(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 777 660**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/24 (2006.01)
G06F 21/55 (2013.01)
G01N 35/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.12.2017 E 17209693 (5)**

(97) Fecha y número de publicación de la concesión europea: **29.01.2020 EP 3343868**

(54) Título: **Detección y alerta de ataques cibernéticos a redes centradas en recursos**

(30) Prioridad:

28.12.2016 US 201662439712 P
13.10.2017 US 201715783512

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.08.2020

(73) Titular/es:

PALANTIR TECHNOLOGIES INC. (100.0%)
100 Hamilton Avenue, Suite 300
Palo Alto, CA 94301, US

(72) Inventor/es:

ZORLULAR, CEM;
BROWN, BARRETT;
TANG, XIAO (RAYMOOND);
SERENHOV, ALEXANDRA;
YEO, CHUO HAO;
ZALUTSKI, IHAR y
WALSH, MATTHEW

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Detección y alerta de ataques cibernéticos a redes centradas en recursos

Campo técnico

La presente descripción se refiere a sistemas y métodos que facilitan la generación y presentación de alertas relacionadas con un ataque cibernético a un recurso.

Antecedentes

Los recursos informáticos importantes ("recursos"), tales como, por ejemplo, los sistemas de control industrial, las bases de datos confidenciales y similares, están continuamente expuestos a la amenaza de ataques cibernéticos ("ataques"). Esos ataques, si tienen éxito, pueden causar daños al hardware industrial o a los sistemas informáticos y/o exponer datos confidenciales. Debido a que el autor de un ataque cibernético puede elegir entre una amplia variedad de diferentes estrategias y técnicas de ataque, los ataques cibernéticos pueden ser muy difíciles de detectar a tiempo.

El documento US2016/0226905 describe un sistema en el que se detectan y evalúan los riesgos de amenazas para una empresa mediante el ensamblaje de amenazas singulares identificadas utilizando indicadores de amenazas tanto directas como conductuales en amenazas compuestas para crear casos de uso complejos en múltiples dominios, y para amplificar los riesgos a lo largo de las cadenas de ataque de los ataques conocidos para su detección temprana. Las puntuaciones del riesgo de amenaza compuesta se calculan a partir de puntuaciones del riesgo de amenazas singulares para aumentar exponencialmente con el número de eventos observados a lo largo de la cadena de eliminación. Las amenazas compuestas se combinan con valores normalizados de riesgo estático y riesgo inherente para que una entidad de la empresa produzca una puntuación del riesgo para la entidad representativo del riesgo general para la entidad.

El documento US2015/0121518 describe un método implementado por ordenador para determinar si una red de ordenadores está comprometida por actividad no autorizada en la red de ordenadores. El método implementado por ordenador comprende identificar una anomalía de comportamiento de una entidad en la red de ordenadores, clasificar la anomalía como un evento del sistema basado en una puntuación asignada para que la anomalía esté al menos en un umbral de puntuación predeterminado, actualizar un incidente basado en al menos un parámetro común entre el evento del sistema y otros eventos del sistema que comprenden el incidente, incluyendo cada evento del sistema del incidente una puntuación asignada de cuando el evento fue una anomalía, actualizar un estado del sistema basado en al menos el incidente y asignar una puntuación de estado del sistema al estado del sistema y determinar si la puntuación de estado del sistema está al menos en un umbral predeterminado de puntuación de estado del sistema que indica que la red informática puede estar comprometida.

Resumen

Los sistemas, métodos y dispositivos descritos en el presente documento tienen varios aspectos, ninguno de los cuales es el único responsable de sus atributos deseables. Sin limitar el alcance de esta descripción, ahora se discutirán brevemente varias características no limitantes.

Los atacantes cibernéticos tienen diferentes herramientas y técnicas a su disposición, tales como, por ejemplo, la explotación de varias vulnerabilidades de seguridad o puertas traseras intencionales en componentes de software y hardware, el uso de "phishing" y otras técnicas de "ingeniería social" para adquirir credenciales de acceso y el uso de técnicas de descifrado por "fuerza bruta" para encontrar credenciales de autentificación para recursos de interés. Si bien muchas de esas técnicas de ataque dejan algún tipo de indicador que podría usarse para inferir que un ataque cibernético está o ha estado en curso, los indicadores pueden no aislarse fácilmente de la actividad normal que no está relacionada con los ataques cibernéticos.

Debido a los diferentes tipos de posibles técnicas y estrategias disponibles para el autor de un ataque cibernético, una gran variedad de diferentes tipos de registros e información pueden ser indicadores de un ataque cibernético. Por ejemplo, los registros de actividad de un usuario en una red informática pueden contener indicadores de ciertos tipos de ataques cibernéticos. Varios tipos de registros y registros pueden contener indicadores de un ataque cibernético. Por ejemplo, los registros de cortafuegos, los registros de autentificación, los registros de conexión de la red privada virtual (VPN), los registros del servidor de bases de datos, etc., pueden contener indicadores de varios tipos de ataques cibernéticos. Un indicador puede incluir datos, información o cosas, tales como una actividad, un evento de un registro de eventos del sistema operativo, un historial de acceso y/o similares.

Los recursos dirigidos pueden incluir, por ejemplo, un sistema de control para un proceso industrial importante o una pieza de equipo tal como, por ejemplo, una centrífuga, un robot, un sistema electromecánico de compuerta o una base de datos de información confidencial tal como la información sanitaria. Dichos recursos pueden presentar objetivos principales para diferentes tipos de atacantes. Ventajosamente, centrar un análisis de los indicadores de un posible ataque cibernético alrededor del recurso potencialmente atacado puede proporcionar una forma de asociar,

agrupar y conciliar diferentes eventos al determinar que esos diferentes eventos pueden dirigirse contra un recurso común.

Un ataque cibernético contra un recurso puede comprender múltiples pasos que implican técnicas y estrategias específicas. Por ejemplo, un ataque cibernético puede usar una técnica particular, como la explotación de una vulnerabilidad de software en un servidor web, para obtener acceso a una red interna de la compañía, luego usar credenciales de autentificación robadas para acceder al recurso, copiar datos del recurso y transmitir los datos fuera de la red a través de una conexión encriptada. Cada uno de estos diferentes pasos y técnicas puede crear indicadores únicos; como tal, el alcance completo de la actividad de un ataque cibernético solamente puede reconocerse cuando se revisan y ponen en contexto múltiples indicadores tan diferentes.

Un indicador, visto de forma aislada, no confirma o niega necesariamente que se esté perpetrando o no un ataque cibernético; más bien, un indicador puede ser probatorio, aunque solo sea ligeramente, en virtud de estar correlacionado positiva o negativamente con un ataque cibernético. Por ejemplo, un fallo de autentificación en un servidor corporativo, visto de forma aislada, puede no justificar la conclusión de que un recurso al que pertenece este servidor está siendo atacado. Visto junto con otros indicadores, sin embargo, el conocimiento del hecho de que hubo un fallo de autentificación puede ayudar a determinar si se está produciendo o no un ataque cibernético.

Como se discutió, varios tipos de información ("indicadores") pueden ayudar a deducir que un ataque está en curso, y de ese modo permitir que se tomen medidas para evitar que el ataque cibernético progrese. Por ejemplo, un número inusual de autentificaciones fallidas en un servidor puede ser indicativo de un atacante que busca obtener acceso no autorizado a ese servidor. Del mismo modo, la presencia de software malicioso ("malware") en uno de los ordenadores, tráfico de red sospechoso u otros factores pueden ser indicativos de un ataque en curso. Los indicadores relevantes se pueden recopilar en diferentes dispositivos en una red, y se pueden utilizar para permitir un análisis exhaustivo de un posible ataque cibernético sobre un recurso. Al revisar dichos indicadores, un analista puede deducir que un ataque a un recurso está en curso. En muchos casos, puede ser que no haya un único indicador disponible que establezca de manera concluyente si un ataque cibernético está en curso o no. Como tal, puede ser ventajoso revisar múltiples indicadores en el contexto para hacer esta determinación. Debido a que estos indicadores pueden estar presentes en una gran cantidad de sistemas diferentes que pueden necesitar consultarse utilizando diferentes protocolos y técnicas, y los indicadores recibidos pueden estar presentes en diferentes formatos y estructuras, la recopilación y agregación de los indicadores para facilitar una revisión exhaustiva plantea desafíos únicos. El monitoreo y la detección en tiempo real de los ataques cibernéticos pueden ser habilitados por sistemas automatizados, pero sería imposible sin ellos. El monitoreo y la detección en tiempo real permiten tomar medidas para evitar que el ataque cibernético progrese.

Incluso con todos los indicadores disponibles para su revisión, aún puede ser difícil distinguir un ataque cibernético de la actividad regular. Debido a la gran cantidad de diferentes herramientas y técnicas disponibles para un atacante, es difícil inferir que un ataque cibernético está en curso en función de uno o un número limitado de indicadores. Por ejemplo, los intentos fallidos de autentificación en los servidores pueden indicar la presencia de un atacante que busca "forzar" su acceso al servidor, pero dichos intentos fallidos de autentificación también pueden indicar que un usuario legítimo simplemente ha olvidado su contraseña.

Además, es deseable que se detecte un ataque cibernético lo antes posible, de modo que se puedan tomar contramedidas antes de que se pueda lograr el objetivo del atacante, es decir, evitar que el ataque cibernético progrese.

Por lo anterior, y por otras razones, sigue existiendo la necesidad de sistemas y métodos novedosos que ayuden a identificar un ataque cibernético contra los recursos en una etapa temprana, sin alertar indebidamente de la actividad que no está relacionada con un ataque cibernético, para presentar alertas relacionadas con la actividad de un supuesto ataque cibernético de una manera que sea comprensible y accesible para un analista humano, y para recopilar y procesar respuestas de un analista humano a dichas alertas con el fin de facilitar una contramedida oportuna y efectiva contra supuestos ataques cibernéticos e informar los futuros monitoreo y detección de ataques cibernéticos.

Como se describe en el presente documento, las realizaciones del sistema de la presente descripción pueden, en algunos casos, combinar conjuntos de más de un indicador utilizando una variedad de operaciones para formar uno o más indicadores nuevos. Dichas combinaciones se denominan en el presente documento agregados. Algunos agregados son, por ejemplo, conteos (recuentos), promedios, medianas, máximos, mínimos, cuartiles, porcentajes, correlación cruzada, etc. Puede ser ventajoso calcular dichos agregados por varias razones, que incluyen, por ejemplo, reducir la cantidad de datos procesados y así reducir el esfuerzo computacional requerido, o combinar indicadores sinérgicamente para revelar información adicional.

En algunas realizaciones, el sistema de advertencia puede utilizar indicadores, o combinaciones de indicadores, para detectar el "movimiento lateral" de un usuario. Esto se refiere al fenómeno de un usuario o dispositivo que presenta credenciales de autentificación correspondientes a más de un usuario. Tal movimiento lateral puede ser indicativo de un ataque cibernético. En una realización de ejemplo, el sistema de advertencia rastrea el movimiento

lateral al revisar los indicadores que reflejan los intentos de autentificación y crear, a partir de esos intentos de autentificación, un recuento de cuántos usuarios diferentes ha intentado autentificar un usuario o dispositivo.

Se conocen sistemas que recopilan y muestran uno o más tipos de indicadores a un analista humano. Sin embargo, estos sistemas pueden lograr un éxito limitado para facilitar la detección oportuna de ataques, en parte porque el número de posibles indicadores de un ataque en curso puede ser extremadamente grande en comparación con la capacidad de un analista humano para revisarlos en tiempo real o casi en tiempo real. Además, la interpretación significativa de los indicadores se dificulta por el fracaso de estos sistemas existentes para proporcionar información contextual adecuada, tal como, por ejemplo, otros indicadores e información histórica. Además, la revisión se vuelve más fácil y más efectiva cuando los indicadores se presentan mediante representaciones gráficas tales como cuadros y gráficos, y valores agregados tales como totales, promedios y valores extremos. Algunos sistemas existentes no logran digerir adecuadamente los indicadores y presentan información pertinente en una forma fácilmente accesible. Por lo tanto, sigue siendo necesario agrupar, clasificar, agregar y filtrar los datos contenidos en estos indicadores, y presentarlos junto con información contextual relevante, de manera que permita a un analista humano revisarlos de manera efectiva para detectar un ataque cibernético y de ese modo permitir que se tomen medidas para evitar que el ataque cibernético progrese.

Ciertas realizaciones de la presente descripción pueden proporcionar una puntuación del riesgo, o una representación gráfica de dicha puntuación del riesgo, para recursos individuales, así como para una colección de recursos (por ejemplo, una puntuación del riesgo "global"). La puntuación del riesgo de cada recurso puede determinarse combinando las estimaciones de riesgo para cada evento y alerta asociada con el recurso. La puntuación del riesgo global puede determinarse combinando la puntuación del riesgo de todos los recursos. Puede ser ventajoso proporcionar una puntuación del riesgo que aumente continuamente a medida que aumenta el número de eventos con riesgo y/o de alertas, pero que no supere un cierto número. Tal puntuación del riesgo puede ser más inmediatamente comprensible para un usuario porque se puede dimensionar en un intervalo conveniente, tal como de 0-100. También se puede ver que refleja el hecho de que para una serie de eventos no correlacionados, que representan intentos de un ataque cibernético contra un recurso, el riesgo (por ejemplo, la probabilidad de al menos un intento exitoso de un ataque cibernético) aumenta monotónicamente con la cantidad de intentos independientes, pero nunca excederá la certeza. La combinación de estimaciones de riesgo constituyentes para formar una puntuación del riesgo puede hacerse ventajosamente usando una función matemática continua que converge monotónicamente a un límite deseado. Por ejemplo, si R1, R2 y R3 representan las estimaciones de riesgos constituyentes (por ejemplo, la puntuación del riesgo de tres recursos individuales), la función para calcular R(R1, R2, R3) puede definirse como R(R1,R2,R3)=arctan (R1+R2+R3)∗100∗2/Pi. Esto asegura que la puntuación del riesgo aumenta continuamente cuando aumentan sus componentes, pero nunca supera los 100.

Los diferentes tipos de usuarios pueden acceder a diferentes recursos en diferentes roles y pueden cumplir diferentes funciones. Como tal, puede ser ventajoso para un sistema de advertencia clasificar, agrupar, filtrar, puntuar y categorizar alertas de un posible ataque cibernético por recursos. En una realización de ejemplo, el sistema de advertencia puede determinar una estimación de cuánto está en riesgo un determinado recurso por un ataque cibernético en un momento dado en función de los indicadores recibidos. Además, si el sistema de advertencia recibe indicadores de múltiples fuentes, todos indicando un ataque cibernético contra el mismo recurso, presentar esos indicadores al analista juntos puede servir al analista para determinar que hay un ataque cibernético en curso contra un recurso dado. Ventajosamente, esto puede permitir que varios indicadores, incluidos aquellos correspondientes a la actividad del usuario, que no sean lo suficientemente sospechosos cuando un analista los revise individualmente, se relacionen entre sí y se relacionen con un ataque cibernético en curso contra un recurso. Por ejemplo, si el administrador de un recurso es víctima de una estafa de ingeniería social y después de un corto período de tiempo, se hacen múltiples solicitudes para operar el hardware desde el recurso que parece estar justo por debajo del umbral para el cual el administrador tendría que buscar aprobación interna, estos dos indicadores cuando se revisan individualmente pueden no ser suficientes para que un analista comience un examen más detallado. Sin embargo, si estos dos indicadores se presentan juntos al analista, el analista puede determinar si hay un ataque cibernético contra este recurso y tomar medidas para evitar que el ataque cibernético progrese.

Las realizaciones de la presente descripción se refieren a un sistema de advertencia que puede recopilar automáticamente indicadores, analizar esos indicadores automáticamente para generar alertas, etiquetar, puntuar y agrupar esas alertas automáticamente, y proporcionar resultados del análisis, etiquetado y agrupación automatizados de forma optimizada a un analista. El análisis automatizado de los indicadores puede incluir una aplicación automatizada de varios criterios o reglas a fin de generar una visualización de los grupos de indicadores relacionados para que el analista pueda evaluar las alertas de manera rápida y eficiente. En particular, los indicadores pueden reagruparse y/o filtrarse dinámicamente en una interfaz de usuario interactiva de modo que guíen a un analista para navegar rápidamente entre la información asociada con varias alertas y evaluar eficientemente los grupos de alertas en el contexto de, por ejemplo, una auditoría por violación de datos u otra actividad relacionada con un ataque cibernético contra un recurso. Las realizaciones de la presente descripción también se relacionan con la puntuación automatizada de las alertas. La interfaz de usuario interactiva puede actualizarse en función de la puntuación, dirigiendo al analista humano a ciertas alertas (por ejemplo, alertas que probablemente estén asociadas con actividades relacionadas con un ataque cibernético contra un recurso) en respuesta a las entradas del analista. Las realizaciones de la presente descripción también se relacionan con la actualización automatizada del método de puntuación en base a hallazgos anteriores. Por ejemplo, si un analista

determina que una alerta generada sobre la base de ciertos indicadores fue un falso positivo, la influencia de estos indicadores en el proceso de puntuación de alertas puede reducirse para la puntuación de alertas futuras. Por el contrario, si un analista determina que se emitió una alerta que, de hecho, debería haberse emitido, la influencia de los indicadores presentes en la alerta en el proceso de puntuación de la alerta puede aumentar para la puntuación de alertas futuras. Las puntuaciones del riesgo pueden actualizarse continuamente para reflejar nueva información, tal como la proporcionada por el auditor en respuesta a alertas o eventos o cuando se reciben nuevos indicadores o se generan nuevas alertas y eventos.

En una realización de ejemplo, la interpretación de los indicadores puede tener lugar en varios pasos. Primero, el sistema de advertencia puede interpretar que uno o más indicadores pertenecen a un único evento. Por ejemplo, si se realiza una conexión desde un cliente de correo electrónico a un servidor de correo electrónico para que el cliente envíe un mensaje de correo electrónico, los indicadores correspondientes que reflejan la conexión exitosa pueden aparecer tanto en el cliente como en los registros del servidor, ambos indicando que la conexión se realizó. Al procesar estos indicadores, el sistema de advertencia puede determinar que se ha producido un evento, es decir, un correo electrónico enviado, y puede asignar varios atributos y propiedades al evento, tales como, por ejemplo, la hora y la fecha de la ocurrencia del evento, y los usuarios, direcciones de IP, ordenadores, servidores u otros actores involucrados. Un evento puede o no ser indicativo de algún riesgo para un recurso. El evento puede entonces analizarse en cuanto al riesgo estimado que representa para el recurso. A menudo, el evento se considerará sustancialmente irrelevante y, por lo tanto, no afectará la exposición del recurso al riesgo; como tal, el sistema de advertencia no solicitará una respuesta de un analista relacionado con la alerta. Sin embargo, aún registrará el evento, ya que puede resultar que sean datos contextuales relevantes para investigaciones de ataques cibernéticos relacionados con el recurso. En algunos casos, se determinará que el evento es indicativo de riesgo para el recurso; en estos casos, el sistema de advertencia puede designar el evento como una alerta y solicitar la respuesta de un analista y, por lo tanto, permitir que se tomen medidas para evitar que el ataque cibernético progrese.

La efectividad de un analista en la detección de actividad relacionada con un ataque cibernético contra un recurso y la evaluación de las alertas puede mejorarse enormemente si se le presentan indicadores que están contextualmente relacionados con la actividad que se está auditando, o con la alerta que se está evaluando. En una aplicación de ejemplo, un analista puede tener la tarea de decidir si la presencia de un determinado indicador representa una actividad relacionada con un ataque cibernético contra un recurso. Sin embargo, un indicador individual a menudo incluye información insuficiente para que el analista tome tales decisiones. Más bien, el analista puede tomar mejores decisiones basadas en una colección de indicadores relacionados. Por ejemplo, un usuario que solicita un número inusualmente alto de solicitudes para operar hardware, tal como una centrífuga, o un ataque de phishing contra un usuario puede, por sí mismo, no ser lo suficientemente probatorio para que un analista suponga que un ataque cibernético está en curso. Por el contrario, si el analista puede ver que el mismo usuario que ha estado recibiendo correos electrónicos de phishing ha introducido un número inusualmente alto de solicitudes para operar el hardware, el analista puede ver un patrón de actividad que se correlaciona más fuertemente con un ataque cibernético.

