(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 442 747**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/00 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **10.02.2011 E 11382033 (6)**

(97) Fecha y número de publicación de la concesión europea: **25.09.2013 EP 2487860**

(54) Título: **Procedimiento y sistema para mejorar la detección de amenazas de seguridad en redes de comunicación**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.02.2014

(73) Titular/es:

TELEFÓNICA, S.A. (100.0%)
Gran Vía, 28
28013 Madrid, ES

(72) Inventor/es:

SANZ HERNANDO, IVÁN y
AMAYA CALVO, ANTONIO MANUEL

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento y sistema para mejorar la detección de amenazas de seguridad en redes de comunicación

Campo Técnico

La presente invención se refiere, en general, a seguridad de redes, y más particularmente a un procedimiento y sistema para aumentar la seguridad en redes y sistemas de comunicación.

Descripción de la técnica anterior

A medida que los sistemas se vuelven más complejos, así se volvía el problema de monitorizar su estado de salud. Esto es exacto para todos los indicadores de salud de un sistema (rendimiento, consumo de recursos), pero es especialmente cierto para su estado de seguridad. Por lo tanto, la monitorización de seguridad se ha trasladado, en unos pocos años, de entornos con un conjunto de dispositivos de seguridad reducido, que generan unos pocos cientos de eventos diarios, a entornos con un inmenso número de dispositivos que generan varios cientos de miles de eventos diarios.

Donde los administradores de seguridad anteriormente estaban realizando un análisis manual de todos los eventos de seguridad, ahora es imposible realizar tal análisis manual, debido al puro volumen de eventos diarios.

Para solucionar este problema, nacieron los sistemas de Gestión de Eventos de Información de Seguridad (SIEM) (puede encontrarse información acerca de estos sistemas en http://www.rsa.com/node.aspx?id=3182) para facilitar ese análisis y automatizar donde sea posible las tareas que, rutinariamente, se ejecutan en el análisis de cualquier registro de seguridad en cada entorno. Los sistemas SIEM están diseñados para centralizar toda la información de seguridad generada por los dispositivos desplegados en cualquier compañía, normalizando al mismo tiempo la información recabada en un formato común que permitirá realizar un análisis integrado de eventos de seguridad, independientemente de los dispositivos de origen.

La expresión Gestión de Eventos de Información de Seguridad (SIEM) describe las capacidades del producto de reunir, analizar y presentar información procedente de la red y los dispositivos de seguridad; aplicaciones de gestión de identidad y acceso; herramientas de gestión de vulnerabilidad y conformidad con políticas; registros del sistema operativo, base de datos y aplicaciones; y datos de amenazas externas. Algunos productos SIEM comerciales incluyen AccelOps, AraKnos, ArcSight, BLUESOC, Cisco Security MARS, ImmuneSecurity, LogLogic, LogICA, NitroSecurity, RSA enVision, SenSage, y otros.

Habitualmente las capacidades SIEM incluyen al menos:

- Agregación de datos: las soluciones SIEM/LM (gestión de registros) agregan datos procedentes de muchas fuentes, incluyendo la red, seguridad, servidores, bases de datos, aplicaciones, proporcionando la capacidad de consolidar los datos monitorizados para ayudar a evitar perder eventos cruciales. La información recabada es estandarizada (adaptada/traducida) a un formato común solicitado.

- Las soluciones SIEM filtran la información no relacionada con la seguridad del sistema.

- Correlación: busca atributos comunes, y enlaza eventos entre sí en paquetes significativos para detectar amenazas conocidas. Esta tecnología proporciona la capacidad de realizar una diversidad de técnicas de correlación para integrar diferentes fuentes, para convertir los datos en información útil.

- Alerta: el análisis automatizado de eventos correlacionados y la producción de alertas, para informar de problemas inmediatos a los destinatarios.

- Tablero de mandos: Las herramientas SIEM/LM toman los datos de eventos y los convierten en gráficos informativos para ayudar a ver patrones, o identificar la actividad que no está formando un patrón estándar.

- Conformidad: las aplicaciones SIEM pueden emplearse para automatizar la reunión de datos de conformidad, produciendo informes que se adapten a la seguridad existente, el gobierno y los procedimientos de auditoría.

- Las soluciones SIEM presentan la información usando diferentes formatos para diferentes tipos de informes o aplicaciones.

- Conservación: las soluciones SIEM/SIM emplean almacenamiento a largo plazo de datos históricos para facilitar la correlación de datos a lo largo del tiempo, y para proporcionar la conservación necesaria por requisitos de conformidad.

Aunque los sistemas SIEM salvaban el vacío entre los incrementos de eventos de seguridad generados y la necesidad de tener un análisis significativo de esos mismos eventos, también aportaron nuevos problemas. El principal es que los módulos de correlación de los sistemas SIEM (módulos que relacionan o interrelacionan eventos individuales para detectar ataques más complejos) están basados en la detección de amenazas conocidas, que deben ser caracterizadas

y configuradas de antemano por un experto. Los módulos de correlación de SIEM están basados en reglas de procedimiento fijas: 'si el evento A ha ocurrido y el evento B ocurre en los X segundos siguientes, y luego ocurre el evento C entonces da una alarma'. Es decir, sólo se detectan eventos específicos relacionados con máquinas, sistemas o aplicaciones específicas. Este procedimiento de detección obliga, por lo tanto, a una revisión continua de las correlaciones configuradas, para detectar las nuevas amenazas que no fueron incluidas o configuradas inicialmente. Cualquier actualización de los medidores/máquinas usados como fuente de información (por ejemplo, enrutadores, antivirus, cortafuegos, servidores web, sistemas de detección de intrusión, sistemas de prevención de intrusión...) requiere revisar las correlaciones configuradas puesto que podría ser necesario modificar alguna de las correlaciones existentes para incluir los eventos recién definidos, o podría ser necesario definir nuevas correlaciones para monitorizar los eventos desconocidos previamente por el sistema. Si se despliega un nuevo dispositivo, de un fabricante desconocido previamente, entonces todas las correlaciones tendrán que ser modificadas para que incluyan los eventos generados por el nuevo dispositivo. Si no, las amenazas que afecten, usen o se originen en el nuevo sistema no serán detectadas.

Además de esas tareas de configuración, que deben ser ejecutadas de manera continua, hay otros problemas que no pueden solucionarse fácilmente o en absoluto con las soluciones de correlación implementadas en los sistemas SIEM comercializados actualmente:

- El módulo de correlación es muy dependiente de los eventos generados por Sistemas de Detección de Intrusión (IDS). Esta dependencia significa que habitualmente se genera un gran número de falsos positivos, lo que a su vez conduce a un esfuerzo desperdiciado al analizarlos y solucionarlos por administradores de seguridad ocupados con ese análisis.

- Como las correlaciones deben ser definidas específicamente para cada amenaza, los módulos de correlación actuales no pueden detectar nuevas clases de amenazas, o incluso las amenazas actuales que usan una secuencia de eventos nueva, desconocida previamente.

Por ejemplo, si queremos detectar un ataque por fuerza bruta exitoso contra nuestro servidor FTP, debemos definir una regla de correlación como:

- Si encontramos más de siete eventos fallidos de autentificación ftp y después un registro de ingreso de autentificación exitoso, debemos generar una alarma que notifique este problema.

