(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 945 836**

(51) Int. CI.:

G06F 21/55 (2013.01)
H04L 9/40 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **10.12.2019 PCT/EP2019/084310**

(87) Fecha y número de publicación internacional: **18.06.2020 WO20120427**

(96) Fecha de presentación y número de la solicitud europea: **10.12.2019 E 19817692 (7)**

(97) Fecha y número de publicación de la concesión europea: **05.04.2023 EP 3895046**

(54) Título: **Sistemas y métodos para la detección de amenazas de comportamiento**

(30) Prioridad:

10.12.2018 US 201816215179

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.07.2023

(73) Titular/es:

BITDEFENDER IPR MANAGEMENT LTD. (100.0%)
P.O. Box 56-61 Acropolis ave. 3rd floor Office 302
2012 Nicosia, CY

(72) Inventor/es:

DICHIU, DANIEL;
NICULAE, STEFAN;
BOSINCEANU, ELENA A.;
ZAMFIR, SORINA N.;
DINCU, ANDREEA y
APOSTOAE, ANDREI A.

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistemas y métodos para la detección de amenazas de comportamiento

Antecedentes

La invención se refiere a sistemas y métodos de seguridad informática y, en particular, a sistemas y métodos para detectar software malicioso y/o una intrusión en un sistema informático y/o una red de comunicación.

En los últimos años, la seguridad informática y de redes se ha vuelto cada vez más importante tanto para particulares como para empresas. El rápido desarrollo de las tecnologías de comunicación electrónica, la creciente dependencia del software en las actividades diarias y la llegada del Internet de las cosas han dejado a las empresas y a las personas vulnerables a la pérdida de privacidad y al robo de datos.

Un atacante experto puede intentar infiltrarse en una red corporativa usando varias técnicas, por ejemplo, usando una puerta trasera instalada en una computadora corporativa por software malicioso. El atacante puede entonces obtener acceso a, modificar o destruir información confidencial. Otros ejemplos de ataques incluyen, entre otros, deshabilitar o incapacitar de otro modo los sistemas de seguridad física (p. ej., una alarma antirrobo), instalar software de espionaje e interferir con los sistemas automatizados que controlan la fabricación o distribución de bienes y servicios (p. ej., la red eléctrica).

El software que se ejecuta en un sistema informático puede usarse para detectar y/o prevenir automáticamente intrusiones no autorizadas y otras actividades maliciosas. Dicho software, comúnmente conocido como sistema de detección de intrusos (IDS), puede monitorear la red y/o las actividades de la computadora en busca de eventos inusuales o violaciones de políticas. Un IDS típico registra información relacionada con eventos observados, notifica a un usuario o administrador de red y genera informes. Algunos IDS pueden ir más allá para evitar que el intruso realice actividades maliciosas, por ejemplo, cambiando la configuración de seguridad (p. ej., reconfigurando un firewall) en respuesta a la detección de una intrusión.

Los documentos US 2016/352759 A1, US 2016/149936 A1, US 2014/215618 A1, US 2004/093510 A1 y US 2014/283067 A1 describen sistemas de detección de intrusos conocidos.

Sin embargo, a medida que los servicios de software se deslocalizan progresivamente y aumenta la cantidad de datos que fluyen a través de las redes informáticas, se vuelve cada vez menos práctico para el software de seguridad cribar esta gran cantidad de información en busca de indicadores de actividad maliciosa. Por lo tanto, existe un interés sustancial en desarrollar sistemas y métodos de detección de intrusos más robustos y escalables.

Sumario

De acuerdo con un aspecto, un sistema informático servidor comprende al menos un procesador de hardware configurado para asignar eventos de un corpus de entrenamiento a una pluralidad de categorías de eventos, comprendiendo el corpus de entrenamiento una colección de eventos que han ocurrido en una pluralidad de sistemas cliente. El procesador de hardware está configurado además, en respuesta a la asignación de eventos a categorías de eventos, para asignar sistemas cliente de la pluralidad de sistemas cliente a una pluralidad de grupos de clientes de acuerdo con la pluralidad de categorías de eventos. El procesador de hardware está configurado además, en respuesta a la asignación de la pluralidad de sistemas cliente a grupos de clientes, para transmitir un indicador de pertenencia a grupo de clientes a un detector de anomalías configurado para determinar si un evento objetivo que ocurre en un sistema cliente objetivo es indicativo de una amenaza a la seguridad informática. Asignar eventos a categorías de eventos comprende seleccionar una pluralidad de eventos del corpus de entrenamiento, habiendo ocurrido la pluralidad de eventos en un sistema cliente de la pluralidad de sistemas cliente, y organizar la pluralidad de eventos de acuerdo con un momento de ocurrencia para formar una secuencia de eventos. Asignar eventos a categorías de eventos comprende además, en respuesta, asignar un evento seleccionado de la secuencia de eventos a una categoría de eventos seleccionados de acuerdo con un primer evento que precede al evento seleccionado y además de acuerdo con el segundo evento que sigue al evento seleccionado dentro de la secuencia de eventos. Asignar sistemas cliente a grupos de clientes comprende asignar el sistema cliente a un grupo de clientes seleccionado de acuerdo con un perfil de evento determinado de acuerdo con un recuento de eventos que ocurren en el sistema cliente y que pertenecen a la categoría de eventos seleccionados. El detector de anomalías está configurado para determinar si el evento objetivo es indicativo de la amenaza a la seguridad informática de acuerdo con un modelo de comportamiento entrenado en un subcorpus de eventos específico del grupo de clientes, seleccionado el subcorpus específico del grupo de clientes del corpus de entrenamiento para incluir solo eventos que han ocurrido en una pluralidad de miembros de un grupo objetivo de la pluralidad de grupos de clientes.

De acuerdo con otro aspecto, un método implementado por computadora comprende método implementado por computadora que comprende emplear al menos un procesador de hardware de un sistema informático para asignar eventos de un corpus de entrenamiento a una pluralidad de categorías de eventos, en el que el corpus de entrenamiento comprende una colección de eventos que ocurren en una pluralidad de sistemas cliente. El método comprende además, en respuesta a la asignación de eventos a categorías de eventos, emplear al menos un procesador de hardware del sistema informático para asignar sistemas cliente de la pluralidad de sistemas cliente a

una pluralidad de grupos de clientes de acuerdo con la pluralidad de categorías de eventos. El método comprende además, en respuesta a la asignación de sistemas cliente a grupos de clientes, emplear al menos un procesador de hardware del sistema informático para transmitir un indicador de pertenencia a grupo de clientes a un detector de anomalías configurado para determinar si un evento objetivo que ocurre en un sistema cliente objetivo es indicativo de una amenaza a la seguridad informática. Asignar eventos a categorías de eventos comprende seleccionar una pluralidad de eventos del corpus de entrenamiento, habiendo ocurrido la pluralidad de eventos en un sistema cliente de la pluralidad de sistemas cliente, y organizar la pluralidad de eventos de acuerdo con un momento de ocurrencia para formar una secuencia de eventos. Asignar eventos a categorías de eventos comprende además, en respuesta, asignar un evento seleccionado de la secuencia de eventos a una categoría de eventos seleccionados de acuerdo con un primer evento que precede al evento seleccionado y además de acuerdo con el segundo evento que sigue al evento seleccionado dentro de la secuencia de eventos. Asignar sistemas cliente a grupos de clientes comprende asignar el sistema cliente a un grupo de clientes seleccionados de acuerdo con un perfil de evento determinado de acuerdo con un recuento de eventos que ocurren en el sistema cliente y que pertenecen a la categoría de eventos seleccionados. El detector de anomalías está configurado para determinar si el evento objetivo es indicativo de la amenaza a la seguridad informática de acuerdo con un modelo de comportamiento entrenado en un subcorpus de eventos específico del grupo de clientes, seleccionado el subcorpus específico del grupo de clientes del corpus de entrenamiento para incluir solo eventos que han ocurrido en una pluralidad de miembros de un grupo objetivo de la pluralidad de grupos de clientes.

Según otro aspecto, un medio no transitorio legible por computadora almacena instrucciones que, cuando son ejecutadas por al menos un procesador de hardware de un sistema informático, hacen que el sistema informático asigne eventos de un corpus de entrenamiento a una pluralidad de categorías de eventos, comprendiendo el corpus de entrenamiento una colección de eventos que han ocurrido en una pluralidad de sistemas cliente. Las instrucciones provocan además que el sistema informático, en respuesta a la asignación de eventos a categorías de eventos, asigne sistemas cliente de la pluralidad de sistemas cliente a una pluralidad de grupos de clientes de acuerdo con la pluralidad de categorías de eventos. Además, las instrucciones hacen que el sistema informático, en respuesta a la asignación de los sistemas cliente a grupos de clientes, transmita un indicador de pertenencia a grupo de clientes a un detector de anomalías configurado para determinar si un evento objetivo que ocurre en un sistema cliente objetivo es indicativo de una amenaza a la seguridad informática. Asignar eventos a categorías de eventos comprende seleccionar una pluralidad de eventos del corpus de entrenamiento, habiendo ocurrido la pluralidad de eventos en un sistema cliente de la pluralidad de sistemas cliente, y organizar la pluralidad de eventos de acuerdo con un momento de ocurrencia para formar una secuencia de eventos. Asignar eventos a categorías de eventos comprende además, en respuesta, asignar un evento seleccionado de la secuencia de eventos a una categoría de eventos seleccionados de acuerdo con un primer evento que precede al evento seleccionado y además de acuerdo con el segundo evento que sigue al evento seleccionado dentro de la secuencia de eventos. Asignar sistemas cliente a grupos de clientes comprende asignar el sistema cliente a un grupo de clientes seleccionados de acuerdo con un perfil de evento determinado de acuerdo con un recuento de eventos que ocurren en el sistema cliente y que pertenecen a la categoría de eventos seleccionados. El detector de anomalías está configurado para determinar si el evento objetivo es indicativo de la amenaza a la seguridad informática de acuerdo con un modelo de comportamiento entrenado en un subcorpus de eventos específico del grupo de clientes, seleccionado el subcorpus específico del grupo de clientes del corpus de entrenamiento para incluir solo eventos que han ocurrido en una pluralidad de miembros de un grupo objetivo de la pluralidad de grupos de clientes.

Breve descripción de los dibujos

Los aspectos y ventajas anteriores de la presente invención se entenderán mejor con la lectura de la siguiente descripción detallada y con la referencia a los dibujos, donde:

La Fig. **1** muestra varios ejemplos de sistemas cliente interconectados, con un servidor de seguridad que actúa como sistema de detección de intrusos de acuerdo con algunas realizaciones de la presente invención.

La Fig. **2** muestra un ejemplo de intercambio de datos llevado a cabo para proteger un sistema cliente de acuerdo con algunas realizaciones de la presente invención.

La Fig. **3-A** ilustra una configuración de hardware ejemplar de un sistema cliente de acuerdo con algunas realizaciones de la presente invención.

La Fig. **3-B** ilustra una configuración de hardware ejemplar de un servidor de seguridad de acuerdo con algunas realizaciones de la presente invención.

La Fig. **4** muestra componentes de software ejemplares que se ejecutan en un sistema cliente protegido de acuerdo con algunas realizaciones de la presente invención.

La Fig. **5** muestra una arquitectura de software ejemplar de un servidor de seguridad de acuerdo con algunas realizaciones de la presente invención.

La Fig. **6** ilustra una operación ejemplar de un motor de perfilado de acuerdo con algunas realizaciones de la presente invención.

La Fig. **7** muestra una secuencia ejemplar de pasos llevados a cabo por el motor de perfilado de acuerdo con algunas realizaciones de la presente invención.

La Fig. **8-A** muestra un entrenamiento ejemplar de un codificador de eventos de acuerdo con algunas realizaciones de la presente invención.

La Fig. **8-B** muestra un entrenamiento ejemplar alternativo del codificador de eventos de acuerdo con algunas realizaciones de la presente invención.

La Fig. **9** muestra una secuencia ejemplar de pasos realizados para entrenar el decodificador de eventos en la configuración de la Fig. **8-A**.

La Fig. **10** ilustra un espacio de incrustación de eventos ejemplar y un conjunto de grupos de eventos ejemplares de acuerdo con algunas realizaciones de la presente invención.

La Fig. **11** ilustra un espacio de perfil de cliente ejemplar y un conjunto de grupos de clientes de acuerdo con algunas realizaciones de la presente invención.

La Fig. **12** muestra un perfil de evento ejemplar de un sistema cliente de acuerdo con algunas realizaciones de la presente invención.

La Fig. **13** muestra componentes ejemplares y el funcionamiento de un detector de anomalías de acuerdo con algunas realizaciones de la presente invención.

La Fig. **14** ilustra una secuencia ejemplar de pasos realizados por el detector de anomalías durante el entrenamiento, de acuerdo con algunas realizaciones de la presente invención.

La Fig. **15** muestra componentes ejemplares de un modelo de comportamiento que forma parte del detector de anomalías de acuerdo con algunas realizaciones de la presente invención.

La Fig. **16** ilustra una secuencia ejemplar de pasos realizados por el detector de anomalías entrenado de acuerdo con algunas realizaciones de la presente invención.

La Fig. **17-A** muestra resultados de un experimento que comprende el empleo de algunas realizaciones de la presente invención para detectar amenazas reales a la seguridad informática.

La Fig. **17-B** muestra otros resultados experimentales del uso de algunas realizaciones para detectar amenazas reales a la seguridad informática.

Descripción detallada de realizaciones preferidas

En la siguiente descripción, se entiende que todas las conexiones mencionadas entre estructuras pueden ser conexiones operativas directas o conexiones operativas indirectas a través de estructuras intermedias. Un conjunto de elementos incluye uno o más elementos. Cualquier enumeración de un elemento se entiende que se refiere a al menos un elemento. Una pluralidad de elementos incluye al menos dos elementos. A menos que se especifique lo contrario, cualquier uso de "O" se refiere a un o no exclusivo. A menos que se requiera lo contrario, no es necesario que los pasos del método descritos se realicen necesariamente en un orden ilustrado particular. Un primer elemento (p. ej., datos) derivado de un segundo elemento abarca un primer elemento igual al segundo elemento, así como un primer elemento generado al procesar el segundo elemento y, opcionalmente, otros datos. Tomar una determinación o decisión de acuerdo con un parámetro abarca tomar la determinación o decisión de acuerdo con el parámetro y opcionalmente de acuerdo con otros datos. A menos que se especifique lo contrario, un indicador de alguna cantidad/datos puede ser la cantidad/datos en sí, o un indicador diferente de la cantidad/datos en sí. Un programa informático es una secuencia de instrucciones del procesador que llevan a cabo una tarea. Los programas informáticos descritos en algunas realizaciones de la presente invención pueden ser entidades o subentidades de software independientes (p. ej., subrutinas, bibliotecas) de otros programas informáticos. A menos que se especifique lo contrario, la seguridad informática abarca la protección de equipos y datos contra el acceso, la modificación y/o la destrucción ilegítimos. Los medios legibles por computadora abarcan medios no transitorios como medios de almacenamiento magnéticos, ópticos y de semiconductor (p. ej., discos duros, discos ópticos, memoria flash, DRAM), así como enlaces de comunicación como cables conductores y enlaces de fibra óptica. De acuerdo con algunas realizaciones, la presente invención proporciona, entre otros, sistemas informáticos que comprenden hardware (p. ej., uno o más procesadores) programados para realizar los métodos descritos en este documento, así como instrucciones de codificación de medios legibles por computadora para realizar los métodos descritos en este documento.

La siguiente descripción ilustra realizaciones de la invención a modo de ejemplo y no necesariamente a modo de limitación.

La Fig. **1** muestra un conjunto ejemplar de sistemas cliente **10a-h** protegido contra amenazas a la seguridad informática de acuerdo con algunas realizaciones de la presente invención. Sistemas cliente **10a-h** representan genéricamente cualquier dispositivo electrónico que tiene un procesador, una memoria y una interfaz de comunicación. Sistemas

cliente ejemplares **10a-h** incluyen computadoras personales, computadoras portátiles, tabletas, dispositivos de telecomunicaciones móviles (p. ej., teléfonos inteligentes), reproductores multimedia, televisores, consolas de juegos, electrodomésticos (p. ej., refrigeradores, sistemas inteligentes de calefacción y/o iluminación) y dispositivos portátiles (p. ej., relojes inteligentes, equipos de gimnasia), entre otros. Sistemas cliente **10a-h** pueden ejecutar varios softwares, por ejemplo, procesamiento de documentos, juegos, mensajería electrónica y aplicaciones de redes sociales, entre otros. Algunos clientes pueden intercambiar información con un servidor de contenido remoto **17**, por ejemplo, la navegación por Internet.

Los sistemas cliente ilustrados están conectados por redes locales **12a-b**, y además a una red extendida **14**, como una red de área extendida (WAN) o Internet. En un ejemplo, los sistemas cliente **10a-d** representan los dispositivos electrónicos de una familia, interconectados por una red doméstica **12a**. Mientras tanto, los sistemas cliente **10e-g** pueden denotar computadoras individuales y/o una computadora central corporativa dentro de un edificio de oficinas. Las redes locales **12-b** pueden entonces representar una sección de una red corporativa (p. ej., una red de área local - LAN).

Un enrutador comprende un dispositivo electrónico que permite la comunicación entre múltiples sistemas cliente y/o el acceso de los respectivos clientes a la red extendida **14.** En el ejemplo de la Fig. **1**, los enrutadores **15a-b** interconectan clientes en redes locales **12a-b** y/o permiten a los clientes **10a-g** acceder a Internet. Los enrutadores **15a-b** pueden actuar como pasarelas entre las redes locales **12a-b**, respectivamente, y la red extendida **14** y pueden además proporcionar un conjunto de servicios de red a los sistemas cliente **10a-g**. Dichos servicios incluyen, por ejemplo, la distribución de parámetros de configuración de red a los sistemas cliente **10a-g** (p. ej., asignación de direcciones de red a través del Protocolo de configuración dinámica de host - DHCP) y enrutamiento de comunicaciones a través de una secuencia de nodos de red. Algunos sistemas cliente, como el sistema cliente ejemplar **10h**, pueden conectarse directamente a la red extendida **14**, por ejemplo, a través de un relé de telecomunicaciones.

La Fig. **1** además muestra un servidor de seguridad **16** conectado a la red extendida **14**. El servidor **16** representa genéricamente un conjunto de sistemas informáticos acoplados comunicativamente, que pueden estar o no en proximidad física entre sí. El servidor **16** protege los sistemas cliente **10a-h** contra amenazas a la seguridad informática como software malicioso e intrusión. En algunas realizaciones, dicha protección comprende la detección por el servidor de seguridad **16** de actividad sospechosa que ocurre en un sistema cliente, por ejemplo, una acción de un atacante que controla el sistema cliente respectivo.

