, mensajes y tópicos.

En algunas realizaciones de la presente divulgación, la red del sistema fuera de banda utiliza un bus de servicio empresarial distribuido (ESB) 116 para la comunicación. Un ESB 116 distribuido es agnóstico al lenguaje y la plataforma, y puede incluir cualquier bus de servicio empresarial que incluya, pero no limitado a, AMQP, NSQ, ZeroMQ, RabitMQ, Adeptia ESB Suite, IBM WebSphere ESB, Microsoft BizTalk Server y Oracle Enterprise Service Bus. Un ESB 116 entrega mensajes de manera confiable y, en la mayoría de las realizaciones, tiene un rendimiento muy alto. Generalmente, un bus de servicio empresarial monitoriza, enruta y resuelve la comunicación desde una variedad de dispositivos. Los dispositivos pueden incluir puntos 120 finales y plano 122 de datos. Los puntos finales incluyen dispositivos 120 de usuario final como servidores de estaciones de trabajo, ordenadores personales y dispositivos móviles como teléfonos celulares y tabletas. El plano 122 de datos incluye dispositivos que transportan tráfico de red, como cortafuegos, conmutadores y enrutadores 132. Además, el tráfico del plano de control al cortafuego, conmutadores, enrutadores 132 y otros dispositivos que forman parte del plano de control también se pasan a la Red de sistema de banda.

En algunas realizaciones, los mensajes en ESB 116 generalmente se dividen en corrientes separadas, a menudo llamados tópicos, cada uno con sus propias colas, de modo que los mensajes relacionado con un tópico no interfiere con los mensajes relacionados con otro tópico. La presente divulgación en una implementación de ejemplo utiliza tópicos para crear colas separadas en el ESB 116, de modo que los diferentes tipos de eventos procesados por los motores de puntuación, los mensajes pasados a diferentes componentes del sistema, los diferentes tipos de TIM, etc., tengan diferentes colas.

Los datos se pasan a la red del sistema fuera de banda para su procesamiento, análisis y visualización de dos formas principales: a través de los sensores 102 y a través de los actores 104 de ingesta. Los sensores 102 y los actores 104 de ingesta se analizan con más detalle a continuación. El procesamiento y análisis de los datos resulta en la creación de registros adicionales y (mensajes de inteligencia de amenazas) TIM, que se pasan a el ESB fuera de banda, y la creación de visualizaciones en tiempo real y diversos informes, todos los cuales se describen con más detalle. abajo.

Sensores 102.

Una forma en que los datos entran en el sistema es a través de sensores. Los sensores 102 capturan y procesan datos desde el plano 122 de datos empresariales y el plano 204 de control empresarial y pasan los datos a la red del sistema fuera de banda para su posterior procesamiento. Las tomas de red, que forman parte del sensor 102, se insertan en puntos clave para la visibilidad de la red y la duplicación del tráfico de la red para admitir procesos en tiempo real. El sensor 102 se describe con más detalle a continuación en la descripción que acompaña a las figuras 7 y 9. Brevemente, el sensor 102 procesa paquetes y genera registros y flujos asociados con los paquetes procesados.

En algunas realizaciones, hay al menos tres puertos: un puerto de datos entrantes, un puerto de datos salientes y un puerto de monitor. Todos los datos, o los datos seleccionados determinados por el sensor, se reflejan en el puerto del monitor. Los datos en el puerto del monitor se procesan para producir registros que se pasan al ESB 116 fuera de banda como se describe a continuación. En algunas realizaciones del sistema, también hay un cuarto puerto que proporciona información de comando y control al sensor y a la toma. El cuarto puerto se puede usar para cambiar qué datos se recopilan y procesan, así como para tomar ciertas medidas de mitigación, como no pasar a través de los paquetes del puerto de salida. Por ejemplo, los paquetes asociados con una IP particular, puerto, datos extraídos o característica computada pueden ser bloqueados.

La figura 3 es un diagrama de sistema que muestra tomas de red insertadas en diferentes partes de una red empresarial, de acuerdo con algunas realizaciones de la presente divulgación. I_0 302 es una toma 314 de red que se encuentra en la puerta de enlace de la empresa entre la red de la empresa y la Internet externa 320. I_0 302 es el punto de visibilidad en la toma 314 de red antes del cortafuegos 312 y se puede colocar en un interruptor 310 externo. I_0 302 es la interfaz que da hacia afuera de la infraestructura del cliente, y representa la primera oportunidad para utilizar modelos estadísticos y analíticos, y otras técnicas para detectar sondeos, intrusiones, reconocimiento de redes, ataques a la empresa y otros comportamientos por parte de malos actores; para comenzar el proceso de atribución (por ejemplo, identificar al actor detrás del comportamiento amenazador); y desarrollar respuestas apropiadas para detener o limitar el impacto del comportamiento. Tradicionalmente, la interfaz I_0 302 es el límite entre el exterior y el interior de la infraestructura de información. Normalmente, esta es la interfaz que da hacia afuera de toda la empresa, pero para estos fines, I_0 302 puede referirse a la interfaz de límite exterior, o la interfaz que da hacia afuera de cualquier infraestructura de información; Empresa, contenedor, nube o grupo de trabajo. I_0 302 es el punto donde los clientes generalmente implementan su protección de primera etapa, generalmente utilizando una Lista de control de acceso (ACL) del enrutador o una solución de cortafuegos comercial. Normalmente, estos dispositivos aplican una política de control de acceso conservadora (en su mayoría restrictiva) y representan el principal punto de protección para la infraestructura. Para muchos sitios, la interfaz I_0 302 también es un punto de Traducción de Direcciones de Red (NAT), que modifica las direcciones de paquetes para minimizar la exposición de los identificadores de infraestructura a entidades externas. Los tipos de comportamiento de mal actor visto en I_0 incluyen:

1) Intentos remotos de descubrir y penetrar las defensas externas;

2) Estrategias externas, pero locales, para penetrar en la infraestructura exterior;

3) Modificaciones de control de acceso externo mediado por expertos;

4) Acceso externo facilitado interno;

5) Ciberexplotación tradicional; y

6) Explotación basada en rootkit de infraestructura.

I_1 304 e I_2 306 son interfaces internas enfrentadas dentro de la empresa y la actividad cibernética anómala dentro de la empresa se denomina aquí como un ataque interno. I_1 304 es una toma 314 de red que se coloca entre el cortafuegos 312 empresarial y el resto de las redes empresariales internas. El aparato sensor I_2 306 permite la visibilidad del tráfico de red lateral dentro de la empresa. Los grifos de red I_2 306 están ubicados en los conmutadores 316 internos y pueden ver el tráfico a dispositivos, como servidores web, servidores empresariales, estaciones de trabajo, equipos de escritorio y otros dispositivos similares. I_3 308 es un dispositivo de red que puede procesar datos en el plano de control de la empresa. En general, en muchos despliegues del sistema, a excepción de las redes más simples, habrá múltiples sensores de los tipos I_2 306 e I_3 308. Para algunas redes complejas puede haber múltiples sensores de los tipos I_0 302 e I_1 304.

En algunas realizaciones, los datos y la actividad de I_0 302, I_1 304, I_2 306 e I_3 308 se correlacionan y califican continuamente para ordenar y controlar todas las redes y componentes empresariales a través de la interfaz del plano de control. El sensor 102 en conjunto con el motor 108 de puntuación y los modelos de comportamiento y RTAE 110 producen TIM, incluyendo la mitigación de TIM y los mensajes de actualización del modelo de TIM que se pasan a lo largo del ESB 116 y son consumidos por los componentes de red y de la empresa para admitir acciones de control y comando en tiempo real. Los ejemplos de los TIM de mitigación y los TIM de actualización de modelo que se usan en algunas realizaciones de la presente divulgación se describen a continuación. Brevemente, un ejemplo de un TIM de mitigación en algunas realizaciones de la presente divulgación es un mensaje para cerrar un puerto particular o aislar un dispositivo particular. Un ejemplo de una actualización de modelo TIM en algunas realizaciones de la presente divulgación es reducir el umbral de una alerta en un elemento de postprocesamiento de un flujo de trabajo de modelo de comportamiento basado en el comportamiento en la red empresarial. Con más detalle, el motor 108 de puntuación analiza una actualización modelo TIM, para identificar el componente apropiado del documento PFA a actualizar, como el valor del umbral en el elemento PFA apropiado en este ejemplo, y reemplaza el valor actual del umbral con el nuevo valor del umbral proporcionado en el modelo de actualización TIM. Otro ejemplo de una actualización de modelo TIM en algunas realizaciones de la presente divulgación es cambiar un coeficiente en un modelo analítico o un coeficiente en los componentes de PFA de preprocesamiento o posprocesamiento de un modelo analítico.

Los actores 104 de ingestión.

Una segunda forma en que los datos ingresan al sistema es mediante los actores 104 de ingesta. Los actores 104 de ingesta pueden diseñarse para procesar datos de aplicaciones de terceros (aplicaciones), fuentes y dispositivos 130. Aplicaciones de terceros (aplicaciones), fuentes y dispositivos 130 puede incluir otros componentes del sistema; archivos de registro producidos por estaciones de trabajo, servidores, dispositivos de red y otros dispositivos informáticos en las redes empresariales; corrientes de información producidos por otras aplicaciones de seguridad, incluidos los sistemas de seguridad basados en anfitrión; fuentes externas de datos de terceros, incluida información sobre amenazas, reputación de IP, información de zona de política de respuesta (RPZ) e información relacionada; otros sistemas con la misma arquitectura, ya sea en otras ubicaciones distribuidas geográficamente de la misma empresa o asociadas con otras empresas; y otros sistemas con una arquitectura diferente pero siguiendo un formato acordado para el intercambio de información.

Los actores 104 de ingesta reciben datos de entrada para procesar desde una de las fuentes descritas anteriormente o directamente desde el ESB 116. Después del procesamiento, los actores 104 de ingesta devuelven el evento procesado al ESB 116 para su procesamiento adicional por parte de otros componentes del sistema. Los actores 104 de ingesta reciben datos de entrada para procesar desde aplicaciones de terceros (aplicaciones), fuentes y dispositivos 130, y realizan el procesamiento de datos y las conversiones necesarias para que los datos de entrada puedan transmitirse al ESB 116, RTAE 110 o la plataforma 106 analítica distribuida para procesamiento adicional. En algunas realizaciones, el procesamiento en los actores 104 de ingesta implica tomar datos de entrada y convertir los datos de entrada en un formato adecuado de ingestión por ESB 116, RTAE 110, o plataforma 106 analítica distribuida.

Motor 108 de puntaje.

Un motor 108 de puntaje es un módulo que puede importar un modelo analítico (o un flujo de trabajo analítico) y toma datos de la red y de otros módulos del sistema. Una vez que se importa un modelo analítico, un motor de puntuación puede leer una corriente de datos y para cada evento en la corriente procesa el evento utilizando uno o más modelos analíticos, para producir resultados, incluidas puntuaciones, alertas y mensajes, así como información relacionada. El motor 108 de puntuación y los flujos de datos asociados con el motor 108 de puntuación se describen con más detalle a continuación en la descripción que acompaña a las figuras 7, 9 y 4.

Como se describió anteriormente, el motor 108 de puntuación es un módulo que puede puntuar datos con modelos estadísticos y de comportamiento a velocidades de red. Los modelos se pueden construir sin conexión a partir de datos históricos o de datos de transmisión. En algunas realizaciones, el motor 108 de puntuación puede emitir mensajes del motor de puntuación, tales como alertas, que contienen datos de metadatos y puntuaciones. En algunas realizaciones, el motor de puntuación cumple con PFA, como se describe con más detalle a continuación. El motor 108 de puntuación puede puntuar datos utilizando modelos estadísticos, predictivos y de minería de datos, como un modelo de agrupación, un modelo de referencia, una red bayesiana o un árbol de clasificación y regresión. Los modelos se pueden construir sin conexión en base a datos históricos. Los modelos también pueden ser modelos analíticos de transmisión, como se explica con más detalle a continuación.

La figura 4 es un diagrama de bloques que muestra un motor de puntuación de acuerdo con algunas realizaciones de la presente divulgación. La figura 4 muestra las entradas al motor 402 de puntuación, el documento 404 PFA, el motor 406 de ejecución de PFA, la información de estado almacenada para los modelos 408 analíticos, los TIM 410 de actualización de modelo y las salidas 412. Las entradas al motor 402 de puntuación pueden ser una corriente de eventos, o más en general, registros de datos. El motor 108 de puntuación procesa las entradas 402 utilizando el motor 406 de ejecución PFA. PFA es un lenguaje que describe cómo las entradas para analítica se transforman y se agregan para producir salidas analíticas. El motor de ejecución de PFA toma entradas al motor de puntuación y produce salidas siguiendo los procesos y procedimientos (también denominados flujos de trabajo analíticos) en el

documento 404 de PFA. Por ejemplo, un documento 404 de PFA puede describir un árbol de clasificación y regresión; el motor 406 de ejecución de PFA toma entradas para los árboles de clasificación y regresión y produce salidas del árbol de clasificación y regresión. El motor 108 de puntuación contiene información de estado almacenada para entidades y actualiza esta información de estado como se especifica en el documento PFA 404. En algunas realizaciones, para actualizar el procesamiento analítico, el motor 108 de puntuación importa un nuevo documento PFA 404.

En algunas realizaciones de la presente divulgación, el procesamiento analítico en el motor 108 de puntuación también puede actualizarse enviando uno o más TIM de actualización del modelo al motor 108 de puntuación, que actualiza los componentes apropiados de los documentos de PFA., según lo especificado por el TIM de actualización de modelo. Como se describió anteriormente, la actualización puede incluir un cambio a un valor de umbral o un coeficiente de un algoritmo que forma parte de un modelo analítico. Este tipo de actualización, a la que se hace referencia aquí como una pequeña actualización, puede ser aplicada por un motor de puntuación a un corriente de datos a mitad de la secuencia sin detener el procesamiento de datos por parte del motor de puntuación. También son posibles actualizaciones mayores, como cambiar un documento 404 completo de PFA.

Más generalmente, un motor 108 de puntuación en algunas realizaciones de la presente divulgación puede basarse en otros formatos de intercambio de modelos. Un formato de Intercambio de Modelo de ejemplo se basa en una especificación que permite actualizar la información del modelo al mismo tiempo que la puntuación de registros de datos del modelo, como la proporcionada por la política de lectura-copia-actualización admitida por celdas y grupos en la especificación PFA. La política de lectura-copia-actualización permite que el motor de puntuación lea el documento 404 PFA al mismo tiempo que la actualización de algunos componentes del documento. La puntuación casi en tiempo real, como se describe en algunas realizaciones del presente documento, se relaciona con la puntuación concurrente compatible de datos usando modelos con actualización concurrente de modelos. De manera más general, un Formato de Intercambio de Modelo de ejemplo para la presente divulgación se basa en una especificación para describir los modelos analíticos y el procesamiento analítico de datos mediante transformaciones y agregaciones que permite pasar los resultados de los modelos analíticos, transformaciones y agregaciones a las entradas de otros Modelos transformaciones y agregaciones analíticas.

Plataforma 106 analítica distribuida.