Si queremos detectar el mismo ataque por fuerza bruta contra un servidor SSH, tenemos que generar otra regla de correlación como:

- Si encontramos más de siete eventos fallidos de autentificación ssh, generamos una alarma de fuerza bruta.

Los módulos de correlación de los sistemas SIEM necesitan definir exactamente qué eventos deben ser analizados para detectar esta clase de ataque. Si añadimos nuevos dispositivos que envían nuevos eventos, tenemos que revisar las reglas de correlación de fuerza bruta actuales para incluir estos nuevos eventos.

- Incluso después de que la amenaza es identificada y caracterizada, el sistema debe ser configurado manualmente para detectarla, y eso requiere un esfuerzo adicional por los administradores de seguridad.

El documento US 2009/064334 es además la técnica anterior relacionada con la detección de amenaza de seguridad.

En otras palabras, el problema global es el uso de módulos de correlación no flexibles en los sistemas actuales (los módulos de correlación actuales tienen elevada dependencia de eventos específicos, para detectar una nueva técnica de ataque deben definirse nuevas correlaciones, pequeños cambios en una técnica de ataque actual hacen que el ataque no sea detectable...).

Por lo tanto, se requieren nuevas herramientas de correlación para ocuparse de esos desafíos. Esas nuevas herramientas deberían permitir disminuir el esfuerzo manual que, continuamente, los administradores de seguridad deben invertir en los sistemas actuales. También deberían reducir los falsos positivos generados por los sistemas, que tienen un impacto directo sobre el tiempo y el esfuerzo requeridos para gestionar los sistemas actuales, y al mismo tiempo reducir el tiempo real disponible para procesar alarmas reales.

Sumario de la Invención

La presente invención usa un nuevo procedimiento y sistema en base a la inteligencia artificial, que reducirá o eliminará las deficiencias presentes en los sistemas SIEM actuales.

La propuesta está basada en dos ejes de alto nivel:

- Definir una agrupación dinámica de eventos de seguridad que permitirá al sistema ser independiente de eventos específicos generados por cualquier dispositivo específico.

- Usar algoritmos de inteligencia artificial para reducir o incluso eliminar las deficiencias presentes en los sistemas de correlación actuales. Concretamente, el nuevo sistema usará redes neuronales debido a las características intrínsecas de tales redes,

que minimizan varias de las deficiencias de los sistemas de correlación actuales.

De ahora en adelante, se usará el término ACS (Sistema de Correlación Avanzado) para referirse a la invención recién desarrollada.

En un primer aspecto, se presenta un procedimiento de mejora de la detección de amenazas de seguridad en una red de comunicación, incluyendo la red de comunicación dispositivos de seguridad que generan eventos de seguridad, siendo esos eventos almacenados en una base de datos de seguridad, comprendiendo el sistema:

a) Definir diferentes tipos de eventos de seguridad, cada tipo de evento de seguridad se denomina una etiqueta dinámica, la etiqueta dinámica asignada a cada evento de seguridad dependerá de ciertas condiciones que se encuentran en la descripción del evento.

b) Definir los modelos de datos, siendo un modelo de datos la recopilación de etiquetas dinámicas que están relacionadas con una cierta amenaza de seguridad; un modelo de datos estará definido por cada tipo de amenaza de seguridad a detectar.

c) En cada intervalo de ejecución configurado, seleccionar los dispositivos a analizar para cada modelo de datos y, para cada dispositivo analizado, leer de la base de datos de seguridad los eventos generados por dicho dispositivo, asignar una etiqueta dinámica a cada evento de seguridad y calcular el valor de cada etiqueta dinámica, el valor de la etiqueta es el número de casos para cada dispositivo analizado del tipo de eventos correspondiente a dicha etiqueta.

d) Agrupar las etiquetas, según la definición del modelo de datos, generando un patrón con los valores de etiquetas para cada modelo de datos y para cada dispositivo analizado.

e) Para cada modelo de datos, leer los patrones correspondientes generados en la etapa d) y aplicar un algoritmo de Inteligencia Artificial en base a la información almacenada en una base de datos de conocimientos de dicho modelo de datos, para decidir si debe generarse una alarma de actividad sospechosa para cada patrón analizado o no; incluyendo cada base de datos de conocimientos, para cada modelo de datos, un conjunto de patrones conocidos con la información de si debe generarse una alarma para dicho patrón o no.

En otro aspecto, se presenta un sistema que comprende medios adaptados para realizar el procedimiento.

Por último, se presenta un programa de ordenador que comprende medios de código de programa de ordenador adaptados para realizar el procedimiento anteriormente descrito.

Para una comprensión más completa de la invención, sus objetos y ventajas, puede hacerse referencia a la siguiente memoria descriptiva y a los dibujos adjuntos.

Breve Descripción de los Dibujos

Para completar la descripción y para asegurar una mejor comprensión de la invención, se proporciona un conjunto de dibujos. Dichos dibujos forman una parte integral de la descripción e ilustran una realización preferente de la invención, que no debería interpretarse como restrictiva del ámbito de la invención, sino más bien como un ejemplo de cómo puede plasmarse la invención. Los dibujos comprenden las siguientes figuras:

La Figura 1 representa un diagrama de bloques del módulo de abstracción de datos en una realización ejemplar de la presente invención.

La Figura 2 representa un diagrama de bloques del módulo de abstracción de datos y el módulo de motor de IA en una realización ejemplar de la presente invención.

La Figura 3 muestra un diagrama de bloques de la arquitectura ACS integrada en un sistema SIEM en una realización ejemplar de la presente invención.

La Figura 4 es un gráfico que muestra el número de alarmas totales generadas por el ACS y un sistema SIEM estándar.

Los números y símbolos correspondientes en las diferentes figuras se refieren a partes correspondientes a menos que se indique otra cosa.

Descripción detallada de la invención

La presente invención propone un procedimiento y sistema que analizan automáticamente la información de seguridad para detectar anomalías y amenazas, de un modo que soluciona los problemas de la técnica anterior. En la presente

invención, la detección es independiente de eventos específicos generados por dispositivos específicos (servidores web, enrutadores...) y permite disminuir el esfuerzo manual y el número de falsos positivos.

Los sistemas de seguridad actuales usan referencias a eventos específicos o grupos de eventos para detectar acciones que reflejarán una actividad sospechosa que debería ser monitorizada, de manera que cuando se introducen nuevos eventos o nuevas máquinas, el sistema de seguridad debe modificarse.

Para evitar una dependencia del sistema de eventos específicos, y para permitir la integración eficiente de nuevas fuentes de datos, se ha diseñado un sistema de etiquetado basado en agrupar dinámicamente eventos según la descripción del evento. Los diferentes eventos se clasifican en una categoría (es decir, son etiquetados con una etiqueta específica) dependiendo del tipo de evento. Estas categorías o etiquetas se denominan “etiquetas dinámicas”. La identificación y definición de cada etiqueta o categoría es una tarea que debe ser ejecutada por un experto, teniendo en cuenta el modelo deseado. Aunque ese trabajo debe realizarse teniendo en cuenta la experiencia previa del experto en el campo, puede usar minería de datos y/o herramientas estadísticas para ayudarle en el procedimiento de definición e identificación, especialmente durante las primeras fases del procedimiento.