Un intercambio de datos ejemplar entre el servidor de seguridad **16** y un sistema cliente **10** se ilustra en la Fig. **2**. El sistema cliente **10** puede representar cualquier cliente **10a-h** en la Fig. **1**. En algunas realizaciones, el servidor **16** está configurado para recibir un indicador de evento **20a** del sistema cliente **10**, indicador **20a** indicativo de la ocurrencia de un tipo particular de evento durante la ejecución del software en el cliente **10**. Ejemplos de tales eventos incluyen el inicio de un proceso/subproceso (p. ej., un usuario inicia una aplicación, un proceso principal crea un proceso secundario, etc.), un intento de acceder a un dispositivo de entrada del sistema cliente respectivo (p. ej., cámara, micrófono), un intento de acceder a un recurso de red local o remota (p, ej., una solicitud de protocolo de transferencia de hipertexto -HTTP- para acceder a un URL particular, un intento de acceder a un depósito de documentos a través de una red local), una solicitud formulada en un esquema de identificador de recurso uniforme particular (p. ej., una solicitud mailto: o ftp:), una ejecución de una instrucción de procesador particular (p. ej., una llamada al sistema), un intento de cargar una biblioteca (p. ej., una biblioteca vinculada dinámica - DLL), un intento de crear un nuevo archivo de disco, un intento de leer o escribir en una ubicación particular del disco (p. ej., un intento de sobrescribir un archivo existente, un intento de abrir una carpeta o documento específico) y un intento de enviar un mensaje electrónico (p. ej., correo electrónico, servicio de mensajes cortos - SMS, etc.), entre otros. En algunas realizaciones, los periodos de inactividad, es decir, los intervalos de tiempo entre eventos y/o los lapsos de tiempo cuando el sistema cliente respectivo está inactivo, no registra actividad del usuario o lleva a cabo solo tareas internas del sistema, también se califican como eventos y pueden notificarse, a través de indicadores de evento, al servidor de seguridad. Dichos periodos inactivos pueden diferenciarse además en breves intervalos de tiempo (p. ej., del orden de un segundo) y largos intervalos de tiempo (p. ej., del orden de minutos a horas). Los eventos detectados pueden o no ser indicativos de malicia *per se*; algunos eventos pueden ser indicativos de malicia cuando ocurren junto con otros eventos y/o cuando ocurren en una secuencia particular. Otros eventos pueden ser maliciosos cuando ocurren en ciertos momentos del día o con una frecuencia inusual, por ejemplo, una secuencia de 1000 lecturas de una carpeta de disco particular en un intervalo de unos pocos segundos.

Cada indicador de evento **20a** puede comprender, entre otros, un indicador de un tipo del evento respectivo y una marca de tiempo indicativa de un momento en el tiempo en que ha ocurrido el evento respectivo. El indicador de evento **20a** puede incluir además un identificador (ID de cliente) del sistema cliente respectivo y/o un indicador de un usuario (ID de usuario) que actualmente opera el sistema cliente respectivo. Por ejemplo, cuando el evento comunicado comprende la creación de un proceso, un indicador de usuario puede indicar el propietario del proceso principal. El indicador de evento **20a** puede codificar otros parámetros, como un nombre de proceso, una ubicación/ruta del sistema de archivos de un proceso que se está iniciando, una dirección de red (p. ej., protocolo de Internet - dirección IP), un localizador universal de recursos (URL) de una solicitud HTTP, etc.

En algunas realizaciones, el servidor **16** también puede recopilar información de los enrutadores **15a-b**, como lo ilustra un indicador de evento **20b** en la Fig. **2**. Dichos indicadores de eventos pueden incluir, por ejemplo, indicadores de eventos de red tales como solicitudes de acceso a la red emitidas por sistemas cliente conectados al respectivo enrutador/pasarela. Por ejemplo, el indicador de evento **20b** puede incluir una dirección IP de origen, una dirección IP de destino, una marca de tiempo y un tamaño de carga útil. En algunas realizaciones, el indicador de evento **20b** comprende datos de eventos del cliente agregados por el enrutador respectivo de acuerdo con varios protocolos de procesamiento de datos (p. ej., flujos de red, registros de red, etc.).

El servidor de seguridad **16** mantiene un conjunto de modelos de comportamiento del usuario que representan una forma de referencia, normal y/o legítima de operar un subconjunto de sistemas cliente **10a-h**. Dichos modelos de comportamiento se consideran aquí perfiles de clientes. Los parámetros de dichos modelos de comportamiento se representan genéricamente como una base de datos de perfiles **19** en la Fig. **1** y pueden incluir una salida de un evento y/o algoritmo de agrupamiento de clientes, como se muestra en detalle a continuación. En una realización ejemplar en la que un perfil está representado por un cliente o grupo de eventos, los parámetros del perfil respectivo pueden incluir coordenadas de un centroide de grupo y un conjunto de números que indican un rango del grupo respectivo a lo largo de varios ejes. Otros parámetros del perfil pueden incluir, entre otros, una medida de excentricidad del grupo respectivo y una distancia promedio entre los miembros del grupo y el centroide del grupo, entre otros. Los perfiles de los clientes pueden generarse automáticamente, utilizando métodos y algoritmos de aprendizaje supervisados o no supervisados, como se muestra a continuación.

Un perfil de cliente puede capturar el comportamiento de un solo usuario o puede capturar colectivamente el comportamiento de múltiples usuarios. Por dar algunos ejemplos, un teléfono inteligente puede ser utilizado principalmente por un solo usuario, por lo tanto, un perfil de cliente ligado al teléfono inteligente respectivo puede capturar esencialmente un comportamiento de referencia de su usuario principal. Por el contrario, las computadoras que pertenecen a un laboratorio de computación de universidad pueden ser utilizadas por muchos estudiantes diferentes; un perfil de cliente ligado a una de estas máquinas puede representar colectivamente un comportamiento de referencia de todos los estudiantes respectivos. Un perfil de cliente puede ligarse a un solo sistema cliente/máquina física (p. ej., teléfono inteligente, computadora portátil). En algunas realizaciones, un perfil de cliente puede representar colectivamente una pluralidad de máquinas físicas. En uno de esos ejemplos, los sistemas cliente **10a-d** en la Fig. **1** pueden estar representados colectivamente por un solo perfil de cliente que captura un comportamiento normal o de referencia de los miembros de una familia en particular. En otro ejemplo, se utiliza un perfil de cliente para representar todas las computadoras en el departamento de contabilidad de una corporación, mientras que otro perfil de cliente representa todas las computadoras utilizadas por el equipo de investigación y desarrollo de la corporación respectiva. En una realización de computación en la nube, como un entorno de infraestructura de escritorio virtual (VDI) en el que una máquina física puede ejecutar una pluralidad de máquinas virtuales para varios usuarios distribuidos, un perfil de cliente puede ligarse a múltiples máquinas virtuales que se ejecutan en la máquina física respectiva.

En algunas realizaciones, un solo usuario puede estar representado por una pluralidad de perfiles de cliente distintos. Por ejemplo, la misma persona puede tener un perfil de cliente/comportamiento de referencia mientras está en el trabajo y un perfil de cliente/comportamiento de referencia diferente mientras está en casa. Otros ejemplos de perfiles de cliente pueden estar asociados con usuarios de un grupo de edad particular (p. ej., adolescentes), un interés personal particular (p. ej., juegos), una ocupación particular (p. ej., ingeniero, artista, educador), etc. En otra realización ejemplar más, distintos perfiles de cliente pueden corresponder a distintas actividades informáticas, p. ej., utilizar distintos programas informáticos: navegar por Internet, utilizar redes sociales, efectuar trabajos de oficina, etc. Otros perfiles de cliente ejemplares más pueden estar ligados a tipos de dispositivo distintos (p. ej., teléfono inteligente frente a PC). Los perfiles colectivos pueden diseñarse de acuerdo con criterios más complejos, por ejemplo, un perfil de cliente que indique una forma típica/de referencia en la que un ingeniero de la empresa X navega por Internet. Otro de estos perfiles ejemplares puede indicar una manera típica en la que los jóvenes usan las tabletas.

Un subconjunto de indicadores de eventos **20a-b** se puede recopilar para formar un corpus de eventos que se utilizará para derivar perfiles de cliente, como se muestra en detalle a continuación. Se puede usar otro subconjunto de indicadores de eventos para detectar amenazas a la seguridad. Por ejemplo, en respuesta a la recepción de indicadores de eventos **20a-b**, el servidor de seguridad **16** puede determinar si el evento comunicado por el indicador de evento respectivo es coherente con un perfil de cliente seleccionado de acuerdo con el indicador de cliente respectivo. Dicho de otra manera, el servidor de seguridad **16** puede determinar si el evento respectivo coincide con un patrón de normalidad/comportamiento de referencia codificado en el perfil de cliente respectivo. Cuando no, el evento respectivo puede indicar actividad sospechosa, en cuyo caso algunas realizaciones pueden tomar medidas de protección, por ejemplo, enviar alertas de seguridad **22a-b** al respectivo sistema cliente y/o a un administrador del respectivo sistema cliente. En otro ejemplo de medida de protección, algunas realizaciones dan instrucciones a un enrutador que pertenece a la misma red local que el sistema cliente sospechoso para bloquear las comunicaciones hacia y/o desde el respectivo sistema cliente sospechoso. Perfiles de cliente y procesamiento de indicadores de eventos por el servidor de seguridad **16** se describen con más detalle a continuación.

La Fig. **3-A** muestra una configuración de hardware ejemplar de un sistema cliente de acuerdo con algunas realizaciones de la presente invención. El sistema cliente **10** puede representar cualquiera de los sistemas cliente **10a-h** en la Fig. **1**. Para mayor claridad, el sistema cliente ilustrado es un sistema informático. Otros sistemas cliente, como teléfonos móviles, tabletas y dispositivos portátiles, pueden tener configuraciones ligeramente diferentes. El

procesador **32** comprende un dispositivo físico (p. ej., microprocesador, circuito integrado multinúcleo formado sobre un sustrato semiconductor) configurado para ejecutar operaciones computacionales y/o lógicas con un conjunto de señales y/o datos. Tales señales o datos pueden codificarse y entregarse al procesador **32** en forma de instrucciones del procesador, p. ej., código máquina. La unidad de memoria **34** puede comprender medios volátiles legibles por computadora (p. ej., memoria dinámica de acceso aleatorio - DRAM) que almacenan datos/señales a los que se accede o generados por el procesador **32** en el curso de la realización de las operaciones.

Los dispositivos de entrada **36** puede incluir teclados, ratones y micrófonos de computadora, entre otros, incluidas las respectivas interfaces de hardware y/o adaptadores que permiten a un usuario introducir datos y/o instrucciones en el sistema cliente **10**. Los dispositivos de salida **38** puede incluir dispositivos de visualización, como monitores, y altavoces, entre otros, así como interfaces/adaptadores de hardware, como tarjetas gráficas, que permiten que el sistema cliente respectivo comunique datos a un usuario. En algunas realizaciones, los dispositivos de entrada y salida **36-38** comparten una pieza común de hardware (p. ej., una pantalla táctil). Los dispositivos de almacenamiento **42** incluyen medios legibles por computadora que permiten el almacenamiento no volátil, la lectura y la escritura de instrucciones de software y/o datos. Ejemplos de dispositivos de almacenamiento incluyen discos magnéticos y ópticos y dispositivos de memoria flash, así como medios extraíbles tales como unidades y discos de CD y/o DVD. El (los) adaptador(es) de red **44** permite(n) al sistema cliente **10** conectarse a una red de comunicación electrónica (p. ej., las redes **12, 14** en la Fig. **1**) y/o a otros dispositivos/sistemas informáticos.

El concentrador de control **40** representa genéricamente la pluralidad de buses de sistema, periféricos y/o de chipset, y/o todos los demás circuitos que permiten la comunicación entre el procesador **32** y el resto de los componentes de hardware del sistema cliente **10**. Por ejemplo, el concentrador de control **40** puede comprender un controlador de memoria, un controlador de entrada/salida (E/S) y un controlador de interrupción. Según el fabricante del hardware, algunos de estos controladores pueden incorporarse en un solo circuito integrado y/o pueden integrarse con el procesador. En otro ejemplo, el concentrador de control **40** puede comprender un controlador de memoria que conecta el procesador **32** a la memoria **34**, y/o un controlador de entrada-salida (southbridge) que conecta el procesador **32** a los dispositivos **36, 38, 42** y **44**.

La Fig. **3-B** muestra una configuración de hardware ejemplar del servidor de seguridad **16** de acuerdo con algunas realizaciones de la presente invención. El servidor **16** comprende al menos un procesador de hardware **132** (p. ej., microprocesador, circuito integrado multinúcleo), una memoria física **134** (p. ej., DRAM), dispositivos de almacenamiento de servidor **142** y un conjunto de adaptadores de red de servidor **144**. Los procesadores de servidor **132** pueden incluir una unidad central de procesamiento (UCP) y/o una matriz de unidades de procesamiento de gráficos (GPU). Los adaptadores **144** pueden incluir tarjetas de red y otras interfaces de comunicación que permiten al servidor de seguridad **16** conectarse a la red de comunicación **14**. Los dispositivos de almacenamiento de servidor **142** pueden almacenar datos tales como indicadores de eventos y/o parámetros del perfil de cliente. En algunas realizaciones, el servidor **16** comprende además dispositivos de entrada y salida, que pueden tener una función similar a los dispositivos de entrada/salida **36** y **38** del sistema cliente **10**, respectivamente.

La Fig. **4** muestra componentes de software ejemplares que se ejecutan en el sistema cliente **10** de acuerdo con algunas realizaciones de la presente invención. Dicho software puede incluir un sistema operativo (SO) **46** que proporciona una interfaz entre el hardware del sistema cliente **10** y otros programas informáticos, como una aplicación de usuario **48** que se ejecuta en el sistema cliente respectivo. Sistemas operativos ejemplares incluyen, entre otros, Windows®, Mac OS®, iOS® y Android®. La aplicación de usuario **48** representa de manera genérica cualquier aplicación como procesamiento de textos, procesamiento de imágenes, hoja de cálculo, calendario, juegos en línea, redes sociales, navegador web y aplicaciones de comunicación electrónica, entre otras. En algunas realizaciones, una aplicación de seguridad **50** está configurada para proteger el sistema cliente **10** contra amenazas a la seguridad informática como software malicioso e intrusión. Entre otras funciones, la aplicación de seguridad **50** está configurada para transmitir indicadores de eventos al servidor de seguridad **16** y/o para recibir alertas de seguridad. En algunas realizaciones, la aplicación **50** comprende además un recolector de eventos **52** y un filtro de red **53**. Alguna funcionalidad de filtro de red **53** puede implementarse directamente en hardware. Cuando el sistema cliente **10** opera una plataforma de virtualización de hardware en la que el OS **46** y la aplicación **48** se ejecutan dentro de una máquina virtual (por ejemplo, en un entorno de computación en la nube), el recolector de eventos **52** y/o el filtro de red **53** pueden ejecutarse fuera de la máquina virtual respectiva, p. ej., a nivel de un hipervisor que expone la máquina virtual respectiva, utilizando técnicas conocidas en la técnica como introspección.

El recolector de eventos **52** está configurado para detectar varios eventos que ocurren durante la ejecución del software por parte del sistema cliente **10**. Algunas realizaciones pueden marcar con fecha y hora cada evento detectado para registrar una hora de ocurrencia del evento respectivo. Los eventos monitoreados pueden ser específicos de la máquina y/o del sistema operativo. Eventos ejemplares incluyen, entre otros, el inicio de un proceso, la finalización de un proceso, la generación de procesos secundarios, solicitudes de acceso a periféricos (p. ej., disco duro, adaptador de red), un comando ingresado por el usuario en una interfaz de línea de comandos, etc. Dichos eventos de hardware y/o software pueden detectarse usando cualquier método conocido en el campo de la seguridad informática, por ejemplo, conectando ciertas funciones del sistema operativo, detectando llamadas al sistema, empleando un minifiltro del sistema de archivos, cambiando un permiso de acceso a la memoria para detectar un intento de ejecutar código desde ciertas direcciones de memoria, etc.

Algunas realizaciones monitorean eventos de hardware y/o software utilizando herramientas de registro del sistema integradas en el SO **46** (p. ej., Syslog en UNIX®). Dichas herramientas pueden generar una lista de descriptores de eventos que incluyen una marca de tiempo para cada evento, un código numérico que identifica un tipo de evento, un indicador de un tipo de proceso o aplicación que generó el evento respectivo y otros parámetros del evento. La aplicación de seguridad **50** puede extraer dicha información del respectivo registro del sistema para formular indicadores de eventos. A continuación, se proporcionan ejemplos de entradas de syslog:

```
<30>Feb 8 21:36:51 dtm charon: 12[IKE] establishing CHILD_SA dtmhq5{5}
<30>Feb 8 21:36:51 dtm charon: 12[IKE] establishing CHILD_SA dtmhq5{5}
<187>Feb 8 21:37:56 example.domain.biz dhcpd: DHCPDISCOVER from 0c:14:7b:11:
      14:64 via eth1: network eth1: no free leases
```

El filtro de red **53** detecta un conjunto de eventos de red que ocurren durante las comunicaciones electrónicas a través de las redes **12-14** entre el sistema cliente **10** y otras partes. Eventos ejemplares detectados por el filtro de red **53** incluyen eventos que forman parte del establecimiento de una conexión entre el sistema cliente **10** y otra entidad de red (p. ej., solicitud de una dirección de red, transmisión de una dirección de red, eventos de protocolo de enlace, etc.), eventos que configuran una conexión cifrada (capa de conexión segura - SSL, red privada virtual - VPN), transmisión de datos y recepción de datos, entre otros. En algunas realizaciones, el filtro de red **53** recopila metadatos del tráfico de red interceptado. Dichos metadatos pueden incluir, por ejemplo, una dirección de red de origen (p. ej., protocolo de Internet - dirección IP), una dirección de destino, una marca de tiempo de un paquete de datos, un indicador de un tipo de protocolo de comunicación y un tamaño de un paquete de datos. Otros metadatos ejemplares pueden incluir un indicador de un tipo de agente de usuario del protocolo de transferencia de hipertexto (HTTP) que transmite el paquete de comunicación/datos respectivo. Algunas realizaciones organizan los metadatos de comunicación en estructuras de datos especializadas, conocidas en la técnica como flujos de red (por ejemplo, NetFlow® de Cisco Systems, Inc.). La Tabla **1** muestra ejemplos de metadatos de comunicación representados como flujos de acuerdo con algunas realizaciones de la presente invención.