La plataforma 106 analítica distribuida o nube analítica es una plataforma informática distribuida que se puede usar para analizar grandes cantidades de datos y producir diversos resultados analíticos. La plataforma 106 analítica distribuida puede contener grandes cantidades de datos para el análisis, tanto utilizando un sistema de archivos distribuido, como Hadoop o MapR, o utilizando una base de datos no relacional (por ejemplo, NoSQL), como HBase, Accumulo, MapR-DB, etc. En algunas realizaciones de la presente divulgación, la plataforma 106 analítica distribuida es una plataforma informática distribuida que incluye soporte para MapReduce y cálculos iterativos de MapReduce, como los que Spark admite. La plataforma 106 analítica distribuida en algunas realizaciones de la presente divulgación, también incluye soporte para realizar cálculos iterativos con datos en disco, en memoria o en disco y en memoria, así como soporte para bases de datos NoSQL y otras aplicaciones y herramientas especializadas para trabajar con datos distribuidos en sistemas como Hadoop, MapR, Spark u otra plataforma informática distribuida. La plataforma 106 analítica distribuida también incluye una API basada en REST para que los diversos componentes del sistema puedan acceder a los datos e información en la plataforma 106 analítica distribuida de una manera uniforme, independiente del proceso, componente o analítica particular dentro de la plataforma analítica distribuida que produjo los datos o información.

La plataforma 106 analítica distribuida recibe los datos de los sensores 102 y los actores 104 de ingesta a través del ESB 116 distribuido. En algunas realizaciones de la presente divulgación, la plataforma 106 analítica distribuida también recibe datos directamente de los actores 104 de ingesta.

Hay varios tipos de salidas de la plataforma 106 analítica distribuida, que incluyen: mensajes de inteligencia de amenazas (TIM) que se envían al ESB 116, y del ESB 116 al motor 114 de plano de control; los datos y las estructuras de datos que describen las visualizaciones de los datos que se envían a la RTAE 110 (como se describe con más detalle a continuación), y desde la RTAE 110 al motor de visualización, la consola central y el monitor 112; flujos de trabajo analíticos, incluidos los modelos analíticos, descritos en formato portátil para análisis (PFA) (como se describe con más detalle a continuación), así como otros lenguajes que se pueden usar para describir modelos analíticos para el motor 108 de puntuación.

La plataforma 106 analítica distribuida recopila, limpia, integra y construye modelos de comportamiento a partir de grandes colecciones de datos de flujo (por ejemplo, corrientes de flujo de red y archivos de datos), datos de paquetes (por ejemplo, archivos PCAP) y archivos de registro de dispositivos de red, servidores, y otros dispositivos. El entorno está diseñado para algoritmos de aprendizaje basados en máquinas que pueden tardar de minutos a horas o más en ejecutarse. Los resultados son flujos de trabajo analíticos, que pueden incluir modelos de comportamiento, y TIM de plataforma analítica distribuida (también conocidos aquí como mensajes de plataforma analítica). En algunas realizaciones, el flujo de trabajo analítico contiene muchos modelos segmentados, cada uno asociado con un segmento lógico. En algunas realizaciones, el flujo de trabajo analítico contiene muchos flujos de trabajo segmentados,

cada uno asociado con un segmento lógico. En algunas realizaciones, este entorno está diseñado para científicos de datos y admite descubrimientos de nuevas amenazas y la producción de modelos analíticos para otros entornos.

La plataforma 106 analítica distribuida también puede incluir una infraestructura de máquina virtual que puede incluir máquinas virtuales para la contención de programa malicioso potencial. Los programas maliciosos se pueden ejecutar en una máquina virtual, que está aislada del marco de ciberseguridad. En algunas realizaciones, las máquinas virtuales incluyen contenedores de Linux.

Motor 110 analítico en tiempo real.

La RTAE 110 recibe datos de ESB 116 y la plataforma 106 analítica distribuida y realiza varias funciones, que incluyen realizar cálculos casi en tiempo real de datos derivados, agregados y transformados utilizando memoria distribuida y procesadores especializados, como GPU; creando visualizaciones casi en tiempo real de la actividad de la red, el comportamiento de las entidades empresariales, los usuarios y los flujos, las amenazas potenciales, los comportamientos correlacionados, etc.; y crear decisiones casi en tiempo real sobre las acciones de mitigación mediante el procesamiento de datos de múltiples motores de puntuación y otras fuentes. Algunos ejemplos de cómo crear decisiones en tiempo casi real sobre las acciones de mitigación se analizan en la descripción que acompaña a las Figuras 10 y 11. En algunas realizaciones, los datos recibidos de la plataforma 106 analítica distribuida incluye flujos de trabajo analíticos y mensajes analíticos distribuidos. En algunas realizaciones, RTAE 110 también recibe mensajes del motor de puntuación del flujo de trabajo analítico del motor de puntuación y las reglas de procesamiento de eventos de al menos una plataforma analítica distribuida, configuraciones configuradas por el usuario y resultados de sistemas analíticos de terceros. Las visualizaciones en tiempo casi real se pasan al motor de visualización, la consola central de mandos y el monitor 112 para su visualización. En algunas realizaciones, las decisiones en tiempo casi real sobre los eventos de mitigación se estructuran en mensajes de comando y control (C2) (por ejemplo, los TIM de mitigación), pasados al ESB 116, que son procesados por el motor 114 de plano de control, que a su vez toma diversos eventos o acciones de mitigación, como cerrar un puerto, modificar paquetes, bloquear una subred, bloquear uno o más Protocolos de Internet (IP) o rangos de IP, bloquear una o más IP internas o externas, controlar la transmisión de paquetes o flujos, desconectar al menos uno de un servidor y una estación de trabajo, crear al menos uno de un nuevo servidor virtualizado y una nueva estación de trabajo virtualizada a partir de una imagen protegida, bloquear una acción asociada con al menos uno del servidor y la estación de trabajo, etc. En algunas realizaciones, una acción de mitigación también puede incluir la eliminación de privilegios de autorización y acceso para una entidad asociada con una actividad anómala. La eliminación de la autorización y los privilegios de acceso pueden incluir al menos bloquear el acceso a la red, bloquear el acceso a los dispositivos de la red, bloquear el acceso a los servidores, bloquear el acceso a las estaciones de trabajo y bloquear el acceso a otros dispositivos informáticos. En algunas realizaciones, RTAE 110 está integrado con uno o más motores de puntuación en una sola aplicación.

En algunas realizaciones, RTAE 110 proporciona un entorno basado en GPU para gestionar un gran número de subprocesos de computación en paralelo para análisis en tiempo real. Todos los actores computacionales también pueden aprovechar una base de datos RTAE para ejecutar tareas de procesamiento de datos a gran escala casi en tiempo real para análisis sofisticados. RTAE 110 incluye un motor estadístico en tiempo real para resumir el estado de la empresa en el motor de visualización, la consola central y el monitor 112; y un motor en tiempo real para procesar los TIM desde múltiples sensores 102, calcular la acción de mitigación adecuada, si corresponde, y enviar el TIM adecuado (incluido el puntaje, alerta, actualización, acción de mitigación, etc.). La RTAE 110 también incluye una API basada en REST, de modo que los diversos componentes del sistema pueden acceder a los datos e información en la RTAE 110 de manera uniforme, independientemente del particular, analítica particular, proceso o componente dentro de la RTAE 110 que produjo los datos o información. Debido al volumen de datos y los cálculos en tiempo casi real requeridos, los procesadores especializados que pueden procesar grandes bloques de datos en paralelo, como las GPU utilizadas en algunas realizaciones de la presente divulgación, se utilizan en el RTAE 110.

El RTAE 110 también puede enviar mensajes de comando y control (C2) llamados mensajes de inteligencia de amenazas (TIM) a otros componentes en el marco de ciberseguridad. Por ejemplo, el RTAE 110 realiza una amplia gama de acciones basadas en eventos, como la actualización de análisis, visualizaciones y alertas, acciones de mitigación para el plano de control y actualizaciones de sensores distribuidos, etc. Los agentes de flujo administrados por el RTAE 110 de manera similar brindan la inteligencia para la gran variedad de agentes que permiten las solicitudes de publicación y suscripción y qué metacanales están relacionados con tópicos específicos, tipos y conceptos.

En algunas realizaciones de la presente divulgación, la RTAE 110 produce TIM de mitigación enviados desde uno o más modelos de comportamiento. En algunas realizaciones, los TIM se envían al ESB 116 mediante motores 108 de puntuación. El RTAE 110 recopila los diversos TIM, se procesa, integra y alimenta a otro modelo, que, dependiendo de los resultados del nuevo modelo, puede dar como resultado una mitigación. En algunas realizaciones, un RTAE 110 comunica un TIM de mitigación a través de ESB 116 a uno o más agentes 210 de mitigación, el TIM de mitigación que incluye instrucciones para tomar medidas de mitigación específicas, como cerrar un puerto.

La figura 5 es un diagrama de flujo que ilustra un método de procesamiento y envío de mensajes por el motor analítico en tiempo real, de acuerdo con algunas realizaciones de la presente divulgación.

Con referencia a la etapa 502, uno de los RTAE 110 recibe un primero o más mensajes, como los TIM, de uno o más motores de puntuación, la plataforma analítica distribuida u otros componentes del sistema. Como se describe con más detalle en este documento, el primer mensaje puede incluir un TIM generado por el motor de puntuación o la plataforma analítica distribuida. El TIM puede incluir datos asociados con una alerta o con realizar una pequeña modificación en un documento de PFA. RTAE 110 también puede recibir flujos de trabajo analíticos del motor analítico distribuido y el flujo de trabajo analítico y las reglas de procesamiento de eventos. En algunas realizaciones, el flujo de trabajo analítico y las reglas de procesamiento de eventos pueden especificar umbrales asociados con modelos analíticos o flujos de trabajo analíticos. Por ejemplo, un flujo de trabajo analítico y una regla de procesamiento de eventos pueden especificar que todas las actividades relacionadas con un determinado flujo de trabajo analítico con puntuaciones más allá de un cierto umbral se clasifiquen como actividades anómalas. Como se describe aquí, la actividad anómala puede incluir un reconocimiento, una explotación, una intrusión, un compromiso, una amenaza interna y un ataque.

Con referencia a la etapa 504, la RTAE 110 procesa el TIM recibido utilizando los flujos de trabajo analíticos y las reglas de procesamiento de eventos y flujo de trabajo analítico. En algunas realizaciones, la información de la entidad se recupera del TIM, la información de estado asociada se recupera del RTAE 110, y la información del estado se actualiza con la información extraída del TIM recibido. En algunas realizaciones, la información de estado almacenada está asociada con mensajes recibidos previamente de al menos uno de los sensores, motores de puntuación y la plataforma analítica distribuida.

Con referencia a la etapa 506, RTAE 110 puede tomar las siguientes acciones según el procesamiento: i) transmitir un mensaje de difusión, ii) transmitir una actualización del modelo a un motor de puntuación cuando la RTAE 110 determina que es probable que un modelo actualizado mejore la tasa de detección o reducir la tasa de falsos positivos del modelo actual; iii) transmitir una acción de mitigación utilizando el motor del plano de control y los agentes de mitigación cuando el RTAE 110 determina que el TIM recibido indica una intrusión o una posible intrusión u otra actividad anómala; iv) transmitir un modelo analítico cuando los cambios en un flujo de trabajo analítico superan un umbral; y v) esperar para recibir los TIM adicionales. En algunas formas de realización, el procesamiento de RTAE 110 también incluye analizar la información de estado actualizado para determinar si se debe tomar alguna acción. En algunas realizaciones, RTAE 110 puede enviar un mensaje de difusión, un mensaje de mitigación y un mensaje de actualización de un modelo después de recibir una primera salida una primera vez de los motores de la puntuación, la plataforma analítica distribuida y la pluralidad de sensores. En algunas realizaciones, RTAE 110 espera recibir varias salidas de los motores de puntuación, la plataforma analítica distribuida y la pluralidad de los sensores antes de enviar un mensaje de difusión, mensaje de mitigación y mensaje de actualización del modelo.

Como se describió anteriormente, RTAE 110 puede transmitir uno de un TIM de mitigación, un TIM de actualización del modelo y un modelo analítico basado en el procesamiento. Por ejemplo, un TIM recibido por un RTAE 110 que indica una posible intrusión en un puerto detectado por un sensor y un motor de puntuación asociado al puerto puede dar lugar a que se envíe un TIM de mitigación, que cerrará el puerto. Al mismo tiempo, RTAE 110, basado en el mismo TIM recibido, puede enviar a todos los motores de puntuación una actualización del modelo cambiando un parámetro en los motores de puntuación para tener en cuenta mejor la intrusión o los efectos relacionados con la intrusión. Si el RTAE 110 determina que un motor de puntuación u otro componente del sistema requiere un cambio más significativo que una cantidad umbral de cambio, el RTAE 110 puede enviar un modelo de comportamiento actualizado en lugar de la actualización del modelo. En algunas realizaciones, RTAE 110 también puede enviar un mensaje de difusión, que puede incluir al menos uno de un mensaje ciberevento y un mensaje de alerta.

Motor 114 plano de control.

El motor 114 del plano de control se refiere a la supervisión, configuración y reconfiguración de dispositivos de red, incluidos conmutadores, enrutadores y cortafuegos. El motor 114 del plano de control es responsable de tomar medidas de mitigación, comunicarse con los agentes de mitigación, enviar alertas relacionadas con el plano de control y suministrar datos para que el motor de visualización, la consola central y el monitor 112 puedan proporcionar información sobre la situación de la infraestructura del plano de control. La conciencia situacional en este contexto se refiere a la información que proporciona un resumen de las entidades en el plano de control; tráfico actual en el plano de control; el tráfico normal en el plano de control; desviaciones, si las hay, entre el tráfico actual y el tráfico normal; y otra información relacionada con actividades inusuales, actividades asociadas con potenciales malos actores o comportamiento relacionado. En algunas realizaciones, el motor 114 de plano de control obtiene los TIM de mitigación de RTAE 110, el motor 108 de puntuación y la plataforma 106 analítica distribuida.

El motor 114 de plano de control incluye actores de cálculo C2 que generan mensajes de comando y control en tiempo real. Las acciones preplanificadas se administran en todo el plano de control y el plano de datos, como bloquear direcciones IP específicas, aislar una estación de trabajo sospechosa o redireccionar flujos de paquetes.

El motor 114 de plano de control incluye DNS, DHCP y gestión de direcciones IP (DDI) 140. El módulo 140 DDI incluye un gráfico de dispositivo global, un ID de protocolo de confianza dentro de los flujos de control y las huellas digitales del dispositivo y el flujo. El gráfico global de dispositivos incluye una representación visual de todos los dispositivos y actividades de la red. El ID de protocolo de confianza dentro de los flujos de control incluye cadenas cifradas dentro

de paquetes. Las huellas digitales del dispositivo y del flujo son administradas por el plano de control y utilizan el protocolo de conexión de anfitrión dinámico (DHCP) para la huella digital única de todos los dispositivos en la red.

Otros componentes del sistema.

Otros componentes del sistema incluyen un registro (no mostrado) al que pueden acceder todos los componentes. En algunas realizaciones, el registro incluye datos de alta disponibilidad acerca de los servicios, las estructuras de datos, los formatos de mensajes y otra información que se utilizan comúnmente y que simplifica el desarrollo y el funcionamiento del sistema.