Para asignar estas etiquetas, se analizan los eventos producidos por las diferentes fuentes de información (dispositivos habitualmente identificados con una dirección IP), y si el evento satisface ciertas condiciones, es etiquetado con una cierta etiqueta. Habitualmente, este procedimiento se realiza analizando la descripción del evento, y si se encuentran ciertas palabras clave en la descripción, el evento se asigna a una categoría/etiqueta específica.

Por consiguiente, la presente invención permite clasificar eventos desconocidos generados por nuevos dispositivos sin ninguna modificación en el sistema (si la descripción del nuevo evento incluye cierta(s) palabra(s) clave, se clasificaría automáticamente sin modificar el sistema), así que el motor de correlación propuesto en la presente invención es independiente de eventos específicos generados por cualquier dispositivo específico.

En una realización preferente, los eventos se clasifican (asignan) con una cierta etiqueta dinámica dependiendo de las palabras clave usadas en su descripción. Así, cada etiqueta dinámica tendrá ciertas palabras clave asociadas y si se encuentran dichas palabras clave en la descripción del evento, el evento se asignará a la etiqueta correspondiente.

Como ejemplo describiremos el procedimiento usado para definir una etiqueta dinámica para identificar todos los eventos en relación con una configuración de servidor web. Hasta ese punto, se analizarán los registros de los dispositivos de monitorización buscando características comunes para eventos relacionados con servidores web. Por ejemplo, como resultado del análisis podríamos identificar como relacionados con el tráfico web todos los eventos que incluyan cualquiera de las siguientes palabras: ‘web’, ‘http’, ‘php’, ‘iis’, ‘script’. Ahora se analizan los registros para las características comunes de las trazas de configuración. Y así, podríamos añadir otro conjunto de palabras que se refieran a algún aspecto de la configuración: ‘conf’, ‘disclos’, ‘reveal’. De este modo, todos los registros/eventos que tengan una palabra del primer conjunto y una palabra del segundo serán detectados y asignados a la categoría de “configuración web” o, en otras palabras, son etiquetados con la etiqueta dinámica “configuración web”.

Una vez que se analizan y clasifican los eventos, se calcula la cantidad de eventos clasificados en cada grupo o etiqueta y se almacena en una base de datos. El valor de la etiqueta se define como la cantidad de eventos para cada dispositivo analizado clasificado en ese grupo o etiqueta específicos. El sistema permite la definición de tantas etiquetas como se necesite. Además de las palabras clave para cada etiqueta es necesario definir, al menos, la siguiente información adicional para definir completamente cada etiqueta:

- Base de datos y tabla donde se almacena el valor real de cada etiqueta.
- Tipo de datos del valor de la etiqueta (habitualmente es un número, pero también podría ser un valor SÍ/NO).
- Condiciones adicionales que podrían ser necesario incluir en la definición de la etiqueta, como por ejemplo:
    - Excepciones.
    - Ventana de tiempo que será consultada para generar un valor para la etiqueta.

Cada vez que el módulo de correlación quiere actualizar el valor de cada etiqueta dinámica, se generará una base de consultas dinámicas de su definición para conseguir el número correcto de casos de este tipo de eventos (el valor de la etiqueta).

Algunos ejemplos de etiquetas definidas en una realización ejemplar de la invención son: web_access, web_atttempts, web_overflow, web_scan, web_error, web_auth, web_highseverty, web_attack, web_password...

Los ataques o amenazas de seguridad se caracterizan habitualmente por el acaecimiento de varios tipos de eventos dentro de un periodo de tiempo, es decir, habitualmente para detectar una amenaza de seguridad, deben detectarse varios tipos de eventos. Como cada tipo de evento está identificado por una etiqueta, es útil agrupar las etiquetas en grupos que caracterizaban un cierto ataque o amenaza. Esta recopilación de etiquetas relacionadas se conoce en este contexto como modelo de datos.

Por ejemplo, podría haber un modelo de datos acerca de una actividad sospechosa de la base de datos SQL. Este modelo de datos contendrá las siguientes etiquetas:

sql= Cualquier evento SQL

sql_access= eventos que implican acceso a la base de datos SQL

sql_command= eventos que implican comandos en la base de datos SQL

sql_scan= eventos que implican un escaneo de la base de datos SQL

La información mínima que se necesita para definir un modelo de datos es la siguiente:

- Nombre del modelo de datos
- Lista de las etiquetas incluidas en el modelo de datos
- Archivo donde se almacenarán los datos de tiempo real leídos
- Identificación de qué grupo de direcciones IP será monitorizado por el modelo de datos. Cada ataque a la seguridad (representado por el modelo de datos) afecta a ciertos dispositivos, así que es un derroche de tiempo y recursos monitorizar todos los dispositivos para cada modelo de datos. Por consiguiente, para cada modelo de datos, sólo se monitorizan ciertos dispositivos (definidos por sus direcciones IP).

En la fase de definición de etiquetas, las etiquetas que serían tenidas en cuenta por un experto que realiza un análisis manual de la seguridad de un sistema dado serán identificadas como relevantes para detectar una actividad maliciosa específica. Estas etiquetas serán agrupadas en el modelo de datos que define dicha actividad maliciosa específica.

En cada intervalo de ejecución configurado, se obtienen los valores de etiquetas para cada dispositivo analizado y agrupado según la definición del modelo. El valor de cada modelo, es decir, los valores de etiquetas específicas obtenidos en cada intervalo de ejecución agrupado en cada modelo de datos, se denomina patrón.

Para el ejemplo anterior, un patrón 5, 0, 0, 5 significará 5 eventos SQL que son 5 escaneos SQL sin acceso y sin comandos. Un patrón como ese será sospechoso, así que debería generarse una alarma.

Una vez que se definen las etiquetas y los modelos de datos, va a explicarse la segunda parte de la presente invención, el uso de algoritmos de Inteligencia Artificial, IA, particularmente un algoritmo de IA de redes neuronales.

Usar algoritmos de IA permite ocuparse de eventos de seguridad como haría un experto en seguridad real, eliminando el tráfico conocido y centrándose en el tráfico sospechoso desconocido pero de una manera automática, sin implicar la participación de un experto en seguridad real.

El sistema incluirá varios algoritmos de IA, basados en las necesidades detectadas en los diferentes entornos donde se usa el ACS. Cada algoritmo de IA incorporará todos los conocimientos aprendidos procedentes de cada entorno. De este modo, los conocimientos procedentes de un entorno estudiado previamente serán utilizables directamente en los siguientes despliegues. Los algoritmos de IA se definen usando etiquetas dinámicas –agrupadas en modelos de datos- como nodos de entrada, no usando eventos específicos.

Tendrá que seguirse el mismo procedimiento para definir todos los modelos diferentes que más tarde serían implementados en algoritmos de IA. Mostraremos, como ejemplo, la definición de una de las redes del ACS, usada para la identificación y detección de ataques web.

1. Primero identificaríamos y definiríamos las etiquetas dinámicas, agrupadas en modelos de datos, que se usarán para crear el modelo de IA, es decir, qué eventos serán procesados por una red neuronal dada.