La efectividad de un analista para detectar ataques cibernéticos y evaluar alertas puede mejorarse aún más si al analista se le presentan agregados, tales como totales, recuentos y promedios, calculados a partir de varios indicadores. Por ejemplo, un analista que revisa si el acto de un determinado usuario de enviar documentos confidenciales por correo electrónico a la cuenta de correo electrónico privada del usuario representa una actividad relacionada con un ataque cibernético contra un recurso puede tomar mejores decisiones cuando se le presenta información relacionada con actividades anteriores del usuario, el departamento del usuario o la organización del usuario.

Además, es ventajoso que los recursos de auditoría se puedan concentrar en las actividades con mayor probabilidad de constituir actividades relacionadas con un ataque cibernético contra un recurso. Algunas realizaciones de la presente descripción realizan una puntuación basada en una estimación de la probabilidad de que cierta alerta esté relacionada con la actividad relacionada con un ataque cibernético contra un recurso para decidir si presentar una alerta a un analista y cómo presentar la alerta. La puntuación se basa en una asignación entre cada indicador y una estimación de la probabilidad de que el indicador sea indicativo de actividad relacionada con un ataque cibernético contra un recurso. Tal asignación se denomina "peso" del indicador correspondiente.

Los tipos de actividad que están o no asociados con un ataque cibernético, y la relevancia de diferentes indicadores, pueden cambiar con el tiempo y pueden no conocerse con precisión. Por ejemplo, los atacantes pueden desarrollar nuevas técnicas de ataque, y la configuración de los recursos puede cambiar para cambiar su perfil de vulnerabilidad. Como tal, en algunas realizaciones, el sistema de advertencia actualiza el peso de los indicadores para reflejar la determinación de un analista sobre si la emisión de una alerta dada estaba o no justificada. Por ejemplo, en algunas realizaciones, si un analista determina que se emitió una alerta dada a pesar de la ausencia de actividad relacionada con un ataque cibernético contra un recurso, los pesos asociados con los indicadores en función de los cuales se emitió la alerta se reducirán. Esto permite que el sistema de advertencia aprenda de alertas anteriores, mejorando su precisión de predicción con el tiempo. Para garantizar que el sistema de advertencia no filtre indebidamente los patrones emergentes indicativos de un ataque cibernético para el cual los pesos existentes no son óptimos, y así ayuda a evitar que el sistema de advertencia se vuelva propenso a errores debido al sesgo de

autorrefuerzo, se puede agregar un valor de compensación aleatorio u otro ajuste aleatorio (incluido el pseudo-aleatorio) o un ajuste no determinista realizado durante el proceso de filtrado para introducir un elemento de azar en la decisión del sistema de advertencia de si se muestra una alerta o no. De manera similar, en otra implementación, las alertas con varias puntuaciones se pueden mostrar aleatoriamente (incluso pseudo-aleatoriamente) al usuario con los mismos fines.

Algunos sistemas actualmente disponibles permiten al analista buscar y revisar indicadores individuales. Aunque estos sistemas actualmente disponibles pueden ser útiles para descubrir indicadores para tipos conocidos de actividad relacionados con un ataque cibernético, generalmente requieren que el analista repita manualmente la misma serie de búsquedas para determinar indicadores relacionados, para calcular manualmente los agregados donde el analista desea usarlos, y revisar manualmente grandes cantidades de datos irrelevantes para encontrar indicadores relevantes contenidos en los mismos. Realizar y repetir continuamente estos procesos manuales es inconsistente con el monitoreo en tiempo real y la detección y reducción de ataques cibernéticos.

En contraste con estos sistemas actualmente disponibles, y como se describió anteriormente, de acuerdo con diversas realizaciones, el sistema de advertencia de la presente descripción recopila automáticamente indicadores de una variedad de fuentes, analiza los indicadores para generar alertas, etiqueta y agrupa las alertas, y genera una interfaz de usuario interactiva en la que, en respuesta a las aportaciones del analista, se puede proporcionar de manera eficiente al analista la información relacionada con las alertas y los indicadores relevantes. En consecuencia, el analista puede estar habilitado para evaluar eficientemente las alertas para identificar que está ocurriendo un ataque cibernético y luego detener el ataque cibernético.

Además, la puntuación automatizada de las alertas (como se mencionó anteriormente) puede permitir una evaluación altamente eficiente de las alertas más relevantes por parte de un analista. Por ejemplo, la interfaz de usuario interactiva se genera para permitir que un analista vea rápidamente grupos críticos de alertas (según lo determine la puntuación automatizada), y luego en respuesta a las entradas del analista, vea e interactúe con la información generada (incluyendo, por ejemplo, ejemplo, gráficos basados en el tiempo y/u otra información) asociada con las alertas. En respuesta a las entradas del usuario, la interfaz de usuario puede actualizarse para mostrar datos sin procesar asociados con cada una de las alertas generadas y sus indicadores correspondientes si el analista desea profundizar en los datos asociados con una alerta dada.

En algunas realizaciones, el sistema de advertencia puede registrar actividades por parte de los analistas, para permitir una auditoría posterior del proceso de auditoría, o de analistas individuales. Por ejemplo, el sistema de advertencia puede almacenar cada elemento de información presentado a un analista, y cada acción tomada por un analista, por ejemplo, cada respuesta a la alerta, en una base de datos de auditoría para que sea posible determinar a qué analista se le presentó qué información, y cuál fue la respuesta del analista. Ventajosamente, esto puede permitir la determinación retroactiva de responsabilidades en cuanto a la decisión de un analista de tomar medidas por una alerta, y por lo tanto mejora la responsabilidad y la confianza.

En algunas realizaciones, el sistema de advertencia permite que un analista responda a una alerta de varias maneras. Por ejemplo, el sistema de advertencia puede permitir que el analista responda a una alerta "cerrando" la alerta, determinando así que la actividad relacionada con la alerta no pone en riesgo el recurso. Alternativamente, el analista puede iniciar una investigación de otro analista sobre la alerta y los eventos relacionados. El analista también puede iniciar la detención del ataque cibernético o intensificar la alerta. El analista también puede enviar comentarios a la alerta, que luego se pueden mostrar cuando la alerta se presente posteriormente. Ventajosamente, esto permite un intercambio de información y una colaboración más eficaces entre analistas y ayuda a evitar que los analistas dupliquen el trabajo de los demás.

Además, como se describe en el presente documento, se puede configurar y/o diseñar un sistema de advertencia para generar datos de interfaz de usuario utilizables para representar las diversas interfaces de usuario interactivas descritas. Los datos de la interfaz de usuario pueden ser utilizados por el sistema de advertencia y/u otro sistema informático, dispositivo y/o programa de software (por ejemplo, un programa de navegador), para representar las interfaces de usuario interactivas. Las interfaces de usuario interactivas pueden mostrarse, por ejemplo, en pantallas electrónicas (incluidas, por ejemplo, las pantallas táctiles).

Además, las interfaces de usuario interactivas y dinámicas descritas en el presente documento están habilitadas mediante innovaciones en interacciones eficientes entre las interfaces de usuario y los sistemas y componentes subyacentes. Por ejemplo, en el presente documento se describen métodos mejorados para la recepción de entradas del usuario, el traslado y la entrega de esas entradas a varios componentes del sistema (por ejemplo, la recuperación de indicadores), la ejecución automática y dinámica de procesos complejos en respuesta a la entrega de entradas (por ejemplo, agrupación, filtrado y puntuación de alertas), la interacción automática entre varios componentes y procesos del sistema de advertencia, y/o la actualización automática y dinámica de las interfaces de usuario.

Ventajosamente, según diversas realizaciones, las técnicas descritas proporcionan un punto de partida e interfaz de usuario más efectivos para una investigación de actividad potencial relacionada con un ataque cibernético contra un recurso de diversos tipos. Un analista puede comenzar una investigación respondiendo a las alertas generadas por

el sistema de advertencia que se generan en base a una estimación empíricamente determinada de la probabilidad de actividad relacionada con un ataque cibernético contra un recurso. Esto puede centrar la atención del analista en revisar la actividad que históricamente ha demostrado ser problemática. Como tal, puede reducir la cantidad de tiempo y esfuerzo necesarios para realizar la investigación. Las técnicas descritas también pueden, según diversas realizaciones, proporcionar una priorización de múltiples alertas relacionadas con la actividad relacionada con un posible ataque cibernético, la reagrupación dinámica de tales alertas y el filtrado de alertas. Por ejemplo, el analista también puede comenzar la investigación desde un grupo de alertas de alta prioridad, lo que puede permitirle enfocarse en las investigaciones más importantes y puede evaluar rápidamente ese grupo de alertas en función de la interfaz de usuario eficiente generada por el sistema de advertencia. En cada caso, los requisitos de tiempo de dicha investigación pueden reducirse significativamente debido a la creación y uso de representaciones altamente eficientes, incluidas las representaciones visuales tales como gráficos y cantidades agregadas, tales como totales, conteos y promedios, de indicadores relacionados, y de ese modo permitir que el ataque cibernético se detenga antes de que progrese y cause daño.

Se describen a continuación realizaciones adicionales de la descripción con referencia a las reivindicaciones adjuntas, que pueden servir como un resumen adicional de la descripción.

En diversas realizaciones, se describen sistemas y/o sistemas informáticos que comprenden un medio de almacenamiento legible por ordenador que tiene instrucciones de programa incorporadas con el mismo, y uno o más procesadores configurados para ejecutar las instrucciones del programa para hacer que uno o más procesadores realicen operaciones que comprenden uno o más aspectos de las realizaciones descritas anteriormente y/o a continuación (incluyendo uno o más aspectos de las reivindicaciones adjuntas).

En diversas realizaciones, se describen métodos implementados por ordenador en los que, mediante uno o más procesadores que ejecutan instrucciones de programa, uno o más aspectos de las realizaciones descritas anteriormente y/o a continuación (incluyendo uno o más aspectos de las reivindicaciones adjuntas) se implementan y/o realizan.

En diversas realizaciones, se describen productos de programas de ordenador que comprenden un medio de almacenamiento legible por ordenador, en donde el medio de almacenamiento legible por ordenador tiene instrucciones de programa incorporadas con el mismo, haciendo las instrucciones de programa ejecutables por uno o más procesadores que uno o más procesadores realicen operaciones que comprenden uno o más aspectos de las realizaciones descritas anteriormente y/o a continuación (incluyendo uno o más aspectos de las reivindicaciones adjuntas).

Breve descripción de los dibujos

Los siguientes dibujos y las descripciones asociadas se proporcionan para ilustrar realizaciones de la presente descripción y no limitan el alcance de las reivindicaciones. Los aspectos y muchas de las ventajas consiguientes de esta descripción se apreciarán más fácilmente a medida que se entiendan mejor mediante la referencia a la siguiente descripción detallada, cuando se toma junto con los dibujos adjuntos, en los que:

La figura 1A es un diagrama de bloques que ilustra un ejemplo de sistema de advertencia de ataque cibernético en un entorno operativo de ejemplo, según algunas realizaciones de la presente descripción.

La figura 1B es un diagrama de flujo que ilustra una representación esquemática que ilustra varios pasos de un ejemplo de ataque cibernético.

La figura 1C es un diagrama de flujo que ilustra una visión general esquemática de varios posibles ataques cibernéticos de ejemplo contra un recurso, y posibles estrategias para su detección.

La figura 2 es un diagrama de flujo que muestra un método de ejemplo de creación de alertas, según algunas realizaciones de la presente descripción.

La figura 3 es un diagrama de flujo que ilustra un método de ejemplo de presentación de alertas y recopilación de respuestas, según algunas realizaciones de la presente descripción.

La figura 4 ilustra una tabla de pesos de ejemplo, según algunas realizaciones de la presente descripción.

La figura 5 ilustra un ejemplo de interfaz de usuario del sistema de advertencia de ataque cibernético que muestra una descripción general de la posición de seguridad de todos los recursos.

La figura 6 ilustra un ejemplo de interfaz de usuario del sistema de advertencia que muestra una página de información que comprende alertas y eventos relacionados con un recurso específico.

La figura 7 ilustra un ejemplo de interfaz de usuario del sistema de advertencia que muestra una página de información que comprende usuarios y recursos relacionados con un recurso específico.

La figura 8 ilustra un ejemplo de interfaz de usuario del sistema de advertencia que presenta una solicitud para que un analista tome medidas sobre eventos y alertas seleccionados.

La figura 9 ilustra un ejemplo de interfaz de usuario del sistema de advertencia que presenta una página de confirmación de un analista que ha cerrado una alerta.

La figura 10 ilustra un sistema informático de ejemplo con el que se pueden implementar ciertos métodos discutidos en el presente documento.

Descripción detallada

Aunque ciertas realizaciones y ejemplos preferidos se describen a continuación, el tema objeto de la invención se extiende más allá de las realizaciones específicamente descritas a otras realizaciones y/o usos alternativos y a modificaciones y equivalentes de las mismas. Por lo tanto, el alcance de las reivindicaciones adjuntas al presente documento no está limitado por ninguna de las realizaciones particulares descritas a continuación.. Por ejemplo, en cualquier método o proceso descrito en el presente documento, los actos u operaciones del método o proceso pueden realizarse en cualquier secuencia adecuada y no están necesariamente limitados a ninguna secuencia descrita en particular. Varias operaciones pueden describirse como operaciones discretas múltiples a su vez, de una manera que puede ser útil para comprender ciertas realizaciones; sin embargo, el orden de la descripción no debe interpretarse como que implica que estas operaciones dependan del orden. Además, las estructuras, sistemas y/o dispositivos descritos en este documento pueden realizarse como componentes integrados o como componentes separados. Con el fin de comparar diversas realizaciones, se describen ciertos aspectos y ventajas de estas realizaciones. No necesariamente todos estos aspectos o ventajas se logran mediante una realización particular. Así, por ejemplo, se pueden llevar a cabo diversas realizaciones de una manera que logre u optimice una ventaja o un grupo de ventajas como se enseña en el presente documento sin lograr necesariamente otros aspectos o ventajas como también se puede enseñar o sugerir en el presente documento.

Términos

Para facilitar la comprensión de los sistemas y métodos analizados en el presente documento, a continuación se definen varios términos. Los términos definidos a continuación, así como otros términos utilizados en el presente documento, deben interpretarse como que incluyen las definiciones proporcionadas, el significado ordinario y habitual de los términos, y/o cualquier otro significado implícito de los términos respectivos. Por lo tanto, las siguientes definiciones no limitan el significado de estos términos, sino que únicamente proporcionan definiciones ejemplares.

Ataque cibernético: el intento de obtener acceso a los recursos informáticos por medios no autorizados o de una manera no autorizada. Un ataque cibernético puede involucrar técnicas tales como la explotación de vulnerabilidades de software o de hardware, de ingeniería social tales como "phishing", de uso de información de autentificación robada, etc.

Recurso: un recurso o sistema basado en ordenador de importancia particular. Por ejemplo, un recurso puede ser un sistema de control industrial, una base de datos confidencial y/o cualquier otro sistema o recurso informático o similar. Los recursos pueden comprender múltiples servidores, bases de datos u ordenadores.

Información contextual: cualquier información sobre un recurso y su entorno, tal como la política de acceso del recurso, el valor del recurso, la localización física del recurso o la localización del recurso en la topología de la red.

Indicador: cualquier información que indique que un ataque cibernético contra un recurso es más o menos probable. Dichos indicadores pueden incluir, por ejemplo, inicios y cierres de sesión en el ordenador, datos enviados y recibidos en una red, datos transferidos hacia o desde una base de datos, datos cambiados o modificados por un usuario, autentificaciones de usuario fallidas o exitosas, intentos fallidos o exitosos de explotar una vulnerabilidad de la seguridad en un recurso informático, intentos fallidos o exitosos de "phishing", intentos fallidos o exitosos de instalar software malicioso, o "malware", en ordenadores, etc. Estos indicadores pueden ser recogidos por aparatos de hardware o dispositivos informáticos localizados dentro de una red o de un sistema informático, por aplicaciones de software localizadas dentro de una red o de un sistema informático, y/o por cualquier otro método adecuado. Por ejemplo, se pueden obtener indicadores en registros de proxy, registros de prevención de pérdida de datos (DLP), registros de cortafuegos, registros de VPN, registros del sistema operativo tales como syslog o Windows Event Log, etc.

Phishing: robo de información de autentificación de un usuario al defraudar al usuario para que proporcione la información voluntariamente. Por ejemplo, un ataque de phishing común puede comprender enviar a un usuario un correo electrónico que pretende falsamente estar enviado por el departamento de TI de una organización a un usuario y solicita la contraseña de un usuario.

Evento: Una ocurrencia que está potencialmente relacionada con un ataque cibernético sobre un recurso. Por ejemplo, un correo electrónico de phishing enviado a un usuario de un recurso, o un intento de inicio de sesión fallido o exitoso por parte de un usuario en un servidor relacionado con un recurso, o las solicitudes para operar hardware

pueden determinarse como eventos. Los eventos pueden estar asociados con una fecha, hora, usuarios asociados, ordenadores asociadas u otra información que proporcione contexto al evento. En particular, algunos eventos pueden generarse en la razón corriente de los negocios; como tal, un evento no está necesariamente relacionado con un ataque cibernético a un recurso.

Filtración de datos al exterior: retirada no autorizada de información (por ejemplo, información confidencial) del control de la organización. La filtración de datos se puede lograr, por ejemplo, copiando información confidencial en un disco extraíble, cargando información confidencial en un servidor web, enviando información confidencial a un destinatario fuera de la organización, etc.

Alerta: una determinación de un sistema de advertencia de que se detectó un posible ataque cibernético contra un recurso.

Información de actividad del usuario: cualquier información relacionada con la actividad de un usuario en un sistema informático o en una red. Dicha información de actividad del usuario puede incluir, por ejemplo, inicios y cierres de sesión del ordenador, datos introducidos, datos transferidos, datos cambiados o modificados, datos creados, datos emitidos, datos impresos, direcciones IP con las que se ha comunicado, sitios web con los que se ha comunicado, aplicaciones de software ejecutadas, etc. Dicha información de actividad del usuario puede recopilarse mediante aparatos de hardware o dispositivos informáticos localizados dentro de una red o sistema informático, aplicaciones de software localizadas dentro de una red o de un sistema informático, y/o cualquier otro método adecuado. Por ejemplo, la información de actividad del usuario puede almacenarse en registros proxy, registros de prevención de pérdida de datos (DLP), registros de correo electrónico, etc.

Almacenamiento de datos: cualquier medio y/o dispositivo de almacenamiento legible por ordenador (o colección de medios y/o dispositivos de almacenamiento de datos). Los ejemplos de almacenamiento de datos incluyen, entre otros, discos ópticos (p. ej., CD-ROM, DVDROM, etc.), discos magnéticos (p. ej., discos duros, disquetes, etc.), circuitos de memoria (p. ej., unidades de estado sólido, memoria de acceso aleatorio (RAM), etc.), y/o similares. Otro ejemplo de un almacén de datos es un entorno de almacenamiento alojado que incluye una colección de dispositivos físicos de almacenamiento de datos a los que se puede acceder de forma remota y que se pueden aprovisionar rápidamente según sea necesario (comúnmente conocido como almacenamiento "en la nube").

Base de datos: cualquier estructura de datos (y/o combinaciones de múltiples estructuras de datos) para almacenar y/u organizar datos, incluidas, entre otras, bases de datos relacionales (por ejemplo, bases de datos Oracle, bases de datos MySQL, etc.), bases de datos no relacionales (por ejemplo, bases de datos NoSQL, etc.), bases de datos en memoria, hojas de cálculo, como archivos de valores separados por comas (CSV), archivos de lenguaje de marcado extensible (XML), archivos TeXT (TXT), archivos planos, archivos de hojas de cálculo y/o cualquier otro formato ampliamente utilizado o patentado para el almacenamiento de datos. Las bases de datos generalmente se almacenan en uno o más almacenes de datos. En consecuencia, cada base de datos a la que se hace referencia en el presente documento (por ejemplo, en la descripción del presente documento y/o en las figuras de la presente solicitud) debe entenderse como almacenada en uno o más almacenes de datos.