Modelado de comportamiento y puntuación en tiempo real

En algunas formas de realización de la presente divulgación, se utilizan modelos de comportamiento para cuantificar la probabilidad de ciberintrusiones, la presencia de actores malos (ya sean actores externos o “conocedores”), y otros comportamientos que garanticen una acción, ya sea el examen manual por un ciberanalista o la acción automatizada de un dispositivo de mitigación.

En la presente divulgación, un modelo de comportamiento se refiere a una estadística, minería de datos u otro tipo de algoritmo que toma entradas (o “eventos”), procesa las entradas para calcular características y procesa las características para calcular salidas (o “puntuaciones”). Los eventos como se describen en este documento generalmente se refieren a una corriente de entradas ordenadas temporalmente que se procesan una por una.

Las Figuras 6A-C, 7 y 8 son diagramas de sistema que muestran diferentes maneras en que los eventos pueden presentarse mediante modelos de comportamiento, de acuerdo con algunas realizaciones de la presente divulgación.

Para los análisis en tiempo real o casi en tiempo real, los eventos se presentan evento por evento y se pueden calificar evento por evento para producir resultados de diversas maneras. La figura 6A es un diagrama de flujo que muestra el procesamiento de entradas o eventos directamente, de acuerdo con algunas realizaciones de la presente invención. Los atributos 602 de datos se usan para producir las características 604. En algunas realizaciones, las características 604 se forman al transformar o agregar atributos de datos. Por ejemplo, si el atributo de datos corresponde a un registro de flujo, un ejemplo de una característica puede incluir una variable binaria que es igual a 1 cuando el flujo es un flujo de corta duración, y 0 de lo contrario. Las características 604 son a su vez procesadas por un modelo 606 para producir salidas 608 modelo. La figura 6B es un diagrama de flujo que muestra la asociación de uno o más vectores de características (también referidos aquí como vectores de estado) con cada evento, de acuerdo con algunas realizaciones de la presente divulgación. Se recibe 610 un evento y los atributos de datos se determinan para el evento 612. Los atributos de datos se usan para producir características para el evento 614. Cuando se procesa un nuevo evento, el vector de característica almacenado asociado o los vectores de característica, que son persistentes del evento para el evento, se recuperan y actualizan con los datos del nuevo evento 616. Después de que el(los) vector(es) de características se actualice 618, se usa como entrada para un modelo 620 de comportamiento para producir salidas 622. Un ejemplo de un vector de características que se actualiza con cada evento es un número normalizado de flujos en una ventana de tiempo específica (por ejemplo, dentro de una ventana de tiempo de movimiento de 10 segundos). La figura 6C es un diagrama de flujo que ilustra el preprocesamiento 638 y el posprocesamiento 640 de un modelo analítico, de acuerdo con algunas realizaciones de la presente divulgación. El preprocesamiento de datos 638 transforma o agrega los datos, crea vectores de características y realiza otro procesamiento como se desee, antes de pasar los datos a un modelo 630 analítico. El postprocesamiento 640 transforma y agrega, calcula salidas adicionales y realiza otro procesamiento según se requiera. Como ejemplo de postprocesamiento, un módulo de postprocesamientor puede compilar y evaluar varias estadísticas para determinar si el modelo ha visto suficientes eventos para ser considerado estadísticamente válido. Si es estadísticamente válido, se envía el puntaje; De lo contrario, se suprime la puntuación. Para los métodos que se muestran en las Figuras 6A, 6B y 6C, se pueden usar varios modelos, con las salidas de uno o más modelos siendo utilizadas, como entradas para uno o más modelos, como se describe con más detalle a continuación en la descripción que acompaña a las Figuras 8A, 8B y 8C.

Para el procesamiento por lotes de datos en análisis, las entradas se reúnen en un archivo, o múltiples archivos, y los archivos se procesan para producir los resultados asociados con los modelos analíticos. Como se mencionó anteriormente, para los tamaños de datos que son típicos en aplicaciones cibernéticas, se utiliza una plataforma analítica distribuida para el procesamiento analítico.

Los modelos en sí mismos que se utilizan para procesar eventos para producir salidas también se pueden producir de diferentes maneras. Como se muestra a continuación en las Figuras 7 y 9, se puede usar una plataforma 106 analítica distribuida para procesar las entradas a los modelos para producir el modelo analítico. En algunas realizaciones de la presente divulgación, el modelo se expresa en un formato de intercambio de modelo, como PFA, cuando luego se puede usar para calificar eventos en lotes utilizando una plataforma analítica distribuida, o en forma de corriente mediante un motor de puntuación. En una de las realizaciones de la presente divulgación, los modelos PFA también pueden ser producidos por otros dos componentes del sistema: el RTAE y el propio motor de puntuación.

La figura 7 es un diagrama de sistema que muestra el procesamiento del tráfico de red para producir modelos analíticos, de acuerdo con algunas realizaciones de la presente divulgación. La figura 7 muestra el tráfico de red 702, el registro de eventos y el archivo. constructor 704, repositorio 706 de modelos PFA, procesador 708 de paquetes, puntajes 710, información del análisis de lotes de datos de eventos 712, eventos 720, modelos PFA importados 722, flujo de red enriquecido y archivos 724 PCAP, modelos PFA exportados 726, sensor 102, plataforma 106 analítica distribuida, y motor 108 de puntuación.

El tráfico de la red 702 es recogido por el sensor 102. El sensor 102 incluye el procesador 708 de paquetes, que está diseñado para procesar paquetes de datos a la velocidad de la línea (es decir, la velocidad a la que los datos se mueven a través de la red). El procesador 708 de paquetes puede procesar paquetes de datos a la velocidad de la línea utilizando pilas de software altamente optimizadas y, en algunas realizaciones de la presente divulgación, hardware especializado. En algunas realizaciones, se usa una técnica de copia cero para mejorar el rendimiento del procesamiento de paquetes. El procesamiento de paquetes incluye la extracción de atributos de paquetes, como puertos de origen y destino e IP, indicadores de protocolo y otros atributos de paquetes TCP, paquetes UDP, etc., buscando combinaciones de atributos extraídos para identificar protocolos específicos y enriqueciendo la información con otros datos, como los datos del Protocolo de configuración dinámica de anfitrión (DHCP), los datos de geolocalización, etc. La información de varios paquetes correspondientes a las mismas IP y puertos de origen y destino se procesan para producir registros de flujo por el registro de eventos y el constructor 704 de archivos que se pasan al motor 108 de puntuación a través del ESB 116. En algunas realizaciones de la presente divulgación, la información de paquetes únicos o múltiples se procesa para producir otros tipos de eventos que se pasan al motor 108 de puntuación a través del ESB 116. Por ejemplo, en algunas realizaciones de la presente divulgación, cada paquete puede puntuarse individualmente por el motor 108 de puntuación; los paquetes seleccionados, como los correspondientes a uno o más tipos de protocolo, u otro atributo o característica, pueden puntuarse; El motor 108 de puntuación puede procesar otras combinaciones de paquetes. El registro de eventos y el constructor 704 de archivos también procesan paquetes múltiples para producir archivos de paquetes (archivos PCAP) que se pasan a la plataforma 106 analítica distribuida. En algunas realizaciones de la divulgación actual, el sensor 102 procesa datos en colaboración con un motor de entidad. La función del motor de la entidad es enriquecer los eventos de flujo y los archivos PCAP con identificadores de entidad únicos, ya que las direcciones IP a menudo cambian dentro de los entornos empresariales que utilizan DHCP.

El sensor 102 transmite los eventos 720 al motor 108 de puntuación para la puntuación en tiempo real sobre un ESB 116. En algunas realizaciones, el motor 108 de puntuación lee un archivo PFA 722 de un repositorio 706 de modelos PFA que contiene una descripción de varios modelos, cómo preprocesar las entradas a los modelos, cómo postprocesar las salidas de los modelos, cómo componer los modelos, cómo enviar eventos a los modelos segmentados, etc. En algunas realizaciones, un archivo PFA 722 importado puede expresar un flujo de trabajo analítico. En algunas realizaciones, el flujo de trabajo analítico contiene múltiples flujos de trabajo analíticos segmentados, cada uno asociado con un segmento lógico. Por ejemplo, la figura 8A muestra cómo se pueden combinar los resultados de múltiples modelos analíticos para producir una salida única, mientras que la figura 8B muestra cómo la salida de un modelo analítico se puede utilizar como entradas para dos o más modelos analíticos. Los modelos analíticos incluyen, pero no se limitan a los modelos de clúster, los modelos de referencia, los árboles de clasificación y regresión, las redes neuronales, los bosques aleatorios, los modelos bayesianos y cualquiera de los otros modelos analíticos estadísticos y de aprendizaje automático conocidos por los expertos en el campo. El motor 108 de puntuación convierte los puntajes de cada evento y crea múltiples tipos de TIM, incluidos los TIM que contienen puntajes, notificación de eventos o notificación de alerta, TIM de actualización del modelo y los TIM 710 de mitigación. En algunas realizaciones, el motor 108 de puntuación puede crear características de evento adicionales a partir de Información recibida del evento. En algunas realizaciones, el sensor 102 está controlado por la RTAE 110, que puede cambiar el tipo de paquetes y flujos recopilados, cómo los eventos y flujos son procesados por el sensor, etc.

El sensor 102 también transmite registros de flujo de red y archivos 724 PCAP a la plataforma 106 analítica distribuida. Los datos transmitidos por el sensor pueden enriquecerse agregando al menos uno de: datos y metadatos sobre entidades observadas, datos y metadatos sobre el tráfico de red, datos y metadatos asociados con usuarios, datos y metadatos sobre estaciones de trabajo y servidores, datos y metadatos sobre enrutadores y conmutadores, datos y metadatos sobre entidades de red externas, y datos y metadatos sobre dispositivos internos y externos que interactúan con la red. La plataforma 106 analítica distribuida procesa la información recibida de múltiples maneras, incluido el uso de algoritmos estadísticos, algoritmos de aprendizaje automático y otros algoritmos para construir modelos analíticos que pueden ejecutarse mediante el motor de puntuación. El procesamiento de la información recibida de múltiples maneras como se describe anteriormente es un ejemplo del procesamiento por lotes de datos de eventos, datos de flujo y otros datos mencionados en otra parte de esta divulgación. El análisis de los datos procesados de esta manera puede conducir a información sobre el cibercomportamiento 712, como la presencia de un comportamiento inusual o sospechoso. Estos modelos se pueden exportar como un formato de intercambio de modelos, por ejemplo, los modelos PFA 726 a un repositorio 706 de modelos PFA. El motor 108 de puntuación recibe los modelos PFA, que se agregan a las colecciones existentes de modelos PFA, lo que modifica la colección de documentos PFA a los que se accede por el motor 108 de puntuación para procesar los eventos. La plataforma 106 analítica distribuida también puede calificar los eventos en el lote 712.

En algunas realizaciones de la presente divulgación, las entradas pueden ser registros de flujo de red producidos por el sensor 102, registros de paquetes producidos por el sensor 102, registros extraídos por el sensor 102 de archivos de registro de dispositivos de red, estaciones de trabajo, servidores, etc. u otros sistemas, o registros extraídos a través de algún otro mecanismo.

En algunas realizaciones de la presente divulgación, las entradas son eventos que están asociados con entidades, como dispositivos de red, usuarios, etc., y las entradas se procesan mediante la recuperación de uno o más vectores de estado que almacenan información persistente para esa entidad, actualizando el vector de estado usando la información del evento, y luego usando el vector de estado de actualización como entrada al modelo.

En algunas realizaciones de la presente divulgación, y como se describió anteriormente con respecto a la figura 2, uno o más sensores 102 recopilan y procesan datos de la empresa que está siendo protegida, producen registros basados en eventos, pasan los registros basados en eventos a el ESB 116 del sistema y uno o más motores 108 de puntuación leen los registros basados en eventos del ESB 116 y procesan los registros basados en eventos para producir diversas salidas.

En algunas realizaciones de la presente divulgación, los modelos analíticos se implementan en motores 108 de puntuación para detectar el cibercomportamiento y los cambios en el cibercomportamiento a la velocidad de la línea a medida que se procesan los datos de la red. Los modelos analíticos desplegados en motores de puntuación se pueden utilizar para muchos casos de uso diferentes en una ciberred. Por ejemplo, un modelo analítico en un motor 108 de puntuación se puede usar para detectar cambios inesperados en dispositivos de red, estaciones de trabajo, servidores, etc. Los cambios inesperados se pueden definir de varias maneras, incluyendo, por ejemplo, los cambios en los patrones de comunicación de los dispositivos. En las redes ("comunidades de interés"). En este caso, se pueden utilizar diferentes tipos de modelos, incluidos los modelos de referencia, para detectar cambios. El uso de modelos de referencia para detectar cambios también se puede emplear para detectar amenazas en movimiento interna o lateral. El motor 108 de puntuación también se puede utilizar para acumular comportamientos sospechosos en todas las fuentes. Por ejemplo, ciertos flujos pueden ocurrir por la noche desde ciertos países. Si también se encuentra que algunos de estos flujos están asociados con intentos fallidos de inicio de sesión, entonces el riesgo asociado con todos estos flujos sería elevado. Cuando la puntuación de riesgo supera un umbral, se envía una alerta.

En algunas realizaciones de la presente divulgación, múltiples modelos están presentes y se pueden combinar de diferentes maneras. La figura 8A es un diagrama de sistema que muestra un conjunto de modelos, de acuerdo con algunas realizaciones de la presente divulgación. Los modelos 1 802 analíticos a n 804 se combinan para obtener un puntaje 806 de salida único. Los modelos analíticos se pueden combinar utilizando promedios, votaciones o cualquier otro método de combinación de los modelos. Por ejemplo, la votación se utiliza para combinar salidas categóricas de varios modelos (correspondientes a una sola entrada), en la cual la categoría que aparece con mayor frecuencia como la salida de los modelos se selecciona como la salida del conjunto. La figura 8B es un diagrama de sistema que muestra una composición o encadenamiento de modelos, de acuerdo con algunas realizaciones de la presente divulgación. La salida del modelo 1 810 analítico se puede alimentar como entradas al modelo 2a 812 analítico y al modelo 2b 814 analítico. Las salidas de los modelos 2a y 812 y 2b 814 analíticos se pueden usar como entradas al modelo 3 816 analítico. En algunas realizaciones, el modelo 1 810 analítico, el modelo 2a 812 analítico, el modelo 2b 814 analítico y el modelo 3 816 analítico pueden ser cualquier modelo. Por ejemplo, los modelos no están restringidos a un subconjunto particular de modelos. Los modelos se pueden encadenar en cualquier configuración. La figura 8C es un diagrama de sistema que muestra modelos segmentados, de acuerdo con algunas realizaciones de la presente divulgación. Cada modelo 820, ... 822 está asociado con una clave única para distinguir los segmentos. Como los modelos en general serán diferentes entre los diferentes segmentos, el mismo evento de entrada creará múltiples salidas diferentes, correspondientes a los diversos modelos diferentes, asociadas con los diversos segmentos.

En algunas realizaciones de la presente divulgación, se usa el Formato Portátil para Análisis (PFA), ya que admite los tres tipos de modelos múltiples mencionados anteriormente, mientras que otros Formatos de Intercambio de Modelos (MIF), como el Lenguaje de Marcado de Modelos Predictivos (PMML), solo admite tipos limitados de composición de modelos, no un encadenamiento arbitrario de las salidas de uno o más modelos en las entradas de uno o más modelos, como es, por ejemplo, el soportado por PFA.