Tabla 1

Flujo	Destino		Origen		Protocolo	Número de bytes	Número de paquetes	Banderas de TCP
#	dirección	puerto	dirección	puerto				
1	10.10.12.71	443	192.168.127.10	54321	TCP	12300	21	SA
2	192.168.127.10	54321	10.10.12.71	443	TCP	2156980	413	FSPA

En algunas realizaciones, la aplicación de seguridad **50** formula indicadores de eventos de acuerdo con los eventos de hardware, software y/o red detectados por el recolector **52** y el filtro de red **53**. La aplicación **50** puede además administrar la comunicación con el servidor de seguridad **16**, para transmitir indicadores de eventos y/o recibir notificaciones de seguridad, entre otros.

En una realización alternativa, en lugar de procesar la comunicación de red en el cliente como se muestra arriba, el filtro de red **53** y/o el enrutador **15** se pueden configurar para redirigir al servidor de seguridad **16** al menos una parte de las comunicaciones electrónicas que entran y/o salen del sistema cliente **10**. Por ejemplo, los parámetros de configuración de red del sistema cliente **10** se pueden configurar para indicar el servidor **16** como pasarela de red predeterminada. Algunas realizaciones emplean entonces el servidor de seguridad **16** para extraer indicadores de eventos del respectivo tráfico redirigido.

La Fig. **5** muestra un software ejemplar ejecutándose en el servidor de seguridad **16** de acuerdo con algunas realizaciones de la presente invención. El software ilustrado incluye un motor de perfilado **60** y un detector de anomalías **62** conectado además a un administrador de alertas **64**. Un experto en la materia apreciará que no todos los componentes ilustrados necesitan ejecutarse en la misma máquina/procesador; por ejemplo, el motor de perfilado **60** puede ejecutarse en un grupo dedicado de procesadores, mientras que las instancias del detector de anomalías **62** pueden ejecutarse en otras máquinas/procesadores.

En algunas realizaciones, el motor de perfilado **60** está configurado para analizar eventos que ocurren en un conjunto de sistemas cliente (p. ej., un subconjunto de clientes **10a-h** en la Fig. **1**) y para construir una pluralidad de perfiles de cliente que representen una forma de referencia, normal y/o legítima de operar los respectivos sistemas cliente. Un subconjunto de indicadores de eventos **20a-b** recibido de los clientes puede usarse para ensamblar un corpus de eventos de entrenamiento, denotado como corpus **18** en las Figs. **1, 5** y **6**. Luego, los perfiles se determinan de acuerdo con el corpus de eventos **18**. Determinar un perfil de cliente puede incluir, entre otras cosas, representar eventos en un espacio de eventos multidimensional abstracto y llevar a cabo procedimientos de agrupamiento de datos, como se muestra con más detalle a continuación. Los perfiles construidos pueden almacenarse entonces como entradas en la base de datos de perfiles **19**. Una entrada de base de datos de perfiles ejemplar comprende un conjunto de parámetros

de perfil, como un conjunto de coordenadas de un centroide de grupo, una medida del diámetro y/o excentricidad del grupo, etc.

La Fig. **6** ilustra componentes ejemplares y el funcionamiento del motor de perfilado **60**. En algunas realizaciones, el motor **60** comprende un codificador de eventos **70**, un motor de agrupamiento de eventos **72** y un motor de agrupamiento de clientes **74** conectado al codificador de eventos **70** y al motor de agrupamiento de eventos **72**. Una secuencia ejemplar de pasos realizados por el motor de perfilado se ilustra en la Fig. **7**.

En una secuencia de pasos **202-204-206**, el motor de perfilado **60** puede ensamblar un corpus de eventos de entrenamiento **18** de acuerdo con los indicadores de eventos recibidos de los sistemas cliente y/o enrutador(es) seleccionados. Algunas realizaciones acumulan indicadores de eventos hasta que se cumple alguna condición de acumulación. Las condiciones de acumulación pueden determinarse de acuerdo con un recuento de eventos (reunir un corpus de 1 millón de eventos), de acuerdo con una condición de tiempo (p. ej., registrar todos los eventos recibidos en un intervalo de 1 hora, etc.), de acuerdo con una identidad de un sistema cliente y/o usuario (p. ej., registrar todos los eventos recibidos de la corporación *X*, rango de IP *Y,* cuenta de suscripción *Z*, etc.), o de acuerdo con cualquier otro método conocido en la técnica. Los eventos individuales se pueden etiquetar de acuerdo con su origen y pueden comprender una marca de tiempo que caracteriza un momento en el tiempo en el que se ha producido, se ha detectado o se ha recibido el evento respectivo en el servidor de seguridad **16**, etc. En algunas realizaciones, el corpus de eventos **18** se actualiza periódicamente y/o bajo demanda mediante la incorporación de indicadores de eventos recién recibidos.

En algunas realizaciones, el codificador de eventos **70** (Fig. **6**) está configurado para ingresar un registro de eventos **26** que comprende datos que caracterizan un evento que ha ocurrido en un sistema cliente (p. ej., el inicio de un proceso en una máquina cliente) y, en respuesta, entregar un vector de evento **28a** que comprende una representación del evento respectivo como un vector en un espacio multidimensional abstracto generalmente considerado *espacio de incrustación* en la técnica. Un espacio de incrustación ejemplar está atravesado por un conjunto de ejes, en el que cada eje representa una característica de evento distinta. Características ejemplares pueden incluir, en el caso de un evento de red, una dirección IP de origen, un puerto de origen, una dirección IP de destino, un puerto de destino y un indicador del protocolo de transporte, entre otros. En otro ejemplo, cada eje del espacio de incrustación corresponde a una combinación lineal de características de eventos (por ejemplo, en una realización de descomposición de componente principal/valor singular). En realizaciones preferidas, los eventos se analizan en el contexto de otros eventos, que preceden y/o siguen al evento respectivo. En tales casos, el codificador **70** está configurado para representar eventos como vectores en un espacio de incrustación de contextos, en el que dos eventos que ocurren predominantemente en contextos similares se ubican relativamente juntos. Algunas realizaciones eligen la dimensionalidad del espacio de incrustación de acuerdo con el tamaño del vocabulario de eventos *N*, es decir, el recuento de distintos tipos de eventos que el sistema de seguridad respectivo está monitoreando (para obtener más información sobre el vocabulario de eventos, véase a continuación). Por ejemplo, la dimensionalidad del espacio de eventos puede ser del orden de la raíz cuadrática de *N,* o de un logaritmo de *N.* Una realización típica de la presente invención utiliza un espacio de contexto de incrustación que tiene varios cientos a varios miles de dimensiones.

El codificador de eventos **70** puede construirse utilizando cualquier método conocido en la técnica del procesamiento automatizado de datos. En una realización preferida, el codificador **70** comprende un sistema de inteligencia artificial, por ejemplo, una red neuronal artificial multicapa (p. ej., una red neuronal recurrente y/o de avance). Para lograr la representación deseada de vectores de eventos, los parámetros del codificador **70** puede afinarse hasta que se cumpla alguna condición de rendimiento. Dicha afinación se denomina en este documento *entrenamiento* y se representa por el paso **208** en la Fig. **7**. En una realización de red neuronal, los parámetros afinables ejemplares del codificador de eventos **70** incluyen un conjunto de pesos de sinapsis, entre otros. En algunas realizaciones, el codificador de entrenamiento **70** equivale a construir el propio espacio de incrustación. Dicho de otra manera, el espacio de incrustación no está predeterminado, sino que depende de la composición del corpus de eventos **18** y del procedimiento de entrenamiento seleccionado.

Los procedimientos de entrenamiento ejemplares se muestran en las Figs. **8-A-B** y comprenden versiones del algoritmo word2vec, como un algoritmo skip-gram y un algoritmo continuo de bolsa de palabras. En tales realizaciones, los eventos no se analizan de forma aislada, sino como componentes de una secuencia de eventos **25** que consta de múltiples eventos ordenados de acuerdo con un tiempo de ocurrencia o detección. En algunas realizaciones, todos los eventos de la secuencia respectiva se seleccionan para que ocurran en el mismo sistema cliente. La secuencia de eventos **25** comprende un evento central E_0 y un contexto de evento que consta de un subconjunto de eventos $E_{-k}...E_{-1}$ ($k \geq 0$) que precede al evento central y/o un subconjunto de eventos $E_1...E_p$ ($p \geq 0$) que sigue al evento central. Las realizaciones típicas utilizan un contexto de evento simétrico ($p=k$), con p en el rango de 2 a 5. Cada evento individual E_i ($-k \leq i \leq p$) puede representarse como un *N*-por-1 vector de números, en el que cada línea representa un tipo de evento distinto (p. ej., iniciar un navegador, iniciar una descarga de archivo, escribir datos en el disco, etc.), *N* representa el tamaño de un "vocabulario" de tipos de eventos, y un elemento distinto de cero indica que el evento respectivo es del tipo de evento respectivo. Tal representación se conoce comúnmente en la técnica como codificación 1-hot. Un tamaño ejemplar *N* del vocabulario de eventos varía de varios cientos a varios miles de tipos de eventos distintos, pero puede llegar a varios millones para aplicaciones específicas. Un experto en la materia apreciará que la codificación one-hot se usa aquí solo como un ejemplo, y de ninguna manera limita el alcance de la presente invención.

En los procedimientos de entrenamiento ejemplares, un codificador de eventos se empareja y se entrena conjuntamente con un decodificador de eventos, los cuales pueden comprender partes de una red neuronal de avance y/o recurrente. En general, el par codificador-decodificador puede configurarse para ingresar un primer subconjunto de una secuencia de entrenamiento (p. ej., evento central E_0) y entregar una "predicción" para un segundo subconjunto de la secuencia respectiva (p. ej., algún evento de contexto E_i, $i \neq 0$). En los ejemplos de las Figs. **8-A-B**, las predicciones se ilustran como vectores one-hot; realizaciones alternativas pueden usar una representación diferente. Por ejemplo, una predicción puede representarse como un vector *N*-dimensional de números, indicando cada número una probabilidad de que un tipo de evento correspondiente esté presente en el segundo subconjunto.

En un procedimiento de entrenamiento skip-gram ilustrado en las Figs. **8-A**, el par codificador-decodificador está entrenado para producir el correcto *contexto de evento*, dado el *evento central* E_0. Para cada secuencia de eventos extraídos del corpus de eventos **18**, un codificador **70a** está configurado para ingresar una codificación one-hot del evento central E_0 y para producir un vector de evento **28c** que comprende una representación del evento central E_0 en el espacio de contexto de incrustación. A su vez, un decodificador **76a** está configurado para ingresar un vector de evento **28c** y entregar una pluralidad de vectores adivinados, cada uno de los cuales representa un evento de contexto "predicho" E_i ($i \neq 0$) de la respectiva secuencia de eventos. El par codificador-decodificador puede luego ser entrenado ajustando parámetros del codificador **70a** y/o decodificador **76a** en un esfuerzo por reducir el error de predicción, es decir, para corregir un desajuste entre el contexto "predicho" y el contexto real de las respectivas secuencias de entrenamiento.

Un procedimiento de entrenamiento alternativo utiliza un algoritmo de entrenamiento continuo de bolsa de palabras y tiene como objetivo producir el correcto *evento central* E_0 de una secuencia de entrenamiento, dado el respectivo *contexto de evento.* En uno de estos ejemplos ilustrado en la Fig. **8-B**, un codificador de eventos **70b** está configurado para ingresar un conjunto de vectores one-hot que representan eventos de contexto E_i ($i \neq 0$) de la secuencia **25**, y para entregar vectores de evento incrustados **28d-f** determinados para cada evento de contexto respectivo. En contraste con la realización skip-gram ilustrada en la Fig. **8-A**, el codificador **70b** ahora está emparejado con un decodificador de eventos **76b** configurado para ingresar la pluralidad de vectores de evento **28d-f**, y para producir una predicción o "pronóstico" para el evento central E_0 de la secuencia **25**. El par codificador-decodificador puede luego ser entrenado ajustando los parámetros del codificador **70b** y/o decodificador **76b** en un esfuerzo por reducir el error de predicción, es decir, el desajuste entre el evento central "predicho" y el evento central real de las respectivas secuencias de entrenamiento.

Una secuencia ejemplar de pasos que implementan el entrenamiento de un codificador de eventos se ilustra en la Fig. **9**. Un paso **222** recupera un conjunto de registros de eventos del corpus de eventos **18** e identifica una secuencia de eventos **25** de acuerdo con las marcas de tiempo de los eventos y de acuerdo con un origen de los respectivos eventos (es decir, los sistemas cliente donde han ocurrido los respectivos eventos). En una realización skip-gram, un paso **224** luego ejecuta el codificador de eventos **70a** para producir una representación del espacio de incrustación del evento E_0 (vector de evento **28c** en la Fig. **8-A**). En un paso **226**, el motor de perfilado **60** ejecuta el decodificador de eventos **76a** para producir un conjunto de predicciones o "pronósticos" para eventos que preceden y/o siguen al evento central E_0 dentro de la secuencia **25**. Un paso **228** compara cada evento de contexto predicho con el evento de contexto real respectivo E_i ($i \neq 0$) de la secuencia **25**, determinando así un error de predicción numérico. El error de predicción, que puede interpretarse como una función de coste o una función objetivo, puede calcularse de acuerdo con cualquier método conocido en la técnica de la inteligencia artificial. Dichos cálculos pueden comprender la determinación de una distancia, por ejemplo, una distancia de Levenshtein, euclidiana o coseno entre los eventos predichos y los reales. Algunas realizaciones determinan una función objetivo de acuerdo con una medida de entropía cruzada. En un paso **230**, el motor de perfilado puede ajustar los parámetros del codificador **70a** en la dirección de minimizar el error de predicción calculado. Algunos ejemplos de algoritmos utilizados para el entrenamiento incluyen la retropropagación mediante un descenso de gradiente, recocido simulado y algoritmos genéticos, entre otros. Algunas realizaciones luego repiten los pasos **222-230** hasta que se cumpla una condición de finalización, por ejemplo, hasta que el error de predicción promedio sobre el corpus de eventos **18** caiga por debajo de un umbral predeterminado. En otra realización, el entrenamiento continúa durante una cantidad de tiempo predeterminada o durante un recuento predeterminado de iteraciones. Un experto en la materia sabrá que la secuencia de pasos ilustrada en la Fig. **9** es igualmente adecuada para una realización de bolsa de palabras (Fig. **8-B**), con pequeñas adaptaciones.

En respuesta al entrenamiento del codificador de eventos como se muestra arriba, algunas realizaciones transforman aún más el espacio de incrustación generado para reducir su dimensionalidad. Esta operación puede comprender cualquier algoritmo de reducción de la dimensionalidad de los datos, por ejemplo, un análisis de componentes principales (PCA) o una descomposición en valores singulares (SVD).

Después del entrenamiento y reducción de dimensionalidad opcional (paso **208** en la Fig. **7**), el codificador de eventos **70** es capaz de representar cada evento como un vector en un espacio de incrustación multidimensional de contextos de eventos, en el que dos eventos que ocurren con frecuencia dentro del mismo contexto de eventos ocupan posiciones similares. Dicho de otro modo, dos de estos eventos están separados en el espacio de incrustación por una distancia menor que la distancia entre dos eventos que ocurren predominantemente en diferentes contextos.

Volviendo a los componentes del motor de perfilado **60** (Fig. **6**), el motor de agrupamiento de eventos **74** está configurado para organizar vectores de eventos producidos por un codificador de eventos entrenado **70** y que

representan los miembros del corpus de entrenamiento **18**, en grupos de acuerdo con una posición de cada vector de evento dentro del espacio de incrustación (ver también el paso 210 en la Fig. **7**). En algunas realizaciones, un grupo comprende una pluralidad de eventos que están relativamente juntos en el espacio de incrustación o, dicho de otro modo, una pluralidad de eventos caracterizados por una distancia entre eventos relativamente pequeña en el espacio de incrustación. En una realización alternativa, un grupo consta de eventos que ocupan una región específica del grupo del espacio de incrustación. Dichas regiones pueden ser mutuamente excluyentes o superponerse parcialmente. La Fig. **10** ilustra un espacio de incrustación ejemplar y un conjunto de grupos de eventos **80a-b** de acuerdo con algunas realizaciones de la presente invención. Los ejes ilustrados pueden comprender, por ejemplo, los componentes principales primero y segundo de los vectores de eventos ilustrados (vectores **28g-h-k**). En una realización que utiliza un espacio de incrustación de contextos de eventos, un grupo puede contener selectivamente eventos que ocurren principalmente dentro de un contexto de eventos similar. Además, el mismo grupo puede incluir eventos que ocurren en varios sistemas cliente y/o que representan la actividad de varios usuarios.

Para construir grupos de eventos, el motor de perfilado **60** puede emplear cualquier algoritmo de agrupamiento de datos conocido en la técnica, por ejemplo, una variante de un algoritmo de k-medias. Otra realización ejemplar puede entrenar un conjunto de perceptrones para tallar el espacio de incrustación en regiones distintas y asignar vectores de eventos ubicados dentro de cada región a un grupo de eventos distinto. El número de grupos y/o regiones puede estar predeterminado (p. ej., de acuerdo con un recuento de sistemas cliente protegidos y/o tipos de eventos monitoreados) o puede determinarse dinámicamente por el propio algoritmo de agrupamiento. Un resultado del agrupamiento de eventos comprende un conjunto de parámetros de grupo de eventos **54** (Fig. **6**), que puede incluir, para cada grupo, las coordenadas del centroide del grupo y una medida de la extensión del grupo, p. ej., un diámetro y/o excentricidad. Otros parámetros de grupo ejemplares **54** pueden incluir, entre otros, una lista de miembros del grupo respectivo y un miembro seleccionado del grupo respectivo considerado como representativo/arquetípico del grupo respectivo. Los parámetros del grupo se pueden pasar al motor de agrupamiento de clientes **74**.

El motor de agrupamiento de clientes **74** (Fig. **6**) está configurado para determinar un conjunto de perfiles de cliente de acuerdo con los grupos de eventos calculados por el motor de agrupamiento de eventos **72**. Dichos perfiles de cliente se ilustran en la Fig. **11**. En algunas realizaciones, cada perfil de cliente comprende un subconjunto seleccionado (grupo) de los sistemas cliente protegidos **10a-h**. Algunos perfiles de cliente pueden incluir varios grupos de clientes. En algunas realizaciones, un perfil de cliente puede comprender un arquetipo de perfil, que puede ser un miembro real del grupo de clientes respectivo, o un sistema cliente ficticio caracterizado por una posición específica en el espacio del perfil. Por ejemplo, un arquetipo de perfil puede comprender un centroide de un grupo de clientes determinado por el motor de agrupamiento de clientes **74**.