Ejemplo de sistema de advertencia y entorno de red

La figura 1A es un diagrama de bloques que ilustra un ejemplo de sistema de advertencia de ataque cibernético en un entorno operativo (por ejemplo, una red), según algunas realizaciones de la presente descripción. Como se muestra en la realización de la figura 1A, el sistema de advertencia comprende un dispositivo 150 de monitoreo conectado a través de una red empresarial con un dispositivo 155 de auditor, un cortafuegos 160 de aplicación, un servidor 170 de intranet, un servidor 192 de prevención de pérdida de datos, una impresora 180 de red, un servidor 173 de correo electrónico, un servidor 152 proxy y uno o más recursos tales como el recurso 102 y el recurso 104. El dispositivo 150 de monitoreo puede usar la red empresarial para adquirir varios indicadores. Dichos indicadores incluyen registros de DLP del servidor 192 de prevención de pérdida de datos, registros 162 de cortafuegos de aplicaciones del cortafuegos 160 de aplicaciones que protege un servidor 164 web, registros 171 de intranet del servidor 170 de intranet, registros 172 de correo electrónico del servidor 173 de correo electrónico, registros 182 proxy del servidor 152 proxy, registros 198 del sistema de detección de intrusiones de un servidor 196 del sistema de detección de intrusiones, etc. Los recursos 102 y 104 pueden incluir, por ejemplo, una base de datos que almacena información confidencial tal como una base de datos de pacientes o un sistema de control para un proceso industrial tal como como un robot, una puerta, un reactor químico o una centrífuga. El dispositivo de monitoreo también puede acceder a los registros 103 de recursos desde los recursos 102 y 104. Dichos registros 103 de recursos pueden ser específicos para la aplicación del recurso y pueden comprender, por ejemplo, solicitudes para operar hardware, información sobre qué usuario accedió al recurso, desde qué localización geográfica o desde qué ordenador el usuario accedió al recurso, etc. Las actividades de los dispositivos del usuario pueden registrarse y grabarse en varios lugares de la red empresarial. Por ejemplo, el acceso de los dispositivos 178, 179 de usuario a servidores 110, 130 remotos puede ser registrado por el servidor 152 proxy en los registros 182 de proxy. Los dispositivos 178, 179 de usuario pueden estar ejecutando el software de prevención de pérdida de datos (DLP) que almacena y envía al servidor DLP información sobre ciertos actos que potencialmente violan la política de DLP (prevención de pérdida de datos) de una empresa, tales como la copia de datos en un medio de almacenamiento extraíble. El servidor DLP puede incluir esta información en los registros 194 de DLP. La red 122

empresarial puede permitir que todos estos dispositivos, y dispositivos adicionales no indicados, intercambien información entre sí y con dispositivos externos (p. ej. alojamientos de internet).

El servidor de correo electrónico es responsable de enrutar los mensajes de correo electrónico que se originan en la red 122 empresarial a sus destinatarios. Durante el funcionamiento, el servidor de correo electrónico crea registros 172 de correo electrónico y pone los registros 172 de correo electrónico a disposición del dispositivo 150 de monitoreo. Por ejemplo, los registros 172 de correo electrónico pueden comprender indicadores relacionados con los mensajes que envió un usuario, quiénes fueron los destinatarios de estos mensajes, y qué tipo de datos adjuntos estaban contenidos en el mensaje.

Una impresora 180 de red también puede estar conectada a la red 122 empresarial. La impresora 180 de red puede crear registros 181 de impresión en el curso de su operación, y hacer que los registros 181 de impresión estén disponibles para el dispositivo 150 de monitoreo a través de la red 122 empresarial. Los registros 181 de impresión pueden comprender indicadores relacionados con qué trabajos de impresión se iniciaron, qué usuario inició cada trabajo de impresión y desde qué ordenador se envió, cuántas páginas tenía cada trabajo de impresión y cuál era el tipo, nombre de archivo y tipo de archivo del documento impreso.

Un servidor 192 de prevención de pérdida de datos (DLP) también puede estar conectado a la red 122 empresarial. El servidor DLP puede proporcionar registros 194 DLP, que pueden comprender indicadores relacionados con las transferencias de archivos de un usuario desde la red 122 empresarial a medios extraíbles (tales como una unidad flash USB), la transferencia de archivos y/o comunicaciones del usuario dentro y/o fuera de la red 122 empresarial, y/u otras actividades del usuario. El servidor DLP puede ser, por ejemplo, cualquier solución DLP de código abierto o disponible comercialmente, que incluye, por ejemplo, RSA DLP o McAfee Total Protection DLP.

Un servidor 196 del sistema de detección de intrusiones (IDS) también puede estar conectado a la red 122 de la empresa. El sistema de detección de intrusiones puede ser, por ejemplo, cualquier solución IDS de código abierto disponible comercialmente, incluyendo, por ejemplo, Snort o Suricata. El sistema de detección de intrusos puede poner a disposición los registros 198 del sistema de detección de intrusos, que pueden comprender indicadores relacionados con intentos potenciales de explotar vulnerabilidades de software o de hardware, tráfico de red que se origina en malware y actividad similar para la cual el IDS está monitoreando la red.

El dispositivo 150 de monitoreo también puede acceder a registros y a otra información de actividad de fuentes además de las ilustradas aquí. Por ejemplo, el dispositivo 150 de monitoreo puede acceder a los registros del sistema operativo de varios sistemas informáticos, tales como los proporcionados por syslog o Windows Event Log. El dispositivo 150 de monitoreo también puede acceder a registros de servicio que pueden ser generados por una variedad de servicios, tales como un servidor web, servidor de base de datos, un servidor de voz sobre IP, durante la operación. El dispositivo 150 de monitoreo también puede acceder a los registros de varios otros dispositivos, tales como conmutadores manejables, fuentes de alimentación ininterrumpida (UPS), cortafuegos de hardware, puntos de acceso inalámbrico, etc.

En diversas realizaciones, el sistema de advertencia puede configurarse de varias maneras que difieren de la configuración de ejemplo de la figura 1. Por ejemplo, uno o más aspectos descritos en referencia a la figura 1 pueden no estar presentes, y/o aspectos adicionales pueden estar presentes en cualquier implementación dada del sistema de advertencia. Por lo tanto, aunque diferentes tipos de información de actividad del usuario e información contextual pueden estar disponibles en diferentes implementaciones, el sistema de advertencia descrito en el presente documento puede funcionar en todo caso de manera similar, y se contemplan todas esas implementaciones.

Por consiguiente, como se mencionó, en diversas realizaciones, el dispositivo de monitoreo está configurado para recopilar y analizar una variedad de indicadores, y generar alertas basadas en el resultado del análisis. Por ejemplo, el dispositivo de monitoreo puede recibir registros 172 de correo electrónico, registros 182 de proxy, registros 194 de DLP, registros 171 de intranet, registros de cortafuegos 161 de aplicaciones y/u otros indicadores.

La figura 1B muestra una representación 700 esquemática que ilustra varios pasos de un ejemplo de ataque cibernético contra un recurso de una organización. El bloque 702 muestra un primer paso del ejemplo de ataque cibernético, que indica la infiltración en la organización. Este paso comprende el agente malicioso que se infiltra en la red electrónica de la organización para obtener acceso a los sistemas internos. Este paso puede realizarse, por ejemplo, utilizando un ordenador portátil robado para acceder a la red corporativa como se examinó o robando la información de autentificación de un empleado mediante ingeniería social o ataques de phishing. El bloque 704 indica un segundo paso del ejemplo de ataque cibernético de intrusión en los recursos. En este paso, el atacante accede al recurso objetivo. Esto puede lograrse, por ejemplo, explotando una vulnerabilidad de software o de hardware presente en el recurso o utilizando credenciales de acceso administrativo robadas para acceder al recurso. El bloque 706 ilustra un tercer paso del ejemplo de ataque cibernético que indica el mal uso de la aplicación. En este paso, el atacante, habiendo obtenido acceso al recurso, ahora abusa del acceso no autorizado adquirido al recurso para lograr el objetivo de su ataque. Por ejemplo, el mal uso de la aplicación se puede lograr volcando una base de datos que contiene información confidencial en un archivo o copiando documentos que contienen información confidencial en un medio de almacenamiento extraíble. El bloque 708 indica un cuarto paso del ejemplo de ataque

cibernético que indica la infiltración. Aquí, el atacante busca retirar la información confidencial adquirida en el paso 3 filtrándola fuera de la red corporativa. Por ejemplo, el atacante puede lograr este paso utilizando un túnel de red encriptado para transferir la información robada de la red corporativa a un servidor controlado por el atacante. Se apreciará que los diferentes pasos, como se ilustra, implican que el atacante interactúa con diferentes recursos de la organización y, por lo tanto, hace que se creen diferentes tipos de indicadores. También se apreciará que un atacante puede ser capaz de combinar e intercambiar diferentes técnicas de ataque, lo que dificulta vincular un ataque potencial a una secuencia de pasos particular. Como tal, para comprender todo el alcance de un ataque cibernético como se ilustra en la figura 1B, puede ser ventajoso no restringir un análisis a ninguno de los pasos constitutivos, sino realizar un análisis exhaustivo, centrado en el recurso, de todos los pasos de un ataque.

La figura 1C muestra una ilustración esquemática de varios ejemplos de posibles ataques cibernéticos contra los recursos de una organización. En el ejemplo de la figura 1C, un agente 202 malicioso busca obtener acceso no autorizado al recurso 204 crítico. El agente malicioso puede, por ejemplo, ser un servicio de inteligencia extranjero, un grupo criminal organizado o un activista. El recurso 204 crítico puede ser una aplicación tal como un sistema de planificación crítica de negocios o un sitio web de comercio electrónico. También puede ser un servidor tal como, por ejemplo, un servidor de base de datos que almacena información confidencial o un servidor de comunicación que ejecuta una infraestructura crítica del negocio. El agente 202 malicioso, que busca obtener acceso al recurso 204, puede intentar llevar a cabo el ataque a través de una variedad diversa de medios técnicos, causando consecuentemente la creación de diferentes tipos de indicadores en varios sistemas de la organización.

Algunas estrategias de ataque pueden tratar de atacar el recurso mediante un paso intermedio, tal como atacar primero otro recurso, obtener acceso a una cuenta administrativa en ese otro recurso y luego ordenar a la cuenta administrativa atacar al recurso. Otras estrategias de ataque pueden renunciar a tal paso intermedio y buscar directamente atacar al recurso. Algunas de estas estrategias de ataque ejemplares se ilustran utilizando líneas discontinuas. Por ejemplo, según la estrategia 1, el agente 202 malicioso puede utilizar un ordenador 206 portátil robado para acceder a la red corporativa a través del servidor VPN. El acceso a la red corporativa mediante el ordenador 206 portátil robado puede, por ejemplo, ser visible en los archivos de registro creados en el servidor 208 VPN. Alternativa o adicionalmente, el atacante puede decidir utilizar la estrategia 2, que comprende intentos de explotar vulnerabilidades de software o de hardware en servidores web o aplicaciones de la organización, por ejemplo, en el servidor 210 web. Alternativa o adicionalmente, el agente 202 malicioso puede, como se ilustra en la estrategia 3, tratar de comprometer el punto 214 de acceso inalámbrico, por ejemplo, explotando las debilidades criptográficas en los esquemas de cifrado y autentificación utilizados en el punto 214 de acceso inalámbrico. Los intentos del agente 202 malicioso de hacerlo pueden estar indicados por registros creados en el punto 214 de acceso inalámbrico, por registros del servidor 212 DHCP, por archivos de registro creados en el servidor 210 web o por el cortafuegos 160 de aplicación, y/o similares.

Alternativa o adicionalmente, el agente malicioso puede tratar de comprometer uno o más puntos finales tales como los ordenadores portátiles, los ordenadores personales, los teléfonos móviles u otros dispositivos de los empleados, como se ilustra en la estrategia 4. Los intentos del agente 202 malicioso de hacerlo pueden estar indicados en los registros 213 del sistema de prevención de pérdida de datos. El agente 202 malicioso también puede tratar de atacar el recurso directamente utilizando una explotación que aprovecha una vulnerabilidad de software o de hardware en el recurso mismo, como se ilustra en la estrategia 5; tal ataque puede ser visible en los registros de un sistema de detección de intrusiones (IDS). Puede ser difícil o incluso imposible determinar que se ha producido una conexión como se ilustra en la estrategia 1 al revisar únicamente los indicadores contenidos en los registros de acceso inalámbrico; por el contrario, puede ser difícil o imposible determinar que se ha producido un ataque como se ilustra en la estrategia 3 al revisar únicamente los indicadores contenidos en los registros de acceso inalámbrico. Se apreciará que al analizar el riesgo para un recurso debido un ataque cibernético, puede ser necesario detectar y responder a diferentes estrategias y técnicas que pueden ser elegidas por los atacantes potenciales; como tal, puede ser ventajoso enfocar el análisis en el recurso que está siendo atacado, en lugar de enfocar el análisis en el indicador individual relacionado con el ataque. Por razones similares, también puede ser ventajoso integrar varios indicadores de una amplia gama de fuentes en un análisis exhaustivo.

Método de ejemplo de generación de alertas

La figura 2 es un diagrama de flujo de un método 200 de ejemplo de generación de alertas, según algunas realizaciones de la presente descripción. En diversas realizaciones, se pueden incluir menos bloques o bloques adicionales en el proceso de la figura 2, o se pueden realizar varios bloques en un orden diferente al mostrado en la figura. En diversas implementaciones, los bloques de la figura 2 pueden realizarse en serie y/o simultáneamente, y pueden realizarse múltiples veces simultáneamente. Además, uno o más bloques de la figura pueden ser realizados por varios componentes del sistema de advertencia, por ejemplo, por el dispositivo 150 de monitoreo (descrito anteriormente en referencia a la figura 1).

En el bloque 201, el sistema de advertencia comienza su análisis accediendo a información sobre un recurso que está potencialmente en riesgo de ataque cibernético. La información sobre diferentes recursos puede, en algunas realizaciones, proporcionarse al sistema de advertencia durante la implementación y puede comprender, por ejemplo, el nombre del recurso, los servidores, las bases de datos y otros recursos informáticos asociados con el recurso, y otra información sobre el recurso. En algunas realizaciones, el sistema de advertencia puede utilizar

técnicas de aprendizaje automático para determinar automáticamente qué recursos, actividad y otras variables observables están relacionadas con cada recurso. Por ejemplo, el sistema de advertencia puede observar patrones de tráfico, actividad del usuario, indicadores y alertas anteriores, y otra información, y aplicar técnicas de aprendizaje supervisado conocidas en la técnica, tales como máquinas de vectores de soporte, a esas observaciones. Esto puede permitir que el sistema de advertencia determine, basándose en una clasificación inicial de ciertos recursos y actividades como parte de un recurso, otros recursos y actividades que probablemente estén relacionados con ese recurso. Ventajosamente, esto permite que el sistema de advertencia se adapte automáticamente a los cambios en la topología y configuración de la red, y reduce el esfuerzo administrativo requerido. En el bloque 202, el sistema de advertencia accede a datos contextuales asociados con el recurso que está en riesgo por un posible ataque cibernético. Por ejemplo, los datos contextuales pueden incluir información sobre qué usuarios pueden acceder al recurso, información sobre patrones de solicitud de control de hardware ordinarios o información sobre patrones de uso típicos del recurso por parte de usuarios autorizados. La información también puede incluir la localización física del recurso, la localización del recurso dentro de la topología de la red de la organización, el valor del recurso, etc. En el bloque 204, el sistema de advertencia accede a indicadores de un posible ataque cibernético relacionado con el recurso. Ejemplos de tales indicadores incluyen registros 182 proxy, los registros 172 de correo electrónico, los registros 194 de prevención de pérdida de datos, los registros de cortafuegos 161 de aplicaciones, etc. El sistema de advertencia puede, por ejemplo, acceder a los indicadores consultando otros dispositivos a través de un protocolo de administración de red tal como SNMP, recopilar la información del acceso al sistema de archivos de un dispositivo remoto y analizar sus archivos de registro o procesando otros tipos de registros, tales como las capturas de paquetes desde un cortafuegos, los registros de un sistema de detección de intrusos, de un sistema antimalware, de una puerta de enlace o de un enrutador. En algunas realizaciones, el sistema de advertencia puede copiar algunos o todos los indicadores a los que se accede en el almacenamiento local para facilitar un análisis más rápido. En el bloque 206, el sistema de advertencia compara los indicadores a los que se accede en el bloque 204 con un conjunto de reglas que corresponden a diferentes tipos de actividad potencialmente relacionada con un ataque cibernético contra un recurso para determinar un conjunto de eventos que reflejen dicha actividad. Para cada evento, el sistema de advertencia puede determinar la información relacionada con el evento en base a las reglas; por ejemplo, el sistema de advertencia puede extraer la hora, la fecha, los usuarios, los servidores y las direcciones IP involucradas, etc. Las reglas pueden estar escritas específicamente para la organización o el recurso, o pueden ser reglas genéricas que representan una actividad que generalmente es indicativa de un ataque cibernético. En algunas realizaciones, un analista puede, incluso después de que el sistema se haya implementado y esté en funcionamiento, ser capaz de definir reglas arbitrarias para procesar la información recopilada de las fuentes de datos disponibles, tales como archivos de registro. Por ejemplo, un analista puede definir reglas que capturen cierta actividad específica del negocio. En algunas realizaciones, las reglas pueden aprenderse automáticamente de la actividad relacionada con un recurso que previamente se determinó que estaba relacionado, o no relacionado, con un ataque cibernético. Por ejemplo, el sistema de advertencia puede extraer varias características, tales como direcciones IP, puertos, firmas, encabezados de paquetes y otras características, de alertas anteriores que un analista determinó que estaban relacionadas con un ataque cibernético sobre un recurso, o que un analista determinó que no estaban relacionadas con tal ataque. Basado en métodos de aprendizaje automático conocidos en la técnica, tales como el aprendizaje supervisado utilizando máquinas de vectores de soporte, el sistema de advertencia puede, a partir de estas características, inferir un conjunto de reglas que se pueden aplicar para determinar un conjunto de indicadores relevantes para detectar ataques futuros.

Por ejemplo, los indicadores de un servidor de correo electrónico pueden compararse con un conjunto de reglas para determinar indicadores relacionados con correos electrónicos que se enviaron a un destinatario dentro de la organización y que parecen ser ataques de ingeniería social contra un empleado de la organización. Como otro ejemplo, los registros 182 de proxy pueden compararse con una lista de dominios maliciosos conocidos para determinar las conexiones realizadas por software malicioso desde dentro de la organización para detectar intentos de filtración al exterior de datos a dichos dominios maliciosos conocidos. En otro ejemplo, los registros 161 de cortafuegos y los registros 171 de intranet pueden coincidir con las reglas que coinciden con las técnicas comunes de sondeo o de explotación. En otro ejemplo más, los registros 194 de prevención de pérdida de datos pueden compararse con reglas para determinar indicadores relacionados con intentos de filtración de datos al exterior.

En el bloque 208, se determinan los datos contextuales asociados con los eventos potencialmente relacionados con un ataque cibernético sobre el recurso. Por ejemplo, en algunas realizaciones, el historial 154 de eventos de recursos puede consultarse para determinar si eventos similares relacionados con un posible ataque cibernético al recurso han ocurrido en el pasado y, de ser así, si un analista determinó que eran falsos positivos o causas genuinas de preocupación. Como otro ejemplo, algunos de los datos contextuales asociados con un posible ataque cibernético en el recurso pueden incluir información sobre eventos relacionados con posibles ataques cibernéticos a otros recursos.

En el bloque 209, los pesos pueden determinarse opcionalmente en base a los datos contextuales asociados con un posible ataque cibernético al recurso según se han determinado en el bloque 208, a los datos asociados con el recurso determinados en el bloque 201 y a otros datos. En una realización de ejemplo, se puede usar una tabla 1000 de pesos para determinar los pesos apropiados.