En algunas realizaciones de la presente divulgación, se usa un productor modelo que exporta un documento MIF que se importa a uno o más motores de puntuación. En algunas realizaciones del sistema, el documento MIF se envía a través del ESB 116 a los motores 108 de puntuación y, en algunas realizaciones, el documento MIF se carga en el motor 108 de puntuación a través de otro mecanismo, incluida una red fuera de banda que vincula la plataforma 106 analítica distribuida a los motores 108 de puntuación. En algunas realizaciones, el documento MIF es un documento PFA.

En algunas formas de realización de la presente divulgación, hay varios tipos diferentes de TIM que son salidas de los modelos. Estos incluyen: i) puntuaciones asociadas con eventos de entrada que se almacenan para un análisis potencial en el futuro; ii) puntuaciones asociadas con los eventos de entrada que se envían para su procesamiento posterior; iii) TIM de actualización de modelo; y iv) TIM de mitigación.

Actualización de modelos de comportamiento.

La figura 9 es un diagrama de flujo que representa el flujo de datos entre los componentes en el marco de la ciberseguridad, de acuerdo con algunas realizaciones de la presente divulgación.

Como se describe brevemente más arriba y con más detalle a continuación, RTAE 110 y los módulos y agentes del motor del plano de control pueden tomar medidas de mitigación. Por ejemplo, el modelo analítico en el motor 108 de puntuación se puede actualizar de una de cuatro maneras. Primero, se puede crear un nuevo modelo analítico en un trabajo analítico por lotes y exportarlo en un formato 902 de intercambio de modelo. En algunas realizaciones de la presente divulgación, el trabajo analítico por lotes se ejecuta en la plataforma 106 analítica distribuida y se exporta como PFA. El trabajo de análisis de lotes utiliza como datos de entrada de los sensores 102, como datos de flujo de red, datos PCAP y datos de otros sistemas y sensores. En segundo lugar, se puede crear un nuevo modelo analítico casi en tiempo real utilizando el RTAE y exportado en un formato 904 de intercambio de modelo. En algunas realizaciones de la presente divulgación, el RTAE 110 exporta el modelo como PFA. Tercero, los cambios en el modelo en sí pueden realizarse a través de un TIM 410 de actualización de modelo. Un TIM 410 de actualización de modelo puede incluir información para que los valores, variables y elementos de PFA particulares en el documento de PFA puedan actualizarse sin reemplazar todo el documento de PFA. Dado que los documentos de PFA pueden ser de gran tamaño, la capacidad de actualizar valores y elementos específicos utilizando un TIM de actualización del modelo que es el resultado del procesamiento de TIM y otra información del RTAE 110 contribuye a la velocidad a la que se procesan los datos. En cuarto lugar, los parámetros del modelo analítico en sí pueden actualizarse en caso de que el modelo sea un modelo de transmisión en el que los parámetros u otros componentes del modelo 914 (frente a la información de estado asociada con entidades) se actualicen cuando se procesan 908 los eventos. El modelo de transmisión en este contexto es un modelo analítico que se construye a partir de datos que se procesan solo una vez a medida que pasan por el motor de puntuación. Esto contrasta con los modelos analíticos que se construyen con análisis por lotes, como se describió anteriormente, en los cuales los registros de datos se conservan en el disco, como el disco asociado con la plataforma 106 analítica distribuida, y se pueden leer y procesar tantas veces como el algoritmo particular o analítico lo requiera.

Como se describió anteriormente, en algunas realizaciones, los sensores 102 reciben eventos de entrada del tráfico de la red. El tipo de eventos de entrada puede incluir eventos de paquetes de red, eventos de flujos de red, eventos de sistemas de monitorización, eventos de archivos de registro y eventos de otros sistemas y aplicaciones. También como se describe anteriormente, una salida del motor 108 de puntuación puede incluir los TIM. En algunas realizaciones, los TIM pueden incluir puntajes asociados con eventos que se almacenan para un análisis potencial en el futuro, puntajes asociados con eventos que se envían para procesamiento dinámico adicional, TIM de actualización de modelos y TIM de mitigación.

Un elemento de la presente divulgación es que los motores 108 de puntuación múltiples, los sensores 102 múltiples u otros componentes del sistema pueden enviar mensajes al ESB 116 de manera concurrente y los motores 102 de puntuación pueden actualizarse de manera simultánea. En algunas realizaciones de la presente divulgación, existen múltiples motores 108 de puntuación, que leen los TIM de actualización del modelo. En otras palabras, se pueden utilizar múltiples sensores 102 con los TIM de actualización de modelo enviados a través del ESB 116 para actualizar simultáneamente un motor 108 de puntuación; un solo sensor 102 puede enviar los TIM de actualización del modelo a través del ESB 116 para actualizar simultáneamente varios motores de puntuación; o múltiples sensores y múltiples motores de puntuación pueden enviar los TIM de actualización del modelo para actualizar simultáneamente múltiples motores 108 de puntuación utilizando múltiples sensores 102. En algunas realizaciones, el sistema descrito aquí incluye solo un motor 108 de puntuación conectado a múltiples sensores 102.

En algunas realizaciones de la presente divulgación, el motor 108 de puntuación está diseñado para que los TIM de actualización del modelo puedan procesarse simultáneamente con la puntuación de eventos por parte del motor de puntuación, de modo que no sea necesario detener el motor de puntuación para actualizarlo con un TIM de actualización de modelo. Esta capacidad de procesar cambios en los documentos de PFA al mismo tiempo que el motor 108 de puntuación puntúa los eventos existe porque el estándar de PFA contiene componentes de lenguaje que admiten la concurrencia como se describió anteriormente. En algunas realizaciones de la presente divulgación, la implementación del motor 108 de puntuación admite los diversos elementos de concurrencia admitidos por el estándar PFA.

El RTAE 110 procesa los TIM y los eventos de los motores 102 de puntuación y otros módulos del sistema y determina las acciones de mitigación. Los TIM que contienen acciones de mitigación se envían a los agentes de mitigación, que realizan las acciones de mitigación, que, en algunas realizaciones, utilizan el plano de control para cambiar los dispositivos de red de control, como los enrutadores y los conmutadores. En algunas realizaciones, el RTAE 110, los motores 108 de puntuación y los módulos del sistema relacionados están en un ESB 116 que se ejecuta en la red del sistema fuera de banda.

Un componente de la presente divulgación actual es el soporte para un marco analítico que puede usar múltiples modelos que se pueden combinar de diferentes maneras, incluyendo lo siguiente: i) modelos segmentados, en los cuales las entradas se envían a uno o más de los modelos individuales, con cada modelo asociado con una o más

restricciones, como el período de tiempo especificado, un segmento de red específico, etc.; ii) conjuntos, en los cuales las entradas a los modelos son comunes y las salidas de dos o más modelos se combinan en una sola salida; o, iii) composiciones de modelos, en las que la salida de uno o más modelos se utiliza como entrada de otro modelo.

En algunas realizaciones, los modelos deben ser reconstruidos o reentrenados periódicamente para tener en cuenta las condiciones cambiadas, como un nuevo comportamiento o una mejora en la tecnología de modelado. Cuando se crea un nuevo modelo, se pueden comparar los nuevos modelos con los modelos actuales para elegir un ganador (por ejemplo, utilizando metodologías de campeón-desafiador).

En algunas realizaciones, el proceso es legible y auditable por humanos. Los modelos también se pueden actualizar de forma incremental. Esto permite que los modelos se muevan a producción y se construyan a partir de datos en vivo en lugar de esperar suficientes datos históricos de entrenamiento válidos y apropiados.

Además de los tipos de TIM ya mencionados, un componente importante de la presente divulgación es el uso de TIM externos. Los TIM externos, como se describe en la presente divulgación, se refieren a los TIM generados fuera de la empresa por otras empresas que emplean instancias de los sistemas o instancias de otros sistemas que generan TIM que pueden interoperar con los TIM utilizados por el sistema descrito en la presente divulgación.

Los TIM externos funcionan como se describió anteriormente, con la excepción de que los TIM externos correspondientes a otras instancias del sistema descrito en la presente divulgación no contienen ninguna información de identificación de la empresa que los generó, sino información tal como información sobre IP externas nuevos umbrales o componentes para documentos de PFA, nuevas reglas de postprocesamiento, etc. que pueden compartirse entre dos empresas más que ejecutan el sistema descrito en la presente divulgación.

En algunas formas de realización de la presente divulgación, los RTAE 110 de la primera empresa crean TIM externos cifrado antes de pasar de la primera empresa a la segunda empresa; descifrado por la segunda empresa; Pasado al RTAE 110 de la segunda empresa. Después de ser recibido por el RTAE 110 de la segunda empresa, el TIM externo se procesa de manera similar a la forma en que se procesan los TIM internos.

Los RTAE 110 de las empresas que los reciben pueden procesar automáticamente los TIM externos y, a diferencia de otros tipos de información de amenazas compartida entre empresas, no están diseñados para el procesamiento manual.

En algunas realizaciones de la presente divulgación, los TIM externos pueden ser generados por otros sistemas utilizando convenciones y estándares elaborados por las diversas empresas que comparten TIM externos. Por ejemplo, los TIM pueden contener un umbral de cambio de información para ciertos tipos de alertas, como las asociadas con movimientos laterales dentro de una empresa o la exfiltración de datos fuera de una empresa. Cuando una empresa que acepta y envía TIM externos detecta una amenaza de uno de estos tipos, puede generar automáticamente un TIM externo que puede enviarse a otras empresas que aceptan TIM externos, que a su vez pueden procesar el TIM externo y tomar medidas para reducir los umbrales para el ataque observado por la primera empresa.

Análisis de transmisión.

En algunas realizaciones de la presente divulgación, se utilizan análisis de transmisión dentro del motor 108 de puntuación para actualizar los parámetros del modelo, las características utilizadas en el modelo o la estructura del propio modelo, en lugar de solo actualizar los estados asociados a entidades que son puntuadas por el modelo. En algunas realizaciones de la presente divulgación, cuando se recibe un primer puntaje en el postprocesamiento, se compilan y evalúan varias estadísticas para determinar si el modelo ha visto suficientes eventos como para ser considerado estadísticamente válido. Si es estadísticamente válido, se envía el puntaje; De lo contrario, se suprime la puntuación.

Por ejemplo, la varianza u otros atributos estadísticos de las distribuciones asociadas con una o más características en el modelo pueden calcularse y cuando estas estadísticas caen por debajo de un umbral, el modelo puede emitir puntuaciones.

Microsegmentos para Ciberanálisis

En algunas realizaciones, una empresa puede dividirse, incluidas las entidades internas y externas que interactúan con la empresa, en segmentos lógicos que pueden modelarse, monitorizarse y mitigarse de manera independiente. Los segmentos lógicos también se mencionan aquí como microcibersegmentos. Como se describe a continuación, cada segmento lógico puede asociar: i) al menos uno de un modelo analítico, un conjunto de modelos analíticos o un flujo de trabajo analítico; ii) una o más fuentes de entradas sobre la actividad dentro del segmento lógico (por ejemplo, puntos de contacto); y un conjunto de acciones para mitigar el impacto de la actividad anómala que ocurre dentro del segmento lógico.

La presente descripción en algunas realizaciones hace uso de miles a cientos de miles o más de microcibersegmentos. En algunas realizaciones de la presente divulgación, se utilizan diferentes formas de dividir una empresa en microcibersegmentos, dependiendo del cibercomportamiento de interés, el modelo analítico que se utiliza y la mitigación que se utiliza. En otras palabras, en algunas formas de realización, se utilizan al mismo tiempo diferentes microcibersegmentos, a menudo superpuestos.

Un microcibersegmento se define al dividir una empresa utilizando una o más dimensiones. Las dimensiones se pueden definir utilizando los atributos de la red, incluyendo IP, segmento de red; atributos de los dispositivos que se están modelando, incluido el tipo de dispositivo, etc.; características de la red o dispositivo, como el número de flujos durante una ventana de tiempo específica, la cardinalidad del gráfico creado cuando un dispositivo se comunica con otro dispositivo, etc.; características de los flujos asociados con un dispositivo, como el tipo de protocolo utilizado, etc.; atributos y características de las entidades internas y externas que interactúan con la red, incluido el tipo de usuario, el rol del usuario, etc.; Dimensiones temporales, como la hora del día, el día de la semana, etc.

Se puede crear un microcibersegmento utilizando una dimensión y creando diferentes segmentos al dividir la dimensión en diferentes regiones; o tomar el producto de dos o más dimensiones, y dividir por separado cada dimensión para crear segmentos multidimensionales.

Una vez que se realiza la partición en diferentes segmentos, se calcula un modelo analítico separado para los datos asociados con las entidades en ese segmento. Para que esto se haga, algunas realizaciones utilizan sensores que monitorizan datos relevantes para entidades, usuarios o flujos asociados con ese segmento y recopilan y procesan los datos.

Además de monitorizar y modelar un microcibersegmento, se definen una o más acciones de mitigación para ese segmento. Las acciones de mitigación pueden incluir una lista negra de las entidades asociadas con ese segmento para que los conmutadores y enrutadores ya no envíen datos a las entidades en ese segmento; lista negra de ciertos puertos asociados con las entidades en ese segmento; modificando los datos que fluyen hacia adentro y fuera del segmento; redireccionar el tráfico hacia o desde el segmento; reiniciar las entidades asociadas con dispositivos en el segmento desde una instalación limpia; utilizando técnicas de virtualización o técnicas de objetivos móviles para aumentar la seguridad de las entidades, etc.

Uno de los criterios para decidir sobre la segmentación apropiada es crear segmentos que sean lo suficientemente homogéneos en su comportamiento ciberanalítico para que puedan modelarse con un modelo analítico. Por ejemplo, los segmentos pueden dividirse hasta que la varianza u otros atributos estadísticos de las distribuciones asociadas con una o más características u otros componentes de los modelos en un segmento caigan por debajo de un umbral y sean estables a lo largo del tiempo. En algunas realizaciones, las divisiones pueden incluir una división de la red, una división del tráfico en la red, una división de usuarios en la red, una división de dispositivos en la red, una división basada en otros datos, incluidos datos de terceros. y los datos asociados con al menos una de las divisiones de la red, el tráfico en la red, los usuarios de la red, los dispositivos en la red y los datos de terceros. En algunas realizaciones, una o más divisiones pueden superponerse con otra división.

En algunas realizaciones de la presente divulgación, los modelos analíticos asociados con cada microcibersegmento se expresan en un formato de intercambio de modelo, como PFA, y se usa un motor de puntuación para que los microcibersegmentos puedan monitorizarse a la velocidad de la línea y los eventos de mitigación pueden enviarse casi en tiempo real a medida que los eventos son puntuados por el motor de puntuación.