2. Una vez que han sido identificadas las etiquetas dinámicas que formarán el modelo de IA, se realizará una primera programación de la red neuronal, basada en el comportamiento teórico que debería tener la red. Hasta ese punto, suministraremos a la red un conjunto inicial de patrones que deberían generar alarmas y un conjunto inicial de patrones que no deberían generar alarmas. Estos patrones consisten en la combinación de valores de etiquetas dentro de cada modelo de datos, que generarán una alarma de seguridad (sí) y la combinación de valores de etiquetas dentro de cada modelo de datos, que no generarán una alarma de seguridad (no).

Como ejemplo, incluimos algunos patrones incluidos en el modelo WEBNeuro antes descrito.

187, 90, 80, 0, 0, 4, 0, 33, 4,15, 0, 17, 0, 0, 0, 0, 0, 0, 0, 0, sí
221, 98, 104, 0, 0, 5, 0, 48, 5, 15, 1, 25, 0, 0, 0, 0, 0, 0, 0, 0, sí
2353, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, no
3106, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, no

Cada valor del patrón, separado por coma, está relacionado con la etiqueta dinámica actual del modelo, descrito en la definición xml del modelo. Así, si vemos el siguiente patrón,

3106, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, no

Podemos deducir que un cierto dispositivo con una cierta IP genera 3106 eventos detectados por la etiqueta de web (primera etiqueta), y 2 eventos detectados por la etiqueta 'web_error' (16ª etiqueta).

Una vez que se han definido las etiquetas y el comportamiento inicial, puede comenzar la programación del modelo de IA. El objetivo es encontrar una configuración de parámetros para el modelo de IA que permitirá a la red resultante satisfacer al 100% los conocimientos incluidos en los patrones predefinidos.

3. Añadir nuevos patrones en la base de conocimientos, normalmente durante una fase de prueba de entorno real, y en base al análisis de alarmas reales, permitirá un rápido aprendizaje de conocimientos. Durante la fase de aprendizaje y ajuste, los falsos positivos deberían disminuir rápidamente a medida que nuevos patrones basados en el comportamiento real del sistema se añaden a la base de conocimientos de la red neuronal. Internamente, cuando el operador del sistema o el experto en el sistema añade un nuevo patrón a la base de conocimientos, el patrón no es incorporado inmediatamente. En cambio, los nuevos patrones se añadirán a una base de conocimientos temporal. Periódicamente, se analizarán los patrones incluidos en las bases de conocimientos permanentes y temporales, y los parámetros de la red se ajustarán para intentar conseguir un 100% de éxito. Si alguno de los nuevos parámetros es incoherente con la base de conocimientos permanentes existente, entonces la red recién configurada no podrán adaptarse al 100% de los patrones. Si se da esta situación, entonces la base de conocimientos temporales no se consolidará en la base de conocimientos permanentes, y un experto tendrá que analizar los nuevos patrones para identificar y desechar los incoherentes.

El motor de correlación avanzado propuesto en la presente invención comprende dos partes diferentes de módulos.

Módulo de abstracción de datos y

Módulo de motor artificial

Algunos detalles del módulo de abstracción de datos se muestran en la figura 1. Como puede verse, la entrada de este módulo es la base de datos de un sistema SIEM. En esta base de datos, el sistema SIEM de seguridad almacena todos los eventos de seguridad (generados por los dispositivos de la red de comunicación como cortafuegos, enrutadores, servidores web...) que serán analizados por el ACS. Es decir, en la presente implementación, los eventos de seguridad a analizar han sido recabados e introducidos en una base de datos por un sistema externo, en esta implementación un sistema SIEM (esta es una técnica bien conocida y no es el objetivo de la presente invención).

El motor de correlación avanzado propuesto en la presente invención es independiente de la solución SIEM desplegada. El único requisito es que el motor debe tener acceso a la base de datos (1) donde el SIEM almacena centralizadamente todos los eventos.

Este módulo comprende los siguientes sub-módulos:

- **Acceso a la base de datos.** Módulo que gestionará el acceso del motor de modelos a la Base de datos SIEM. Traducirá los eventos en el formato usado por la base de datos SIEM al formato usado por el sistema ACS. Este módulo fortalecerá la independencia entre el Motor de Modelos y la Base de datos SIEM.

- **Definición de etiquetas dinámicas.** Conjunto de archivos que incluye la información acerca de cada etiqueta dinámica. Este archivo de configuración y el archivo de definición de modelos alimentan al Motor de Modelos, que generará patrones durante su tiempo de ejecución.

- **Definición de modelos de datos.** Conjunto de archivos que incluye la información acerca de las etiquetas dinámicas que forman cada modelo, y también acerca de los dispositivos que deben ser analizados para cada modelo de datos. Para cada modelo de datos, sólo se monitorizan ciertos dispositivos (definidos por su dirección IP), así que para cada modelo de datos se aplica una definición de filtro de IP para seleccionar los dispositivos cuyos eventos deben ser analizados.

- **Motor de modelos.** Módulo que generará patrones para cada modelo de datos basados en los eventos almacenados del SIEM. Generará un archivo de datos para cada modelo de datos, que incluirá los patrones generados para cada dispositivo analizado (cada dispositivo identificado por su dirección IP).

  En cada intervalo de ejecución configurado, el motor de modelos analiza los eventos almacenados en la base de datos SIEM y calcula el valor de cada etiqueta definida (el número de casos para cada dispositivo analizado, del tipo de eventos correspondiente a dicha etiqueta según la definición de etiqueta). El motor de modelos agrupa las etiquetas, según la definición de modelo de datos, generando patrones reales (un patrón por modelo de datos y por dispositivo). Los patrones se dividirán en N subgrupos (6) (modelo de datos 1 a modelo de datos N). El modelo de datos de subgrupo m incluirá los K_m patrones generados por el modelo m, siendo K_m el número de dispositivos que

han de analizarse para el modelo de datos m. Todos estos patrones serán la entrada del módulo de Motor de IA.

La arquitectura del Módulo de Motor Artificial se muestra en la figura 2. Este módulo comprende los siguientes sub-módulos (como se muestra en la figura 2):

- **Bases de datos de conocimientos de IA.** Hay al menos una base de datos de conocimientos de IA para cada modelo de datos, cada base de datos incluirá un archivo que describirá las etiquetas dinámicas incluidas por el modelo, y todos los patrones que forman los conocimientos iniciales usados para programar la red neuronal (conjunto inicial de patrones). Para cada patrón, se señalará si debe generarse una alarma de seguridad o no (por ejemplo, "si el patrón para cada modelo de datos m=221, 98, 104, 0, 0, 5, 0, 48, 5, 15, 1, 25, 0, 0, 0, 0, 0, 0, 0, 0, entonces alarma generada). A estas bases de datos de conocimientos se les suministran nuevos patrones (con la información correspondiente acerca de si debe generarse una alarma o no) durante todo el periodo de funcionamiento.