Para calcular perfiles de cliente, algunas realizaciones del motor de agrupamiento de clientes **74** asignan sistemas cliente **10a-h** a grupos de acuerdo con un perfil de evento indicativo de una distribución típica de eventos que ocurren en los respectivos sistemas cliente. En una realización ejemplar, un perfil de evento de un sistema cliente comprende un vector de números, determinado cada uno de acuerdo con un recuento de eventos que ocurren en el sistema cliente respectivo y que pertenece a un grupo de eventos distinto previamente determinado por el motor de agrupamiento de eventos **72**. En el ejemplo ilustrado en la Fig. **12**, cada componente del perfil de evento se determina de acuerdo con una medida de fidelidad al grupo indicativa de una proporción de eventos que pertenecen al grupo de eventos C_i respectivo, determinada como una fracción de un recuento total de eventos disponibles del sistema cliente respectivo. Por ejemplo, cuando el motor de agrupamiento de eventos **72** ha identificado tres grupos de eventos C_1, C_2 y C_3, un vector de perfil de eventos [0,1, 0,75, 0,15] puede representar un sistema cliente en el que el 10 % de los eventos que ocurren en el sistema cliente respectivo pertenecen al grupo de eventos C_1, mientras que el 75 % de los eventos pertenecen al grupo de eventos C_2 y el 15 % de los eventos pertenecen al grupo de eventos C_3.

En la realización ejemplar ilustrada en la Fig. **11**, cada sistema cliente se representa en un espacio de perfil multidimensional de acuerdo con el perfil de evento respectivo. Dicho de otra manera, cada coordenada de un sistema cliente representa un componente del perfil de evento del cliente respectivo. La Fig. **11** muestra tres grupos/perfiles de cliente ejemplares **82a-c**. Un experto en la materia puede utilizar cualquier método conocido en la técnica del aprendizaje automático o la extracción de datos para construir dichos perfiles; métodos ejemplares incluyen variantes de un algoritmo de agrupamiento de k-medias y redes neuronales, entre otros. Realizaciones alternativas pueden usar otros criterios de asignación de un sistema cliente a un grupo, o usar tales criterios además del perfil de evento del cliente respectivo. Criterios ejemplares adicionales de agrupamiento de clientes incluyen, entre otros, un propietario y/o usuario del respectivo sistema cliente, una dirección de red del respectivo sistema cliente, un tipo de dispositivo del respectivo sistema cliente, etc. Por ejemplo, los clientes que pertenecen a la misma familia, la misma corporación o el mismo dominio de red pueden agruparse en el mismo grupo.

Después del agrupamiento de clientes, el motor de perfilado **60** puede guardar parámetros de grupos, como una lista de sistemas cliente asignados a cada grupo/perfil, coordenadas de arquetipos de grupos (p. ej., centroides), diámetros de grupos, etc., en la base de datos de perfiles **19**.

La Fig. **13** ilustra componentes ejemplares y el funcionamiento del detector de anomalías **62** de acuerdo con algunas realizaciones de la presente invención (véase también la Fig. **5**). El detector de anomalías **62** está configurado para recibir un flujo de eventos **24** que comprende indicadores de eventos indicativos de eventos que ocurren en varios sistemas cliente y, en respuesta, para entregar una etiqueta de seguridad **88** que indica si los eventos respectivos son

indicativos de una amenaza a la seguridad, como una intrusión o ejecución de software malicioso. En algunas realizaciones, el detector de anomalías **62** comprende un administrador de perfiles **84** configurado, en respuesta a la recepción de una notificación de evento indicativa de un evento que ocurre en un sistema cliente protegido, para seleccionar un perfil de cliente de acuerdo con el evento respectivo. El administrador de perfiles **84** está conectado además a un modelo de comportamiento **86** configurado para determinar si el evento respectivo se ajusta a un patrón de comportamiento normal/de referencia representado por el perfil respectivo. Cuando no, el evento respectivo puede ser considerado una anomalía, indicando así un posible ataque al sistema cliente respectivo.

Como preparación para realizar la detección de anomalías como se muestra a continuación, algunas realizaciones del detector de anomalías **62** primero se entrenan en un corpus de eventos, utilizando una salida del motor de perfilado **60**. Uno de los propósitos de entrenar el detector de anomalías **62** es determinar un comportamiento de usuario normal/de referencia para cada perfil de cliente identificado por el motor de perfilado **60**. El entrenamiento comprende ajustar un conjunto de parámetros del modelo de comportamiento **86** hasta que se cumpla un criterio de finalización. El corpus de eventos utilizado para entrenar el detector de anomalías **62** puede diferir del corpus de entrenamiento **18** utilizado para entrenar componentes del motor de perfilado **60**.

La Fig. **14** muestra una secuencia ejemplar de pasos realizados por el detector de anomalías **62** durante un procedimiento de entrenamiento de acuerdo con algunas realizaciones de la presente invención. En respuesta al motor de anomalías **60** que construye un conjunto de perfiles de cliente, un paso **242** selecciona uno de esos perfiles de cliente de la base de datos de perfiles **19**. En algunas realizaciones, cada uno de estos perfiles de cliente comprende un conjunto de grupos de clientes, por ejemplo, el grupo **82a** en la Fig. **11**. Cada grupo de clientes incluye además un subconjunto seleccionado de sistemas cliente protegidos. Un paso **244** puede seleccionar un conjunto de entrenamiento de eventos registrados como ocurridos en cualquier sistema cliente asociado con el perfil/grupo respectivo. En algunas realizaciones, el paso **244** puede comprender el conjunto de eventos de entrenamiento seleccionado del corpus de entrenamiento **18** ya usado para construir perfiles de cliente como se muestra arriba. Un paso más **246** puede usar el conjunto de eventos de entrenamiento respectivo como corpus de entrenamiento para entrenar el modelo de comportamiento **86**.

En algunas realizaciones, el modelo de comportamiento **86** comprende componentes que son similares en estructura y función a algunos componentes del motor de perfilado **60**. Por ejemplo, algunas realizaciones del modelo **86** incluyen un par codificador-decodificador como se ilustra en la Fig. **15**, que puede construirse utilizando tecnología de redes neuronales y entrenarse de acuerdo con un miembro de la familia de algoritmos word2vec (véase la descripción anterior en relación con las Figs. **8-A-B**). Entrenar el modelo de comportamiento **86** puede entonces equivaler a ajustar parámetros del codificador **70c** y/o decodificador **76c** (p. ej., un conjunto de pesos de sinapsis) con el objetivo de representar cada evento del grupo/perfil de cliente respectivo como un vector en un espacio de incrustación de eventos. En una realización preferida, el codificador **70c** analiza cada evento en el contexto de una secuencia de eventos y genera un espacio de incrustación en el que los eventos que ocurren predominantemente en contextos similares están separados por una distancia menor, en comparación con los eventos que ocurren en otros contextos. Sin embargo, el espacio de incrustación de eventos (es decir, el significado de los ejes, el tamaño de las distancias entre eventos, etc.) resultante del codificador de entrenamiento **70c** puede diferir sustancialmente del espacio de incrustación de eventos resultante del codificador de eventos de entrenamiento **70**, porque los corpus de entrenamiento utilizados para los dos codificadores son distintos.

En una realización preferida, el paso **246** comprende entrenar el par codificador-decodificador usando una versión del algoritmo de bolsa de palabras (ver Fig. **8-B**). En uno de esos ejemplos, el par codificador-decodificador (Fig. **15**) está configurado para recibir una pluralidad de eventos E_{-k},...E_{-1}, E_1, ... E_p que representan un contexto de evento de una secuencia de eventos actualmente analizada, y producir un vector de puntuación de predicción N-dimensional **90**, en el que cada elemento está asociado con un tipo de evento distinto, representando cada elemento una probabilidad de que el evento central de la secuencia de eventos respectiva sea del tipo de evento respectivo. Por ejemplo, un valor de puntuación más alto puede indicar que es más probable que ocurra el tipo de evento respectivo como el evento central de la secuencia de eventos respectiva que otros tipos de eventos que tienen puntuaciones más bajas. En tales realizaciones, un entrenamiento ejemplar del modelo **86** puede comprender seleccionar secuencias de eventos del subconjunto de eventos identificados en el paso **244** (Fig. **14**), ingresar el contexto de evento de la secuencia respectiva al codificador **70c**, ejecutar el decodificador **76c** para producir una predicción para el evento central E_0 de la secuencia de eventos respectiva y sancionar las predicciones incorrectas retropropagando el error de predicción a través de las redes neuronales que forman el codificador **70c** y/o decodificador **76c**. En respuesta a un entrenamiento exitoso, un paso **248** puede guardar los valores de parámetros del modelo de comportamiento entrenado. El procedimiento de entrenamiento puede repetirse para cada perfil de cliente identificado por el motor de perfilado **60**.

La Fig. **16** ilustra una secuencia ejemplar de pasos realizados por el detector de anomalías **62** para proteger un sistema cliente objetivo (como clientes **10a-h** en la Fig. 1) contra amenazas a la seguridad informática de acuerdo con algunas realizaciones de la presente invención. El sistema cliente objetivo puede o no ser miembro del subconjunto de clientes que proporcionan el corpus de entrenamiento de eventos que han producido modelos de comportamiento y/o perfiles de cliente como se muestra arriba. Para proteger el sistema cliente objetivo, los eventos pueden detectarse en el sistema cliente objetivo y/u otros dispositivos, como enrutadores **15a-b** (ver Fig. **1**) y pueden ser comunicados al servidor de seguridad **16** en forma de indicadores de eventos. Dichos indicadores de eventos pueden preprocesarse entonces según su origen, tipo de evento, tiempo, configuración de la cuenta de servicio, etc., y organizarse como un

flujo de eventos **24**. Los eventos se pueden procesar individualmente o por lotes. En respuesta a la recepción de un indicador de evento del sistema cliente objetivo, en un paso **254**, el detector de anomalías **62** puede ensamblar una secuencia de eventos para analizar de acuerdo con el indicador de evento respectivo. El paso **254** puede incluir identificar el origen del evento (es decir, el sistema cliente donde ocurrió el evento respectivo), seleccionar del flujo de eventos **24** una pluralidad de otros eventos para formar una secuencia de eventos. En algunas realizaciones, los miembros de la secuencia se eligen para que todos se originen en el mismo sistema cliente objetivo. En otro ejemplo, todos los miembros de la secuencia deben ocurrir en un subconjunto predeterminado de sistemas cliente, como un subdominio de red o una dirección IP común, por ejemplo. Los eventos elegidos también se pueden ordenar de acuerdo con su hora de ocurrencia y/o detección, por ejemplo, utilizando una marca de tiempo provista del indicador de evento entrante. La secuencia de eventos se puede dividir además en partes, por ejemplo, identificando un evento central y un contexto de evento (ver, p. ej., Fig. **8-A**).

En un paso **256**, el administrador de perfiles **84** puede seleccionar un perfil de cliente de acuerdo con el indicador de evento respectivo, p. ej., de acuerdo con una identidad del sistema cliente objetivo donde ha ocurrido el evento respectivo. Cuando el respectivo sistema cliente objetivo ha proporcionado eventos de entrenamiento para el desarrollo de perfiles de cliente y/o para el entrenamiento de modelos de comportamiento, el paso **256** puede comprender seleccionar un grupo/perfil de cliente que tenga el respectivo sistema cliente objetivo como miembro. También se pueden utilizar otros criterios de selección de perfiles. Por ejemplo, el paso **256** puede comprender seleccionar un perfil de cliente de acuerdo con una posición del sistema cliente objetivo dentro de un espacio de perfiles de cliente (ver Fig. **11**), por ejemplo, comparando la posición del sistema cliente objetivo con un conjunto de arquetipos de grupo o centroides y seleccionando el grupo/perfil cuyo centroide esté más cerca del sistema cliente objetivo. En un ejemplo de este tipo, el perfil de cliente puede seleccionarse de acuerdo con un perfil de evento determinado para el sistema cliente objetivo (p. ej., de acuerdo con un recuento de eventos recibidos del sistema cliente objetivo, que se ajustan a una categoría/grupo de eventos en particular). Otros criterios de selección del perfil de cliente pueden incluir seleccionar el perfil de cliente de acuerdo con una dirección de red del sistema cliente objetivo (p. ej., seleccionar un perfil de cliente que contenga clientes que tengan la misma dirección IP que el sistema cliente objetivo), con un propietario/usuario del sistema cliente objetivo (p. ej., seleccionar un perfil que contenga miembros del mismo hogar que el sistema cliente objetivo), etc.

En un paso más **258**, el detector de anomalías puede instanciar el modelo de comportamiento **86** con valores de parámetros específicos para el respectivo perfil de cliente seleccionado. En algunas realizaciones, siguiendo la instanciación específica del perfil, ejecutar el modelo **86** (paso **260**) comprende proyectar eventos de la respectiva secuencia de eventos en el espacio de incrustación de eventos asociado con el respectivo perfil de cliente.

Un paso **262** ahora puede determinar si el (los) evento(s) de la secuencia de eventos respectiva es (son) o no representativo(s) del comportamiento normal/de referencia del usuario asociado con el perfil de cliente respectivo. En una realización, en el paso **260**, comprende alimentar el contexto del evento (E_i, $i \neq 0$) de la secuencia respectiva al modelo de comportamiento **86** y calcular el vector de puntuación de predicción **90** de la secuencia respectiva. El paso **262** entonces puede comprender identificar el elemento del vector **90** correspondiente al tipo de evento del evento central real E_0 de la secuencia, y comparar la puntuación respectiva con un umbral predeterminado (p. ej., 0,95). En algunas realizaciones, un valor de puntuación inferior al umbral indica que el evento respectivo E_0 es sustancialmente improbable que ocurra en el contexto de evento respectivo y, por lo tanto, indica una anomalía coherente con una posible amenaza a la seguridad informática. En algunas realizaciones, un usuario o administrador del servidor de seguridad **16** puede ajustar la sensibilidad del método ajustando el valor del umbral. En uno de esos ejemplos, diferentes valores de umbral están asociados con diferentes grupos de sistemas cliente.

En una realización alternativa, el paso **260** puede comprender utilizar el modelo **86** para determinar una representación de un evento E_i de la secuencia en el espacio de incrustación del evento específico del perfil de cliente respectivo. El paso **262** entonces puede comprender determinar si el evento E_i se ajusta a un patrón de comportamiento normal para el perfil de cliente respectivo de acuerdo con una posición del evento respectivo dentro del espacio de incrustación. Por ejemplo, un evento puede considerarse normal cuando se posiciona dentro de un grupo de eventos de entrenamiento (p. ej., más cerca de un centroide de grupo que un umbral predeterminado). En otro ejemplo, un evento puede considerarse normal/benigno cuando se ubica en ciertas regiones del espacio de incrustación y anómalo cuando se ubica en otras regiones.

Cuando un evento de la secuencia (p. ej., E_0) se considera una anomalía, en otras palabras, no se ajusta al patrón de normalidad establecido a través del entrenamiento para el perfil de cliente respectivo, un paso **264** puede marcar el evento respectivo para su posterior análisis. En algunas realizaciones, una anomalía puede desencadenar la transmisión de una alerta de seguridad por parte de un administrador de alertas **64** del servidor de seguridad **16** (ver Fig. **5**). Las alertas de seguridad pueden enviarse al sistema cliente donde ocurrió el evento anómalo y/o a un administrador del sistema cliente respectivo. Los incidentes de eventos anómalos también pueden recopilarse e informarse para su posterior análisis en un laboratorio de seguridad informática.

Los sistemas y métodos ejemplares descritos anteriormente permiten una detección eficiente de amenazas a la seguridad informática tales como software malicioso e intrusión. Los sistemas y métodos divulgados implementan un enfoque de comportamiento para la seguridad informática, en el que el sistema infiere automáticamente un

comportamiento de usuario normal/de referencia de acuerdo con un corpus de eventos de entrenamiento, y en el que una desviación de un patrón de comportamiento de referencia puede indicar una amenaza.

Algunas realizaciones detectan varios eventos que ocurren en una pluralidad de sistemas cliente, p. ej., computadoras, teléfonos móviles, dispositivos de red y máquinas virtuales. Eventos ejemplares incluyen inicios de procesos específicos, intentos de acceder a ciertos archivos o ubicaciones de red y eventos de tráfico de red como acceder a ciertos puertos y direcciones, entre otros. Un experto en la materia comprenderá que los sistemas y métodos descritos en este documento pueden adaptarse a otros tipos de eventos, como eventos relacionados con la actividad de un usuario en las redes sociales, el historial de navegación de un usuario y la actividad de juego de un usuario, entre otros. Las notificaciones de eventos se agregan en un servidor de seguridad. Una colección de dichos eventos se puede usar como corpus de entrenamiento para construir un conjunto de perfiles de cliente, donde cada perfil de cliente puede representar un solo usuario, una sola máquina o múltiples usuarios/máquinas. En algunas realizaciones, cada perfil de cliente comprende un subconjunto de sistemas cliente y/o un subconjunto de eventos que han ocurrido en los respectivos subconjuntos de sistemas cliente. Cada perfil de cliente puede representar un patrón de uso normal y/o benigno de los respectivos sistemas cliente. Dichos perfiles de cliente pueden usarse entonces para detectar incidentes de comportamiento anómalo, que pueden ser indicativos de una amenaza a la seguridad informática.

Cierta seguridad informática convencional opera de acuerdo con un conjunto de reglas que cuantifican el comportamiento que es indicativo de malicia. Dado que los desarrolladores suelen estar interesados en ofrecer tales soluciones a una amplia variedad de clientes, las reglas de comportamiento suelen ser genéricas y no adaptadas a usuarios específicos. Sin embargo, en la práctica, los usuarios son muy heterogéneos. Incluso dentro de la misma empresa o familia, la forma en que cada miembro utiliza una computadora puede variar sustancialmente. Un conjunto de acciones que pueden considerarse normales para un desarrollador o ingeniero de software pueden ser muy inusuales cuando se detectan en una computadora en el departamento de contabilidad. Además, el mismo usuario puede tener comportamientos sustancialmente diferentes en el trabajo y en el hogar. Por lo tanto, las reglas de comportamiento genéricas pueden no capturar la diversidad y especificidad de los usuarios reales. A diferencia de dichos sistemas convencionales, en algunas realizaciones de la presente invención, los eventos que ocurren en cada sistema cliente se revisan y analizan selectivamente frente a un modelo que captura un comportamiento normal/de referencia del propio sistema cliente respectivo y/o de clientes similares. Dicho de otra manera, los límites de la "normalidad" del comportamiento pueden definirse con una especificidad sustancial: una máquina cliente específica, un grupo específico de usuarios (p. ej., un departamento particular de una empresa, miembros de una familia, un grupo de edad particular), etc.