Defensa de objetivo móvil utilizando entornos virtuales

En algunas realizaciones, el RTAE 110 incluye un módulo de defensa virtual (VDM) 150 que se integra con microcibersegmentos para crear, administrar y eliminar entornos virtuales, incluidas sus redes virtuales correspondientes. Las redes virtuales asociadas con estos entornos virtuales, incluida la información de enrutamiento de I_0 y I_1 a I_2, como se describe anteriormente en la figura 3. El módulo 150 de defensa virtual recibe el ID I_0 y el ID I_1. Como se mencionó anteriormente, la ID I_0 incluye datos recibidos de forma externa a un cortafuegos, e ID I_1 incluye los datos recibidos internamente a un cortafuegos. En algunas formas de realización, ID es un ID cifrado, inmutable, globalmente único (GUID) para todos los paquetes de red y datos dentro del marco de ciberseguridad, que permite a las máquinas separar de manera única la actividad “permitida” de la actividad “sospechosa”. La ID puede permitir que los entornos paralelos del mundo real y el mundo virtual funcionen simultáneamente, además de su gestión, visualización, análisis, alertas, etc. La ID permite que las referencias y el análisis únicos se basen en el historial completo de todos los paquetes que ingresan al marco de ciberseguridad en todo su procesamiento e historial de utilización. En algunas formas de realización, los activadores de eventos se habilitan para mitigaciones preplaneadas a la velocidad de la máquina cuando se detectan paquetes de ID (por ejemplo, movimiento lateral, cambios de infraestructura no autorizados, VPN no autorizadas, falsificación, etc.).

En algunas realizaciones, el módulo 150 de defensa virtual utiliza máquinas virtuales seguras o contenedores virtuales con ID para crear y gestionar entornos físicos y virtuales “de confianza” y “no de confianza” para la complejidad dinámica. De esta manera, se puede crear una “superficie de ataque virtual” para identificar actividades sospechosas.

Esto obliga al atacante a distinguir los datos y procesos empresariales reales (“confiables”) de cientos a decenas de miles de entornos virtuales (“no confiables”) que reducen dramáticamente la probabilidad de que un atacante tenga éxito y aumentan la probabilidad de detección y mitigación. La infraestructura DDI también se puede utilizar para manipular flujos de paquetes e interconexiones dentro y entre las redes y componentes del mundo real y virtual. El módulo 150 de defensa virtual puede redirigir dinámicamente desde el plano de control activo sospechoso a entornos virtuales específicos para acciones preplanificadas activadas por el motor de puntaje. Las relaciones de confianza se pueden habilitar entre el contenedor, su contenido y el marco, extendiendo así los usos de gestión de accedo de identidad (IDAM) y control de acceso basado en atributo (ABAC) para el control de acceso basado en políticas a todos los procesos de datos y máquinas dentro del marco de ciberseguridad.

Ejemplo de detección y mitigación

La figura 10 es un diagrama de sistema que ilustra una respuesta a una amenaza externa al marco de ciberseguridad, de acuerdo con algunas realizaciones de la presente divulgación. El proceso incluye un mal actor 1006 externo que inicia un ataque, el sensor 102/motor 1 1002 de puntuación detecta una amenaza y publica un TIM 1005, RTAE 110 recibe un mensaje y decide sobre la mitigación y publica al ESB 116, el motor 114 del plano de control recibe una acción de mitigación (MA) 1003 dentro del TIM 1008 de mitigación, los sensores 102 y el motor 2 1004 de puntuación recibe el TIM 906 de actualización de modelo y el estado de actualización, y el motor 114 de plano de control toma medidas al cerrar el puerto. El motor 1 1002 de puntuación y el motor 2 1004 de puntuación tienen una funcionalidad similar a la del motor 108 de puntuación descrito aquí.

En la etapa 1011, el ataque iniciado por el mal actor 1006 externo pasa por alto las reglas de la lista de control de acceso (ACL) de IDS y cortafuegos y pasa a través del cortafuegos 132.

En la etapa 1012, el sensor 102 procesa paquetes y fluye desde la amenaza 1006 externa. El motor 1 1002 de puntuación genera el TIM 1005 cuando detecta un evento de amenaza. El motor 1 1002 de puntuación publica un evento de amenaza y TIM 1005 a ESB 116 distribuido.

En la etapa 1013, RTAE 110 recibe el evento de amenaza y el TIM enviado por el ESB 116. RTAE 110 procesa el TIM 1005 desde el motor 1 1002 de puntuación, y RTAE 110 decide la mitigación en función del TIM 1005.

En la etapa 1014, la RTAE 110 decide la mitigación. RTAE 110 publica uno de un TIM 906 de actualización de modelo y un TIM 1008 de mitigación para todos los elementos conectados en ESB 116.

En la etapa 1015, el motor 114 de plano de control recibe un TIM 1008 de mitigación asociado con los cambios de reputación de IP que dan como resultado acciones tales como el bloqueo de la IP o el puerto o los analistas de alerta de actividad anómala. El motor 114 de plano de control realiza la acción 1003 de mitigación cerrando el puerto utilizado por el actor 1006 externo.

En la etapa 1016, el motor 2 1004 de puntuación y otros motores de puntuación conectados en el ESB 116 reciben un TIM 906 de actualización de modelo de RTAE 110 y cambian su comportamiento de puntuación para detectar mejor los actores malos que emplean un comportamiento similar.

La figura 11 es un diagrama de sistema que ilustra una respuesta y una amenaza interna al marco de ciberseguridad, de acuerdo con algunas realizaciones de la presente divulgación. El proceso incluye un mal actor 1106 interno que inicia un ataque, el sensor 102/motor de puntuación 1 1102 detecta una amenaza y publica un TIM 1005, el mensaje RTAE 110 recibe un mensaje, la RTAE 110 decide la mitigación y publica en el ESB 116, el motor 114 del plano de control recibe un TIM 1008 de mitigación, sensores 102/motor 2 1104 de puntuación recibe el TIM 906 de actualización de modelo y actualiza el estado, y el plano de control del motor 114 toma el puerto de cierre de acción. El motor de puntuación 1 1102 y el motor 2 1104 de puntuación tienen una funcionalidad similar a la del motor 108 de puntuación descrito aquí.

En la etapa 1111, un actor 1106 interno inicia el reconocimiento de la red (por ejemplo, el reconocimiento de activos críticos) dentro de la red de la empresa.

En la etapa 1112, el sensor 102 procesa paquetes y flujos asociados con la amenaza interna. El motor 1102 de puntuación crea eventos a partir de los paquetes y flujos y envía un TIM 1005 a ESB 116.

En la etapa 1113, la RTAE 110 procesa el TIM 1005 enviado por el ESB 116. En la etapa 3, la RTAE 110 decide la mitigación en función de la TIM. La RTAE 110 publica el TIM 1008 de mitigación sobre el ESB 116 para controlar el plano 114 del motor y para todas las entidades afiliadas a las acciones de mitigación en el plano 122 de datos, como cortafuegos, enrutadores, conmutadores 132 o puntos 120 finales como estaciones de trabajo, servidores o dispositivos móviles.

En la etapa 1114, el TIM de mitigación se envía al ESB 116.

En la etapa 1115, el motor 114 del plano de control recibe el TIM 1008 de mitigación. El motor 114 del plano de control toma medidas al cerrar el puerto utilizado por el mal actor 1106 interno.

En la etapa 1116, el motor 2 1104 de puntuación (y cualquier otro motor de puntuación en ESB 116) recibe el TIM 906 de actualización de modelo de RTAE 110 y cambia su comportamiento de puntuación para detectar mejor a los actores malos con un comportamiento similar.

La materia objeto descrita en el presente documento puede implementarse en circuitos electrónicos digitales, o en software de ordenador, firmware o hardware, incluidas las estructuras divulgadas en esta memoria descriptiva y sus equivalentes estructurales, o en combinaciones de ellas. 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 programa, software, aplicación de software o código) se puede escribir en cualquier forma de lenguaje de programación, incluidos los lenguajes compilados o interpretados, y se pueden desplegar 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 porción 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 porciones 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, incluyen los pasos del método de la materia objeto descrita en este documento, pueden ser realizados por uno o más procesadores programables que ejecutan uno o más programas de ordenador para realizar funciones de la materia objeto descrita en este documento operando en los datos de entrada y generando salida. Los procesos y flujos lógicos también pueden ser realizados por, y el aparato de la materia objeto descrita aquí puede implementarse como, circuitos lógicos 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, incluyendo multiprocesadores, tales como GPU, 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 acoplado 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, o discos ópticos. Los portadores de información adecuados para incorporar instrucciones e información de programas informáticos 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, la materia objeto descrita aquí se puede implementar en un ordenador que tenga un dispositivo de visualización, por ejemplo, una pantalla LCD (pantalla de cristal líquido), un LED (diodo emisor de luz), OLED (diodo emisor de luz orgánica). o CRT (tubo de rayos catódicos), para mostrar información al usuario y un teclado y un dispositivo señalador (por ejemplo, un ratón o una bola de seguimiento), mediante los cuales el usuario puede proporcionar información al ordenador. 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, del habla o táctil.

La materia objeto descrita en este documento puede implementarse en un sistema de computación que incluye uno o más componentes de “back-end” (por ejemplo, un servidor de datos), componentes de “middleware” (por ejemplo, un servidor de aplicaciones) o componentes de “front-end” (por ejemplo, un ordenador de cliente que tiene una interfaz gráfica de usuario o un navegador de red a través del cual un usuario puede interactuar con una implementación de la materia objeto descrita aquí), o cualquier combinación de dichos componentes de “back-end”, “middleware” y “front-end”, ya sea en hardware físico, en entornos virtuales, o el uso de tecnología basada en contenedores para desplegar aplicaciones, como los contenedores de Linux. Los componentes del sistema pueden interconectarse mediante 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 establecidos en la siguiente descripción o ilustrados en los dibujos. La materia objeto divulgada es capaz de otras realizaciones y de ser practicada y llevada a cabo de diversas 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 objeto 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 alcance de la materia objeto divulgada.

Aunque la materia objeto divulgada se ha descrito e ilustrado en las realizaciones de ejemplo 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 de la materia objeto divulgada se realizará sin apartarse del alcance de la materia objeto divulgada, que está limitada únicamente por las reivindicaciones que siguen.

REIVINDICACIONES

1. Un sistema de ciberseguridad para procesar eventos para producir puntajes, alertas y acciones de mitigación, el sistema que comprende:

una pluralidad de sensores, cada uno de los cuales está configurado para:

recibir datos de sensores de una red,

procesar los datos de sensores para formar eventos y transmitir los eventos;

una plataforma (106) analítica distribuida, la plataforma (106) analítica distribuida configurada para:

recibir los eventos de la pluralidad de sensores,

procesar los eventos para formar flujos de trabajo analíticos y mensajes de plataforma analítica distribuida, cada uno de los mensajes de plataforma analítica distribuida asociados con al menos uno de una alerta, una actualización de un primer modelo analítico, e información de cibercomportamiento, cada uno de los flujos de trabajo analíticos:

asociado con uno o más segmentos lógicos, e

incluye al menos uno del primer modelo analítico, un segundo modelo analítico, una regla, una transformación de datos y una agregación de datos, y

transmitir los flujos de trabajo analíticos y los mensajes distribuidos de la plataforma analítica;

una pluralidad de motores (108) de puntuación, y cada uno de la pluralidad de motores (108) de puntuación está configurado para:

recibir los flujos de trabajo analíticos de la plataforma (106) analítica distribuida,

recibir los eventos de al menos uno de la pluralidad de sensores,

procesar los eventos recibidos utilizando los flujos de trabajo analíticos para producir mensajes del motor de puntuación y transmitir los mensajes del motor de puntuación; y

un motor analítico en tiempo real, el motor analítico en tiempo real configurado para:

recibir los flujos de trabajo analíticos de la plataforma (106) analítica distribuida,
recibir el flujo de trabajo analítico y las reglas de procesamiento de eventos,
recibir los mensajes del motor de puntuación de la pluralidad de motores (108) de puntuación,
recibir los mensajes de la plataforma analítica distribuida de la plataforma (106) analítica distribuida, y
procesar los mensajes del motor de puntuación y los mensajes de la plataforma analítica distribuida utilizando los flujos de trabajo analíticos de la plataforma (106) analítica distribuida y las reglas de procesamiento de eventos y flujo de trabajo analítico para formar un mensaje de inteligencia de amenazas, en el que el mensaje de inteligencia de amenazas comprende al menos uno de:

un mensaje de difusión, el motor analítico en tiempo real configurado para transmitir el mensaje de difusión,
un mensaje de mitigación, el motor de análisis en tiempo real configurado para transmitir el mensaje de mitigación a un motor de plano de control para realizar una acción de mitigación asociada con un primer segmento lógico de uno o más segmentos lógicos cuando el procesamiento por el motor analítico en tiempo real indica que la acción de mitigación limita el impacto de la actividad anómala, y
un mensaje de actualización del modelo, el motor analítico en tiempo real configurado para transmitir el mensaje de actualización del modelo para actualizar uno o más flujos de trabajo analíticos cuando el procesamiento por el motor analítico en tiempo real indica que el mensaje de actualización del modelo mejora al menos uno de una tasa de detección de la actividad anómala y una reducción en una tasa de falsos positivos,

cada uno de los uno o más segmentos lógicos que asocian:

al menos uno del primer modelo analítico, el segundo modelo analítico, un tercer modelo analítico, un conjunto de modelos analíticos y un flujo de trabajo analítico,
una o más fuentes de entradas acerca de la actividad dentro del segmento lógico, y
un conjunto de acciones para mitigar un impacto de la actividad anómala que ocurre dentro del segmento lógico.

2. El sistema de la reivindicación 1, en el que al menos uno de:

La pluralidad de los sensores, la pluralidad de los motores (108) de puntuación, la plataforma (106) analítica distribuida, el motor analítico en tiempo real y el motor de plano de control están conectados utilizando una red fuera de banda y/o
la pluralidad de los sensores, la pluralidad de motores (108) de puntuación, la plataforma (106) analítica distribuida, el motor analítico en tiempo real y el motor del plano de control se comunican mediante el envío de mensajes asociados a través de un bus del sistema empresarial.

3. El sistema de la reivindicación 1, que comprende un módulo de actores (104) de ingesta, el módulo de actores (104) de ingesta configurado para:

recibir datos de aplicación de terceros a partir de al menos una de una aplicación de tercera y un dispositivo de terceros, y
transmitir los datos de aplicación de terceros para procesamiento adicional por al menos uno de la pluralidad de motores de puntuación, la plataforma (106) analítica distribuida y el motor analítico en tiempo real, y opcionalmente en donde:

la pluralidad de sensores, la pluralidad de motores (108) de puntuación, la plataforma (106) analítica distribuida, el motor analítico en tiempo real, el motor del plano de control y el módulo de actores (104) de ingesta están conectados mediante una red de banda, y/o
la pluralidad de sensores, la pluralidad de motores de puntuación, la plataforma (106) analítica distribuida, el motor analítico en tiempo real, el motor del plano de control y el módulo de actores (104) de ingesta se comunican mediante el envío de mensajes asociados a través de un bus del sistema empresarial.

4. El sistema de la reivindicación 1, en el que el motor (108) de puntuación está configurado además para:

recibir los mensajes de actualización del modelo, y procesar los mensajes de actualización simultáneamente con el procesamiento de los eventos.