- **Motores de IA.** Este módulo implementará todos los algoritmos de IA que procesarán los patrones generados por el módulo de abstracción de datos. Habrá N Motores de IA (uno por modelo de datos) y cada uno procesará los patrones del modelo de datos correspondiente. Los patrones serán incluidos en un archivo de datos, y serán evaluados por el Motor de IA correspondiente. Los Motores de IA usan redes neuronales o bayesianas estándar para la implementación del algoritmo de detección de alarma en base a la base de conocimientos procedente de cada Motor de IA. Usa técnicas de agrupamiento para la identificación de patrones inusuales y puede incluir otros algoritmos patentados si es necesario. Para los nuevos patrones (no incluidos en la base de datos de conocimientos), el algoritmo de IA estimará un resultado en base a la similitud ponderada entre los nuevos patrones y los patrones conocidos incluidos en la base de datos de conocimientos. Cuando un patrón analizado es demasiado diferente de los patrones conocidos, el motor puede advertir al administrador de que el patrón diferente puede generar probablemente un falso positivo o negativo. Los motores de IA procesarán los patrones y, como resultado, se decidirá si debería generarse una alarma o no para cada patrón procesado. Esta información se transmitirá a un Módulo de Generación de Alarma y luego al módulo de compilación de alarma del sistema de seguridad (habitualmente un sistema SIEM) en el que están integrados los módulos. Si una falsa alarma es generada por el motor, el patrón correspondiente se almacena en la base de datos de conocimientos, así que no se generarán más falsas alarmas para estos patrones.

Una vez que se ha definido el comportamiento teórico, se implementará y probará en un entorno real donde se comprobará la configuración inicial. Durante un primer periodo (periodo de aprendizaje) habrá un ajuste de los parámetros iniciales de los Motores de IA y de los datos en las bases de datos de conocimientos, para conseguir un modelo final. Esta fase enriquecerá la base de conocimientos hasta que se defina un modelo funcional completo. Incluso después de este periodo de aprendizaje, cuando el modelo funcional está definido, es posible que aparezcan algunos nuevos patrones que deberían ser incluidos en la base de conocimientos, aunque el número de nuevos patrones será pequeño y disminuirá rápidamente una vez que todos los conocimientos específicos han sido incorporados a la base de conocimientos (debido al rápido aprendizaje de los algoritmos de IA).

Resumiendo, el flujo de trabajo del ACS puede describirse de la siguiente manera:

0) Se definen las etiquetas y modelos. Los motores de IA (redes neuronales) se configuran incluyendo en las bases de datos de conocimientos un conjunto inicial de patrones conocidos. Luego es momento de comenzar a analizar el evento real para detectar actividad sospechosa.

1) Cada cierto intervalo de tiempo configurado, el Módulo de Abstracción de Datos del ACS averigua qué dispositivos (IPs) deben ser analizados (habitualmente identificados por una Definición de Filtro de IP) para cada posible ataque a la seguridad (modelo de datos), es decir, los dispositivos cuyos eventos generados deben ser analizados para cada modelo de datos.

2) El Módulo de Abstracción de Datos del ACS genera una consulta basada en la definición de etiqueta, construyendo un patrón para cada IP seleccionada (habitualmente una consulta SQL).

3) Todos los patrones son evaluados por la Red Neuronal implementada en el Módulo de Motor de IA del ACS para el modelo de datos analizado. Si un patrón analizado es considerado sospechoso por la red neuronal, el ACS enviará una alarma para notificar esta actividad sospechosa.

En una realización de la presente invención, el ACS ha sido integrado en una arquitectura SIEM estándar (SIEM de la suite de distribución libre OSSIM Open Source Security Information Management). Los algoritmos de inteligencia artificial usados en esta realización son redes neuronales y técnicas de agrupamiento de eventos. La figura 3 muestra la arquitectura de la realización.

El SIEM estándar realiza una compilación de todos los eventos enviados por las fuentes de información (2). Todos estos eventos son procesados por un motor servidor y almacenados en una base de datos centralizada usada por el motor de correlación nativo para analizar toda esta información para generar alarmas cuando se descubre alguna actividad sospechosa.

El ACS ha sido configurado como un complemento al correlador nativo, aunque permite dos procedimientos de configuración posibles:

- Notificación de cualquier actividad sospechosa detectada por cualquiera de los algoritmos basados en IA.
- Generación de alarma sólo cuando el motor de correlación nativo no la ha detectado.

Como se dijo en el párrafo previo, el módulo ACS lleva a los datos de entrada los eventos almacenados en la base de datos SIEM centralizada. Los eventos se leen y procesan en el Módulo de Abstracción de Datos que genera los patrones para cada uno de los modelos así que pueden ser analizados por el Módulo de Motor de Inteligencia Artificial, IA. La actividad sospechosa detectada puede ser tratada por el algoritmo SIEM como eventos a compilar y analizados para decidir si debe darse una alarma (habitualmente, si el evento es una actividad sospechosa detectada por el módulo ACS, se dará una alarma).

Para mostrar los beneficios de la presente invención, se mostrará un caso de uso real. En este caso de uso mostraremos una comparación entre un SIEM que usa su conjunto de correlaciones por defecto, con el ACS de la presente invención. Lo primero que nos gustaría destacar es que el número de alarmas generadas por el ACS es menor que las que generó el SIEM típico. La figura 4 muestra el número de alarmas totales generadas por el ACS y un SIEM típico, por días.

Pueden observarse dos periodos distintos en la figura:

- Un primer periodo, hasta el quinto día, que corresponde al periodo de formación/aprendizaje para el ACS, durante el cual fue ajustado al entorno en el que estaba funcionando.
- Un segundo periodo, desde el quinto día hasta el final, que se corresponde con el periodo efectivo real para el ACS, una vez que ha incorporado en todos los modelos las particularidades del entorno en el que estaba funcionando.

En ambos periodos, el ACS genera menos alarmas que el SIEM típico, y finamente se estabiliza alrededor de 5 alarmas diarias. Otro punto importante que hay que considerar, asociado a la eficiencia del sistema, es el número total de alarmas no relevantes generadas. Este punto de datos es importante porque, desde el punto de vista de un operador del sistema, cuantas menos alarmas no relevantes genera un sistema, menos tiempo y esfuerzo se desperdicia.

También es importante definir qué entendemos por alarmas relevantes y no relevantes. Consideramos una alarma como relevante cuando implica un problema real, que requerirá intervención del operador o el experto, para solucionar el problema o al menos para atenuar los riesgos producidos por el problema. Por lo tanto, las alarmas que no requieren ninguna intervención, porque son de poca gravedad, o informativas, o son simplemente falsos positivos, son etiquetadas como no relevantes. En el caso mostrado, el ACS genera un número muy pequeño de alarmas no relevantes (30 alarmas, o un 9% de las alarmas totales generadas), mientras que el SIEM generó un número mucho más alto (310 alarmas, o el 91% de las alarmas totales generadas).

Otro punto importante que se ha de evaluar es la capacidad del nuevo sistema para detectar nuevas alarmas que no son generadas por el SIEM usado. En este modo de funcionamiento, el ACS sólo genera alarmas cuando detecta que el SIEM no la ha generado. En este sentido, en el presente caso, el ACS genera un 88% de las alarmas relevantes totales, mientras que el SIEM típico genera sólo el 12%.