Debido a la proliferación del software y el uso de Internet, un intento de desarrollar perfiles de comportamiento altamente específicos, por ejemplo, perfiles ligados a cada usuario individual, puede requerir recursos computacionales irrazonables y, por lo tanto, puede resultar poco práctico. Además, la recopilación de eventos de usuarios/máquinas individuales puede no proporcionar suficientes datos para desarrollar modelos de comportamiento estadísticamente robustos. En contraste con este enfoque, algunas realizaciones de la presente invención agrupan múltiples usuarios y/o máquinas en un solo perfil de cliente, asegurando así un compromiso útil entre especificidad, robustez y costos computacionales. Además, la forma en que los usuarios y las máquinas se agrupan en perfiles se basa en sí misma en criterios de comportamiento, para garantizar que dicho agrupamiento conserve la especificidad. En algunas realizaciones, cada perfil de cliente agrupa a usuarios/máquinas que tienen perfiles de eventos sustancialmente similares. Dicho de otra manera, todos los miembros de un perfil de cliente muestran un comportamiento de referencia similar en términos de estadísticas de eventos que ocurren en las máquinas miembro.

Algunos sistemas y métodos de seguridad informática convencionales analizan principalmente eventos individuales. Muchos eventos que ocurren durante el funcionamiento de un sistema informático (p. ej., abrir un archivo, acceder a una página web) pueden no ser indicativos de malicia cuando se toman de forma aislada. Sin embargo, pueden ser maliciosos cuando ocurren en el contexto de otros eventos, por ejemplo, como una secuencia particular de acciones. A diferencia de las soluciones más convencionales, algunas realizaciones de la presente invención analizan explícitamente los eventos en contexto y, por lo tanto, se adaptan mejor a tales situaciones de correlación de eventos. Una realización preferida representa eventos individuales como vectores en un espacio de incrustación multidimensional que tiene la propiedad distintiva de que un par de eventos que ocurren con una frecuencia relativamente alta en el mismo contexto de eventos están separados por una distancia menor que otro par de eventos que ocurren con menos frecuencia en el mismo contexto de evento.

El modelado de comportamiento exitoso puede requerir la detección de una gran cantidad (p. ej., cientos o miles) de distintos tipos de eventos, pero no todos los tipos de eventos pueden ser igualmente importantes en el modelado de comportamiento. Recopilar y analizar datos estadísticos sobre tantos tipos de eventos recibidos de un gran número de fuentes puede resultar poco práctico. Para abordar este problema, algunas realizaciones agrupan eventos en categorías o grupos de eventos según un grado de similitud entre eventos, creando así estadísticas más robustas y/o relevantes. La construcción de perfiles de cliente puede verse sustancialmente facilitada por tal reducción significativa de la dimensionalidad. La similitud de eventos puede determinarse de acuerdo con varios criterios, por ejemplo, de acuerdo con la distancia que separa dos eventos en un espacio de incrustación de eventos. En una realización preferida, dos eventos pueden considerarse similares si ocurren predominantemente en el mismo contexto (p. ej., los eventos *A* y *B* se consideran similares cuando ambos *A* y *B* son frecuentemente precedidos por un evento *X* y/o seguidos por un evento *Y,* es decir, como en secuencias ejemplares *XAY* y *XBY*).

Las Figs. **17-A-B** ilustran un experimento de aplicación de algunos de los sistemas y métodos descritos anteriormente para la detección de amenazas a la seguridad informática. Se utilizó un corpus de eventos recopilados de múltiples clientes monitoreados para entrenar los componentes de un motor de perfilado, como se muestra arriba, lo que resultó en que los clientes monitoreados se dividieran en 11 grupos/perfiles de clientes. Los eventos se agruparon en categorías de eventos de acuerdo con una representación de cada evento en un espacio de incrustación de 15 dimensiones. Se desarrollaron modelos de comportamiento específicos del perfil para cada uno de los respectivos grupos de clientes. Luego, se simuló un tipo particular de ataque en una máquina de prueba. Las secuencias de eventos recolectadas de la máquina de prueba se enviaron a un detector de anomalías instanciado, a su vez, con parámetros específicos para cada uno de los modelos de comportamiento. Algunas de estas secuencias de eventos se detectaron como anomalías.

La Fig. **17-A** muestra las puntuaciones de anomalías específicas del grupo, representadas en una escala en la que una puntuación de 1 indica un 100 % de certeza de una anomalía (p. ej., al menos un evento de una secuencia de eventos recibida de la máquina de prueba no se había visto durante el entrenamiento). El gráfico representa valores de puntuación promediados sobre secuencias de eventos anómalos y las desviaciones estándar asociadas. La figura muestra que la(s) misma(s) secuencia(s) puede(n) considerarse anomalías con un nivel de certeza que es específico del grupo. Dicho de otra manera, las mismas secuencias de eventos se consideran "menos anómalas" en ciertos clientes que en otros. Por ejemplo, los modelos de comportamiento asociados con los grupos 1, 2 y 7 no solo detectan el ataque con una eficiencia relativamente mayor que otros modelos, sino que todas las secuencias de eventos asociadas con los ataques se consideraron "igualmente anómalas". Por el contrario, los modelos asociados con los grupos 0 y 9 indican algunas secuencias de eventos del mismo ataque como "menos anómalas" que otras.

La Fig. **17-B** muestra las tasas de detección promedio específicas del perfil logradas para tres tipos distintos de ataques. Las secuencias de eventos recopiladas de la máquina de prueba durante cada tipo de ataque se analizaron utilizando cada uno de los 11 modelos de comportamiento entrenados específicos del perfil. La tasa de detección difiere entre modelos y tipos de ataque, lo que da más fe de la especificidad de algunos de los sistemas y métodos descritos en este documento.

Dichos resultados experimentales indican otra aplicación potencial de algunas realizaciones de la presente invención. Una solución de seguridad informática centralizada puede desarrollar selectivamente estrategias de protección para cada conjunto de clientes identificados por un perfil de cliente y/o para otros clientes que tengan una similitud con un arquetipo de cada grupo de clientes. Algunas realizaciones pueden identificar grupos de clientes para los cuales los métodos descritos aquí ofrecen un grado de seguridad satisfactorio, y otros grupos de clientes que requieren medidas de seguridad adicionales. Adaptar la protección a cada grupo de clientes puede mejorar la experiencia del usuario y reducir los gastos computacionales innecesarios.

Será evidente para un experto en la técnica que las realizaciones anteriores pueden modificarse de muchas maneras sin apartarse del alcance de la invención. En consecuencia, el alcance de la invención debería estar determinado por las siguientes reivindicaciones.

REIVINDICACIONES

1. Un sistema informático de servidor (16) que comprende al menos un procesador de hardware configurado para:

asignar (210) eventos de un corpus de entrenamiento (18) a una pluralidad de categorías de eventos, comprendiendo el corpus de entrenamiento una colección de eventos que han ocurrido en una pluralidad de sistemas cliente (10);

en respuesta a la asignación de eventos a categorías de eventos, asignar (212) sistemas cliente de la pluralidad de sistemas cliente a una pluralidad de grupos de clientes (19) de acuerdo con la pluralidad de categorías de eventos; y

en respuesta a la asignación de sistemas cliente a grupos de clientes, transmitir (256) un indicador de pertenencia a grupo de clientes a un detector de anomalías configurado para determinar si un evento objetivo que ocurre en un sistema cliente objetivo es indicativo de una amenaza a la seguridad informática;

en el que asignar eventos a categorías de eventos comprende:

seleccionar (222) una pluralidad de eventos del corpus de entrenamiento, habiendo ocurrido la pluralidad de eventos en un sistema cliente de la pluralidad de sistemas cliente,

organizar la pluralidad de eventos de acuerdo con un tiempo de ocurrencia para formar una secuencia de eventos (25), y

en respuesta, asignar (226) un evento seleccionado de la secuencia de eventos a una categoría de eventos seleccionados de acuerdo con un primer evento que precede al evento seleccionado y además de acuerdo con un segundo evento que sigue al evento seleccionado dentro de la secuencia de eventos;

en el que asignar sistemas cliente a grupos de clientes comprende asignar el sistema cliente a un grupo de clientes seleccionado de acuerdo con un perfil de evento determinado de acuerdo con un recuento de eventos que ocurren en el sistema cliente y que pertenecen a la categoría de eventos seleccionados; y

en el que el detector de anomalías está configurado para determinar (262) si el evento objetivo es indicativo de la amenaza a la seguridad informática de acuerdo con un modelo de comportamiento entrenado (258) en un subcorpus de eventos específico del grupo de clientes, seleccionado el subcorpus específico del grupo de clientes del corpus de entrenamiento para incluir solo eventos que han ocurrido en una pluralidad de miembros de un grupo objetivo de la pluralidad de grupos de clientes.

2. El sistema informático de la reivindicación 1, en el que asignar eventos a categorías de eventos comprende:

determinar una posición del evento seleccionado en un espacio de incrustación de eventos multidimensional de acuerdo con los eventos primero y segundo; y

asignar el evento seleccionado a la categoría de eventos seleccionados de acuerdo con la posición del evento seleccionado en el espacio de incrustación de eventos.

3. El sistema informático de la reivindicación 2, configurado además para determinar la categoría de eventos seleccionados de acuerdo con un grupo de eventos que ocupan posiciones similares en el espacio de incrustación de eventos.

4. El sistema informático de la reivindicación 2, en el que determinar la posición del evento seleccionado en el espacio de incrustación de eventos comprende entrenar un codificador de eventos para producir un conjunto de coordenadas que indiquen la posición, y en el que entrenar el codificador de eventos comprende:

acoplar el codificador de eventos a un decodificador de eventos configurado para recibir el conjunto de coordenadas y para entregar un indicador de predicción indicativo de una probabilidad de que la secuencia de eventos comprenda los eventos primero y segundo; y

ajustar un conjunto de parámetros del codificador de eventos de acuerdo con el indicador de predicción.

5. El sistema informático de la reivindicación 2, en el que determinar la posición del evento seleccionado en el espacio de incrustación de eventos comprende entrenar un codificador de eventos para producir un conjunto de coordenadas que indiquen la posición, y en el que entrenar el codificador de eventos comprende:

acoplar el codificador de eventos a un decodificador de eventos configurado para recibir el conjunto de coordenadas y para entregar un contexto predicho del evento seleccionado, comprendiendo el contexto predicho un primer evento predicho y un segundo evento predicho;

comparar el primer evento predicho con el primer evento y el segundo evento predicho con el segundo evento; y

ajustar un conjunto de parámetros del codificador de eventos de acuerdo con un resultado de la comparación.

6. El sistema informático de la reivindicación 1, en el que el perfil de evento comprende una pluralidad de componentes, perteneciendo cada componente determinado de acuerdo con una proporción de eventos a cada categoría de eventos de la pluralidad de categorías de eventos, calculada la proporción a partir de un recuento total de eventos del corpus de entrenamiento que ocurren en el sistema cliente.

7. El sistema informático de la reivindicación 1, en el que asignar sistemas cliente a grupos de clientes comprende asignar sistemas cliente que tienen perfiles de eventos similares al mismo grupo de clientes.

8. El sistema informático de la reivindicación 1, en el que el evento del corpus de entrenamiento comprende un inicio de un proceso seleccionado en un sistema cliente de la pluralidad de sistemas cliente.

9. Un método implementado por computadora que comprende:

emplear al menos un procesador de hardware de un sistema informático para asignar eventos de un corpus de entrenamiento a una pluralidad de categorías de eventos, en el que el corpus de entrenamiento comprende una colección de eventos que ocurren en una pluralidad de sistemas cliente;

en respuesta a la asignación de eventos a categorías de eventos, emplear al menos un procesador de hardware del sistema informático para asignar sistemas cliente de la pluralidad de sistemas cliente a una pluralidad de grupos de clientes según la pluralidad de categorías de eventos; y

en respuesta a la asignación de sistemas cliente a grupos de clientes, emplear al menos un procesador de hardware del sistema informático para transmitir un indicador de pertenencia a grupo de clientes a un detector de anomalías configurado para determinar si un evento objetivo que ocurre en un sistema cliente objetivo es indicativo de una amenaza a la seguridad informática;

en el que asignar eventos a categorías de eventos comprende:

seleccionar una pluralidad de eventos del corpus de entrenamiento, habiendo ocurrido la pluralidad de eventos en un sistema cliente de la pluralidad de sistemas cliente,

organizar la pluralidad de eventos de acuerdo con un tiempo de ocurrencia para formar una secuencia de eventos, y

en respuesta, asignar un evento seleccionado de la secuencia de eventos a una categoría de eventos seleccionados de acuerdo con un primer evento que precede al evento seleccionado y además de acuerdo con el segundo evento que sigue al evento seleccionado dentro de la secuencia de eventos;

en el que asignar sistemas cliente a grupos de clientes comprende asignar el sistema cliente a un grupo de clientes seleccionado según un perfil de evento determinado de acuerdo con un recuento de eventos que ocurren en el sistema cliente y que pertenecen a la categoría de eventos seleccionados; y

en el que el detector de anomalías está configurado para determinar si el evento objetivo es indicativo de la amenaza a la seguridad informática de acuerdo con un modelo de comportamiento entrenado en un subcorpus de eventos específico del grupo de clientes, seleccionado el subcorpus específico del grupo de clientes del corpus de entrenamiento para incluir solo eventos que han ocurrido en una pluralidad de miembros de un grupo objetivo de la pluralidad de grupos de clientes.

10. El método de la reivindicación 9, en el que asignar eventos a categorías de eventos comprende:

determinar una posición del evento seleccionado en un espacio de incrustación de eventos multidimensional de acuerdo con los eventos primero y segundo; y

asignar el evento seleccionado a la categoría de eventos seleccionados de acuerdo con la posición del evento seleccionado en el espacio de incrustación de eventos.

11. El método de la reivindicación 10, que comprende además determinar la categoría de eventos seleccionados de acuerdo con un grupo de eventos que ocupan posiciones similares en el espacio de incrustación de eventos.

12. El método de la reivindicación 10, en el que determinar la posición del evento seleccionado en el espacio de incrustación de eventos comprende entrenar un codificador de eventos para producir un conjunto de coordenadas que indiquen la posición, y en el que entrenar el codificador de eventos comprende:

acoplar el codificador de eventos a un decodificador de eventos configurado para recibir el conjunto de coordenadas y entregar un indicador de predicción indicativo de una probabilidad de que la secuencia de eventos comprenda los eventos primero y segundo; y

ajustar un conjunto de parámetros del codificador de eventos de acuerdo con el indicador de predicción.

13. El método de la reivindicación 10, en el que determinar la posición del evento seleccionado en el espacio de incrustación de eventos comprende entrenar un codificador de eventos para producir un conjunto de coordenadas que indiquen la posición, y en el que entrenar el codificador de eventos comprende:

acoplar el codificador de eventos a un decodificador de eventos configurado para recibir el conjunto de coordenadas y para entregar un contexto predicho del evento seleccionado, comprendiendo el contexto predicho un primer evento predicho y un segundo evento predicho;

comparar el primer evento predicho con el primer evento y el segundo evento predicho con el segundo evento; y

ajustar un conjunto de parámetros del codificador de eventos de acuerdo con un resultado de la comparación.

14. El método de la reivindicación 9, en el que el perfil de evento comprende una pluralidad de componentes, perteneciendo cada componente determinado de acuerdo con una proporción de eventos a cada categoría de eventos de la pluralidad de categorías de eventos, calculada la proporción a partir de un recuento total de eventos del corpus de entrenamiento que ocurren en el sistema cliente.

15. El método de la reivindicación 9, en el que asignar la pluralidad de sistemas cliente a grupos de clientes comprende asignar sistemas cliente que tienen perfiles de eventos similares al mismo grupo de clientes.

16. El método de la reivindicación 9, en el que el evento del corpus de entrenamiento comprende un inicio de un proceso seleccionado en un sistema cliente de la pluralidad de sistemas cliente.

17. Un medio no transitorio legible por computadora que almacena instrucciones que, cuando son ejecutadas por al menos un procesador de hardware de un sistema informático, llevan el sistema informático a:

asignar eventos de un corpus de entrenamiento a una pluralidad de categorías de eventos, comprendiendo el corpus de entrenamiento una colección de eventos que han ocurrido en una pluralidad de sistemas cliente;

en respuesta a la asignación de eventos a categorías de eventos, asignar sistemas cliente de la pluralidad de sistemas cliente a una pluralidad de grupos de clientes de acuerdo con la pluralidad de categorías de eventos; y

en respuesta a la asignación de los sistemas cliente a los grupos de clientes, transmitir un indicador de pertenencia a grupo de clientes a un detector de anomalías configurado para determinar si un evento objetivo que ocurre en un sistema cliente objetivo es indicativo de una amenaza a la seguridad informática;

en el que asignar eventos a categorías de eventos comprende:

seleccionar una pluralidad de eventos del corpus de entrenamiento, habiendo ocurrido la pluralidad de eventos en un sistema cliente de la pluralidad de sistemas cliente,

organizar la pluralidad de eventos de acuerdo con un tiempo de ocurrencia para formar una secuencia de eventos, y

en respuesta, asignar un evento seleccionado de la secuencia de eventos a una categoría de eventos seleccionados de acuerdo con un primer evento que precede al evento seleccionado y además de acuerdo con el segundo evento que sigue al evento seleccionado dentro de la secuencia de eventos;

en el que asignar sistemas cliente a grupos de clientes comprende asignar el sistema cliente a un grupo de clientes seleccionado según un perfil de evento determinado de acuerdo con un recuento de eventos que ocurren en el sistema cliente y que pertenecen a la categoría de eventos seleccionados; y

en el que el detector de anomalías está configurado para determinar si el evento objetivo es indicativo de la amenaza a la seguridad informática de acuerdo con un modelo de comportamiento entrenado en un subcorpus de eventos específico del grupo de clientes, seleccionado el subcorpus específico del grupo de clientes del corpus de entrenamiento para incluir solo eventos que han ocurrido en una pluralidad de miembros de un grupo objetivo de la pluralidad de grupos de clientes.