En el bloque 210, la información sobre el recurso, los datos contextuales asociados con el recurso y los indicadores de un posible ataque cibernético relacionado con el recurso según lo determinado en el bloque 204 se combinan

para determinar, para cada evento, una estimación de riesgo que indica en cuánto riesgo está el evento poniendo al recurso. En el bloque 212, la estimación de riesgo determinada en el bloque 210 se compara con un umbral o, en una realización alternativa, se compara con un umbral más un valor aleatorio. Si la estimación del riesgo excede el umbral, o el umbral más el valor aleatorio, el control pasa al bloque 214 en el que se genera una alerta para indicar a un analista la información sobre un posible ataque cibernético contra el recurso. Por ejemplo, la alerta puede comprender información sobre la hora y la fecha en que ocurrió la actividad sospechosa, qué recurso se está poniendo en riesgo, qué usuarios, qué servidores y qué tipo de servicios están involucrados en la actividad sospechosa, y cuál es el riesgo estimado. En el bloque 216, la una o más alertas generadas en el bloque 214 se envían a una cola 158 de alertas desde donde se pueden presentar a un analista. La cola 158 de alertas puede, aunque no necesariamente, implementarse como una cola secuencial, tal como una estructura de datos primero en entrar, primero en salir. La cola 158 de alertas también se puede implementar como una lista dentro de una aplicación desde la cual se pueden recuperar las alertas en cualquier orden (por ejemplo, en orden aleatorio). A continuación se ilustran ejemplos de cómo, en una realización de ejemplo, se pueden mostrar las alertas con referencia a las figuras 6 a 9.

En el bloque 222, el historial 154 de eventos de recursos se actualiza para reflejar la nueva alerta o el nuevo evento, cualquiera que sea el caso. Por ejemplo, el bloque 222 puede comprender el sistema de advertencia que accede a una base de datos que almacena todos los eventos y alertas para un recurso dado e insertar un registro que indica el nuevo evento o alerta, la fecha y hora de ocurrencia, la estimación de riesgo y otros datos contextuales a lo que se puede haber accedido durante uno de los pasos anteriores según se ilustra en la figura 2. En el bloque 224, las estimaciones de riesgo combinadas de las alertas y los eventos en el historial de eventos de recursos que aún no han sido respondidas por un auditor se están combinando para determinar una nueva puntuación del riesgo para el recurso. Notablemente, incluso los eventos que no alcanzaron el umbral de riesgo en el bloque 212 y para los cuales, por consiguiente, no se ha emitido ninguna alerta, aún pueden tomarse en consideración en el bloque 224 cuando se calcula la puntuación del riesgo para los recursos. Esto refleja la observación de que un posible ataque cibernético puede ocurrir sin ningún evento o indicador en particular que sugiera un riesgo extraordinariamente alto, sino una serie de indicadores o eventos vistos en conjunto sugieren que un posible ataque cibernético está en curso. En una realización de ejemplo, la puntuación del riesgo para los recursos es un valor numérico que puede ir de 0 a 100. En una realización de ejemplo, se utiliza una función matemática monotónicamente convergente para combinar las estimaciones de riesgo individuales de modo que la puntuación del riesgo aumente con cada alerta adicional y cada evento, pero aun así nunca excede un valor dado, tal como 100, o cae por debajo de cero. En el bloque 226, la puntuación del riesgo global se actualiza en función de las puntuaciones del riesgo para los recursos según se han determinado en 224. La puntuación del riesgo global puede determinarse combinando las puntuaciones del riesgo para los recursos utilizando una función matemática similar a la utilizada para determinar la puntuación del riesgo para los recursos en el paso 224. En una realización de ejemplo, la puntuación del riesgo global vuelve a ser un valor entre cero y 100. En una realización de ejemplo, la puntuación del riesgo global puede mostrarse de forma destacada en la primera página presentada cuando un analista accede a la interfaz de usuario del sistema de advertencia, confiriendo así inmediatamente una visión general de la posición de seguridad de la organización. Simultáneamente, se pueden presentar puntuaciones del riesgo para los recursos de recursos seleccionados, tales como los recursos que contribuyen más a la puntuación del riesgo global. Al seleccionar un recurso individual, el analista puede ser dirigido a una página que muestre de manera destacada la puntuación del riesgo para el recurso, junto con información sobre las alertas y los eventos individuales que contribuyen a la puntuación del riesgo para el recurso.

Método de ejemplo de presentación de alertas y respuestas

La figura 3 es un diagrama de flujo de un método 300 de ejemplo de presentación de alertas y respuestas, según algunas realizaciones de la presente descripción. En diversas realizaciones, se pueden incluir menos bloques o bloques adicionales en el proceso de la figura 4, o se pueden realizar varios bloques en un orden diferente del que se muestra en la figura. En diversas implementaciones, los bloques de la figura 3 pueden realizarse en serie y/o simultáneamente, y pueden realizarse múltiples veces simultáneamente. Además, uno o más bloques de la figura pueden ser realizados por varios componentes del sistema de advertencia, por ejemplo, por el dispositivo 150 de monitoreo (descrito anteriormente en referencia a la figura 1).

En el bloque 302, se recuperan una o más alertas de la cola 158 de alertas. En el bloque 304, las -una o más- alertas recuperadas de la cola 158 de alertas se agrupan, filtran y clasifican. Las alertas se pueden agrupar y filtrar dinámicamente, por ejemplo, según diferentes tipos de alertas. En algunas realizaciones, las alertas pueden clasificarse por la puntuación del riesgo, por ejemplo, para mostrar las alertas que comienzan con la puntuación del riesgo más alta.

En el bloque 306, las alertas, agrupadas y filtradas, se muestran al analista en una o más interfaces de usuario interactivas (por ejemplo, como se describe a continuación en referencia a las figuras 5-9), y se recibe una respuesta del analista. La información o las representaciones interactivas asociadas con las alertas, o los indicadores asociados, pueden presentarse dentro de una interfaz de usuario que se presenta al analista, como se describe a continuación. Por ejemplo, las representaciones pueden proporcionar indicaciones visuales (por ejemplo, gráficos u otras visualizaciones) de los indicadores relacionados con las alertas y/o los grupos de alertas. Un servidor web u otro tipo de motor de interfaz de usuario puede configurarse y/o diseñarse para generar datos de interfaz de usuario

utilizables para representar las interfaces de usuario interactivas descritas en el presente documento, tales como una aplicación y/o una página web dinámica mostrada dentro del dispositivo 153 del analista. En diversas realizaciones, los datos de la interfaz de usuario pueden transmitirse al dispositivo 153 del analista, y/o a cualquier otro dispositivo informático, de modo que las interfaces de usuario de ejemplo se muestran al analista (y/o a otros usuarios del sistema de advertencia). Según algunas realizaciones, los analistas también pueden asignarse tareas a sí mismos o entre sí a través de una interfaz de usuario. Los auditores pueden optar por responder a las alertas de varias maneras, por ejemplo, descartando la alerta (por ejemplo, indicando que se emitió por error), elevando la alerta a un supervisor o confirmando la alerta sin elevarla a un supervisor.

El sistema de advertencia pasa a uno de los bloques 308, 310 o 312 dependiendo de la respuesta del analista. Si el analista decide descartar la alerta, el sistema de advertencia ajustará la tabla 1000 de pesos para reflejar el hecho de que había emitido una alerta que no debería haberse emitido. El sistema de advertencia reducirá así los pesos de los indicadores que han contribuido a la emisión de la alerta y, por el contrario, aumentará los de los indicadores que no hayan contribuido a la alerta. Si el analista elige confirmar la alerta, el sistema de advertencia se mueve al bloque 310, dejando el conjunto de pesos sin cambios, lo que refleja la determinación del analista de que se emitan alertas similares en el futuro. Si el analista elige elevar la alerta a un supervisor, el sistema de advertencia pasa al bloque 308, haciendo que la alerta se presente a un supervisor. La alerta se puede presentar a un supervisor de manera similar a como se le presentó al analista, o se puede presentar por correo electrónico, mensaje de texto u otra forma de comunicación. Una vez que se ha presentado la alerta, el sistema de advertencia se mueve al bloque 310, dejando el conjunto de pesos sin cambios. Después de que un analista haya respondido a una alerta, el sistema de advertencia, en el bloque 314, marca la alerta como histórica, lo que indica que ya no hay ningún riesgo asociado con la alerta. Cuando una alerta se marca como histórica, el sistema de advertencia también recalcula la puntuación del riesgo para los recursos y la puntuación del riesgo global para reflejar la eliminación de las alertas, y vuelve a dibujar los gráficos u otras visualizaciones que incluyen la alerta eliminada o una de las puntuaciones del riesgo actualizadas.

Tabla de pesos de ejemplo

La figura 4 ilustra una tabla 400 de pesos de ejemplo según algunas realizaciones de la presente descripción.. La tabla de pesos comprende una serie de pesos almacenados en un formato de fila-columna. Cada columna de las columnas 402 corresponde a un recurso. Los diferentes recursos pueden ser, como se ilustra, un robot, un sistema electromecánico de compuerta o un sistema de control de centrífuga nuclear. En las filas 410, cada fila corresponde a un indicador. Por ejemplo, puede haber una fila para un servidor que es parte del recurso que muestra fallos repetidos de autentificación, o una fila para un ordenador que pertenece al usuario administrativo del recurso que ha sido infectado con malware.

En cada intersección de una fila y una columna hay un elemento de la tabla que corresponde al peso del indicador en su fila, en relación con el recurso indicado en su columna. Por ejemplo, el elemento 420 de la tabla de ejemplo corresponde al peso de un indicador "infección de virus del ordenador del administrador de recursos" para el recurso del robot. Algunos indicadores, como los señalados por la selección 414 de la columna, pueden estar relacionados con el riesgo planteado a un recurso específico; otros indicadores, como los señalados por la selección 412 de la columna, pueden estar relacionados con un tipo de amenaza más general, que pone en riesgo varios recursos o todos los recursos.

En base a la tabla de pesos, a diferentes eventos se les pueden asignar diferentes estimaciones de riesgo en función del recurso al que corresponden. En algunas realizaciones, el sistema de advertencia puede actualizar la tabla 400 de pesos en función de la respuesta del analista a una alerta, de modo que se supriman las alertas futuras que se determinó que eran falsos positivos y se aumente el tipo de alertas emitidas que se determinó que eran correctas.

Ejemplo de interfaces de usuario auditor

Las figuras 5, 6, 7, 8 y 9, descritas a continuación, ilustran métodos e interfaces de usuario del sistema de advertencia, según diversas realizaciones, en las que los indicadores relacionados con posibles ataques cibernéticos se analizan automáticamente y, en base al análisis, se generan las alertas y se presentan automáticamente a un analista de modo que el analista pueda evaluarlas de manera rápida y eficiente y determinar con mayor precisión si un ataque cibernético contra un recurso de la organización está en curso. En particular, como se describe a continuación, el sistema de advertencia puede aplicar uno o más criterios o reglas de análisis a los indicadores (por ejemplo, indicadores de procesamiento, incluidas la información de actividad del usuario y la información contextual) para generar una puntuación del riesgo y, opcionalmente, una alerta. La alerta puede mostrarse en una interfaz de usuario de análisis a través de la cual el analista puede evaluarlos y/o acceder a datos más detallados relacionados con las alertas y los indicadores relacionados. En algunas realizaciones, uno o más indicadores pueden estar asociados con cada alerta, y pueden determinarse en función de los indicadores relacionados con la alerta.

Como se mencionó anteriormente, en algunas realizaciones, la puntuación de la alerta puede agruparse en uno de, por ejemplo, tres compartimientos correspondientes a una alerta alta, una alerta media o una alerta baja. Cada nivel de alerta puede estar asociado con un indicador, un icono, un color y/o similar. Por ejemplo, una alerta alta puede

estar asociada con el rojo (y/u otro color), una alerta media puede estar asociada con el naranja (y/u otro color), y una alerta baja puede estar asociada con el gris (y/u otro color).

En diversas realizaciones de las interfaces de usuario de ejemplo descritas a continuación en referencia a las figuras 5-9, varios aspectos de las interfaces de usuario pueden o no estar incluidos, pueden parecer visualmente diferentes y/o pueden estar dispuestos de manera diferente.

Con referencia a la figura 5, la interfaz 900 de usuario de ejemplo ilustra una visión general de la red proporcionada por el sistema de advertencia a un analista para permitirle al analista revisar el nivel de riesgo de todos los recursos en la red que están siendo monitoreados por el sistema de advertencia. La interfaz 900 de usuario de ejemplo incluye un gráfico 902 de riesgo histórico, un indicador 908 de tendencia del riesgo, un gráfico 916 del riesgo del sistema, una lista 914 de recursos, un contador 912 de eventos, un indicador 906 del sistema en mayor riesgo, un contador 917 de alertas, un campo 903 de la última actualización y un indicador 904 de puntuación del riesgo total. La lista 914 de recursos comprende una columna 922 de nombre de recurso, una columna 924 de puntuación del riesgo, una columna 926 de vida de la alerta, una columna 928 de conteo de alertas, una columna 930 de conteo de eventos, una columna 932 de indicador de riesgo superior, y una columna 934 cuantificadora del riesgo cibernético.

El gráfico 902 de riesgo histórico muestra una representación gráfica del riesgo global en todos los recursos monitoreados por el sistema de advertencia a lo largo del tiempo. Por ejemplo, el gráfico 902 del riesgo histórico puede mostrar en el eje x los últimos tres meses y en el eje y mostrar la puntuación del riesgo global. El indicador 908 de tendencia del riesgo muestra el recurso que se ha determinado que tiene el mayor aumento de riesgo en un período de tiempo reciente, tal como por ejemplo, las últimas veinticuatro horas. El indicador 906 del sistema en mayor riesgo muestra el recurso con la puntuación del riesgo más alta, y la puntuación del riesgo correspondiente a ese recurso, entre paréntesis. Al seleccionar el indicador del sistema en mayor riesgo, el analista se dirige a una página de resumen del sistema del sistema en mayor riesgo, según se ilustra en la figura 6. La etiqueta 903 de última actualización indica la última vez que se han actualizado los datos mostrados en la interfaz 900 de usuario. El indicador 904 de puntuación del riesgo total muestra la puntuación del riesgo global, así como una representación gráfica de esa puntuación del riesgo y una categorización del nivel de riesgo tal como, por ejemplo, medio. El contador 917 de alertas muestra cuántas alertas hay actualmente en el sistema de advertencia que aún no han sido respondidas por un analista. El contador 912 de eventos muestra la cantidad de eventos de los que el sistema de advertencia está actualmente realizando un seguimiento. El gráfico 916 de riesgo del sistema muestra una representación de la edad promedio de una alerta frente el riesgo del sistema según lo determinado por la puntuación del riesgo para el recurso. Esto puede permitir que un analista vea qué sistemas están en riesgo y si el riesgo proviene del recurso que tiene una acumulación de alertas antiguas que no han sido respondidas, o si el riesgo es causado por alertas recientes. La lista 914 de recursos muestra información sobre cada uno de los diversos sistemas monitoreados por el sistema de advertencia. Por ejemplo, la columna 922 de nombre de recurso muestra el nombre del recurso. La columna 924 de puntuación del riesgo muestra la puntuación del riesgo correspondiente al recurso. La columna 926 de vida útil de la alerta muestra el tiempo promedio desde la emisión de una alerta hasta la respuesta de un analista a la alerta. La columna 928 de recuento de alertas indica el número total de alertas abiertas para cada recurso. La columna 930 de recuento de eventos indica el número total de eventos para cada sistema. La columna 932 del indicador del riesgo superior indica el tipo de evento o alerta que está asociado con la contribución general más alta a la puntuación del riesgo. La columna 934 del cuantificador de riesgo cibernético indica una estimación numérica del riesgo cibernético, p. ej. la vulnerabilidad inherente a la explotación del software relacionada con el recurso en cuestión. Esto puede determinarse mediante una estimación empírica o teórica de la vulnerabilidad a la explotación del software subyacente del recurso. Esto puede calcularse, por ejemplo, teniendo en cuenta un promedio histórico de vulnerabilidades encontradas, o estimando teóricamente la vulnerabilidad a la explotación (por ejemplo, al software que se ejecuta en un sistema operativo con técnicas anti-explotación más sofisticadas, tales como la aleatorización del diseño del espacio de direcciones, se le puede asignar un menor riesgo cibernético que al software que se ejecuta en un sistema operativo que no incorpora tales técnicas).

La interfaz 1008 de usuario de ejemplo, según se muestra en la figura 6, ilustra una descripción general de recursos proporcionada por el sistema de advertencia a un analista para permitirle revisar la información, incluidas las alertas y los eventos, relacionados con un posible ataque cibernético, contra un recurso elegido que está siendo monitoreado por el sistema de advertencia. La interfaz 1008 de usuario de ejemplo comprende un indicador 1010 del riesgo para los recursos, un contador 1004 de eventos, un panel 1002 de las principales estrategias, un campo 1012 de descripción de recursos, un selector 1014 de columnas, un campo 1018 de filtro de alertas y de eventos, un gráfico 1016 de alertas y de eventos, una tabla 122 de alertas y de eventos, y una barra 1020 de acción rápida. El gráfico 1007 de riesgo histórico ilustra una representación gráfica del riesgo estimado del recurso seleccionado a lo largo del tiempo.

El panel 1002 de estrategias principales muestra los tipos de actividades o indicadores monitoreados que generaron recientemente la mayoría de los eventos relacionados con este recurso. Ventajosamente, esto le permite al analista determinar si existe o no una tendencia de cierta actividad sospechosa que aumenta en volumen, y si las fuentes de alertas están concentradas o no. El contador 1009 de alertas abiertas indica el número de alertas que actualmente requieren una respuesta del analista. El campo 1018 de filtro de alertas y de eventos acepta la entrada de texto del analista y le permite filtrar las alertas y los eventos que se muestran. Por ejemplo, el analista puede introducir el nombre de un usuario específico o puede introducir el tipo de una actividad sospechosa específica, tal como el fallo

de autentificación para filtrar las alertas que se muestran. Ventajosamente, esto permite al analista investigar ciertos tipos de actividades relacionadas con un ataque cibernético contra un recurso con mayor detalle. La barra 1020 de acción rápida permite al analista seleccionar una de entre varias respuestas a las -una o más- alertas seleccionadas. Por ejemplo, el analista puede ser capaz de elevar las -una o más- alertas a un supervisor seleccionando la opción de elevar, el analista puede descartar las -una o más- alertas como no críticas pinchando en la opción de cierre, el analista puede ser capaz de asignar a otro analista para que realice una investigación pinchando en la opción de iniciar investigación.

El gráfico 1016 de alertas y de eventos muestra una representación gráfica de alertas y de eventos para el recurso; muestra las alertas y los eventos según su ocurrencia en el tiempo y su puntuación del riesgo. Por ejemplo, las alertas 1052a y 1052b se dibujan en el gráfico con sus posiciones que representan su hora de ocurrencia y puntuación del riesgo. El interruptor 1019 de conmutación para mostrar alertas históricas permite al analista, seleccionándolo y deseleccionándolo, determinar si las alertas históricas, es decir, las alertas que ya han sido respondidas por un analista, deben mostrarse o no en el gráfico 1016 de alertas y eventos. El interruptor 1021 de conmutación para mostrar eventos permite al analista al habilitarlo o deshabilitarlo determinar si los eventos deben mostrarse o no en el gráfico 1016 de alertas y eventos. Si se selecciona por medio del interruptor 1019 de conmutación para mostrar alertas históricas la visualización de alertas históricas, los eventos históricos pueden mostrarse en el gráfico 1016 de alertas y eventos como círculos rayados (o como cualquier otro indicador, icono o color, por ejemplo), tal como con el evento 1051 histórico. Si se habilita en el interruptor 1021 de conmutación para mostrar eventos la visualización de eventos, los eventos se muestran como círculos grises sombreados (o como cualquier otro indicador, icono o color, por ejemplo) en el gráfico 1016 de alertas y eventos, tal como con los eventos 1050a y 1050b.