5. El sistema de la reivindicación 1, en el que para formar al menos uno de los mensajes de difusión, el mensaje de mitigación y el mensaje de actualización del modelo, el motor de análisis en tiempo real está configurado además para:

recibir una primera salida por primera vez de al menos uno de la pluralidad de motores (108) de puntuación, la plataforma (106) analítica distribuida y la pluralidad de sensores;
recuperar la primera información de estado correspondiente a la primera salida;
actualizar la primera información de estado con los primeros datos de salida;
procesar la primera información de estado actualizada mediante un flujo de trabajo analítico asociado con el motor analítico en tiempo real para formar la información de primer estado procesada actualizada;
almacenar la primera información de estado actualizada procesada en el motor analítico en tiempo real;
recibir una segunda salida en un segundo momento de al menos uno de la pluralidad de motores (108) de puntuación, la plataforma (106) analítica distribuida y la pluralidad de sensores;
recuperar la segunda información de estado correspondiente a la segunda salida;
actualizar la segunda información de estado con segundos datos de salida;
procesar la segunda información de estado actualizada mediante el flujo de trabajo analítico asociado con el motor analítico en tiempo real para formar la segunda información de estado actualizada procesada;
formar el al menos uno del mensaje de difusión, el mensaje de mitigación y el mensaje de actualización del modelo en función de la segunda información de estado actualizada procesada; y
almacenar la información de segundo estado actualizada procesada en el motor analítico en tiempo real y, opcionalmente, en el que el motor analítico en tiempo real está además configurado para:

recibir una salida interina en un tercer momento desde al menos uno de la pluralidad de motores (108) de puntuación, la plataforma (106) analítica distribuida y la pluralidad de sensores, en donde la tercera vez es posterior a la primera vez y antes de la segunda vez;
recuperar información de estado interino correspondiente a la salida interina;
actualizar la información de estado interino con datos de salida interinos;
procesar la información de estado interina actualizada mediante el flujo de trabajo analítico asociado con el motor analítico en tiempo real para formar información de estado interina actualizada procesada; y
almacenar la información de estado interina actualizada procesada en el motor analítico en tiempo real.

6. El sistema de la reivindicación 1, en el que los flujos de trabajo analíticos comprenden un documento en formato de intercambio de modelos, en el que el documento en formato de intercambio de modelos admite:

una composición de modelos analíticos;
una segmentación de modelos analíticos;
un conjunto de modelos analíticos;
una composición de modelos analíticos con reglas;

una composición de modelos analíticos con etapas de preprocesamiento y posprocesamiento, en la que las etapas de preprocesamiento y posprocesamiento incluyen transformaciones de datos y agregaciones de datos; y
los flujos de trabajo analíticos, cada uno de los cuales comprende además composiciones de al menos uno de los modelos analíticos, las reglas, las transformaciones de datos, las agregaciones de datos, las segmentaciones y los conjuntos.

7. El sistema de la reivindicación 1, en el que al menos uno de:

el motor analítico en tiempo real está además configurado para transmitir un modelo de comportamiento actualizado a uno o más de la pluralidad de motores (108) de puntuación cuando los cambios en uno o más de los flujos de trabajo analíticos exceden un umbral;
Los eventos comprenden al menos uno de los datos sobre flujos de red, datos sobre paquetes, datos sobre entidades, datos sobre usuarios, datos sobre estaciones de trabajo y servidores, datos sobre enrutadores y conmutadores, datos sobre entidades de red externas y datos sobre dispositivos internos y externos que interactúan con la red;
uno o más de la pluralidad de sensores y la pluralidad de motores (108) de puntuación están integrados en una sola aplicación; y/o
el motor analítico en tiempo real está integrado con uno o más de la pluralidad de motores (108) de puntuación.

8. El sistema de la reivindicación 1, en el que la acción de mitigación comprende al menos uno de:

cerrar al menos un puerto,
modificar al menos un paquete de datos,
controlar la transmisión de paquetes o flujos,
bloquear una subred,
bloquear uno o más (IP) internos o externos,
tomar al menos uno de un servidor y una estación de trabajo fuera de línea,
crear al menos uno de un nuevo servidor virtualizado y una nueva estación de trabajo virtualizada a partir de una imagen protegida, y
bloquear una acción asociada con al menos uno del servidor y la estación de trabajo.

9. El sistema de la reivindicación 1, en el que la actividad anómala comprende al menos uno de reconocimiento, explotación, intrusión, compromiso, amenaza interna y ataque; y opcionalmente, en donde:

la acción de mitigación comprende al menos uno de:

modificar al menos un paquete de datos, controlar la transmisión de paquetes o flujos, y eliminar los privilegios de autorización y acceso para una entidad asociada con la actividad anómala, en donde la eliminación de privilegios de autorización y acceso comprende al menos uno de bloquear el acceso a la red, bloquear el acceso a los dispositivos de la red, bloquear el acceso a los servidores, bloquear el acceso a las estaciones de trabajo y bloquear el acceso a otros dispositivos informáticos, y/o
la actividad anómala está asociada con al menos uno de un actor interno y un mal actor externo.

10. El sistema de la reivindicación 1, que comprende además un motor de visualización, el motor de visualización que incluye un monitor, el motor de visualización configurado para:

recibir estadísticas e imágenes gráficas asociadas con el procesamiento de los mensajes del motor de puntuación por el motor analítico en tiempo real; y
mostrar las estadísticas e imágenes gráficas en el monitor.

11. El sistema de la reivindicación 1, configurado para intercambiar un mensaje externo de inteligencia de amenazas con un sistema de terceros compatible, en el que:

el mensaje de inteligencia de amenazas externo está cifrado para proporcionar un mecanismo seguro para transferir información;
la información en el mensaje de inteligencia de amenazas externa no expone información interna sensible sobre el sistema que transmite el mensaje de inteligencia de amenazas externa; y
el mensaje de inteligencia de amenazas externo está formateado con un Formato de intercambio de modelos común.

12. El sistema de la reivindicación 1, en el que la plataforma (106) analítica distribuida está configurada además para recibir los mensajes del motor de puntuación y procesar los mensajes del motor de puntuación para formar mensajes de inteligencia de amenaza, y/o
en el que el mensaje de difusión comprende al menos uno de un mensaje de información, un mensaje ciberevento y un mensaje de alerta.

13. El sistema de la reivindicación 1, en el que cada uno de la pluralidad de segmentos lógicos está asociado con al menos uno de una división de la red, una división del tráfico en la red, una división de usuarios en la red, una división

de dispositivos en la red, una división basada en datos de terceros, y datos asociados con al menos una de las divisiones de la red, el tráfico en la red, los usuarios en la red, los dispositivos en la red y los datos de terceros; y opcionalmente en donde al menos una primera división se solapa con al menos una segunda división, y además opcionalmente

en donde la pluralidad de sensores, la pluralidad de motores (108) de puntuación, la plataforma (106) analítica distribuida, el motor analítico en tiempo real y el motor del plano de control se comunica mediante el envío de mensajes asociados a través de un bus de sistema empresarial.

14. Una red de ciberseguridad que comprende una pluralidad de los sistemas de ciberseguridad de la reivindicación 1, en donde cada uno de los sistemas de ciberseguridad está configurado para intercambiar un mensaje de inteligencia de amenazas seleccionado con uno o más de los otros sistemas de ciberseguridad, en donde:
el mensaje de inteligencia de amenazas seleccionada es cifrado para proporcionar un mecanismo seguro para transferir información, en el que la información en el mensaje de inteligencia de amenaza seleccionado no expone información interna sensible sobre el sistema de ciberseguridad de transmisión.

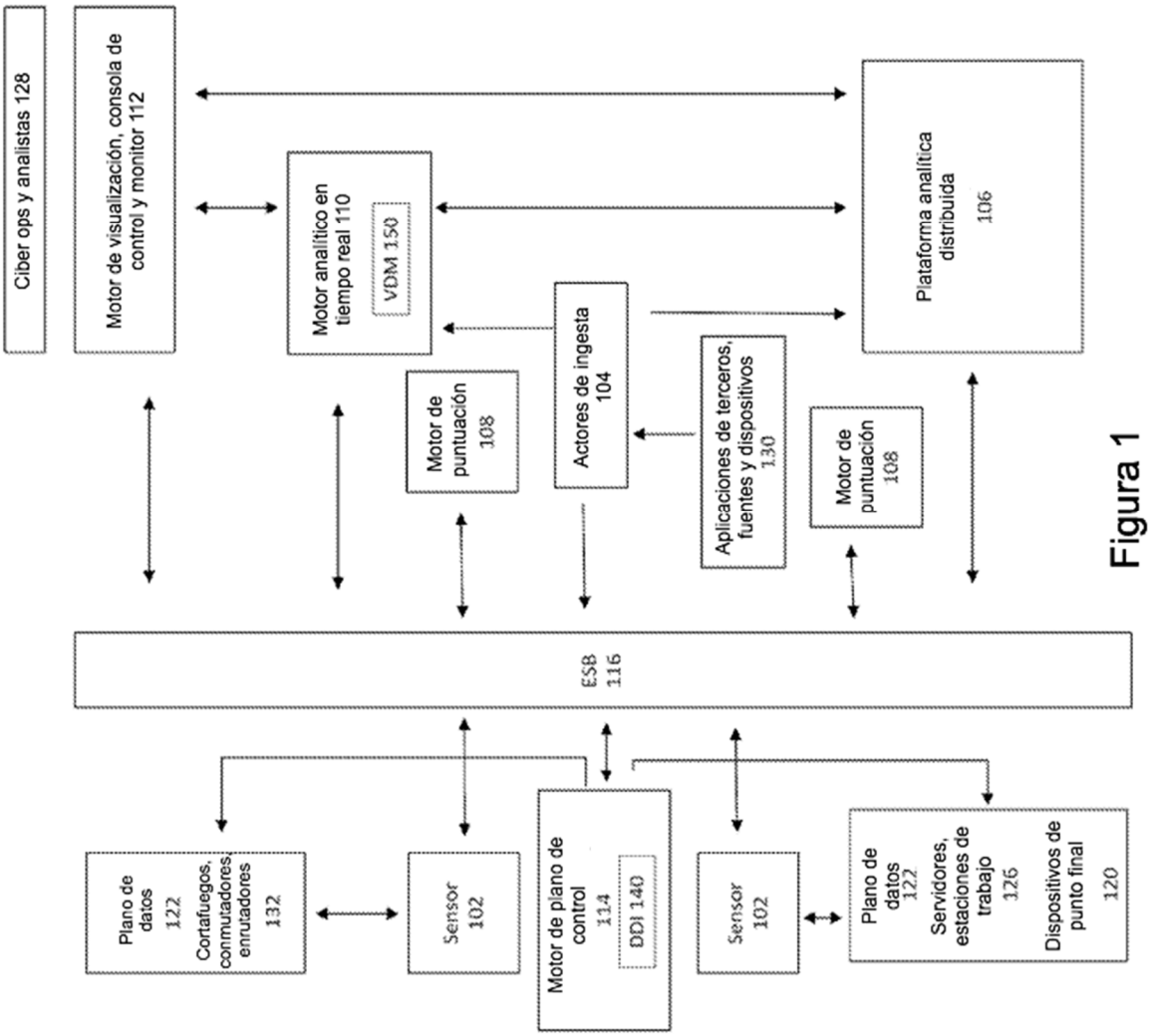
Ciber ops y analistas 128
Motor de visualización, consola de control y monitor 112
Motor analítico en tiempo real 110
VDM 150
Plataforma analítica distribuida 106
Motor de puntuación 108
Actores de ingesta 104
Aplicaciones de terceros, fuentes y dispositivos 130
Motor de puntuación 108
ESB 116
Plano de datos 122 Cortafuegos, conmutadores, enrutadores 132
Sensor 102
Motor de plano de control 114
DDI 140
Sensor 102
Plano de datos 122 Servidores, estaciones de trabajo 126 Dispositivos de punto final 120

Figura 1

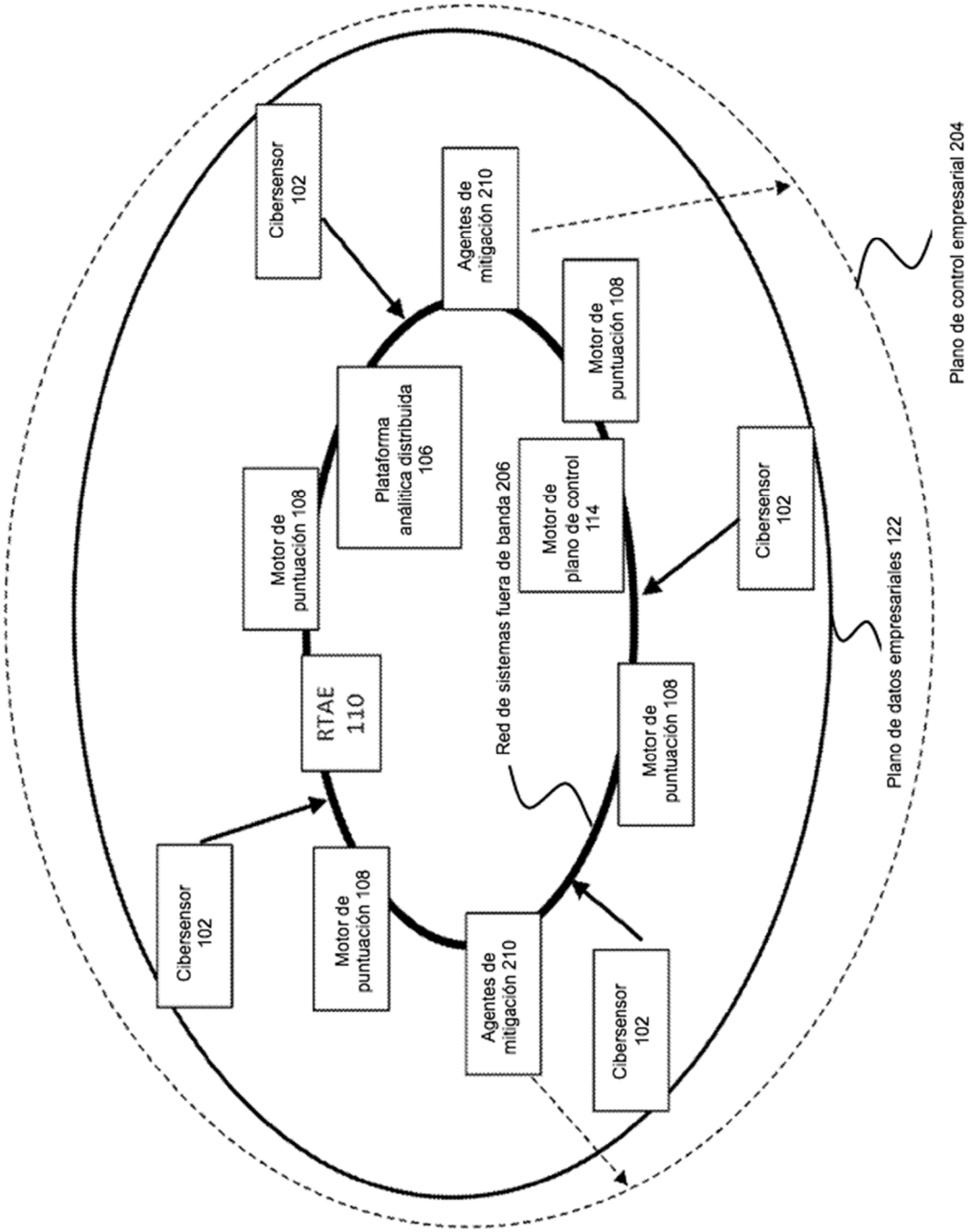
Cibersensor 102
Agentes de mitigación 210
Motor de puntuación 108
Plataforma analítica distribuida 106
Motor de puntuación 108
Motor de plano de control 114
Cibersensor 102
RTAE 110
Red de sistemas fuera de banda 206
Motor de puntuación 108
Cibersensor 102
Motor de puntuación 108
Agentes de mitigación 210
Cibersensor 102
Plano de control empresarial 204
Plano de datos empresariales 122