Resumiendo, las ventajas de la presente invención comparadas con el SIEM actual son:

- El ACS es independiente de los eventos generados por Sistemas de Detección de Intrusión (IDS). El sistema de etiquetas dinámicas descrito es responsable de esa independencia, y deja a la invención usar la misma configuración independientemente del IDS desplegado. Una actualización sobre los eventos detectados por el IDS desplegado, o por cualquier otro dispositivo, no requiere una actualización de la configuración del ACS debido a la definición de etiqueta dinámica basada en la descripción de eventos (común a todos los dispositivos fabricados) y no en el evento específico generado por un dispositivo específico.
- Los módulos de correlación de los sistemas SIEM están basados en la detección de amenazas conocidas, que deben ser caracterizadas y configuradas de antemano por un experto. Este procedimiento de detección obliga a una revisión continua de las correlaciones configuradas, para detectar las nuevas amenazas que no fueron incluidas o configuradas inicialmente. Por otra parte, los algoritmos de inteligencia artificial usados en la invención permiten la detección de nuevas amenazas desconocidas previamente usando como base la configuración inicial (conocimientos). Este comportamiento de aprendizaje es intrínseco a los algoritmos usados.
- La invención puede advertir al sistema cuando el resultado no es fiable (detectar cuándo es probable que se genere un falso positivo o negativo).
- El tiempo de formación del ACS, desde su instalación hasta el punto de funcionamiento óptimo es muy bajo, y también tienen un coste de mantenimiento muy bajo, ya que no hay necesidad de definir reglas específicas para cada nueva amenaza.

- El ajuste para el ACS consiste básicamente en detectar y declarar los falsos positivos (actualizando las bases de datos de conocimientos del motor de IA con esta información) así no aparecerán de nuevo. Si la formación se ha realizado correctamente, entonces el número de falsos positivos tenderá a cero rápidamente.

Por consiguiente, las principales mejoras del ACS sobre un SIEM estándar son:

- **Eficiencia más alta,** ya que las alarmas generadas por el ACS pueden catalogarse como de la más alta prioridad, y la mayoría de ellas requieren intervención del operador o el administrador de seguridad.
- **Efectividad más alta,** ya que detecta muchas alarmas que no son detectadas por un SIEM típico.
- **Costes más bajos,** tanto en costes de puesta en marcha como de operación.

Aunque la presente invención se ha descrito con referencia a realizaciones específicas, debería entenderse por parte de los expertos en la materia que lo anterior y otros diversos cambios, omisiones y añadidos en la forma y detalle de los mismos pueden realizarse en la misma sin apartarse del espíritu y alcance de la invención tal como se define por las siguientes reivindicaciones.

REIVINDICACIONES

1.- Un procedimiento de mejora de la detección de amenazas de seguridad en una red de comunicación, incluyendo la red de comunicación dispositivos de seguridad que generan eventos de seguridad, siendo esos eventos almacenados en una base de datos de seguridad, comprendiendo el sistema:

a) Definir diferentes tipos de eventos de seguridad, cada tipo de evento de seguridad se denomina una etiqueta dinámica, la etiqueta dinámica asignada a cada evento de seguridad dependerá de ciertas condiciones que se encuentran en la descripción del evento.

b) Definir los modelos de datos, siendo un modelo de datos la recopilación de etiquetas dinámicas que están relacionadas con una cierta amenaza de seguridad; un modelo de datos estará definido por cada tipo de amenaza de seguridad a detectar.

c) En cada intervalo de ejecución configurado, seleccionar los dispositivos a analizar para cada modelo de datos y, para cada dispositivo analizado, leer de la base de datos de seguridad los eventos generados por dicho dispositivo, asignar una etiqueta dinámica a cada evento de seguridad y calcular el valor de cada etiqueta dinámica, el valor de la etiqueta es el número de casos para cada dispositivo analizado del tipo de eventos correspondiente a dicha etiqueta.

d) Agrupar las etiquetas, según la definición del modelo de datos, generando un patrón con los valores de etiquetas para cada modelo de datos y para cada dispositivo analizado.

e) Para cada modelo de datos, leer los patrones correspondientes generados en la etapa d) y aplicar un algoritmo de Inteligencia Artificial en base a la información almacenada en una base de datos de conocimientos de dicho modelo de datos, para decidir si debe generarse una alarma de actividad sospechosa para cada patrón analizado o no; incluyendo cada base de datos de conocimientos, para cada modelo de datos, un conjunto de patrones conocidos con la información de si debe generarse una alarma para dicho patrón o no.

2.- Un procedimiento según la reivindicación 1, donde el algoritmo de Inteligencia Artificial es un algoritmo de Red Neuronal.

3.- Un procedimiento según cualquiera de las reivindicaciones previas, donde los dispositivos de seguridad que generan los eventos de seguridad pueden ser enrutadores, cortafuegos, servidores web, sistemas de detección de intrusión o sistemas de prevención de intrusión.

4.- Un procedimiento según cualquiera de las reivindicaciones previas, donde la etapa de definir las etiquetas dinámicas comprende la etapa de definir las palabras clave asociadas a cada etiqueta dinámica y la etapa de asignar una etiqueta dinámica a un evento de seguridad, comprende la etapa de analizar la descripción del evento de seguridad y asignar una etiqueta dinámica al evento de seguridad si las palabras clave asociadas a dicha etiqueta dinámica se encuentran en la descripción del evento de seguridad.

5.- Un procedimiento según cualquiera de las reivindicaciones previas, donde la etapa de definir los modelos de datos incluye además:

- definir la lista de las etiquetas dinámicas incluidas en cada modelo de datos

- definir la lista de dispositivos que deben ser analizados para cada modelo de datos

6.- Un procedimiento según cualquiera de las reivindicaciones previas, donde cada dispositivo está identificado por su dirección IP.

7.- Un procedimiento según cualquiera de las reivindicaciones previas, donde las alarmas de actividades sospechosas generadas son enviadas a un sistema de Gestión de Eventos de Información de Seguridad, SIEM, y la base de datos de seguridad es parte de este sistema y en el que los eventos de seguridad generados por los dispositivos de seguridad son almacenados en la base de datos de seguridad por el sistema SIEM.

8.- Un procedimiento según cualquiera de las reivindicaciones previas donde, antes de que comience el primer intervalo de ejecución, un conjunto inicial de patrones conocidos con la información de si debe generarse una alarma para dicho patrón o no, es almacenado en cada base de datos de conocimientos y, en cada intervalo de ejecución, pueden añadirse nuevos patrones a las bases de datos de conocimientos con la información de si debe generarse una alarma para dicho patrón o no, en base al análisis de alarmas reales.

9.- Un procedimiento según la reivindicación 8 donde si, como resultado de analizar un patrón, el algoritmo toma la decisión de generar una alarma, y esta alarma es una falsa alarma, entonces la información de no generar una alarma para dicho patrón, es almacenada en la base de datos de conocimientos correspondiente.

10.- Un procedimiento según la reivindicación 1, donde el procedimiento, antes de la etapa c), incluye además una etapa de traducir el formato de los eventos almacenados en la base de datos de seguridad a un formato común solicitado.

11.- Un procedimiento según cualquiera de las reivindicaciones previas, donde el procedimiento es usado para mejorar el módulo de correlación de un sistema de Gestión de Eventos de Información de Seguridad, SIEM.

12.- Un sistema que comprende medios adaptados para realizar el procedimiento según cualquiera de las reivindicaciones precedentes.

13.- Un programa de ordenador que comprende medios de código de programa de ordenador adaptados para realizar el procedimiento según cualquiera de las reivindicaciones 1 a 11 cuando dicho programa se ejecuta en un ordenador, un procesador de señales digitales, una matriz de puertas programable en campo, un circuito integrado de aplicación específica, un microprocesador, un microcontrolador, o cualquier otra forma de hardware programable.