La tabla 1022 de alertas y eventos comprende, para cada evento mostrado en la tabla 1022 de alertas y eventos, una casilla 1024 de verificación de la selección, una columna 1026 de descripción de la alerta o el evento, una columna 1028 del tipo de alerta o evento y una columna 1030 de estado así como una columna 1032 de tiempo de la alerta o del evento. La casilla 1024 de verificación de la selección permite al analista incluir en una selección marcando -o excluir de una selección desmarcando- la casilla 1024 de verificación de la selección, correspondiente a una o más alertas. Esto le permite al analista elegir una o más alertas para tomar medidas. Por ejemplo, el analista puede marcar la casilla 1024 de verificación correspondiente a una o más alertas para bien cerrarlas, elevarlas o iniciar una investigación sobre esas -una o más- alertas.

La columna 1026 de descripción de la alerta o del evento muestra un resumen conciso del tipo y la naturaleza de la actividad que dio lugar a una alerta o a un evento. Esto puede incluir información específica de alertas, tal como el nombre de una persona, de un ordenador, de un servidor, etc. Ventajosamente, esto puede permitir una búsqueda de texto libre para captar esos detalles en diferentes alertas. Por ejemplo, la columna 1026 de descripción de la alerta o del evento puede indicar que cierto usuario ha intentado sin éxito iniciar sesión en un recurso informático de la organización, que se ha determinado que el ordenador de cierto usuario está infectado con software malicioso o que un determinado usuario ha estado recibiendo correos electrónicos de ingeniería social, el nombre del usuario y la dirección de correo electrónico a la que fueron enviados. La columna 1028 del tipo de alerta o de evento indica si una entrada dada en la tabla 1022 de alertas y eventos es una alerta o un evento. La columna 1030 de estado indica si para un evento determinado el sistema de advertencia espera o no alguna acción del analista. Por ejemplo, para un evento, la columna de estado indicará que no se precisa ninguna acción del analista, mientras que para una alerta, la columna 1030 de estado puede indicar que se solicita una acción del analista para una alerta. Por ejemplo, se le puede solicitar al analista que revise y, según corresponda, decida elevar, cerrar o iniciar una investigación sobre la alerta. Si un analista ha tomado una acción con respecto a una alerta, el estado cambiará, lo que indica que ya no es necesaria ninguna otra acción porque la alerta ya ha sido cerrada, elevada o sometida al inicio de una investigación por parte de este u otro analista. La columna 1032 de hora de alerta o de evento indica la fecha y hora en que se crearon la alerta o el evento.

Ventajosamente, al presentarle al analista las alertas junto con los eventos, como en la interfaz de usuario de ejemplo de la figura 6, el analista puede ser más efectivo al revisar las alertas. El analista tiene acceso tanto a las alertas que ya ha determinado el sistema de advertencia que son un riesgo significativo, como a los eventos que el sistema de advertencia ha determinado que, como tales, no representan un riesgo sustancial, pero que podrían ser valiosos para comprender el contexto y determinar la causa o la naturaleza de otras actividades sospechosas que actualmente tienen lugar contra el recurso. El contador 1004 de eventos indica el número total de eventos de los que el sistema de advertencia está realizando un seguimiento con respecto a este recurso. El contador 1009 de alertas abiertas indica el número total de alertas que están abiertas actualmente con respecto a este recurso. El campo 1012 de descripción del recurso contiene una breve descripción de la naturaleza y del uso del recurso.

La elevación de una o más alertas notifica a un supervisor de las alertas, permitiendo así que el supervisor tome medidas inmediatas contra un ataque cibernético. Al seleccionar "iniciar investigación", el analista puede asignar a otro analista para que investigue las -una o más- alertas seleccionadas. El cierre de una o más alertas refleja la decisión del analista de que la alerta no requiere acción. Esto hace que el sistema de advertencia marque la alerta seleccionada como histórica; las -una o más- alertas seleccionadas ya no contribuirán a la puntuación del riesgo para los recursos. Una vez que una alerta se marca como histórica, el sistema de advertencia actualiza la puntuación del riesgo para los recursos y la puntuación del riesgo global para reflejar la eliminación de la alerta. Si el

interruptor de conmutación para las alertas históricas está fijado en deshabilitado, las -una o más- alertas seleccionadas también se eliminarán del gráfico 1016 de alertas y eventos; de lo contrario, las alertas permanecerán en el gráfico 1016 de alertas y eventos, pero se dibujarán allí como un círculo negro sombreado (o como cualquier otro indicador, icono o color, por ejemplo). Otros elementos de la interfaz de usuario, incluido el contador 1004 de eventos, también se actualizarán para reflejar la eliminación de la alerta.

La figura 7 ilustra un ejemplo de interfaz 1100 de usuario del sistema de advertencia en el que se presenta una vista de los servidores, servicios, aplicaciones, bases de datos y otros recursos que están asociados con un recurso dado, así como una lista de usuarios asociados con un determinado recurso. Específicamente, en la tabla 1112 de servidores relacionados, se muestra información sobre qué recursos informáticos están asociados con un recurso dado. En la columna 1114 del tipo, se identifica el tipo de recurso informático, tal como una aplicación, una base de datos, un servidor web, otro tipo de servidor u otro tipo de recurso. En la columna 1116 de alojamiento, se identifica el nombre del alojamiento en el que se encuentra el recurso. En la columna 1118 de IP, se identifica la dirección de protocolo de Internet (IP) del alojamiento asociado con el recurso dado. En la columna 1120 del entorno, se identifica el entorno del recurso dado, tal como por ejemplo si se trata de un servidor de producción o de un servidor de pruebas. En la etiqueta 1134 de recursos relacionados, se identifica el número de recursos relacionados que están siendo seguidos actualmente por el sistema de advertencia. En el panel 1130 de usuarios relacionados, se presenta información sobre los usuarios asociados con el recurso. En la columna 1124 de nombre de usuario, se presenta el nombre del usuario. En la columna 1126 de funciones, se presenta el rol del usuario. En la columna 1128 de título, se presenta el título del trabajo del usuario. En la columna 1131 de ordenador se presenta información sobre el ordenador del usuario tal como, por ejemplo, la dirección de hardware del ordenador. En la columna 1132 de nivel de acceso, se indica el nivel de acceso del usuario tal como, por ejemplo, si el usuario tiene privilegios administrativos o simplemente privilegios de usuario normal. El campo 1135 de filtro de servidor permite al analista introducir una cadena de caracteres, lo que hace que el sistema de advertencia filtre la tabla 1112 de servidores relacionados de modo que se muestren únicamente aquellos servidores en los que al menos uno de los atributos coincide con la cadena de caracteres introducida. En la etiqueta 1116 de usuarios relacionados, se identifica el número de usuarios actualmente rastreados por el sistema de advertencia y relacionados con el recurso. El campo 1117 de filtro de usuarios relacionados permite al analista introducir una cadena de caracteres, haciendo que el sistema de advertencia filtre la lista de usuarios de modo que únicamente muestre aquellos usuarios en los que al menos uno de los atributos coincide con la cadena de caracteres introducidos en el campo 1117 de filtro de usuarios relacionados. En una interfaz de usuario de ejemplo del sistema de advertencia, se presenta una vista de 360° de un recurso seleccionado.

La figura 8 ilustra un ejemplo de interfaz 1200 de usuario en el que se presenta a un analista una solicitud de elevación, lo que permite al analista elevar eventos y alertas, por ejemplo, alertas y eventos que se seleccionaron en una interfaz 1008 de usuario, según se ilustra en la figura 6. La solicitud de elevación comprende una barra 1202 de título, el campo 1204 de nombre del investigador, el campo 1206 de tiempo, el campo 1208 de cesionario, la columna 1201 de ID de la alerta, la columna 1212 de introducción de la alerta, la columna 1214 de tipo de alerta, la columna 1216 de estado de alerta y la columna 1218 de tiempo de alerta, así como el campo 1220 común y el botón 1222 de envío. La barra de título indica el número de alertas y el número de eventos que se elevarán si el analista actúa. El campo 1204 de nombre del investigador muestra la identidad del analista a quien se elevarán las alertas y los eventos en ausencia de una elección contraria por parte del analista. El campo 1206 de tiempo muestra el tiempo en que las alertas o los eventos se elevarán. La columna 1208 del cesionario permite al analista elevar la alerta para especificar uno o más analistas a los que se debe elevar la alerta, anulando así el cesionario predeterminado en 1208. La columna 1210 de ID de la alerta muestra, para cada alerta, un identificador numérico único que puede identificar la alerta dentro del sistema de advertencia. La columna 1212 de información de la alerta muestra, para cada alerta o evento, una breve descripción de las circunstancias fácticas que condujeron a la emisión de la alerta. Por ejemplo, la columna de información de alerta o evento puede contener una descripción de que la alerta se emitió en respuesta a una infección de malware de un ordenador, indicar el tipo de malware que se encontró e indicar si la infección de malware se purgó o no. La columna 1214 de tipo indica si la entrada es un evento o una alerta. La columna 1216 de estado indica si el sistema de advertencia solicita o no algún tipo de acción relacionada con la alerta o con el evento por parte del auditor, o si dicha acción no es necesaria. La columna 1218 de tiempo indica la hora en que se emitieron la alerta o el evento. El cuadro 1220 de comentarios permite al analista agregar información tal como la descripción o una anotación que será visible para el cesionario y para otros analistas cuando revisen la alerta. El botón 1222 de envío, cuando se selecciona, permite al analista confirmar la elevación de la alerta al cesionario especificado en el campo 1208 de cesionario. Al ser seleccionado, el sistema de advertencia actualiza sus registros para hacer que las alertas y los eventos se eleven según se solicita, y, si tiene éxito, muestra una confirmación al analista, por ejemplo en una interfaz 1300 de usuario según se ilustra en la figura 9.

La figura 9 ilustra un ejemplo de interfaz 1300 de usuario, que muestra un mensaje 1301 de confirmación que confirma a un analista que el sistema de advertencia ha recibido la acción del analista sobre una alerta o un evento, por ejemplo, que se ha cerrado una alerta, y además permite al analista proporcionar información adicional relacionada con la alerta. La etiqueta 1302 del mensaje de confirmación indica al analista el número de alertas o eventos en los que se tomó acción. Un analista también puede agregar comentarios a través de un cuadro 1304 de comentarios que se mostrará a otras personas que revisen esa alerta, incluidos, por ejemplo, otros analistas o supervisores. Específicamente, un analista puede usar el cuadro de comentarios para incluir información relacionada

con la actividad del usuario al elevar una alerta, lo que facilita que la información contextual proporcionada por el sistema de advertencia así como cualquier comentario o anotación del analista que ya haya revisado la alerta se les presente a un supervisor que revisa la alerta elevada o a otro analista que investiga una alerta. Ventajosamente, esto puede permitir un intercambio de información más efectivo y, por lo tanto, una colaboración más fácil entre analistas. El botón 1310 de envío, cuando se selecciona, permite al analista enviar cualquier comentario introducido en el cuadro 1304 de comentarios, descartar el mensaje 1301 de confirmación y regresar a la interfaz de usuario anterior.

En diversas implementaciones, varias tablas y paneles pueden incluir más o menos columnas o elementos de información que los mostrados en los ejemplos de las figuras 5, 6, 7, 8 y 9. Además, el usuario puede seleccionar opcionalmente cualquier parte de cada fila para ver información más detallada asociada con una alerta. En una implementación, cada alerta o evento puede incluir elementos adicionales de la interfaz de usuario mediante los cuales un analista puede tomar acción con respecto a la alerta (por ejemplo, elevar, descartar, confirmar, etc.)

Realizaciones y detalles de implementación adicionales

Distinguir la falta de actividad relacionada con un ataque cibernético contra un recurso en una red informática de la actividad relacionada con un ataque cibernético sobre un recurso es difícil, especialmente debido a la gran cantidad de indicadores a revisar, y porque puede no ser posible concluir si un evento determinado es o no indicativo de un ataque cibernético teniendo en cuenta solamente uno o un subconjunto de indicadores. Las realizaciones de la presente descripción permiten implementar un sistema de advertencia que reúne los diversos indicadores, los procesa utilizando información contextual para determinar el riesgo de un ataque cibernético contra un recurso y genera alertas, según corresponda, en función de la estimación del riesgo. La estimación del riesgo se puede utilizar para crear alertas para su revisión por un analista humano, y para clasificar, ordenar, agregar y filtrar las alertas. Cuando se presentan alertas a un analista humano, la información contextual, tal como otros eventos asociados con el recurso, se presenta con la alerta. Cuando es apropiado, las alertas se pueden presentar utilizando agregados tales como totales, promedios y máximos. Las alertas se presentan en una interfaz de usuario que incorpora representaciones visuales, tales como cuadros y gráficos, según corresponda, para permitir al analista revisar cómodamente grandes conjuntos de datos y aprovechar las capacidades de reconocimiento de patrones particularmente pronunciadas de los humanos relacionadas con los estímulos visuales.

En algunas realizaciones, las notificaciones de nuevas alertas, o de otros desarrollos, tales como una puntuación del riesgo que excede un valor crítico, pueden generarse y transmitirse automáticamente a un dispositivo operado por el usuario asociado con un activador correspondiente. La notificación y/o notificación puede transmitirse en el momento en que se genera la notificación o en un momento determinado después de la generación de la notificación y/o notificación. Cuando es recibida por el dispositivo, la notificación y/o notificación puede hacer que el dispositivo muestre la notificación y/o notificación a través de la activación de una aplicación en el dispositivo (por ejemplo, un navegador, una aplicación móvil, etc.). Por ejemplo, la recepción de la notificación y/o notificación puede activar automáticamente una aplicación en el dispositivo, tal como una aplicación de mensajería (por ejemplo, una aplicación de mensajería SMS o MMS), una aplicación independiente (por ejemplo, una aplicación de monitoreo del sistema de advertencia) o un navegador, por ejemplo, y mostrar información incluida en la notificación o información adicional relacionada. Si el dispositivo está fuera de línea cuando se transmiten las notificaciones y/o notificaciones, la aplicación puede activarse automáticamente cuando el dispositivo está en línea de modo que se muestre la notificación y/o notificación. Como otro ejemplo, la recepción de la notificación y/o notificación puede hacer que un navegador se abra y se redirija a una página de inicio de sesión generada por el sistema de advertencia para que el usuario pueda iniciar sesión en el sistema de advertencia y ver la notificación y los datos relacionados. Alternativamente, la notificación y/o notificación puede incluir una URL de una página web (u otra información en línea) asociada con la notificación, de modo que cuando el dispositivo (por ejemplo, un dispositivo móvil) recibe la notificación, se activa automáticamente un navegador (u otra aplicación) y se accede a la URL incluida en la notificación y/o notificación a través de Internet. Ventajosamente, esto mantiene informados a los analistas y a otros miembros interesados de una organización sobre el desarrollo crítico, sin requerir que verifiquen periódicamente el estado del sistema de advertencia.

Varias realizaciones de la presente descripción pueden ser un sistema, un método y/o un producto de programa informático en cualquier posible nivel de detalle técnico de integración. El producto de programa de ordenador puede incluir un medio (o medios) de almacenamiento legible por ordenador que tiene instrucciones de programa legibles por ordenador sobre el mismo para hacer que un procesador lleve a cabo aspectos de la presente descripción.

Por ejemplo, la funcionalidad descrita en el presente documento puede realizarse a medida que las instrucciones de software se ejecutan y/o en respuesta a instrucciones de software que están siendo ejecutadas por uno o más procesadores de hardware y/o cualquier otro dispositivo informático adecuado. Las instrucciones del software y/u otro código ejecutable pueden leerse de un medio (o medios) de almacenamiento legible por ordenador.

El medio de almacenamiento legible por ordenador puede ser un dispositivo tangible que puede retener y almacenar datos y/o instrucciones para su uso por un dispositivo de ejecución de instrucciones. El medio de almacenamiento legible por ordenador puede ser, por ejemplo, pero no se limita a, un dispositivo de almacenamiento electrónico (incluidos los dispositivos de almacenamiento electrónico volátiles y/o no volátiles), un dispositivo de

almacenamiento magnético, un dispositivo de almacenamiento óptico, un dispositivo de almacenamiento electromagnético, un dispositivo de almacenamiento semiconductor, o cualquier combinación adecuada de los anteriores. Una lista no exhaustiva de ejemplos más específicos del medio de almacenamiento legible por ordenador incluye los siguientes: un disquete de ordenador portátil, un disco duro, una unidad de estado sólido, una memoria de acceso aleatorio (RAM), una memoria de solo lectura (ROM), una memoria de solo lectura programable y borrable (EPROM o memoria Flash), una memoria de acceso aleatorio estática (SRAM), una memoria de solo lectura de disco compacto portátil (CD-ROM), un disco versátil digital (DVD), una tarjeta de memoria, un disquete, un dispositivo codificado mecánicamente tal como tarjetas perforadas o estructuras elevadas en una ranura que tiene instrucciones grabadas en las mismas, y cualquier combinación adecuada de los anteriores. Un medio de almacenamiento legible por ordenador, como se usa en el presente documento, no debe interpretarse como señales transitorias per se, tales como ondas de radio u otras ondas electromagnéticas que se propagan libremente, ondas electromagnéticas que se propagan a través de una guía de ondas o de otros medios de transmisión (por ejemplo, pulsos de luz que pasan a través de un cable de fibra óptica), o señales eléctricas transmitidas a través de un cable.

Las instrucciones del programa legible por ordenador descritas en el presente documento se pueden descargar a los respectivos dispositivos informáticos/de procesamiento desde un medio de almacenamiento legible por ordenador o a un ordenador externo o a un dispositivo de almacenamiento externo a través de una red, por ejemplo, Internet, de una red de área local, de una red de área amplia y/o de una red inalámbrica. La red puede comprender cables de transmisión de cobre, fibras de transmisión óptica, transmisión inalámbrica, enrutadores, cortafuegos, conmutadores, ordenadores de puerta de enlace y/o servidores perimetrales. Una tarjeta adaptadora de red o una interfaz de red en cada dispositivo informático/de procesamiento recibe instrucciones de programa legibles por ordenador de la red y reenvía las instrucciones de programa legibles por ordenador para almacenamiento en un medio de almacenamiento legible por ordenador dentro del dispositivo informático/de procesamiento respectivo.

Las instrucciones de programa legibles por ordenador (también denominadas en este documento como, por ejemplo, "código", "instrucciones", "módulo", "aplicación", "aplicación de software" y/o similares) para llevar a cabo operaciones de la presente descripción pueden ser instrucciones de ensamblador, instrucciones de arquitectura de repertorio de instrucciones (ISA), instrucciones de máquina, instrucciones dependientes de máquina, microcódigo, instrucciones de firmware, datos de configuración de estado, datos de configuración para circuitos integrados, o código fuente o código objeto escrito en cualquier combinación de uno o más lenguajes de programación, incluido un lenguaje de programación orientado a objetos tal como Smalltalk, C++ o similares, y lenguajes de programación por procedimientos, como el lenguaje de programación "C" o lenguajes de programación similares. Las instrucciones de programa legibles por ordenador pueden invocarse desde otras instrucciones o desde sí mismas, y/o pueden invocarse en respuesta a eventos o interrupciones detectados. Las instrucciones de programa legibles por ordenador configuradas para su ejecución en dispositivos informáticos pueden proporcionarse en un medio de almacenamiento legible por ordenador y/o como una descarga digital (y pueden almacenarse originalmente en un formato comprimido o instalable que requiere instalación, descompresión o descifrado previo a la ejecución) que luego puede almacenarse en un medio de almacenamiento legible por ordenador. Dichas instrucciones de programa legibles por ordenador pueden almacenarse, parcial o totalmente, en un dispositivo de memoria (por ejemplo, un medio de almacenamiento legible por ordenador) del dispositivo informático en ejecución, para su ejecución por el dispositivo informático. Las instrucciones del programa legible por ordenador pueden ejecutarse completamente en el ordenador de un usuario (por ejemplo, el dispositivo informático en ejecución), en parte en el ordenador del usuario, como un paquete de software independiente, en parte en el ordenador del usuario y en parte en un ordenador remoto o completamente en el ordenador remoto o servidor. En el último escenario, el ordenador remoto puede conectarse al ordenador del usuario a través de cualquier tipo de red, incluida una red de área local (LAN) o una red de área amplia (WAN), o la conexión puede realizarse a un ordenador externo (para ejemplo, a través de Internet utilizando un proveedor de servicios de Internet). En algunas realizaciones, los circuitos electrónicos que incluyen, por ejemplo, circuitos lógicos programables, matrices de compuertas programables en campo (FPGA) o matrices lógicas programables (PLA) pueden ejecutar las instrucciones de programa legibles por ordenador utilizando información de estado de las instrucciones de programa legibles por ordenador para personalizar la circuitería electrónica, para realizar aspectos de la presente descripción.