Figura 2

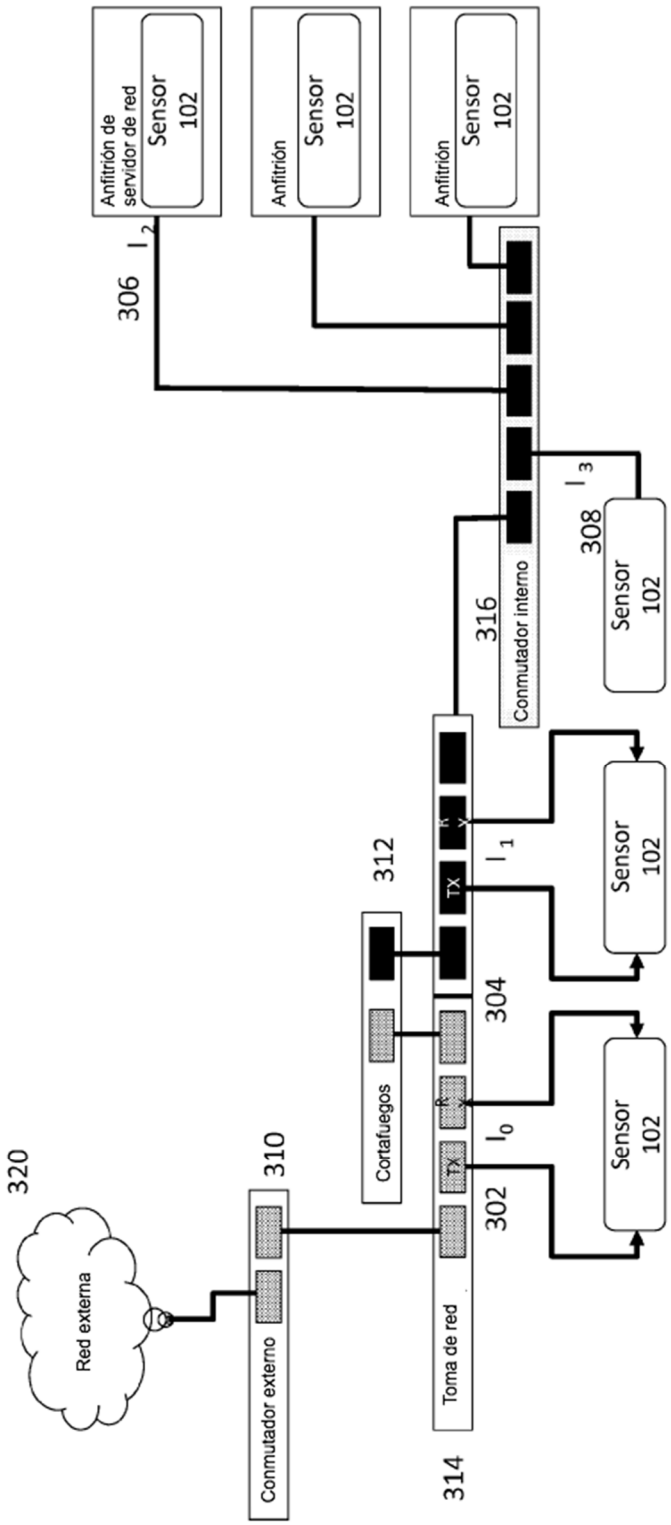
Anfitrión de servidor de red
Sensor 102
Anfitrión
Sensor 102
Anfitrión
Sensor 102
306
l_2
316
Conmutador interno
l_3
308
Sensor 102
312
TX
Rx
l_1
Sensor 102
Cortafuegos
304
Rx
TX
l_0
Sensor 102
320
Red externa
310
Conmutador externo
302
Toma de red
314

Figura 3

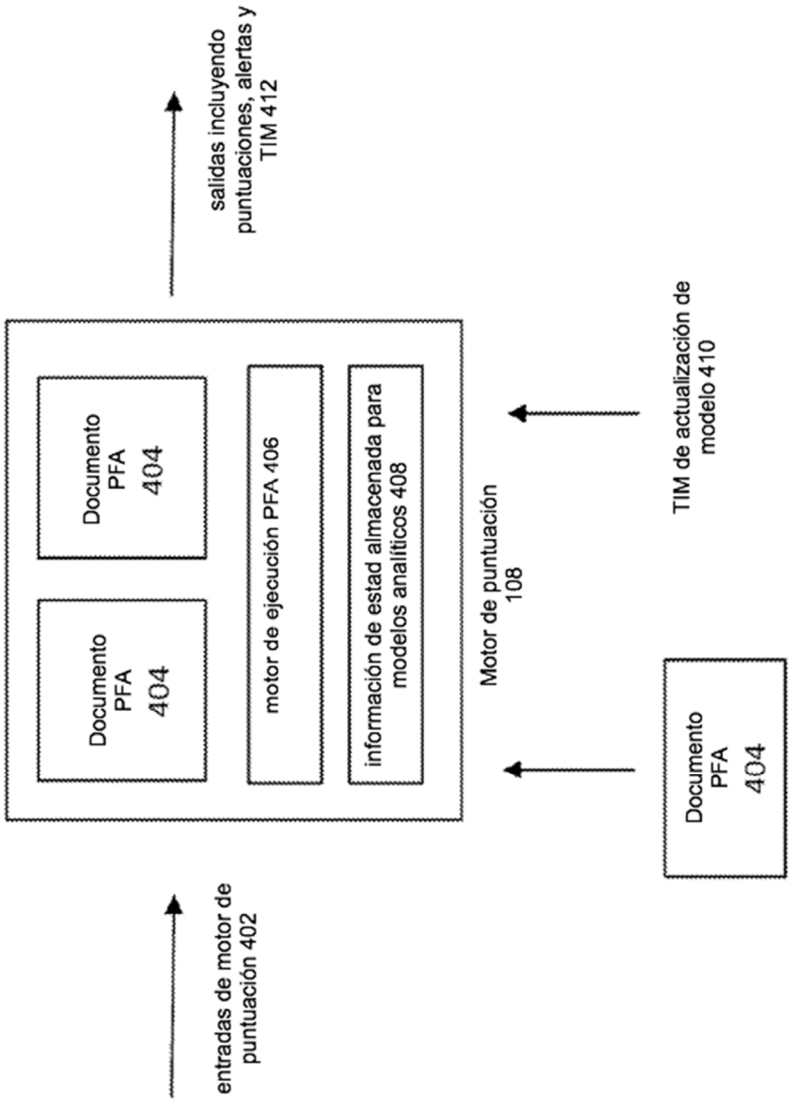
salidas incluyendo puntuaciones, alertas y TIM 412
Documento PFA 404
Documento PFA 404
motor de ejecución PFA 406
información de estad almacenada para modelos analíticos 408
Motor de puntuación 108
TIM de actualización de modelo 410
Documento PFA 404
entradas de motor de puntuación 402

Figura 4

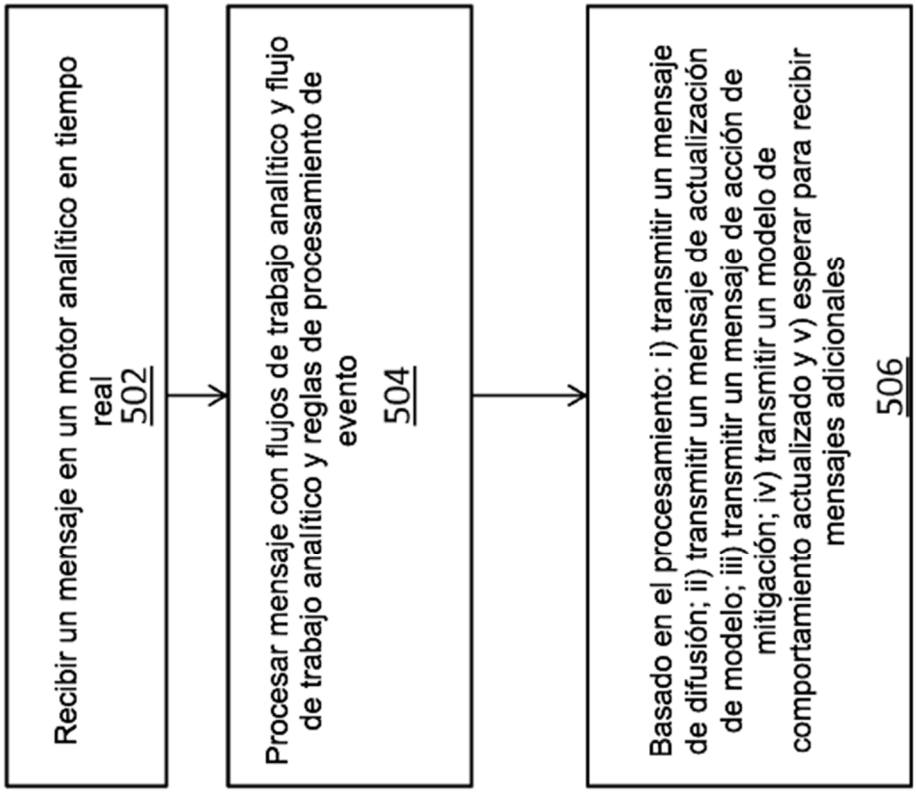
Recibir un mensaje en un motor analítico en tiempo real
502
Procesar mensaje con flujos de trabajo analítico y flujo de trabajo analítico y reglas de procesamiento de evento
504
Basado en el procesamiento: i) transmitir un mensaje de difusión; ii) transmitir un mensaje de actualización de modelo; iii) transmitir un mensaje de acción de mitigación; iv) transmitir un modelo de comportamiento actualizado y v) esperar para recibir mensajes adicionales
506

Figura 5

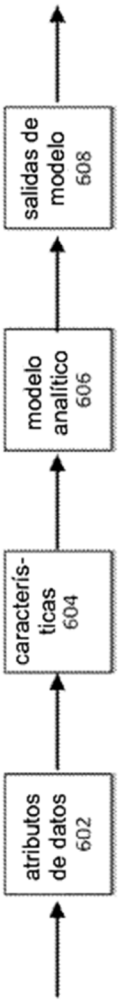

Figura 6A

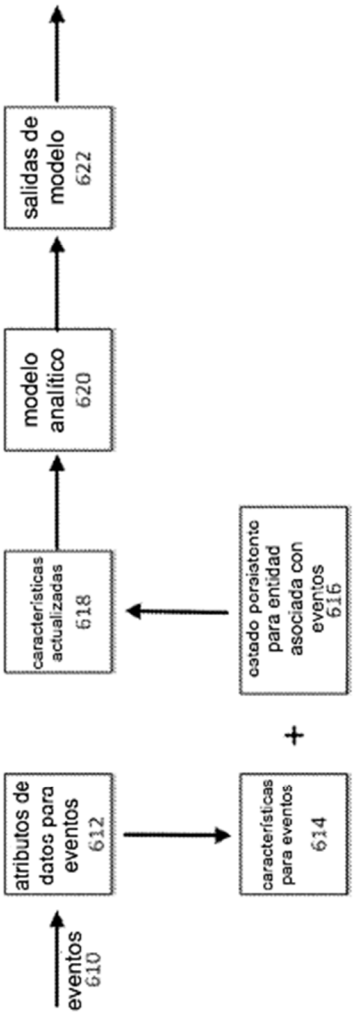

Figura 6B

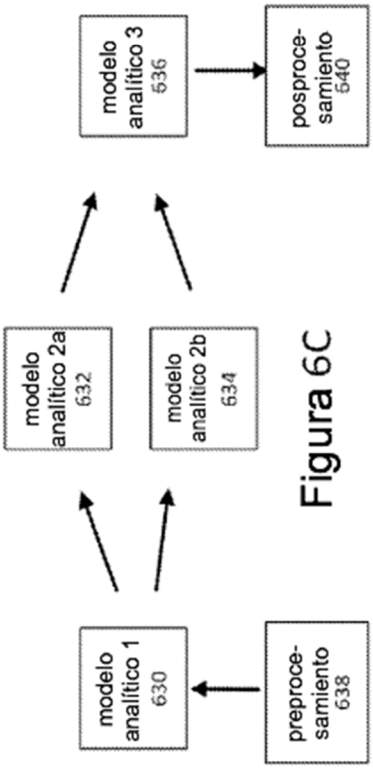

Figura 6C

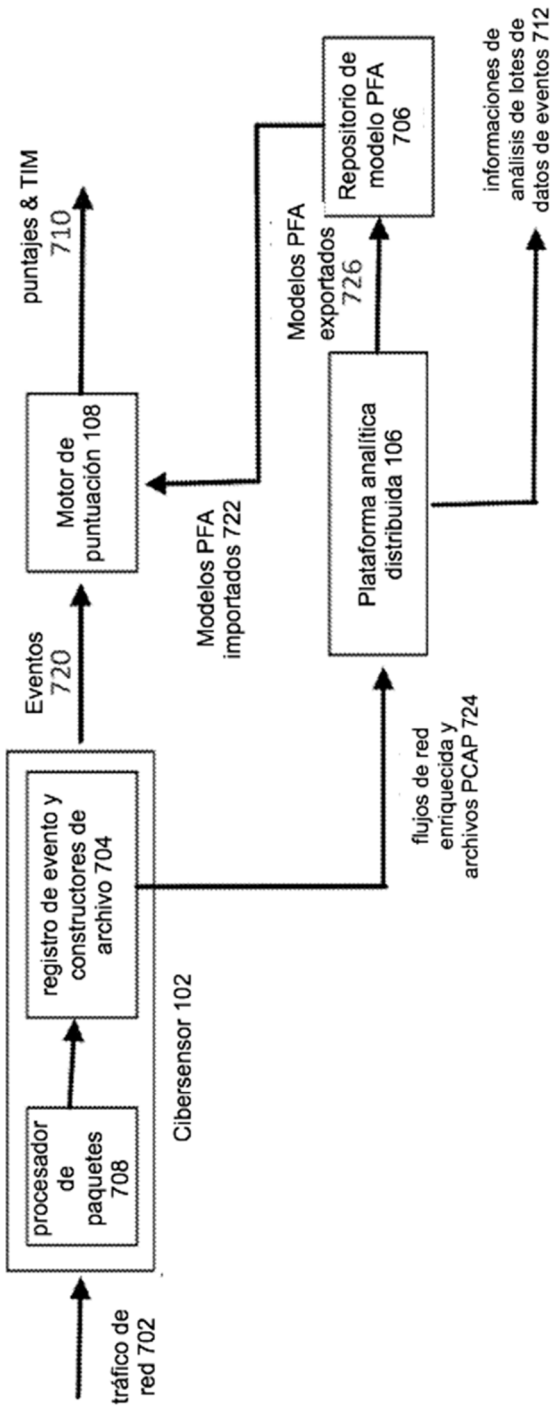
tráfico de red 702
Cibersensor 102
procesador de paquetes 708
registro de evento y constructores de archivo 704
Eventos 720
Motor de puntuación 108
puntajes & TIM 710
flujos de red enriquecida y archivos PCAP 724
Modelos PFA importados 722
Plataforma analítica distribuida 106
Modelos PFA exportados 726
Repositorio de modelo PFA 706
informaciones de análisis de lotes de datos de eventos 712