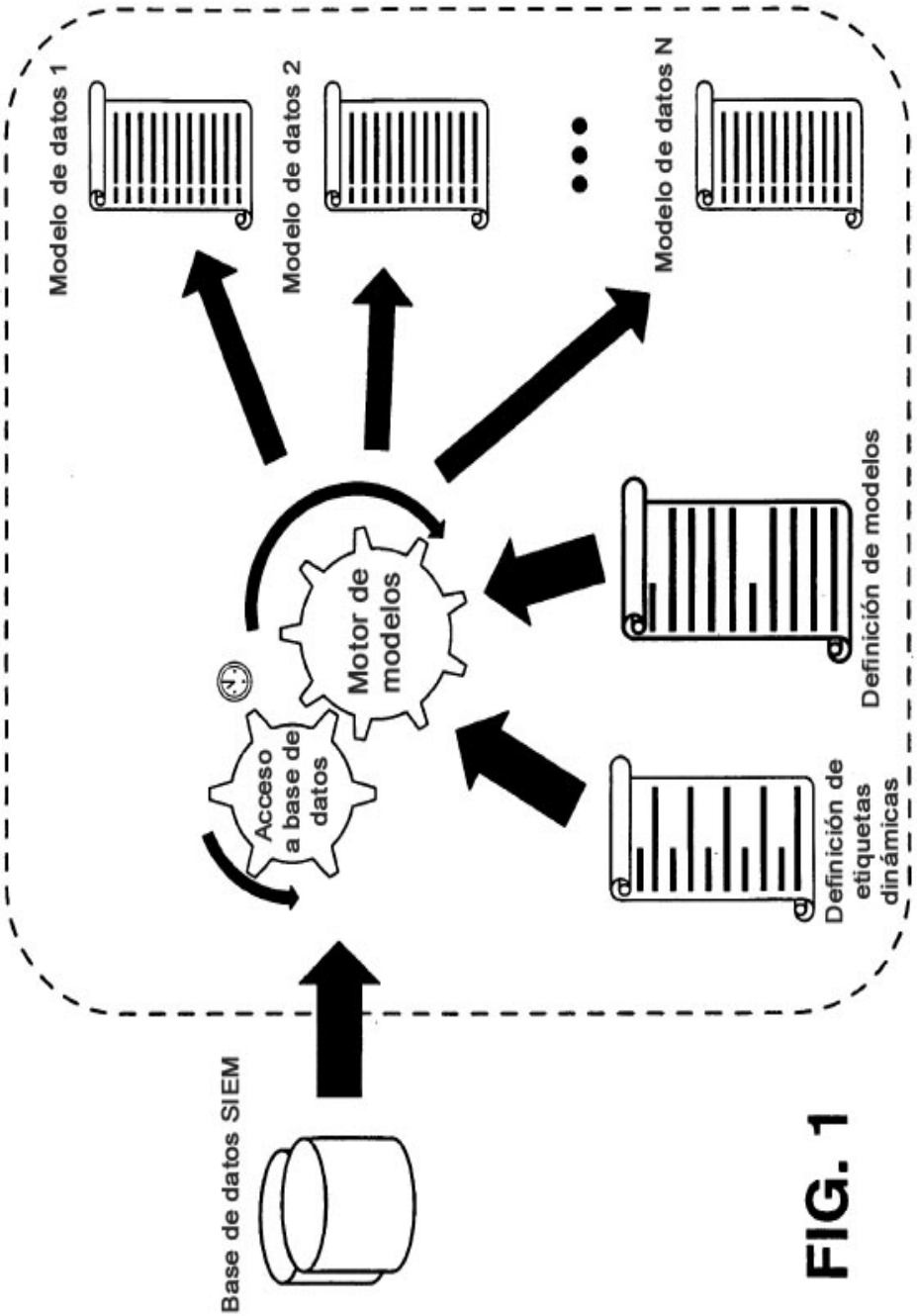
Modelo de datos 1
Modelo de datos 2
Modelo de datos N
Motor de modelos
Acceso a base de datos
Definición de modelos
Definición de etiquetas dinámicas
Base de datos SIEM

FIG. 1

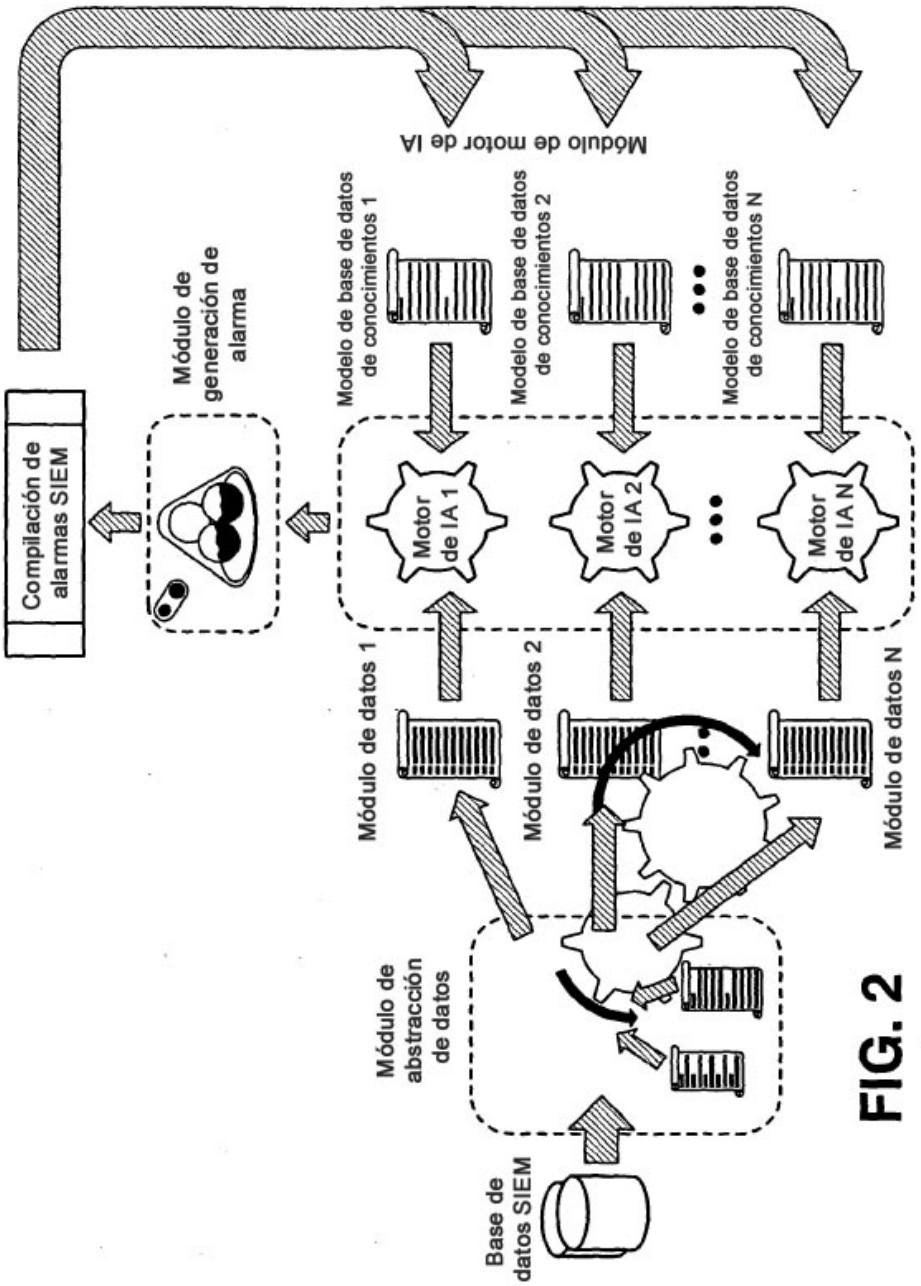
Módulo de motor de IA
Modelo de base de datos de conocimientos 1
Modelo de base de datos de conocimientos 2
Modelo de base de datos de conocimientos N
Módulo de generación de alarma
Compilación de alarmas SIEM
Motor de IA 1
Motor de IA 2
Motor de IA N
Módulo de datos 1
Módulo de datos 2
Módulo de datos N
Módulo de abstracción de datos
Base de datos SIEM