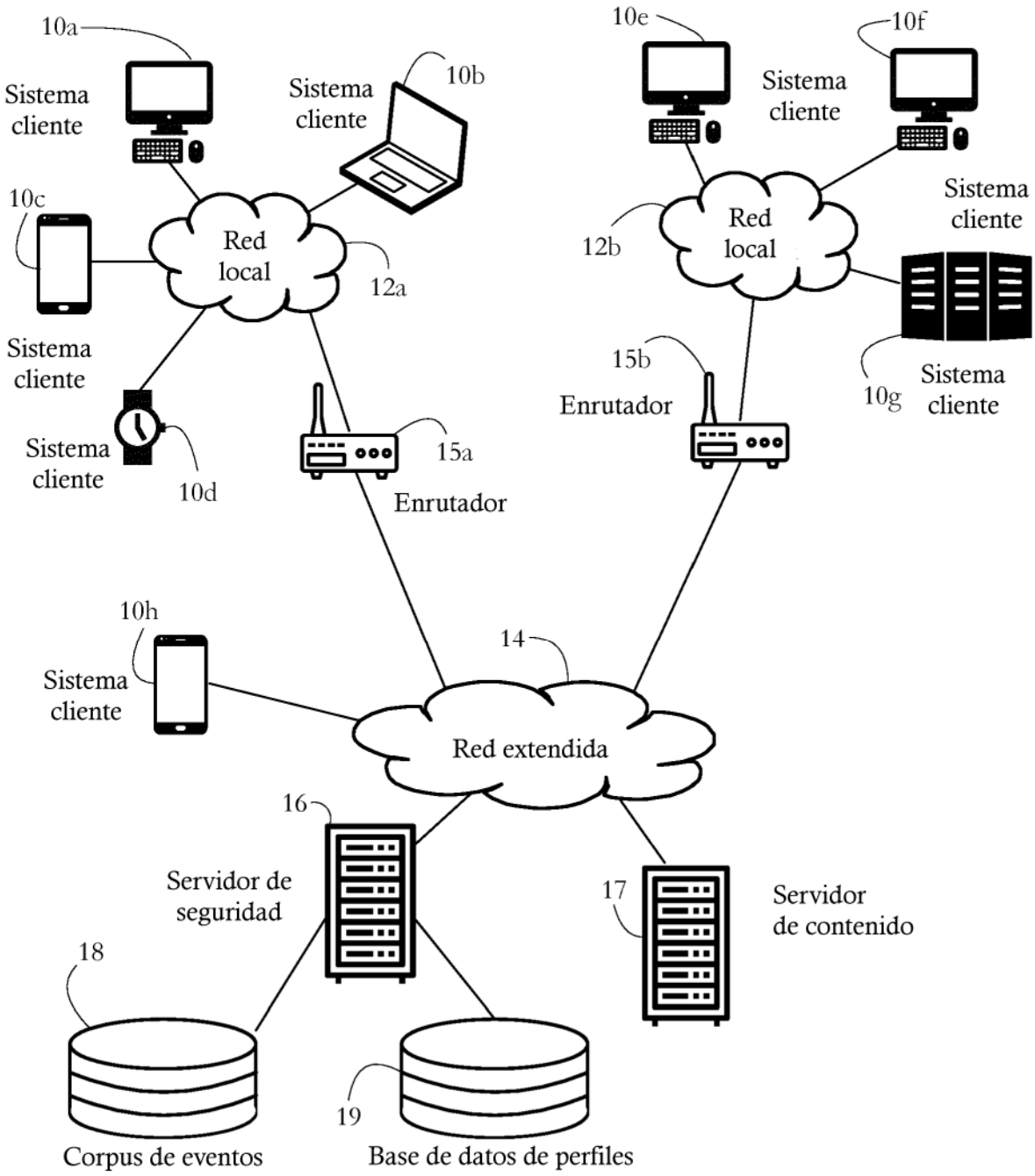
10a
Sistema cliente
Sistema cliente
10b
10c
Red local
12a
Sistema cliente
Sistema cliente
10d
15a
Enrutador
10e
Sistema cliente
10f
Red local
12b
Sistema cliente
15b
Enrutador
10g
Sistema cliente
10h
Sistema cliente
14
Red extendida
16
Servidor de seguridad
17
Servidor de contenido
18
19
Corpus de eventos
Base de datos de perfiles

FIG. 1

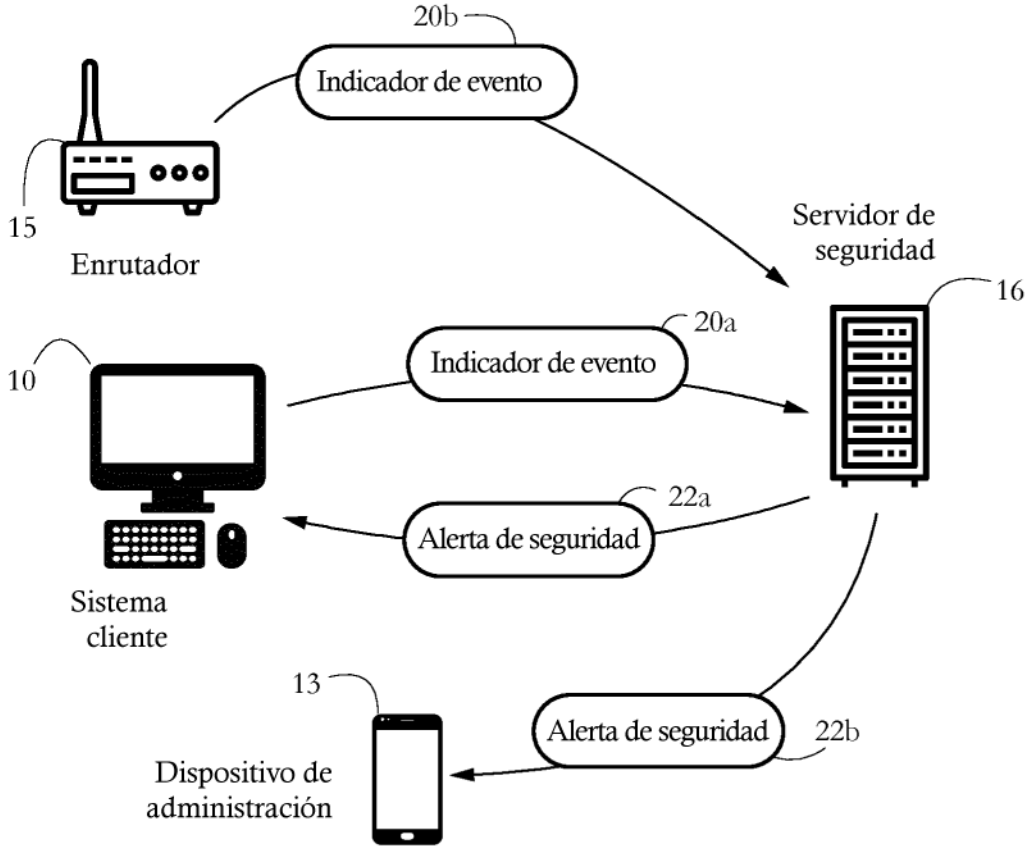
20b
Indicador de evento
15
Enrutador
Servidor de seguridad
16
20a
Indicador de evento
10
22a
Alerta de seguridad
Sistema cliente
13
Alerta de seguridad
22b
Dispositivo de administración

FIG. 2

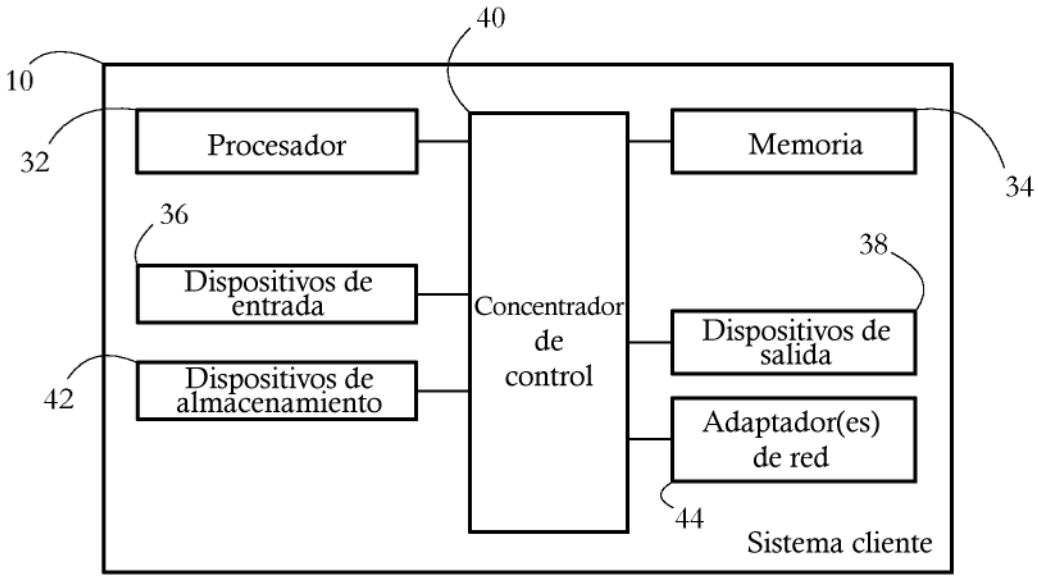
10
40
32
Procesador
Concentrador de control
Memoria
34
36
Dispositivos de entrada
38
Dispositivos de salida
42
Dispositivos de almacenamiento
Adaptador(es) de red
44
Sistema cliente

FIG. 3-A

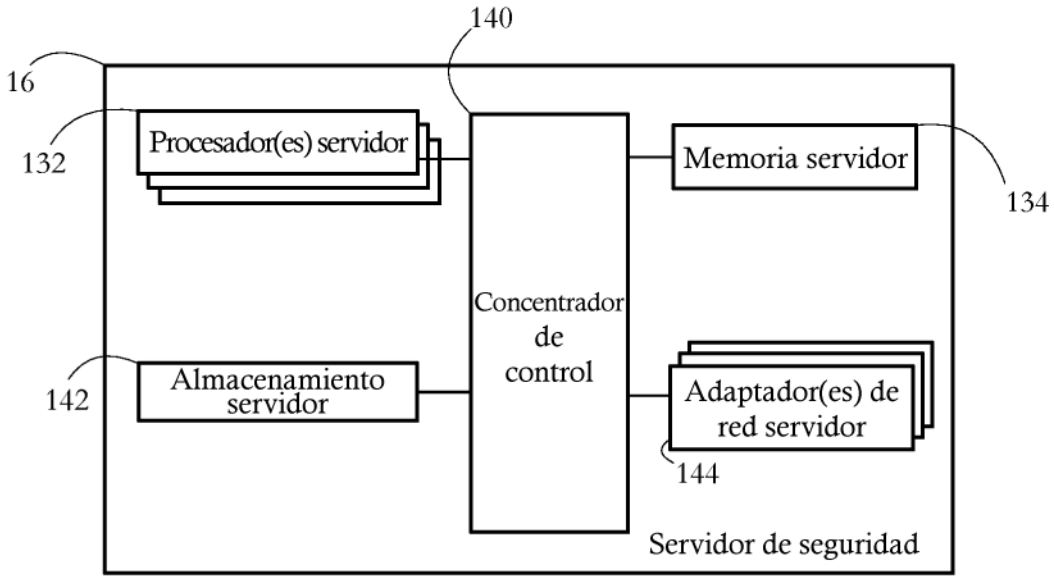
140
16
132
Procesador(es) servidor
Memoria servidor
134
Concentrador de control
142
Almacenamiento servidor
Adaptador(es) de red servidor
144
Servidor de seguridad

FIG. 3-B

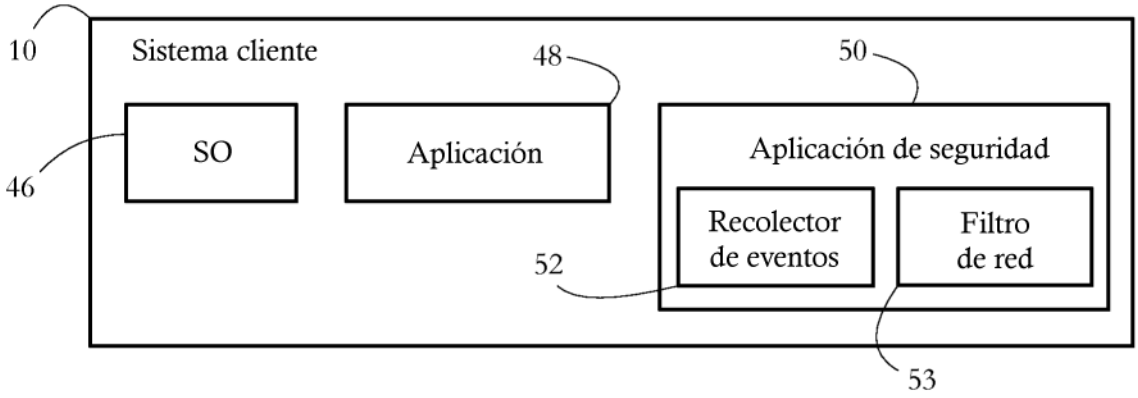
10
Sistema cliente
48
50
SO
46
Aplicación
Aplicación de seguridad
Recolector de eventos
Filtro de red
52
53

FIG. 4

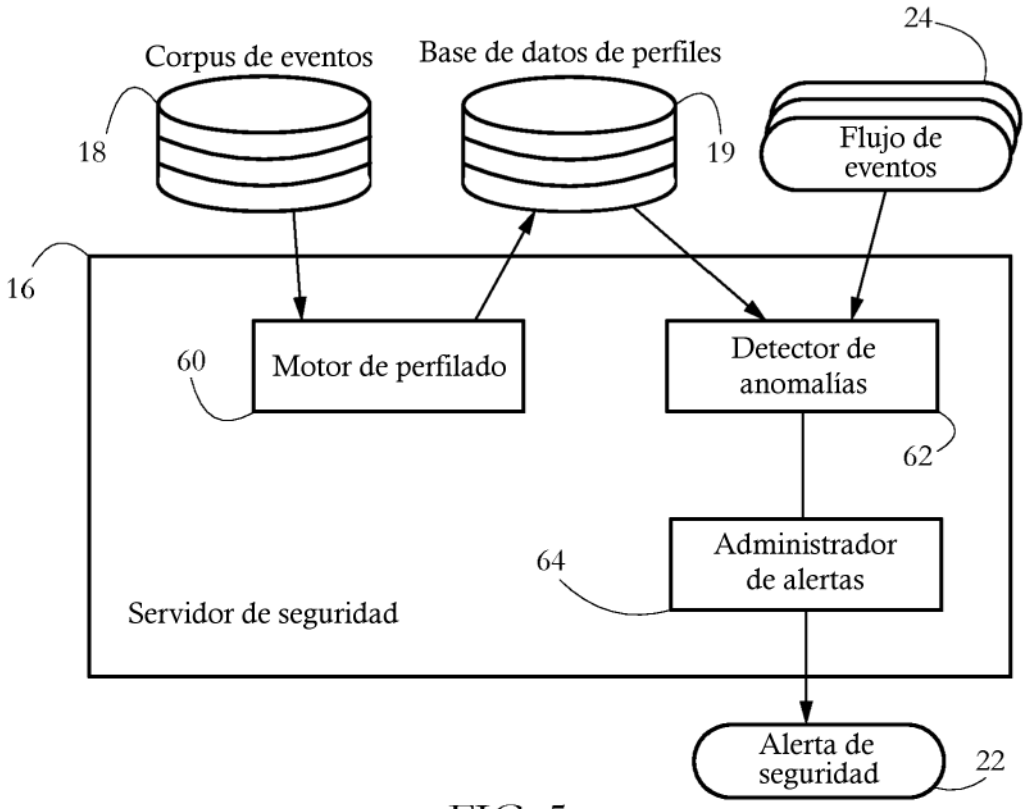
24
Corpus de eventos
Base de datos de perfiles
18
19
Flujo de eventos
16
60
Motor de perfilado
Detector de anomalías
62
64
Administrador de alertas
Servidor de seguridad
Alerta de seguridad
22

FIG. 5

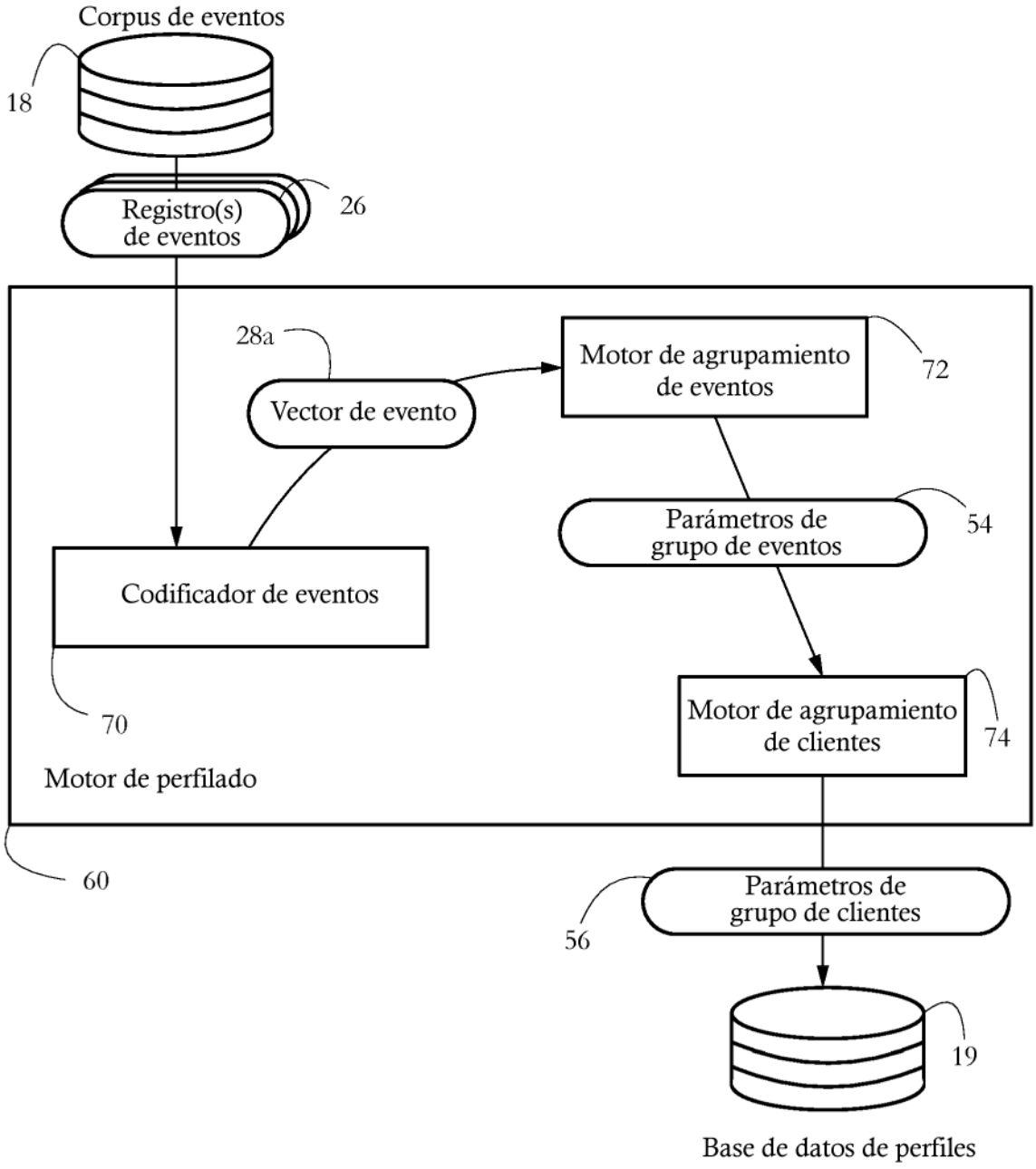
Corpus de eventos
18
Registro(s) de eventos
26
28a
Vector de evento
Motor de agrupamiento de eventos
72
Parámetros de grupo de eventos
54
Codificador de eventos
70
Motor de agrupamiento de clientes
74
Motor de perfilado
60
Parámetros de grupo de clientes
56
19
Base de datos de perfiles