Figura 7

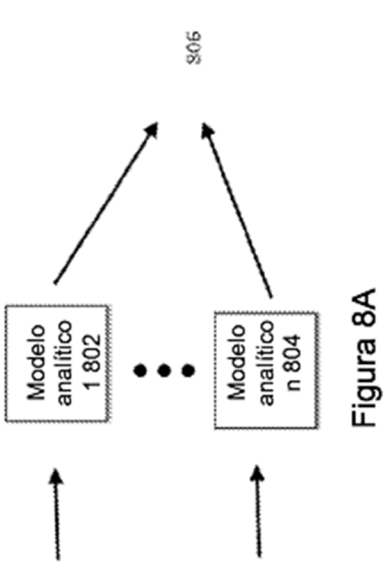

Figura 8A

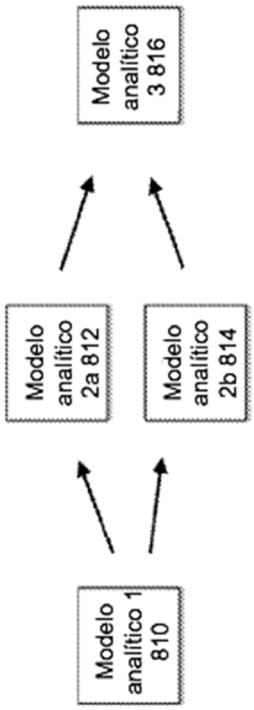

Figura 8B

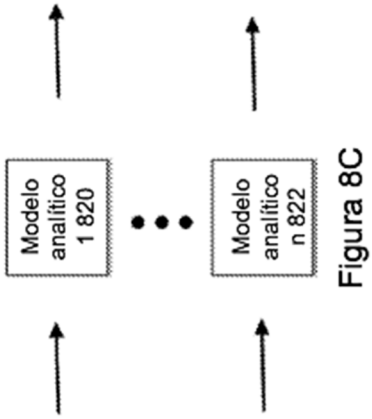

Figura 8C

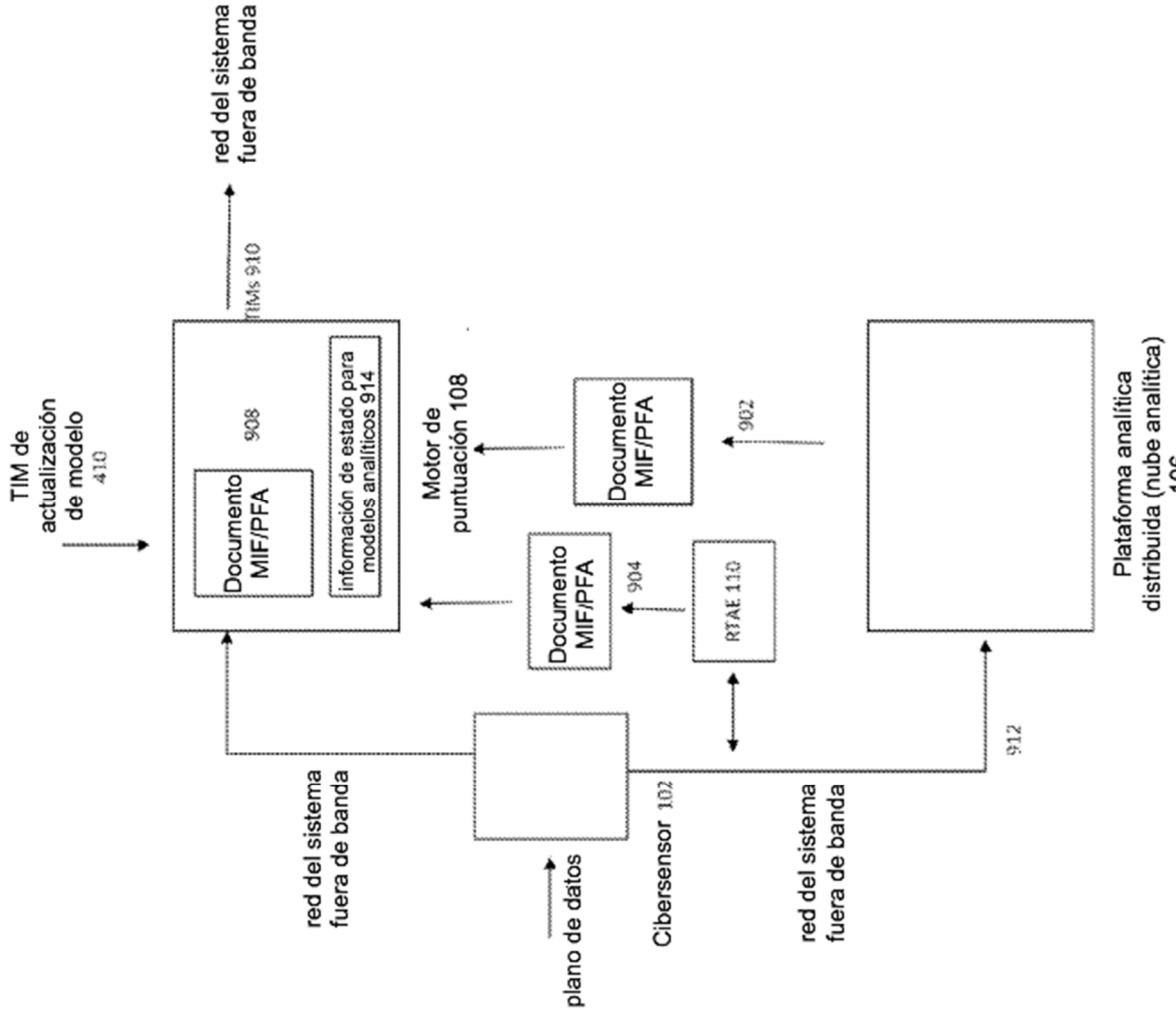
TIM de actualización de modelo
410
Documento MIF/PFA
908
información de estado para modelos analíticos 914
TIMs 910
red del sistema fuera de banda
Motor de puntuación 108
Documento MIF/PFA
902
Documento MIF/PFA
904
RTAE 110
Plataforma analítica distribuida (nube analítica) 106
912
red del sistema fuera de banda
plano de datos
Cibersensor 102
red del sistema fuera de banda

Figura 9

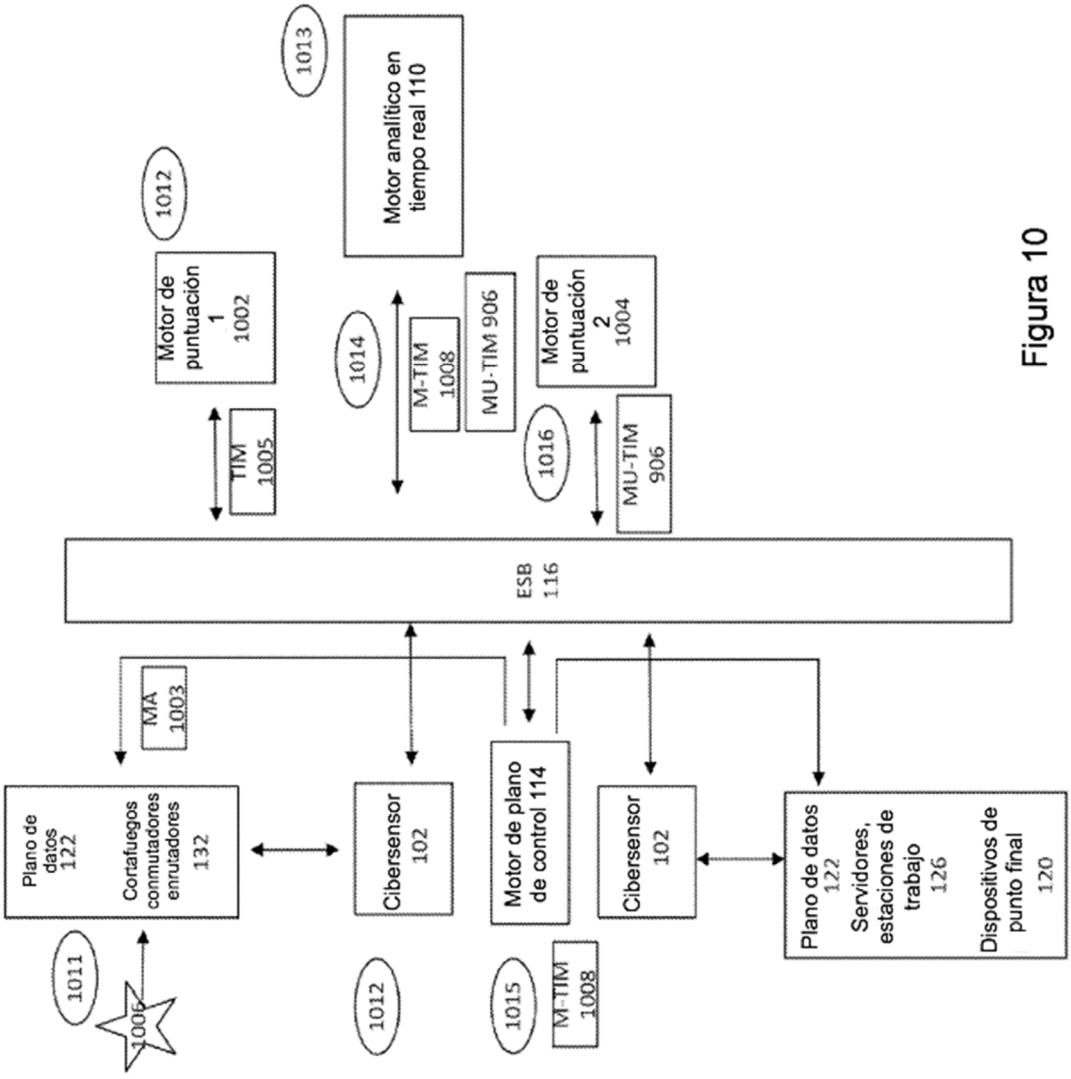
1013
Motor analítico en tiempo real 110
1012
Motor de puntuación 1 1002
1014
M-TIM 1008
MU-TIM 906
Motor de puntuación 2 1004
1016
TIM 1005
MU-TIM 906
ESB 116
MA 1003
Plano de datos 122
Cortafuegos conmutadores enrutadores 132
Cibersensor 102
Motor de plano de control 114
Cibersensor 102
Plano de datos 122
Servidores, estaciones de trabajo 126
Dispositivos de punto final 120
1011
1006
1012
1015
M-TIM 1008

Figura 10

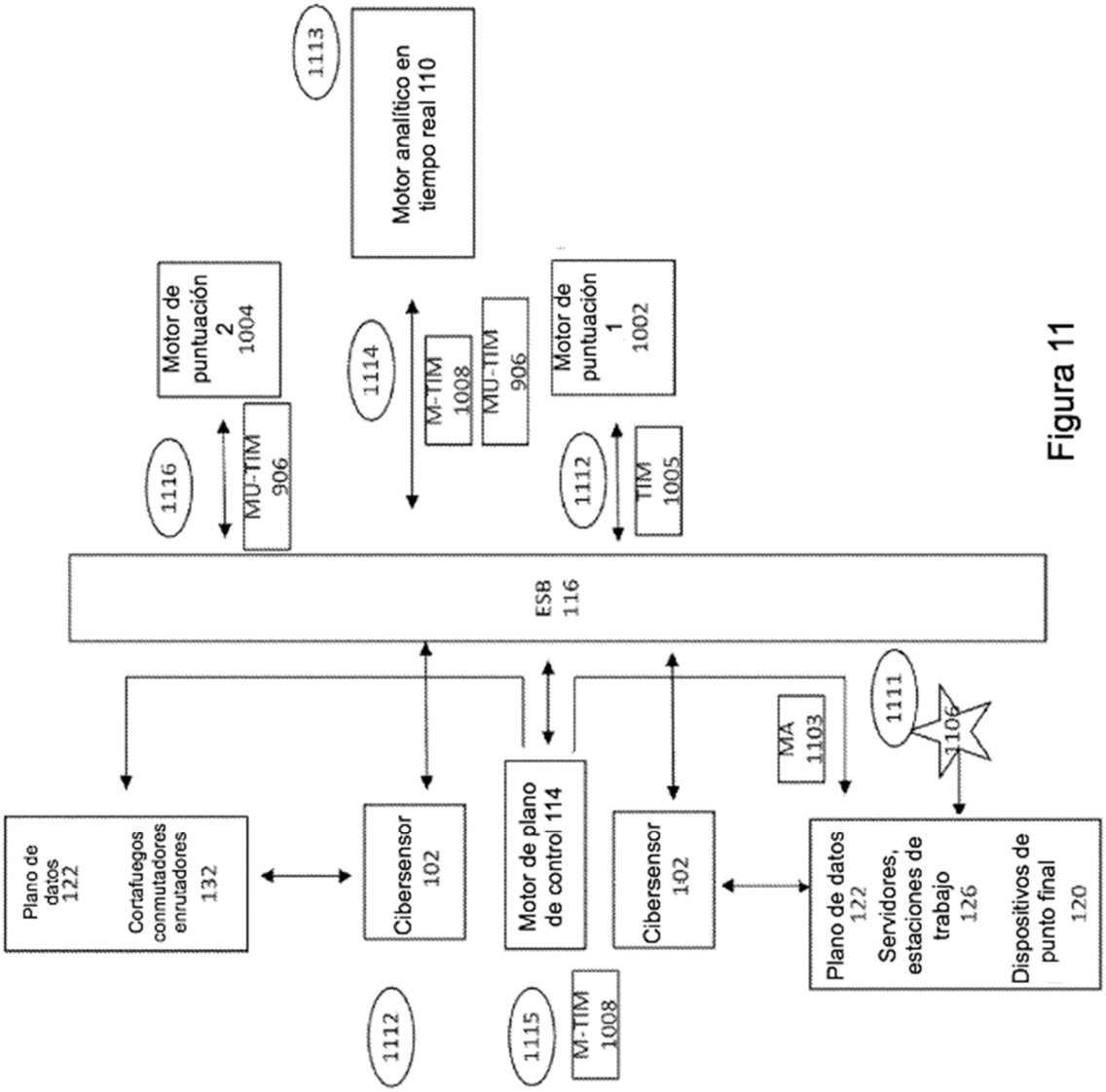
Motor analítico en tiempo real 110
1113
Motor de puntuación 2 1004
Motor de puntuación 1 1002
1114
M-TIM 1008
MU-TIM 906
1116
MU-TIM 906
1112
TIM 1005
ESB 116
Plano de datos 122
Cortafuegos conmutadores enrutadores 132
Cibersensor 102
Motor de plano de control 114
Cibersensor 102
MA 1103
1111
1106
Plano de datos 122
Servidores, estaciones de trabajo 126
Dispositivos de punto final 120
1112
1115
M-TIM 1008

Figura 11