Los aspectos de la presente descripción se describen en el presente documento con referencia a diagramas de flujo y/o a diagramas de bloques de métodos, aparatos (sistemas) y productos de programas informáticos según las realizaciones de la descripción. Se entenderá que cada bloque de las ilustraciones del diagrama de flujo y/o los diagramas de bloque, y las combinaciones de bloques en las ilustraciones del diagrama de flujo y/o los diagramas de bloque, se pueden implementar mediante instrucciones de programa legibles por ordenador.

Estas instrucciones de programa legibles por ordenador se pueden proporcionar a un procesador de un ordenador de propósito general, a un ordenador de propósito especial o a otro aparato de procesamiento de datos programable para producir una máquina, tal que las instrucciones, que se ejecutan a través del procesador del ordenador o de otro aparato de procesamiento de datos programable, crea medios para implementar las funciones/actos especificados en el diagrama de flujo y/o el bloque o bloques del diagrama de bloques. Estas instrucciones de programa legibles por ordenador también pueden almacenarse en un medio de almacenamiento legible por ordenador que puede dirigir un ordenador, un aparato de procesamiento de datos programable y/u otros dispositivos para que funcionen de una manera particular, de modo que el medio de almacenamiento legible por ordenador que tiene instrucciones almacenadas en el mismo comprenda un artículo de fabricación que incluye instrucciones que

implementan aspectos de la función/acto especificados en el (los) diagrama(s) de flujo y/o en el bloque o bloques del (de los) diagrama(s) de bloques.

Las instrucciones del programa legible por ordenador también se pueden cargar en un ordenador, otro aparato de procesamiento de datos programable u otro dispositivo para hacer que se realicen una serie de pasos operativos en el ordenador, en otro aparato programable o en otro dispositivo para producir un proceso implementado por ordenador, de modo que las instrucciones que se ejecutan en el ordenador, en otro aparato programable o en otro dispositivo implementen las funciones/actos especificados en el diagrama de flujo y/o en el bloque o bloques del diagrama de bloques. Por ejemplo, las instrucciones pueden llevarse a cabo inicialmente en un disco magnético o en una unidad de estado sólido de un ordenador remoto. El ordenador remoto puede cargar las instrucciones y/o los módulos en su memoria dinámica y enviar las instrucciones por teléfono, cable o línea óptica utilizando un módem. Un módem local para un sistema informático de servidor puede recibir los datos en el teléfono/cable/línea óptica y usar un dispositivo convertidor que incluya los circuitos apropiados para colocar los datos en un bus. El bus puede llevar los datos a una memoria, desde la cual un procesador puede recuperar y ejecutar las instrucciones. Las instrucciones recibidas por la memoria pueden almacenarse opcionalmente en un dispositivo de almacenamiento (por ejemplo, una unidad de estado sólido) antes o después de la ejecución por parte del procesador del ordenador.

El diagrama de flujo y los diagramas de bloques de las figuras ilustran la arquitectura, la funcionalidad y el funcionamiento de posibles implementaciones de sistemas, métodos y productos de programas informáticos según diversas realizaciones de la presente descripción. A este respecto, cada bloque en el diagrama de flujo o en los diagramas de bloques puede representar un módulo, un segmento o una parte de las instrucciones, que comprende una o más instrucciones ejecutables para implementar las funciones lógicas especificadas. En algunas implementaciones alternativas, las funciones indicadas en los bloques pueden ocurrir fuera del orden indicado en las figuras. Por ejemplo, dos bloques mostrados en sucesión pueden, de hecho, ejecutarse de manera sustancialmente concurrente, o los bloques a veces pueden ejecutarse en el orden inverso, dependiendo de la funcionalidad involucrada. Además, ciertos bloques pueden omitirse en algunas implementaciones. Los métodos y procesos descritos en el presente documento tampoco están limitados a ninguna secuencia particular, y los bloques o estados relacionados con los mismos pueden realizarse en otras secuencias que sean apropiadas.

También se observará que cada bloque de los diagramas de bloques y/o de la ilustración del diagrama de flujo, y las combinaciones de bloques de los diagramas de bloques y/o de la ilustración del diagrama de flujo, pueden implementarse mediante sistemas basados en hardware de propósito especial que realizan las funciones o actos especificados o realizar combinaciones de hardware de propósito especial e instrucciones de ordenador. Por ejemplo, cualquiera de los procesos, métodos, algoritmos, elementos, bloques, aplicaciones u otra funcionalidad (o partes de funcionalidad) descritas en las secciones anteriores pueden incorporarse y/o automatizarse total o parcialmente a través de dicha aplicación de hardware electrónico tal como procesadores específicos de la aplicación (p. ej., circuitos integrados específicos de la aplicación (ASIC)), procesadores programables (p. ej., matrices de compuertas programables en campo (FPGA)), circuitos específicos de la aplicación y/o similares (cualquiera de los cuales también puede combinar lógica cableada personalizado, circuitos lógicos, ASIC, FPGA, etc. con programación/ejecución personalizada de instrucciones de software para realizar las técnicas).

Cualquiera de los procesadores y/o dispositivos mencionados anteriormente que incorporan cualquiera de los procesadores mencionados anteriormente, puede denominarse en el presente documento, por ejemplo, "ordenadores", "dispositivos informáticos", "dispositivos informáticos", "hardware de dispositivos informáticos", "procesadores de hardware", "unidades de procesamiento" y/o similares. Los dispositivos informáticos de las realizaciones anteriores pueden generalmente (pero no necesariamente) ser controlados y/o coordinados por el software del sistema operativo, tal como Mac OS, iOS, Android, Chrome OS, Windows OS (por ejemplo, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10, Windows Server, etc.), Windows CE, Unix, Linux, SunOS, Solaris, Blackberry OS, VxWorks u otros sistemas operativos adecuados. En otras realizaciones, los dispositivos informáticos pueden ser controlados por un sistema operativo propietario. Los sistemas operativos convencionales controlan y programan procesos informáticos para la ejecución, realizan la gestión de memoria, proporcionan sistema de archivos, redes, servicios de E/S y proporcionan una funcionalidad de interfaz de usuario, tal como una interfaz gráfica de usuario ("GUI"), entre otras cosas.

Por ejemplo, la figura 10 es un diagrama de bloques que ilustra un sistema 800 informático sobre el que se pueden implementar diversas realizaciones. Por ejemplo, el dispositivo 150 de monitoreo puede implementarse proveyendo al sistema 800 informático de instrucciones de software apropiadas. El sistema 800 informático incluye un bus 802 u otro mecanismo de comunicación para comunicar información, y un procesador de hardware, o procesadores 804 múltiples, acoplados con el bus 802 para procesar información. Los procesadores 804 de hardware pueden ser, por ejemplo, uno o más microprocesadores de uso general. Debido a que se precisa que el dispositivo 150 de monitoreo, en algunas realizaciones, procese cantidades sustanciales de actividad de red en tiempo casi real, pueden ser necesarios varios procesadores o procesadores con múltiples núcleos físicos, y velocidades de reloj apropiadas, dependiendo del volumen de actividad en el entorno de red supervisado. Cuando se configura como dispositivo 150 de monitoreo, el sistema 800 informático puede aprovechar ventajosamente el procesamiento paralelo, particularmente durante el procesamiento de indicadores y eventos, y así lograr beneficios de rendimiento significativos al utilizar múltiples procesadores o núcleos físicos.

El sistema 800 informático también incluye una memoria 806 principal, tal como una memoria de acceso aleatorio (RAM), caché y/u otros dispositivos de almacenamiento dinámico, acoplados al bus 802 para almacenar información e instrucciones para ser ejecutadas por el procesador 804. La memoria 806 principal también se puede usar para almacenar variables temporales u otra información intermedia durante la ejecución de las instrucciones que debe ejecutar el procesador 804. Dichas instrucciones, cuando se almacenan en medios de almacenamiento accesibles para el procesador 804, convierten el sistema 800 informático en una máquina especial que está personalizada para realizar las operaciones especificadas en las instrucciones. Ventajosamente, el sistema 800 informático puede, cuando se configura como dispositivo 150 de monitoreo, utilizar arquitecturas de acceso a memoria no uniforme (NUMA) para el beneficio del rendimiento. Por ejemplo, el sistema 800 informático puede asignar diferentes procesadores o núcleos físicos de procesadores a un recurso o grupo de recursos diferente, y puede almacenar los indicadores, reglas y eventos correspondientes en una localización de memoria "cerca" de ese procesador o núcleo físico. Esto permite que el sistema de advertencia concentre los accesos de memoria en localizaciones de memoria "cercanas" durante el procesamiento de los indicadores y, por lo tanto, permite obtener más beneficios de rendimiento del paralelismo.

El sistema 800 informático incluye además una memoria 808 de solo lectura (ROM) u otro dispositivo de almacenamiento estático acoplado al bus 802 para almacenar información estática e instrucciones para el procesador 804. Se provee un dispositivo 810 de almacenamiento, tal como un disco magnético, disco óptico o una unidad de memoria USB (unidad flash), etc., y se acopla al bus 802 para almacenar información e instrucciones.

El sistema 800 informático puede estar acoplado a través del bus 802 a una pantalla 812, tal como una pantalla de tubo de rayos catódicos (CRT) o de LCD (o una pantalla táctil), para mostrar información a un usuario del ordenador. Un dispositivo 814 de entrada, que incluye teclas alfanuméricas y otras, está acoplado al bus 802 para comunicar información y selecciones de comandos al procesador 804. Otro tipo de dispositivo de entrada de usuario es el control 816 del cursor, tal como un ratón, una bola de seguimiento o teclas de dirección del cursor para comunicar información de dirección y selecciones de comandos al procesador 804 y para controlar el movimiento del cursor en la pantalla 812. Este dispositivo de entrada tiene normalmente dos grados de libertad en dos ejes, un primer eje (por ejemplo, x) y un segundo eje (por ejemplo, y), que permite que el dispositivo especifique posiciones en un plano. En algunas realizaciones, la misma información de dirección y selecciones de comando que el control del cursor se puede implementar mediante toques en una pantalla táctil sin cursor.

El sistema 800 informático puede incluir un módulo de interfaz de usuario para implementar una GUI que puede almacenarse en un dispositivo de almacenamiento masivo como instrucciones de programa ejecutables por ordenador que son ejecutadas por el dispositivo o dispositivos informáticos. El sistema 800 informático puede además, como se describe a continuación, implementar las técnicas descritas en el presente documento utilizando lógica cableada personalizada, uno o más ASIC o FPGA, firmware y/o lógica de programa que, en combinación con el sistema informático, hace o programa el sistema 800 informático para que sea una máquina de propósito especial. Según una realización, las técnicas en el presente documento son realizadas por el sistema 800 informático en respuesta a los procesadores 804 que ejecutan una o más secuencias de una o más instrucciones de programa legibles por ordenador contenidas en la memoria 806 principal. Dichas instrucciones pueden leerse en la memoria 806 principal desde otro medio de almacenamiento, tal como el dispositivo 810 de almacenamiento. La ejecución de las secuencias de instrucciones contenidas en la memoria 806 principal hace que los procesadores 804 realicen los pasos del proceso descritos en el presente documento. En realizaciones alternativas, se pueden usar circuitos cableados en lugar de o en combinación con instrucciones de software.

Diversas formas de medios de almacenamiento legibles por ordenador pueden estar involucradas en llevar una o más secuencias de una o más instrucciones de programa legibles por ordenador al procesador 804 para su ejecución. Por ejemplo, las instrucciones pueden llevarse a cabo inicialmente en un disco magnético o en una unidad de estado sólido de un ordenador remoto. El ordenador remoto puede cargar las instrucciones en su memoria dinámica y enviar las instrucciones a través de una línea telefónica utilizando un módem. Un módem local para el sistema 800 informático puede recibir los datos en la línea telefónica y usar un transmisor infrarrojo para convertir los datos en una señal infrarroja. Un detector infrarrojo puede recibir los datos transportados en la señal infrarroja y los circuitos apropiados pueden colocar los datos en el bus 802. El bus 802 transporta los datos a la memoria 806 principal, desde la cual el procesador 804 recupera y ejecuta las instrucciones. Las instrucciones recibidas por la memoria 806 principal pueden almacenarse opcionalmente en el dispositivo 810 de almacenamiento antes o después de la ejecución por el procesador 804.

El sistema 800 informático también incluye una interfaz 818 de comunicación acoplada al bus 802. La interfaz 818 de comunicación proporciona un acoplamiento de comunicación de datos bidireccional a un enlace 820 de red que está conectado a una red 822 local. Por ejemplo, la interfaz 818 de comunicación puede ser una tarjeta de red digital de servicios integrados (ISDN), un módem por cable, un módem por satélite o un módem para proporcionar una conexión de comunicación de datos a un tipo correspondiente de línea telefónica. Como otro ejemplo, la interfaz 818 de comunicación puede ser una tarjeta de red de área local (LAN) para proporcionar una conexión de comunicación de datos a una LAN compatible (o un componente de WAN para comunicarse con una WAN). También se pueden implementar enlaces inalámbricos. En cualquier implementación de este tipo, la interfaz 818 de comunicación envía y recibe señales eléctricas, electromagnéticas u ópticas que transportan flujos de datos digitales que representan diversos tipos de información.

El enlace 820 de red normalmente proporciona comunicación de datos a través de una o más redes a otros dispositivos de datos. Por ejemplo, el enlace 820 de red puede proporcionar una conexión a través de la red 822 local a un ordenador 824 de alojamiento o al equipo de datos operado por un proveedor 826 de servicios de Internet (ISP). El ISP 826 a su vez proporciona servicios de comunicación de datos a través de la red mundial de comunicación de paquetes de datos, ahora comúnmente conocida como "Internet" 828. La red 822 local e Internet 828 utilizan ambas señales eléctricas, electromagnéticas u ópticas que transportan flujos de datos digitales. Las señales a través de las diversas redes y las señales en el enlace 820 de red y a través de la interfaz 818 de comunicación, que transportan los datos digitales hacia y desde el sistema 800 informático, son formas ejemplares de medios de transmisión.

El sistema 800 informático puede enviar mensajes y recibir datos, incluido el código del programa, a través de la(s) red(es), del enlace 820 de red y de la interfaz 818 de comunicación. En el ejemplo de Internet, un servidor 830 podría transmitir un código solicitado para un programa de aplicación a través de Internet 828, del ISP 826, de la red 822 local y de la interfaz 818 de comunicación.

El código recibido puede ser ejecutado por el procesador 804 a medida que se recibe, y/o almacenado en el dispositivo 810 de almacenamiento, o en otro almacenamiento no volátil para su posterior ejecución.

Como se describió anteriormente, en diversas realizaciones, un usuario puede acceder a cierta funcionalidad a través de un visor basado en la web (tal como un navegador web) u otro programa de software adecuado. En tales implementaciones, la interfaz de usuario puede ser generada por un sistema informático del servidor y transmitida a un navegador web del usuario (por ejemplo, ejecutándose en el sistema informático del usuario). Alternativamente, el sistema informático del servidor puede proporcionar los datos (por ejemplo, datos de la interfaz de usuario) necesarios para generar la interfaz de usuario al navegador, donde la interfaz de usuario puede generarse (por ejemplo, los datos de la interfaz de usuario pueden ser ejecutados por un navegador que accede a un servicio web y puede configurarse para representar las interfaces de usuario en función de los datos de la interfaz de usuario). El usuario puede entonces interactuar con la interfaz de usuario a través del navegador web. Las interfaces de usuario de ciertas implementaciones pueden ser accesibles a través de una o más aplicaciones de software dedicadas. En ciertas realizaciones, uno o más de los dispositivos y/o sistemas informáticos de la descripción pueden incluir dispositivos informáticos móviles, y las interfaces de usuario pueden ser accesibles a través de dichos dispositivos informáticos móviles (por ejemplo, teléfonos inteligentes y/o tabletas). En una realización de ejemplo, cuando se configura como dispositivo 150 de monitoreo, el sistema 800 informático aloja un servidor web que sirve una interfaz de usuario basada en HTML a los analistas que se conectan a través de un dispositivo remoto.

Se pueden hacer muchas variaciones y modificaciones a las realizaciones descritas anteriormente, cuyos elementos deben entenderse como pertenecientes a otros ejemplos aceptables. Todas estas modificaciones y variaciones están destinadas a ser incluidas en el presente documento dentro del alcance de esta descripción. La descripción anterior detalla ciertas realizaciones. Sin embargo, se apreciará que no importa cuán detallado aparezca lo anterior en el texto, los sistemas y métodos se pueden emplear de muchas maneras. Como también se indicó anteriormente, debe tenerse en cuenta que el uso de una terminología particular al describir ciertas características o aspectos de los sistemas y métodos no debe implicar que la terminología se está redefiniendo en el presente documento para restringirla a la inclusión de características específicas de elementos o aspectos de los sistemas y métodos con los que está asociada esa terminología.

El lenguaje condicional, tal como, entre otros, "puede", "podría", o "pudiera", a menos que se indique específicamente lo contrario, o se entienda de otro modo dentro del contexto tal como se usa, generalmente pretende transmitir que ciertas realizaciones incluyen, mientras que otras realizaciones no incluyen, ciertas características, elementos y/o pasos. Por lo tanto, dicho lenguaje condicional generalmente no pretende implicar que las características, los elementos y/o los pasos sean de alguna manera necesarios para una o más realizaciones o que una o más realizaciones necesariamente incluyan lógica para decidir, con o sin entrada o solicitud del usuario, si estas características, elementos y/o pasos están incluidos o deben realizarse en cualquier realización particular.

El término "sustancialmente" cuando se usa junto con el término "en tiempo real" forma una frase que será entendida fácilmente por un experto en la técnica. Por ejemplo, se entiende fácilmente que dicho lenguaje incluirá velocidades en las que no se puede percibir si hay o no un retraso o espera, o donde dicho retraso es lo suficientemente corto como para no ser disruptivo, irritante o, de otro modo, molesto para el usuario.

El lenguaje conjunto tal como la frase "al menos uno de X, Y y Z" o "al menos uno de X, Y o Z", a menos que se indique específicamente lo contrario, debe entenderse con el contexto tal como se utiliza en general para transmitir que un elemento, término, etc. puede ser X, Y o Z, o una combinación de los mismos. Por ejemplo, el término "o" se usa en su sentido inclusivo (y no en su sentido exclusivo) de modo que cuando se usa, por ejemplo, para conectar una lista de elementos, el término "o" significa uno, algunos o todos los elementos de la lista. Por lo tanto, dicho lenguaje conjuntivo generalmente no implica que ciertas realizaciones requieran que al menos uno de X, al menos uno de Y, y al menos uno de Z estén presentes.

El término "un", "una", "uno" como se usa en el presente documento debe recibir una interpretación inclusiva en lugar de exclusiva. Por ejemplo, a menos que se indique específicamente, el término "un", "una", "uno" no debe

entenderse como "exactamente uno" o "uno y solo uno"; en cambio, el término "un", "una", "uno" significa "uno o más" o "al menos uno", ya sea que se use en las reivindicaciones o en otra parte de la especificación e independientemente de los usos de cuantificadores tales como "al menos uno", "uno o más" o "una pluralidad" en otra parte de las reivindicaciones o de las especificaciones.

El término "que comprende" como se usa en el presente documento debe recibir una interpretación inclusiva en lugar de exclusiva. Por ejemplo, un ordenador de propósito general que comprende uno o más procesadores no debe interpretarse como excluyente de otros componentes del ordenador, y posiblemente puede incluir componentes tales como memoria, dispositivos de entrada/salida y/o interfaces de red, entre otros.