FIG. 6

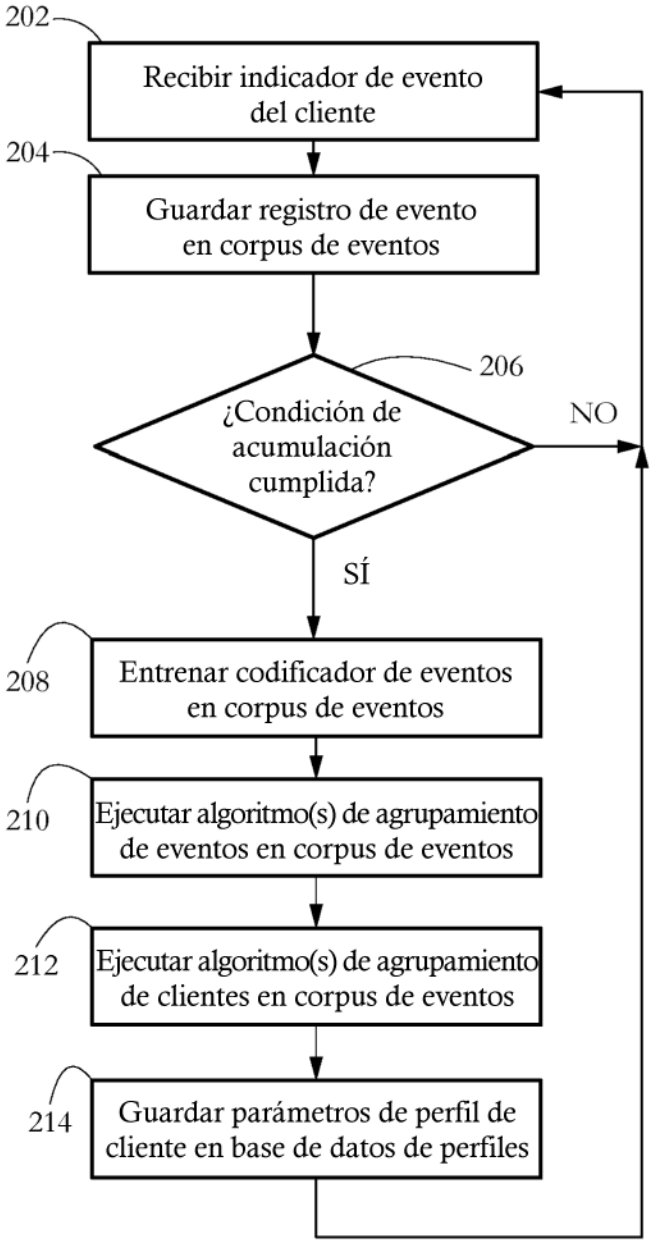
202
Recibir indicador de evento del cliente
204
Guardar registro de evento en corpus de eventos
206
¿Condición de acumulación cumplida?
NO
SÍ
208
Entrenar codificador de eventos en corpus de eventos
210
Ejecutar algoritmo(s) de agrupamiento de eventos en corpus de eventos
212
Ejecutar algoritmo(s) de agrupamiento de clientes en corpus de eventos
214
Guardar parámetros de perfil de cliente en base de datos de perfiles

FIG. 7

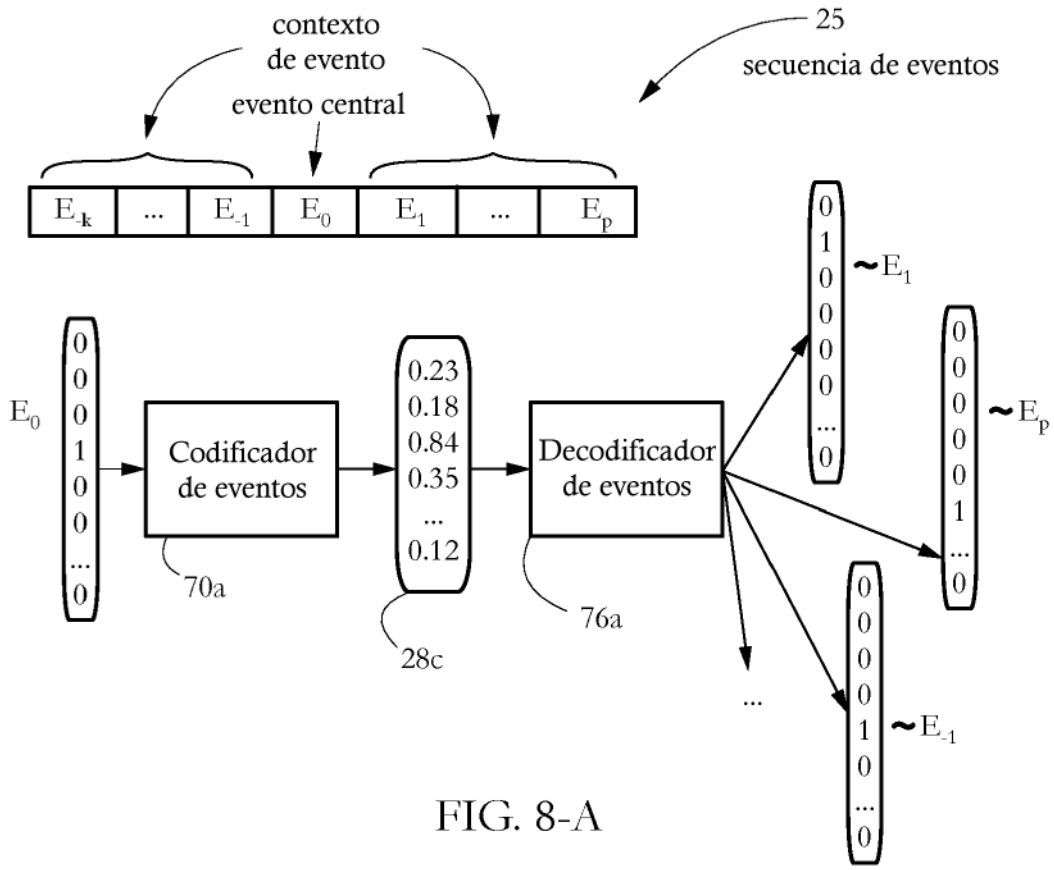
contexto
de evento
evento central
25
secuencia de eventos
E-k
...
E-1
E0
E1
...
Ep
E0
0 0 0 1 0 0 0 ... 0
Codificador
de eventos
70a
0.23
0.18
0.84
0.35
...
0.12
28c
Decodificador
de eventos
76a
0 1 0 0 0 0 ... 0
~E1
0 0 0 0 0 1 ... 0
~Ep
0 0 0 0 1 0 ... 0
~E-1
...

FIG. 8-A

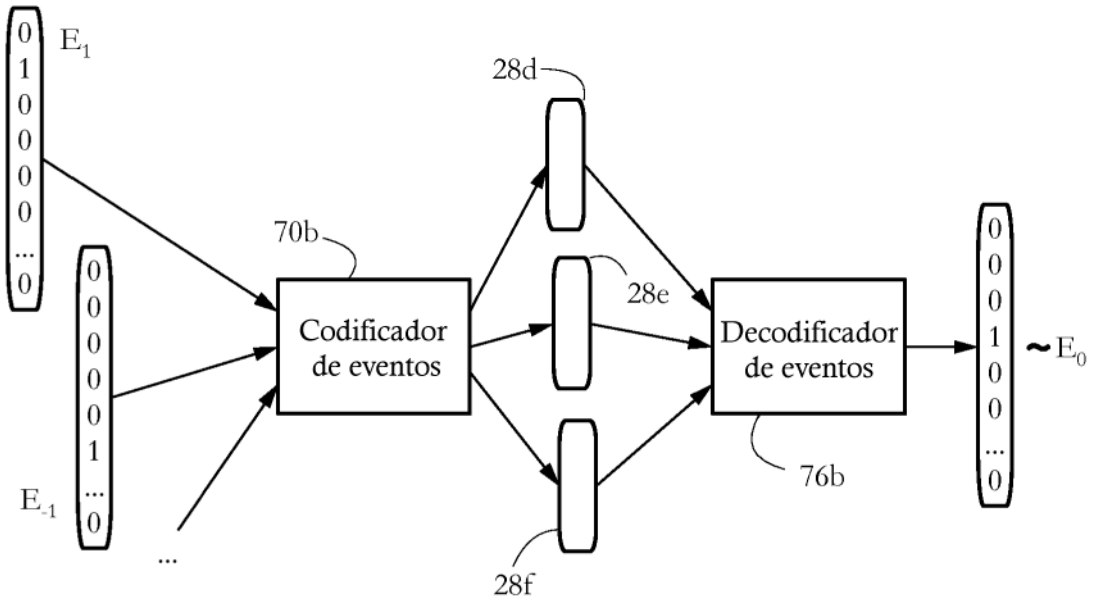
E1
0 1 0 0 0 0 ... 0
E-1
0 0 0 0 0 1 ... 0
...
70b
Codificador
de eventos
28d
28e
28f
Decodificador
de eventos
76b
0 0 0 1 0 0 ... 0
~E0

FIG. 8-B

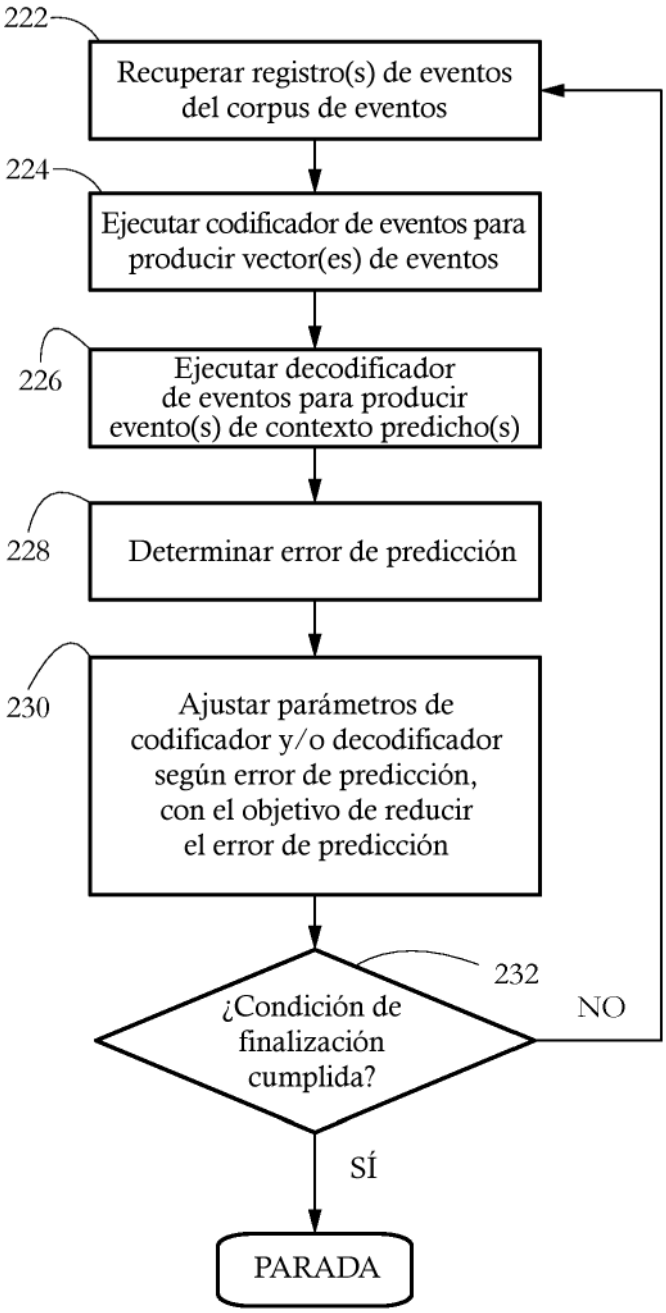
222
Recuperar registro(s) de eventos del corpus de eventos
224
Ejecutar codificador de eventos para producir vector(es) de eventos
226
Ejecutar decodificador de eventos para producir evento(s) de contexto predicho(s)
228
Determinar error de predicción
230
Ajustar parámetros de codificador y/o decodificador según error de predicción, con el objetivo de reducir el error de predicción
232
¿Condición de finalización cumplida?
NO
SÍ
PARADA

FIG. 9

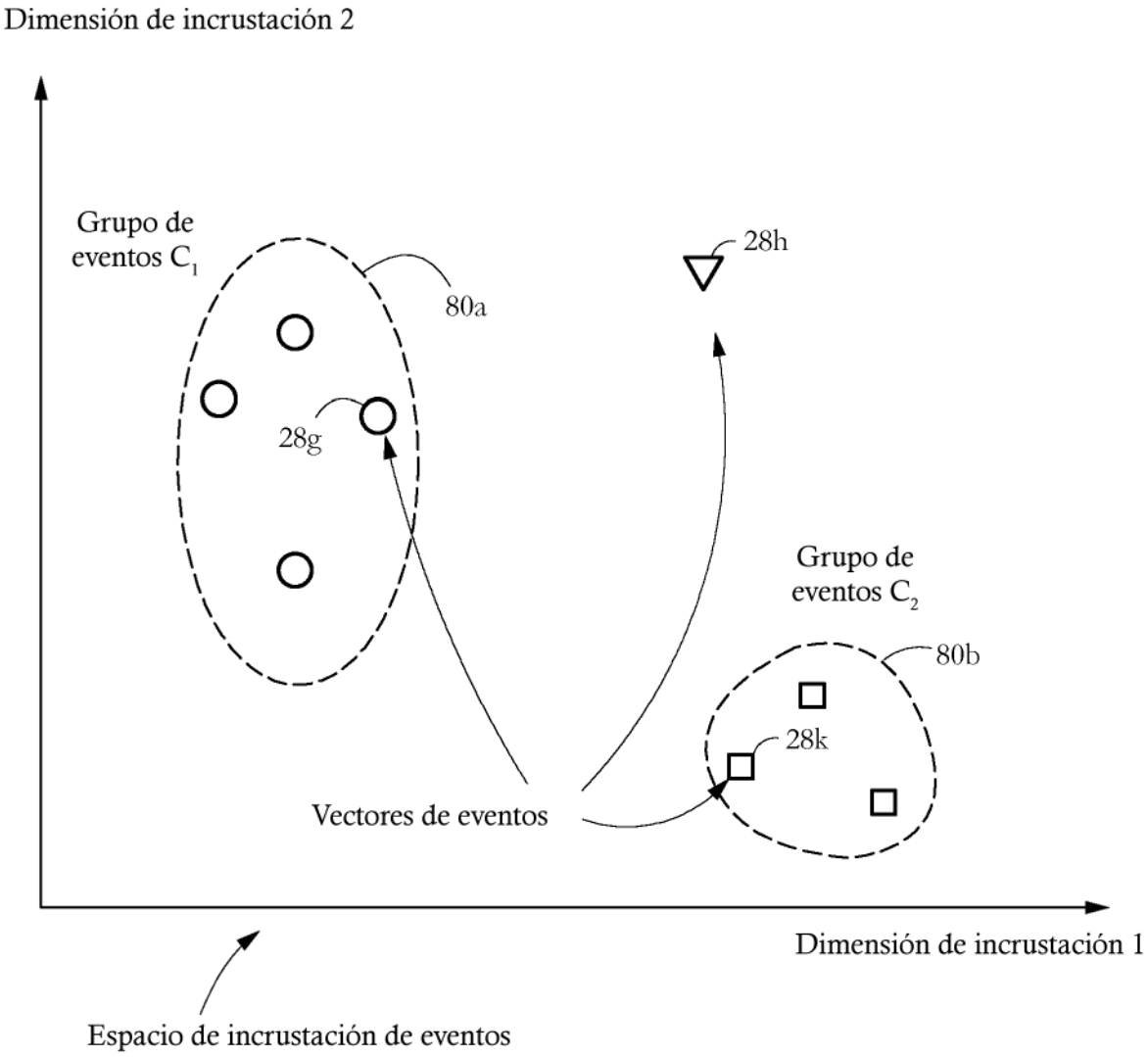
Dimensión de incrustación 2
Grupo de eventos C_1
80a
28h
28g
Grupo de eventos C_2
80b
28k
Vectores de eventos
Dimensión de incrustación 1
Espacio de incrustación de eventos