FIG. 2

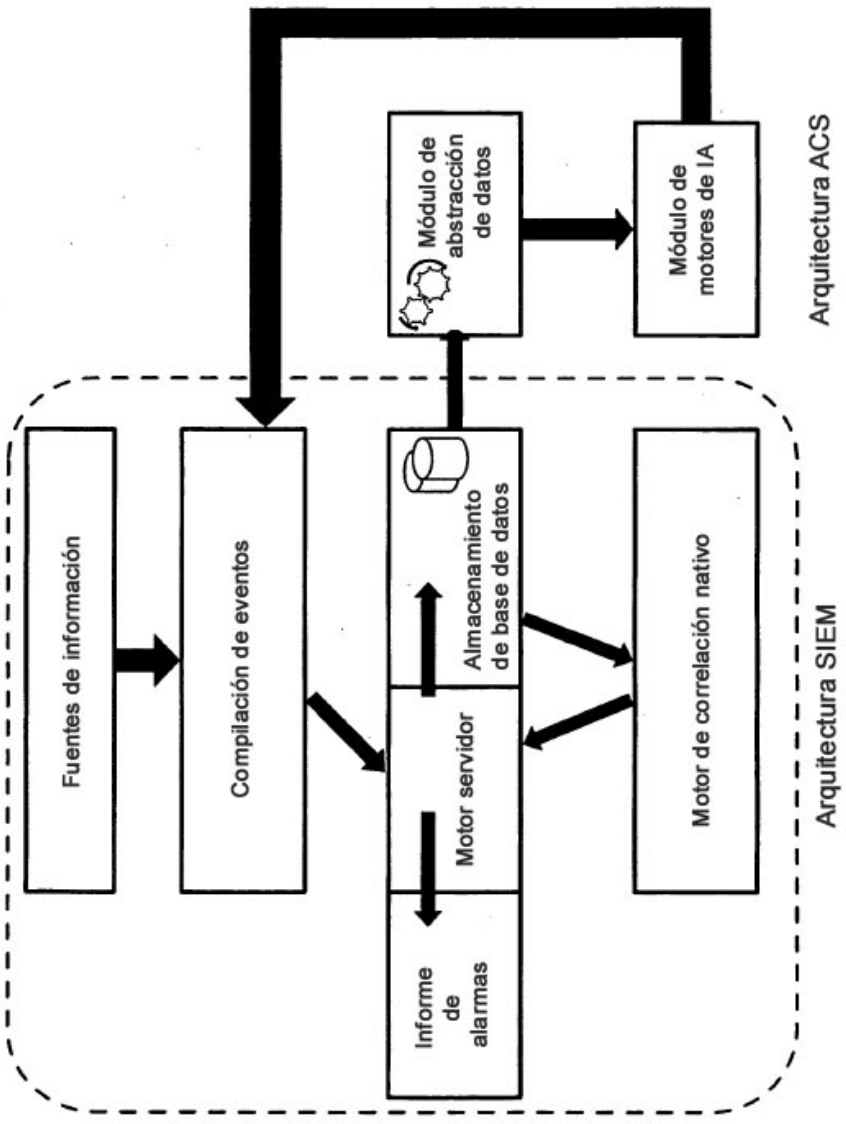
Fuentes de información
Compilación de eventos
Almacenamiento de base de datos
Motor servidor
Informe de alarmas
Motor de correlación nativo
Arquitectura SIEM
Módulo de abstracción de datos
Módulo de motores de IA
Arquitectura ACS

FIG. 3

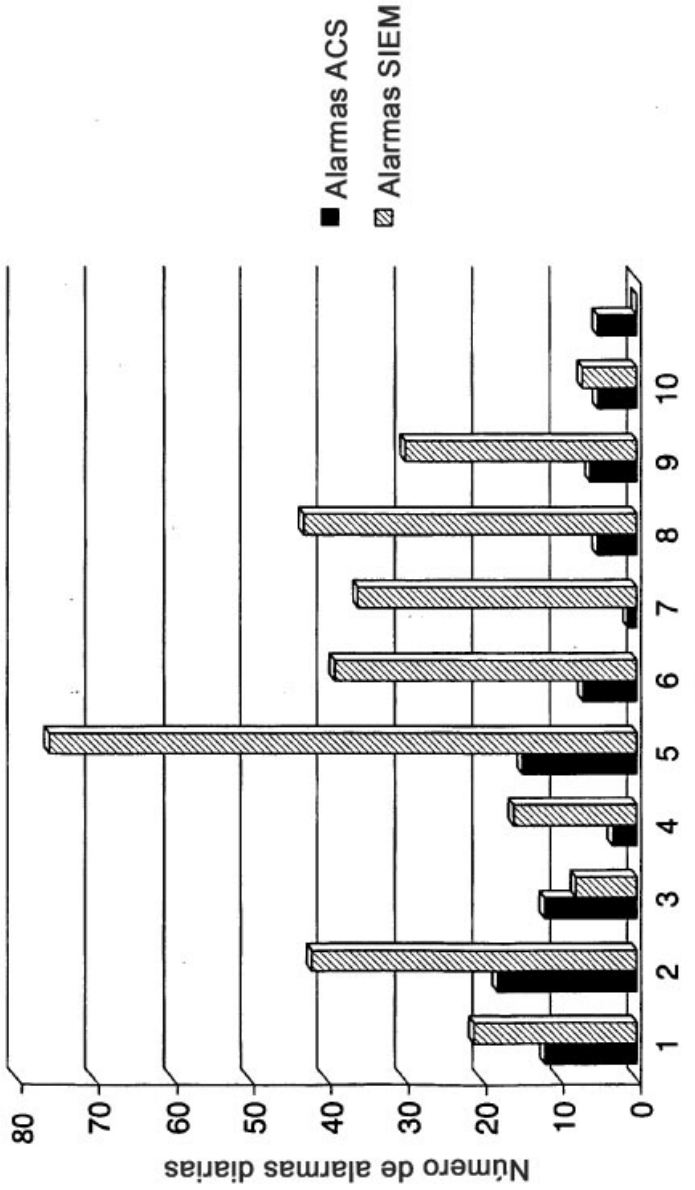
Alarmas ACS
Alarmas SIEM
Número de alarmas diarias
0
10
20
30
40
50
60
70
80
1
2
3
4
5
6
7
8
9
10
Día

FIG. 4