Si bien la descripción detallada anterior ha mostrado, descrito y señalado características novedosas aplicadas a diversas realizaciones, puede entenderse que se pueden haber hecho diversas omisiones, sustituciones y cambios en la forma y en los detalles de los dispositivos o procesos ilustrados. Como puede reconocerse, ciertas realizaciones de las invenciones descritas en el presente documento pueden realizarse en una forma que no proporciona todas las características y beneficios establecidos en el presente documento, ya que algunas características pueden usarse o emplearse por separado de otras. El alcance de ciertas invenciones descritas en el presente documento se indica mediante las reivindicaciones adjuntas más que por la descripción anterior. Todos los cambios que entran dentro del significado y rango de equivalencia de las reclamaciones deben ser incluidos dentro de su alcance.

REIVINDICACIONES

1. Un sistema informático configurado para generar una alerta relacionada con un ataque cibernético contra un recurso, comprendiendo el sistema informático:

un medio (810) de almacenamiento legible por ordenador que tiene instrucciones de programa incorporadas en el mismo; y

uno o más procesadores (804) configurados para ejecutar las instrucciones del programa para hacer que uno o más procesadores:

reciban (202) información contextual sobre un recurso, comprendiendo la información contextual información sobre qué usuarios tienen permitido acceder al recurso, información sobre patrones de solicitud de control de hardware ordinarios, información sobre patrones de uso típicos del recurso por usuario autorizado o una política de acceso, localización física o localización del recurso en la topología de red del recurso;

reciban (204) una primera pluralidad de indicadores asociados con una actividad que se realiza en una red informática;

cotejen (206), en base al menos en parte a la información contextual, la primera pluralidad de indicadores con reglas que corresponden a diferentes tipos de actividad que son indicativos de un ataque cibernético contra el recurso para formar un conjunto de eventos que reflejan dicha actividad;

determinen (210), en base al menos en parte al conjunto de eventos y la información contextual, una puntuación del riesgo para cada evento, en donde la puntuación del riesgo indica una probabilidad de que el recurso esté en riesgo por el evento de un ataque cibernético;

comparen (212) la puntuación del riesgo para un evento con un valor umbral, en donde el valor umbral se basa al menos en parte en un valor aleatorio; y

si la puntuación del riesgo para un evento excede el umbral, generen (214) una alerta.

2. El sistema informático de la reivindicación 1 o de la reivindicación 2, en donde los -uno o más- procesadores están configurados además para ejecutar las instrucciones del programa para hacer que uno o más procesadores:

generen una pluralidad de alertas basadas en uno o más eventos que satisfagan uno o más valores umbral; y

presenten la pluralidad de alertas en un orden que está determinado al menos parcialmente por la puntuación del riesgo respectiva de la pluralidad de alertas.

3. El sistema informático de cualquier reivindicación precedente, en donde los -uno o más- procesadores están configurados además para ejecutar las instrucciones del programa para hacer que los -uno o más- procesadores:

hagan que la alerta se presente utilizando una interfaz gráfica de usuario que comprende una representación de la puntuación del riesgo para el recurso.

4. El sistema informático de la reivindicación 3, en donde la interfaz gráfica de usuario comprende además una representación de una puntuación del riesgo total de una pluralidad de recursos, en donde la puntuación del riesgo total se determina combinando las puntuaciones del riesgo de la pluralidad de recursos.

5. El sistema informático de la reivindicación 4, en donde los -uno o más- procesadores están configurados además para ejecutar las instrucciones del programa para hacer que los -uno o más- procesadores combinen las puntuaciones del riesgo de la pluralidad de recursos usando una función monotónicamente convergente.

6. El sistema informático de cualquier reivindicación precedente, en donde los -uno o más- procesadores están configurados además para ejecutar las instrucciones del programa para hacer que los -uno o más- procesadores:

registren una o más interacciones entre un usuario y el sistema de advertencia.

7. El sistema informático de cualquier reivindicación precedente, en donde los -uno o más- procesadores están configurados además para ejecutar las instrucciones del programa para hacer que los -uno o más- procesadores:

reciban una entrada de comentario de un usuario;

asocien la entrada con una o más alertas; y hagan que se presente la entrada junto con las -una o más- alertas.

8. El sistema informático de cualquier reivindicación precedente, en donde los -uno o más- procesadores están configurados además para ejecutar las instrucciones del programa para hacer que los -uno o más- procesadores:

generen una pluralidad de alertas integradas en una visualización de cuadro o gráfico.

9. El sistema informático de la reivindicación 8, en donde los -uno o más- procesadores están configurados además para ejecutar las instrucciones del programa para hacer que los -uno o más- procesadores: integren en el cuadro o gráfico una pluralidad de eventos relacionados con un posible ataque cibernético contra el recurso y para el que no se ha generado ninguna alerta.

10. El sistema informático de la reivindicación 9, en donde los -uno o más- procesadores están configurados además para ejecutar las instrucciones del programa para hacer que los -uno o más- procesadores incluyan adicionalmente en el cuadro o gráfico las alertas históricas que previamente han sido respondidas por un analista.

11. Un método para generar una alerta relacionada con un ataque cibernético contra un recurso, comprendiendo el método: ejecutar instrucciones del programa mediante uno o más procesadores (804):

recibir (202) información contextual sobre un recurso, comprendiendo la información contextual información sobre qué usuarios pueden acceder al recurso, información sobre patrones de solicitud de control de hardware ordinarios, información sobre patrones de uso típicos del recurso por parte de un usuario autorizado o una política de acceso, localización física o localización en la topología de red del recurso;

recibir (204) una primera pluralidad de indicadores asociados con una actividad que se realiza en una red informática;

cotejar (206), en base al menos en parte a la información contextual, la primera pluralidad de indicadores con reglas que corresponden a diferentes tipos de actividad que son indicativos de un ataque cibernético contra el recurso para formar un conjunto de eventos que reflejen dicha actividad;

determinar (210), en base al menos en parte al conjunto de eventos y a la información contextual, una puntuación del riesgo para cada evento, en donde la puntuación del riesgo indica una probabilidad de que el recurso esté en riesgo por el evento de un ataque cibernético;

comparar (212) la puntuación del riesgo para un evento con un valor umbral, en donde el valor umbral se basa al menos en parte en un valor aleatorio; y

si la puntuación del riesgo para un evento excede el umbral, generar (214) una alerta.

12. Un programa informático que comprende instrucciones para hacer que uno o más dispositivos informáticos realicen un método según la reivindicación 11.

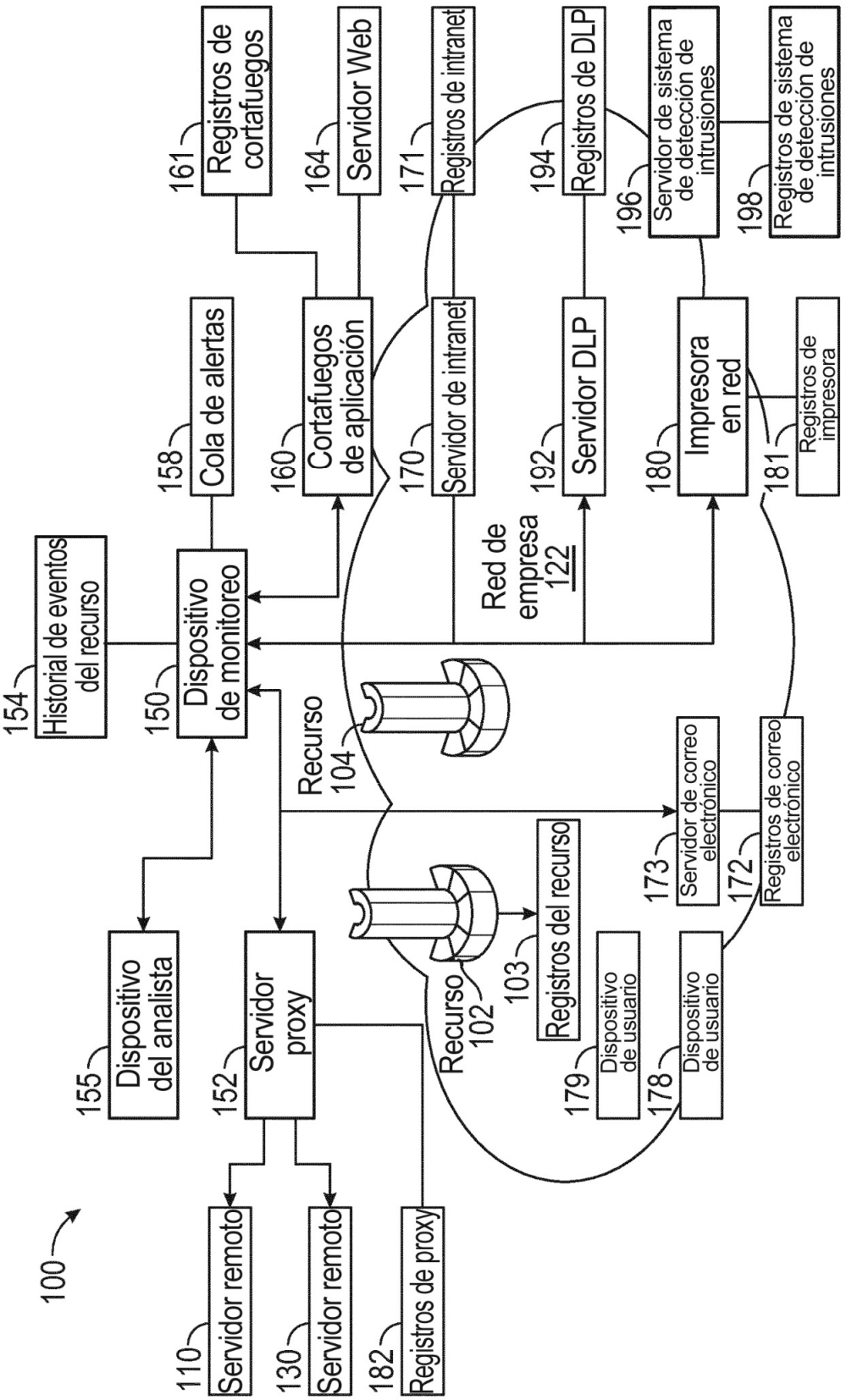

100
110 Servidor remoto
130 Servidor remoto
182 Registros de proxy
155 Dispositivo del analista
152 Servidor proxy
Recurso 102
103 Registros del recurso
179 Dispositivo de usuario
178 Dispositivo de usuario
173 Servidor de correo electrónico
172 Registros de correo electrónico
Recurso 104
154 Historial de eventos del recurso
150 Dispositivo de monitoreo
158 Cola de alertas
160 Cortafuegos de aplicación
170 Servidor de intranet
192 Servidor DLP
180 Impresora en red
181 Registros de impresora
Red de empresa 122
161 Registros de cortafuegos
164 Servidor Web
171 Registros de intranet
194 Registros de DLP
196 Servidor de sistema de detección de intrusiones
198 Registros de sistema de detección de intrusiones

FIG. 1A

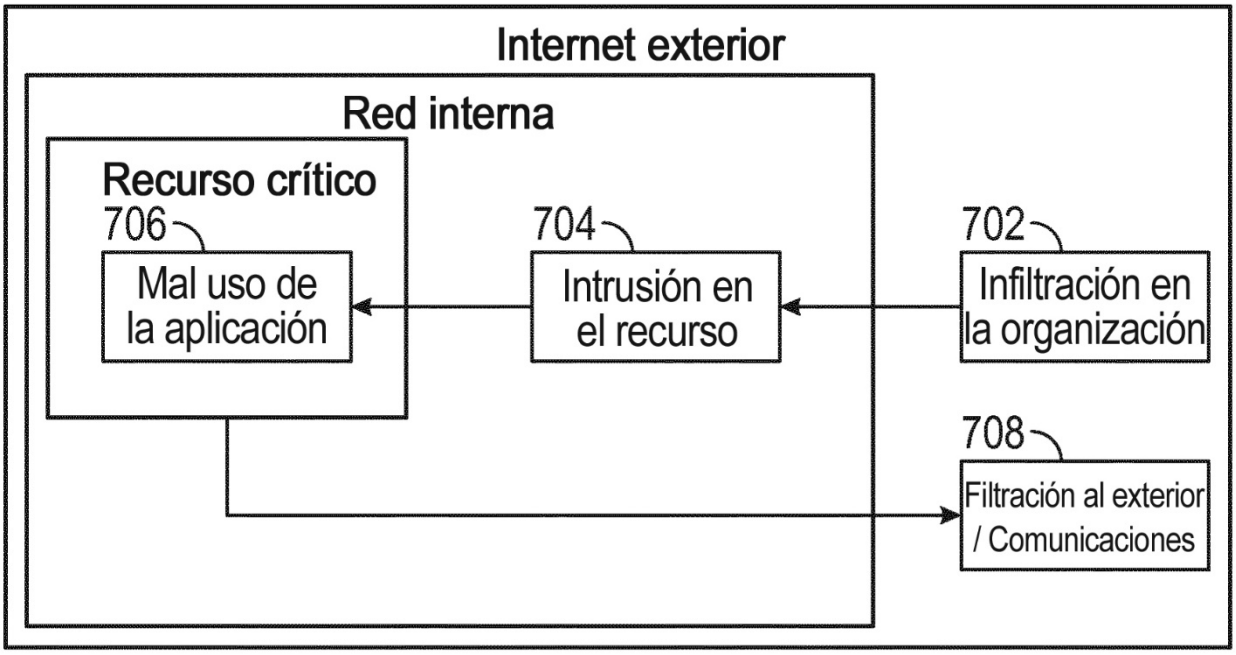

Internet exterior
Red interna
Recurso crítico
706
Mal uso de la aplicación
704
Intrusión en el recurso
702
Infiltración en la organización
708
Filtración al exterior / Comunicaciones

FIG. 1B

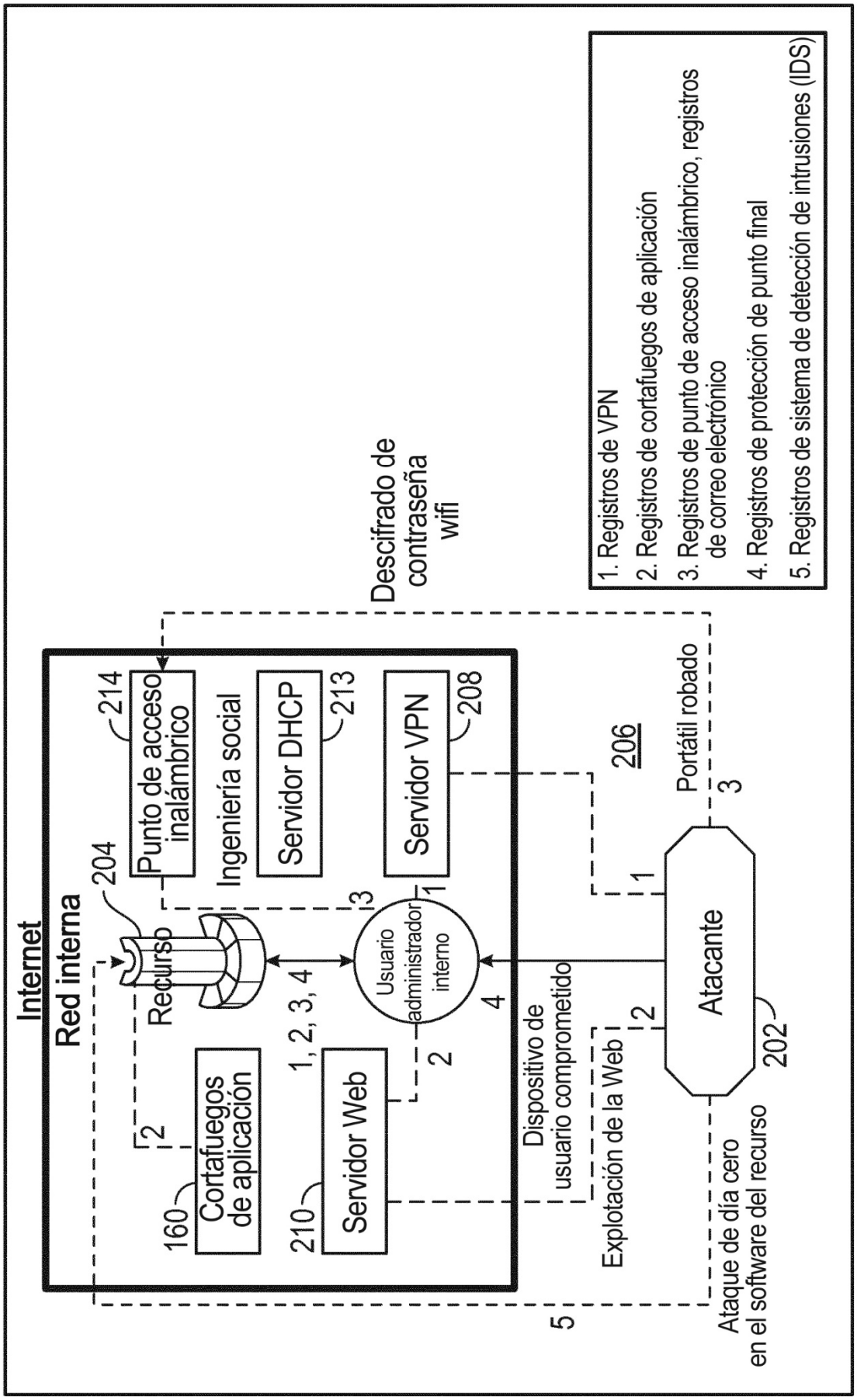

Internet
Red interna
204
Punto de acceso inalámbrico
214
Ingeniería social
Servidor DHCP
213
Servidor VPN
208
Recurso
1, 2, 3, 4
Usuario administrador interno
3
1
2
4
160
Cortafuegos de aplicación
210
Servidor Web
Dispositivo de usuario comprometido
206
Explotación de la Web I
Portátil robado
Atacante
202
Ataque de día cero en el software del recurso
5
Descifrado de contraseña wifi
1. Registros de VPN
2. Registros de cortafuegos de aplicación
3. Registros de punto de acceso inalámbrico, registros de correo electrónico
4. Registros de protección de punto final
5. Registros de sistema de detección de intrusiones (IDS)