FIG. 10

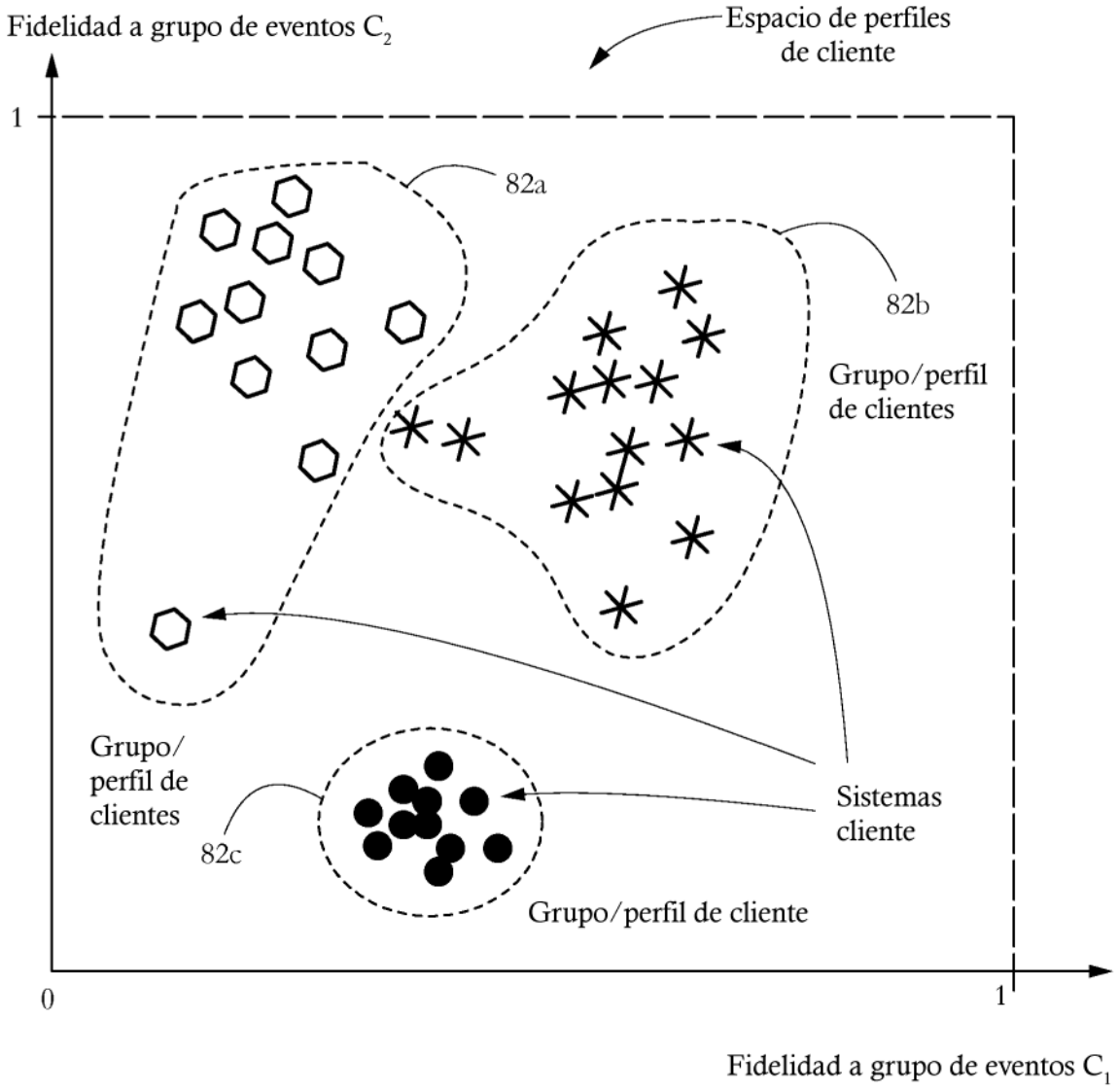
Fidelidad a grupo de eventos C_2
Espacio de perfiles de cliente
1
82a
82b
Grupo/perfil de clientes
Grupo/ perfil de clientes
82c
Sistemas cliente
Grupo/perfil de cliente
0
1
Fidelidad a grupo de eventos C_1

FIG. 11

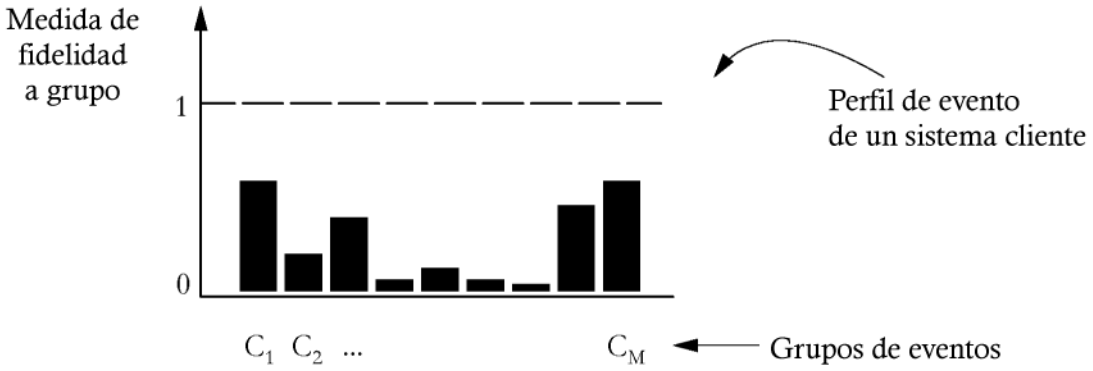
Medida de fidelidad a grupo
1
0
Perfil de evento de un sistema cliente
C1 C2 ...
CM
Grupos de eventos

FIG. 12

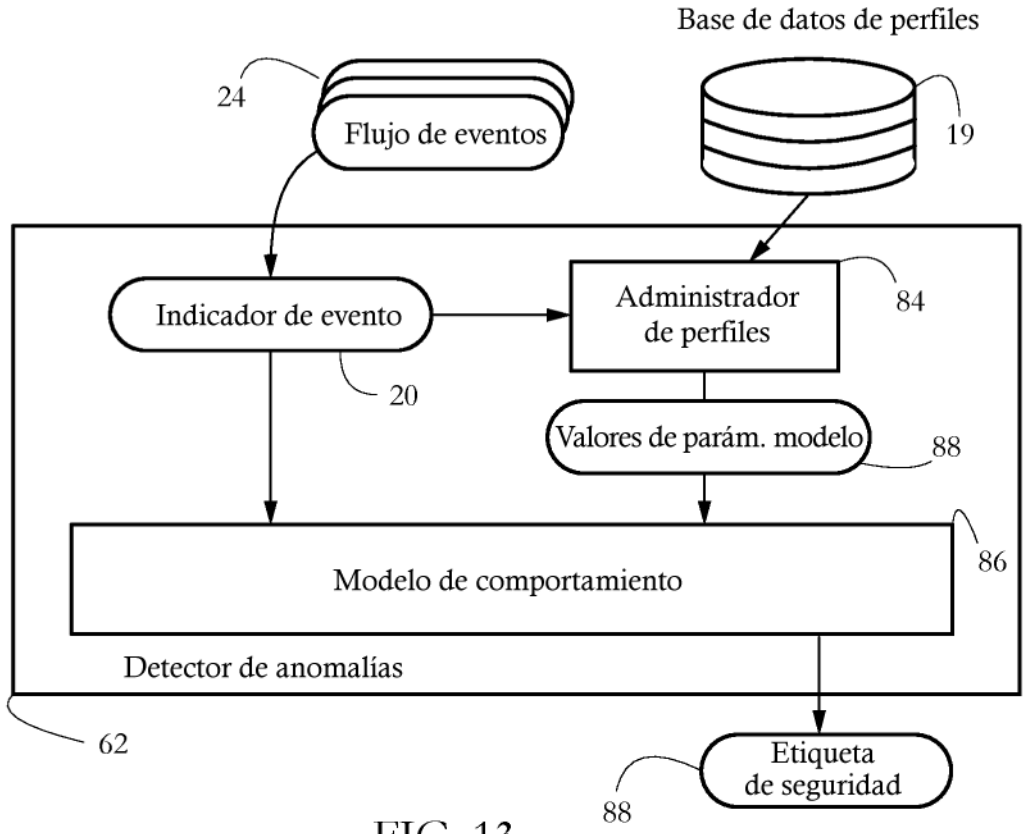
Base de datos de perfiles
24
Flujo de eventos
19
Indicador de evento
Administrador de perfiles
84
20
Valores de parám. modelo
88
Modelo de comportamiento
86
Detector de anomalías
62
Etiqueta de seguridad
88

FIG. 13

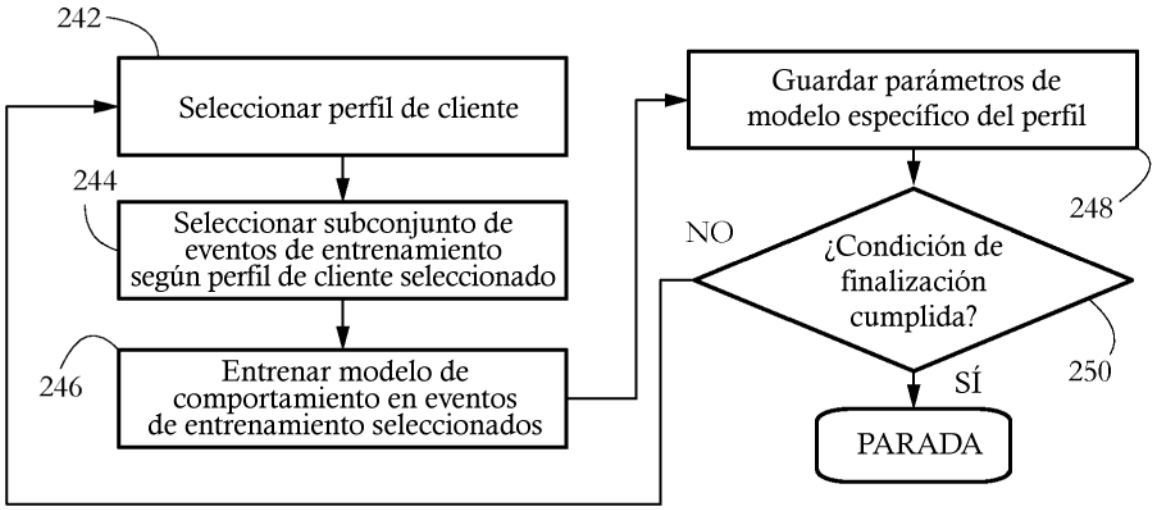
242
Seleccionar perfil de cliente
244
Seleccionar subconjunto de eventos de entrenamiento según perfil de cliente seleccionado
246
Entrenar modelo de comportamiento en eventos de entrenamiento seleccionados
Guardar parámetros de modelo específico del perfil
248
NO
¿Condición de finalización cumplida?
250
SÍ
PARADA

FIG. 14

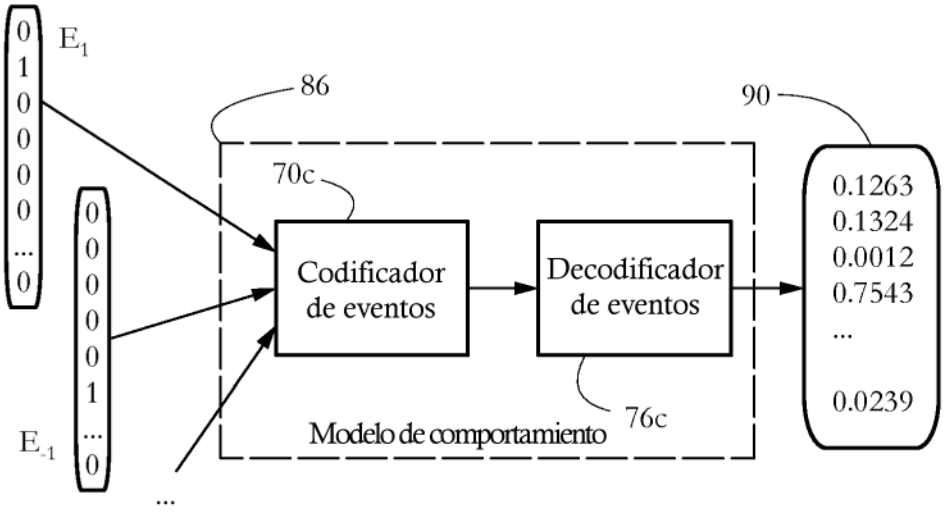
E1
0 1 0 0 0 0 ... 0
E-1
0 0 0 0 0 1 ... 0
...
86
70c
Codificador de eventos
Decodificador de eventos
76c
Modelo de comportamiento
90
0.1263
0.1324
0.0012
0.7543
...
0.0239

FIG. 15

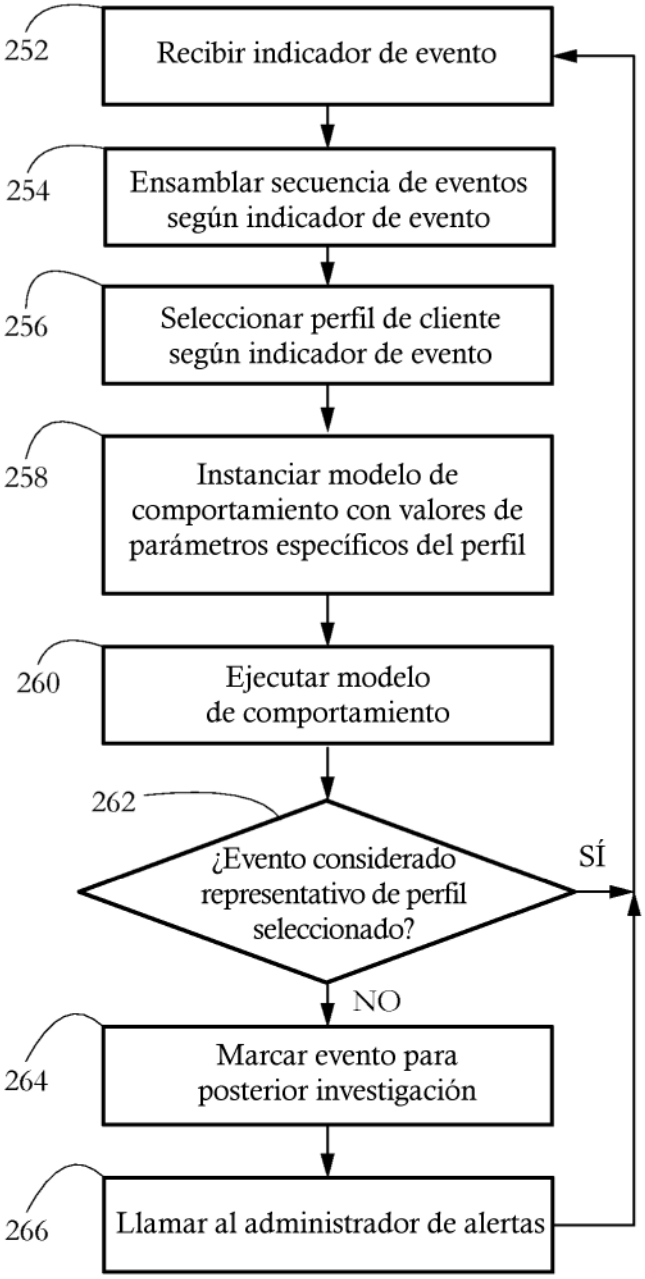
252
Recibir indicador de evento
254
Ensamblar secuencia de eventos según indicador de evento
256
Seleccionar perfil de cliente según indicador de evento
258
Instanciar modelo de comportamiento con valores de parámetros específicos del perfil
260
Ejecutar modelo de comportamiento
262
¿Evento considerado representativo de perfil seleccionado?
SÍ
NO
264
Marcar evento para posterior investigación
266
Llamar al administrador de alertas

FIG. 16

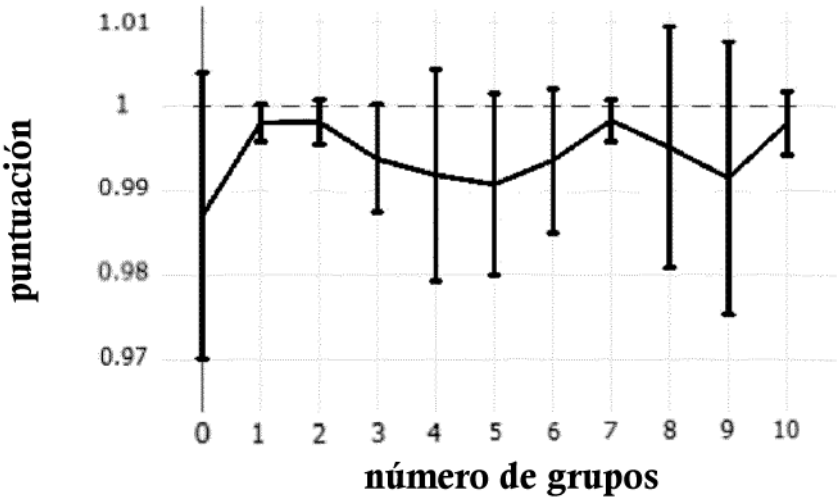

FIG. 17-A

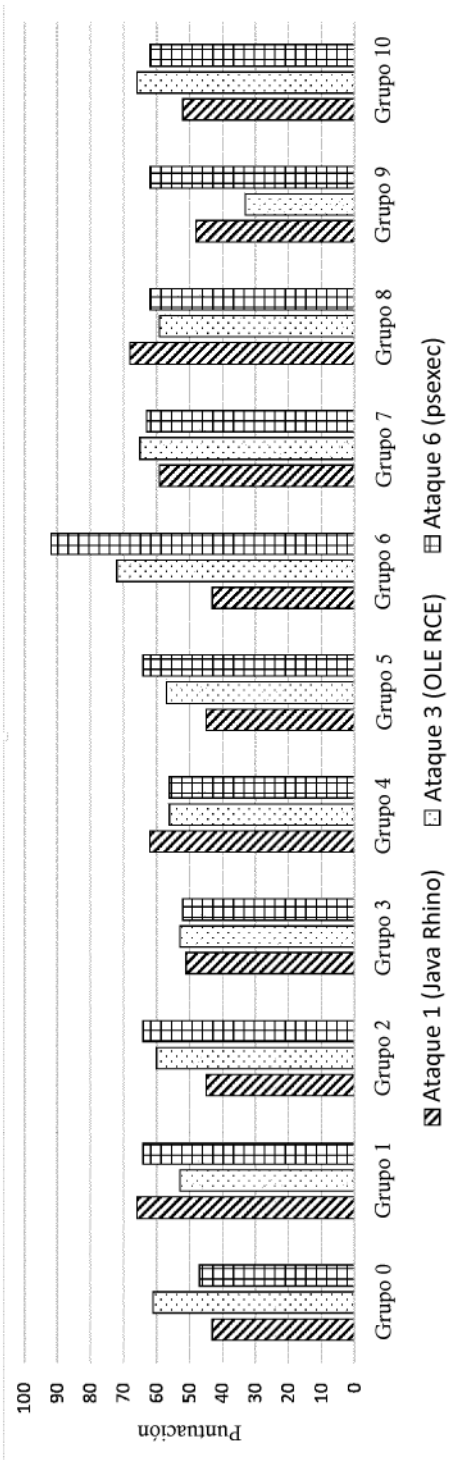
Puntuación
100
90
80
70
60
50
40
30
20
10
0
Grupo 0
Grupo 1
Grupo 2
Grupo 3
Grupo 4
Grupo 5
Grupo 6
Grupo 7
Grupo 8
Grupo 9
Grupo 10
Ataque 1 (Java Rhino)
Ataque 3 (OLE RCE)
Ataque 6 (psexec)

FIG. 17-B