FIG. 1C

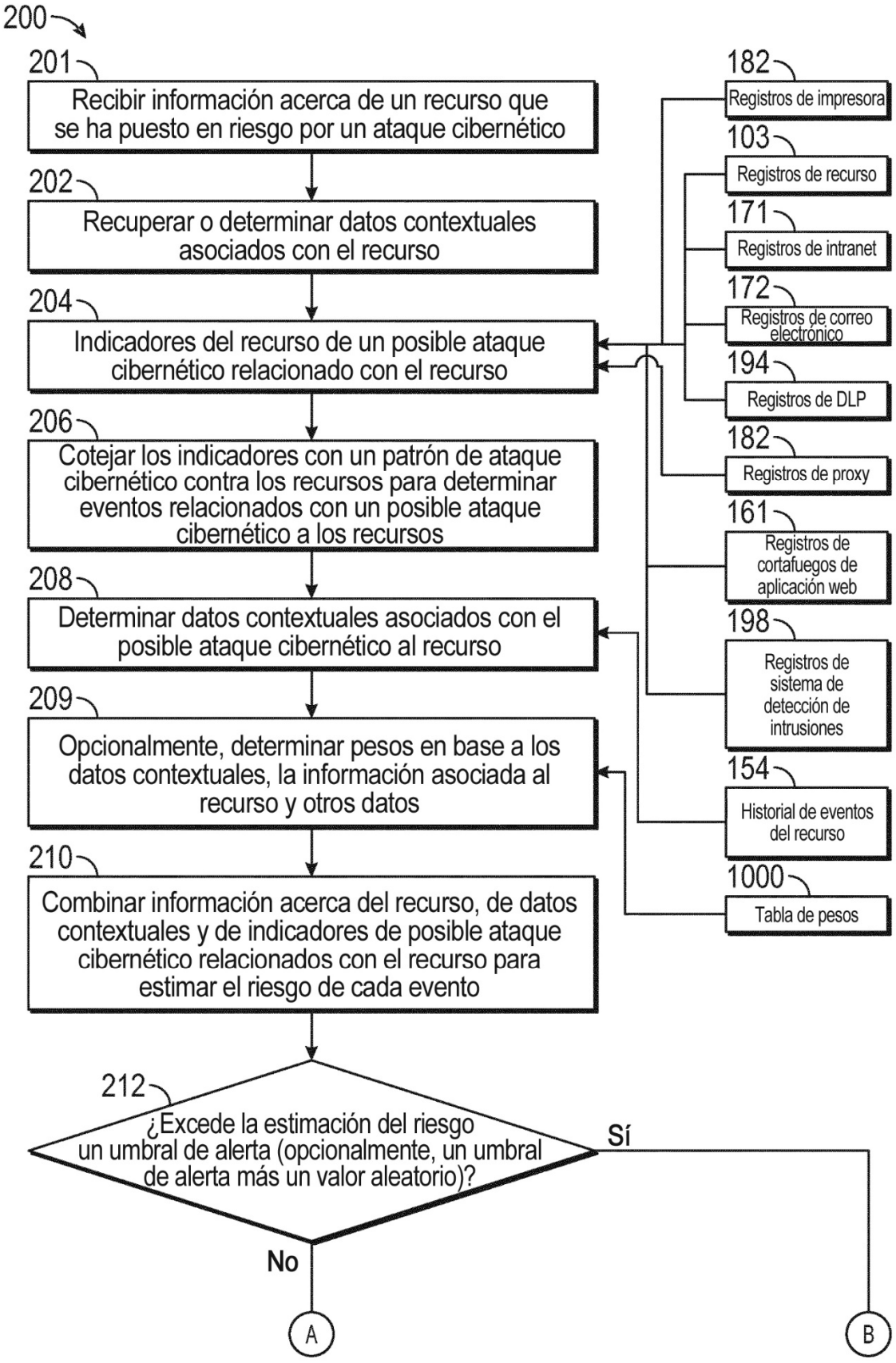

200
201
Recibir información acerca de un recurso que se ha puesto en riesgo por un ataque cibernético
202
Recuperar o determinar datos contextuales asociados con el recurso
204
Indicadores del recurso de un posible ataque cibernético relacionado con el recurso
206
Cotejar los indicadores con un patrón de ataque cibernético contra los recursos para determinar eventos relacionados con un posible ataque cibernético a los recursos
208
Determinar datos contextuales asociados con el posible ataque cibernético al recurso
209
Opcionalmente, determinar pesos en base a los datos contextuales, la información asociada al recurso y otros datos
210
Combinar información acerca del recurso, de datos contextuales y de indicadores de posible ataque cibernético relacionados con el recurso para estimar el riesgo de cada evento
212
¿Excede la estimación del riesgo un umbral de alerta (opcionalmente, un umbral de alerta más un valor aleatorio)?
Sí
No
A
B
182
Registros de impresora
103
Registros de recurso
171
Registros de intranet
172
Registros de correo electrónico
194
Registros de DLP
182
Registros de proxy
161
Registros de cortafuegos de aplicación web
198
Registros de sistema de detección de intrusiones
154
Historial de eventos del recurso
1000
Tabla de pesos

FIG. 2

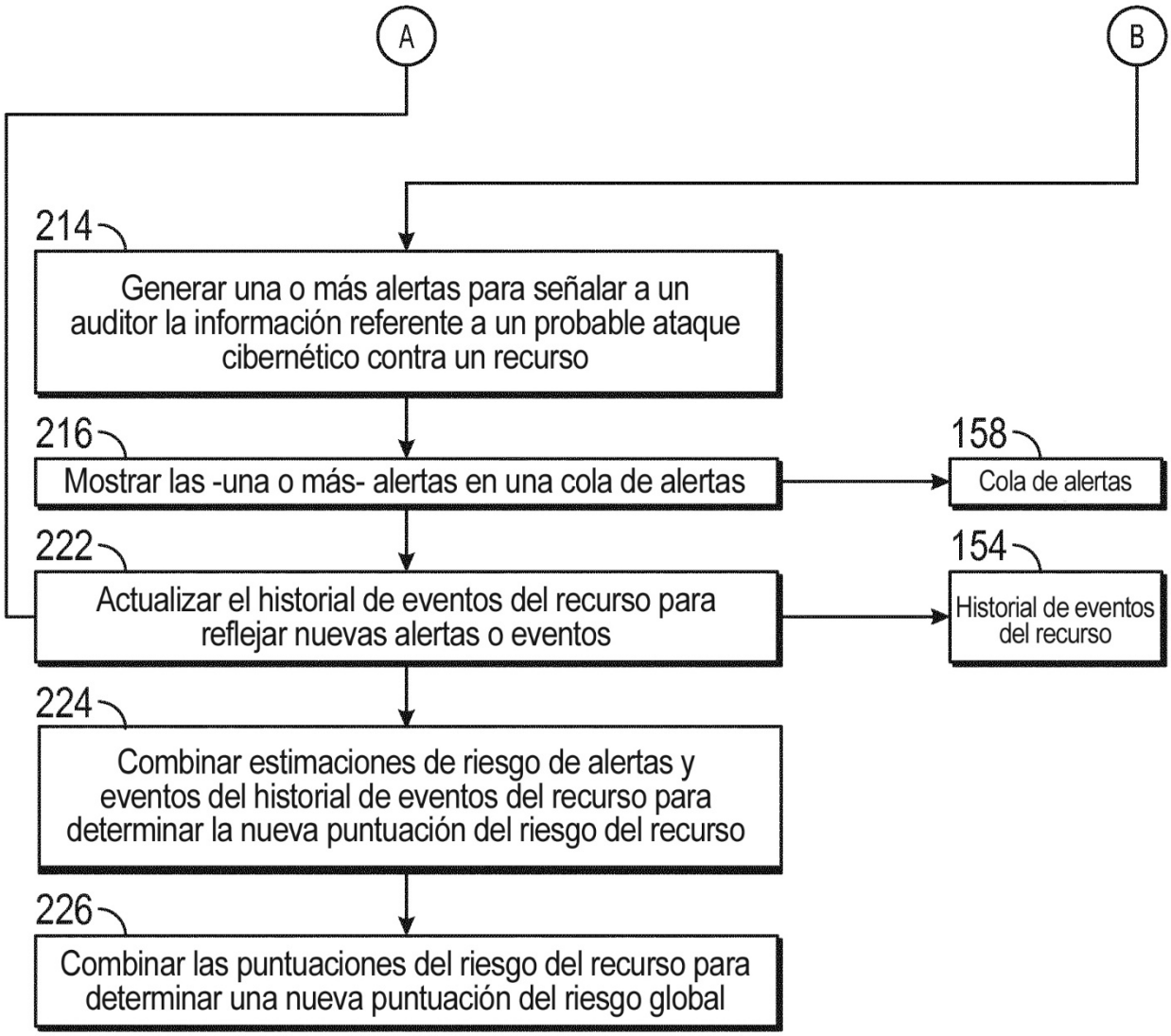


FIG. 2
(Continuación)

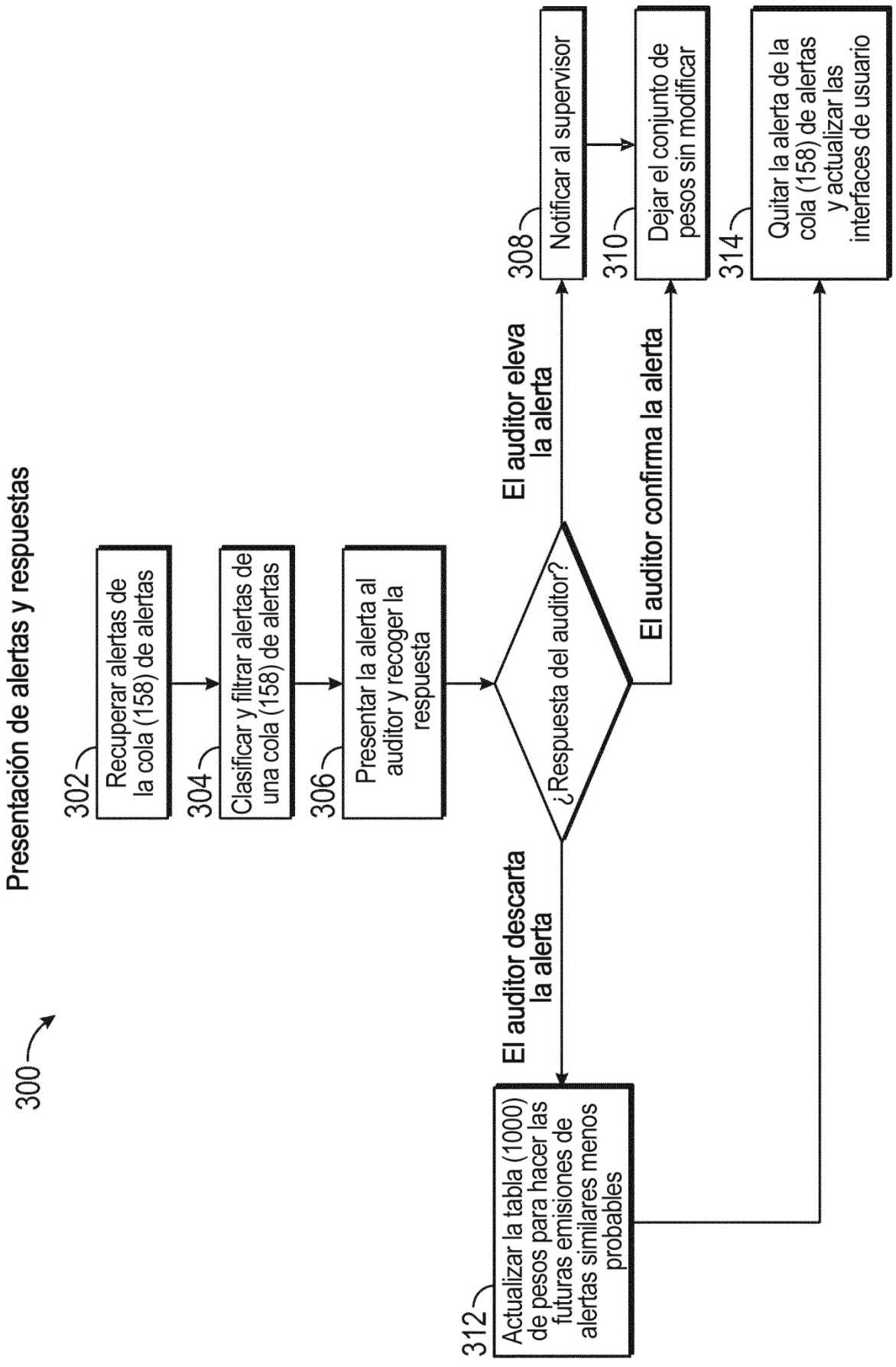

Presentación de alertas y respuestas
300
302
Recuperar alertas de la cola (158) de alertas
304
Clasificar y filtrar alertas de una cola (158) de alertas
306
Presentar la alerta al auditor y recoger la respuesta
¿Respuesta del auditor?
El auditor eleva la alerta
El auditor confirma la alerta
El auditor descarta la alerta
308
Notificar al supervisor
310
Dejar el conjunto de pesos sin modificar
312
Actualizar la tabla (1000) de pesos para hacer las futuras emisiones de alertas similares menos probables
314
Quitar la alerta de la cola (158) de alertas y actualizar las interfaces de usuario

FIG. 3

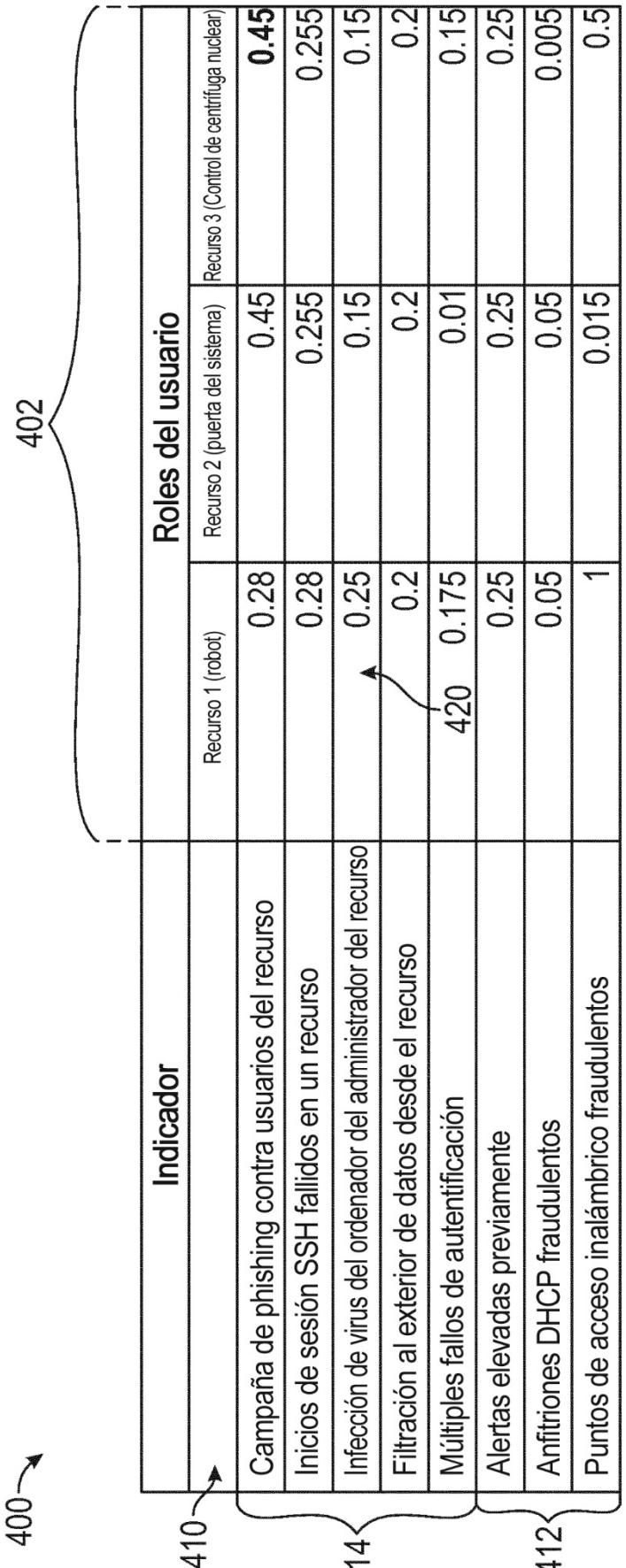
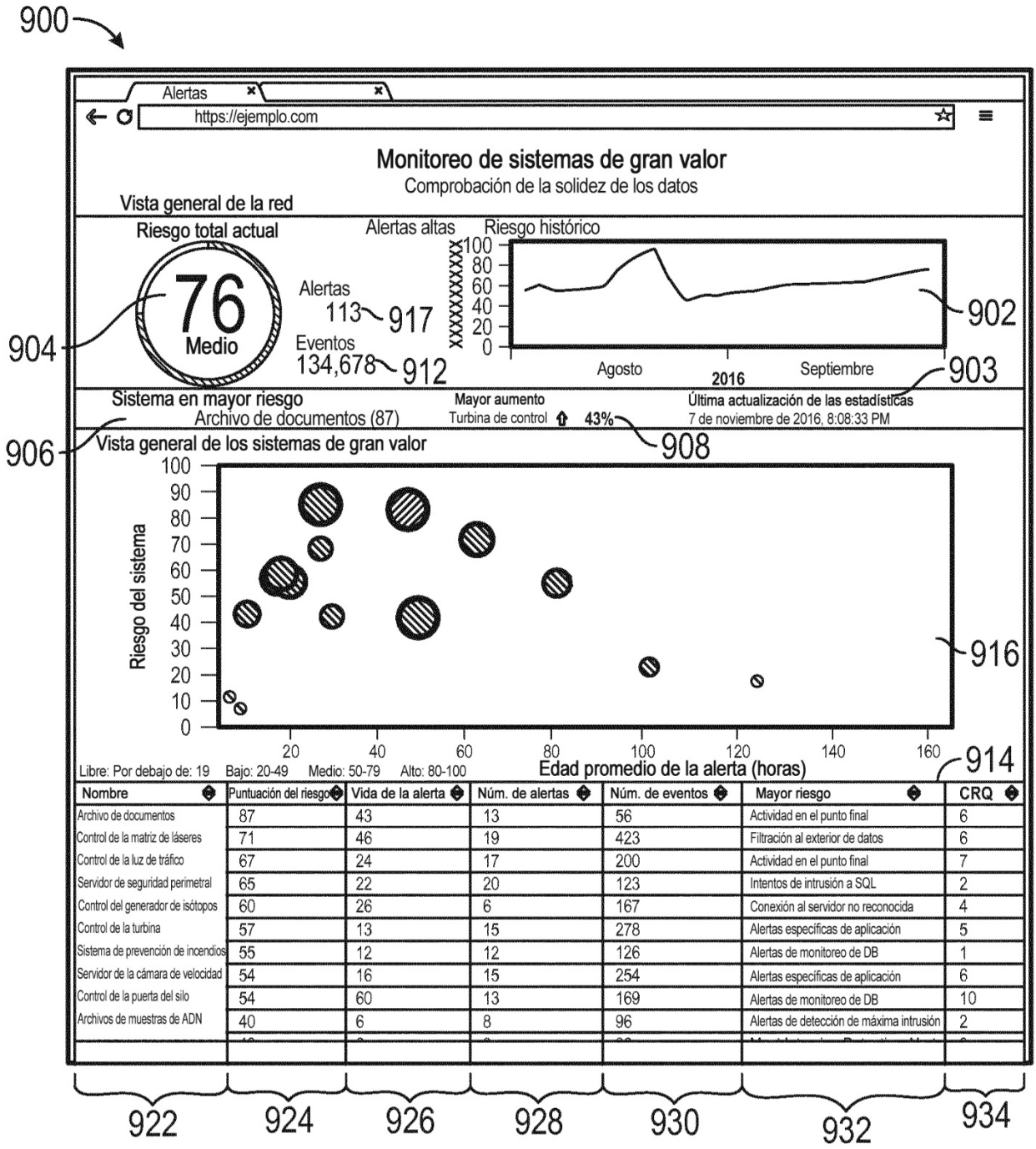

400
402
410
414
412
420
Indicador
Roles del usuario
Recurso 1 (robot)
Recurso 2 (puerta del sistema)
Recurso 3 (Control de centrífuga nuclear)
Campaña de phishing contra usuarios del recurso
0.28
0.45
0.45
Inicios de sesión SSH fallidos en un recurso
0.28
0.255
0.255
Infección de virus del ordenador del administrador del recurso
0.25
0.15
0.15
Filtración al exterior de datos desde el recurso
0.2
0.2
0.2
Múltiples fallos de autentificación
0.175
0.01
0.15
Alertas elevadas previamente
0.25
0.25
0.25
Anfitriones DHCP fraudulentos
0.05
0.05
0.005
Puntos de acceso inalámbrico fraudulentos
1
0.015
0.5

FIG. 4



Nombre	Puntuación del riesgo	Vida de la alerta	Núm. de alertas	Núm. de eventos	Mayor riesgo	CRQ
Archivo de documentos	87	43	13	56	Actividad en el punto final	6
Control de la matriz de láseres	71	46	19	423	Filtración al exterior de datos	6
Control de la luz de tráfico	67	24	17	200	Actividad en el punto final	7
Servidor de seguridad perimetral	65	22	20	123	Intentos de intrusión a SQL	2
Control del generador de isótopos	60	26	6	167	Conexión al servidor no reconocida	4
Control de la turbina	57	13	15	278	Alertas específicas de aplicación	5
Sistema de prevención de incendios	55	12	12	126	Alertas de monitoreo de DB	1
Servidor de la cámara de velocidad	54	16	15	254	Alertas específicas de aplicación	6
Control de la puerta del silo	54	60	13	169	Alertas de monitoreo de DB	10
Archivos de muestras de ADN	40	6	8	96	Alertas de detección de máxima intrusión	2

FIG. 5

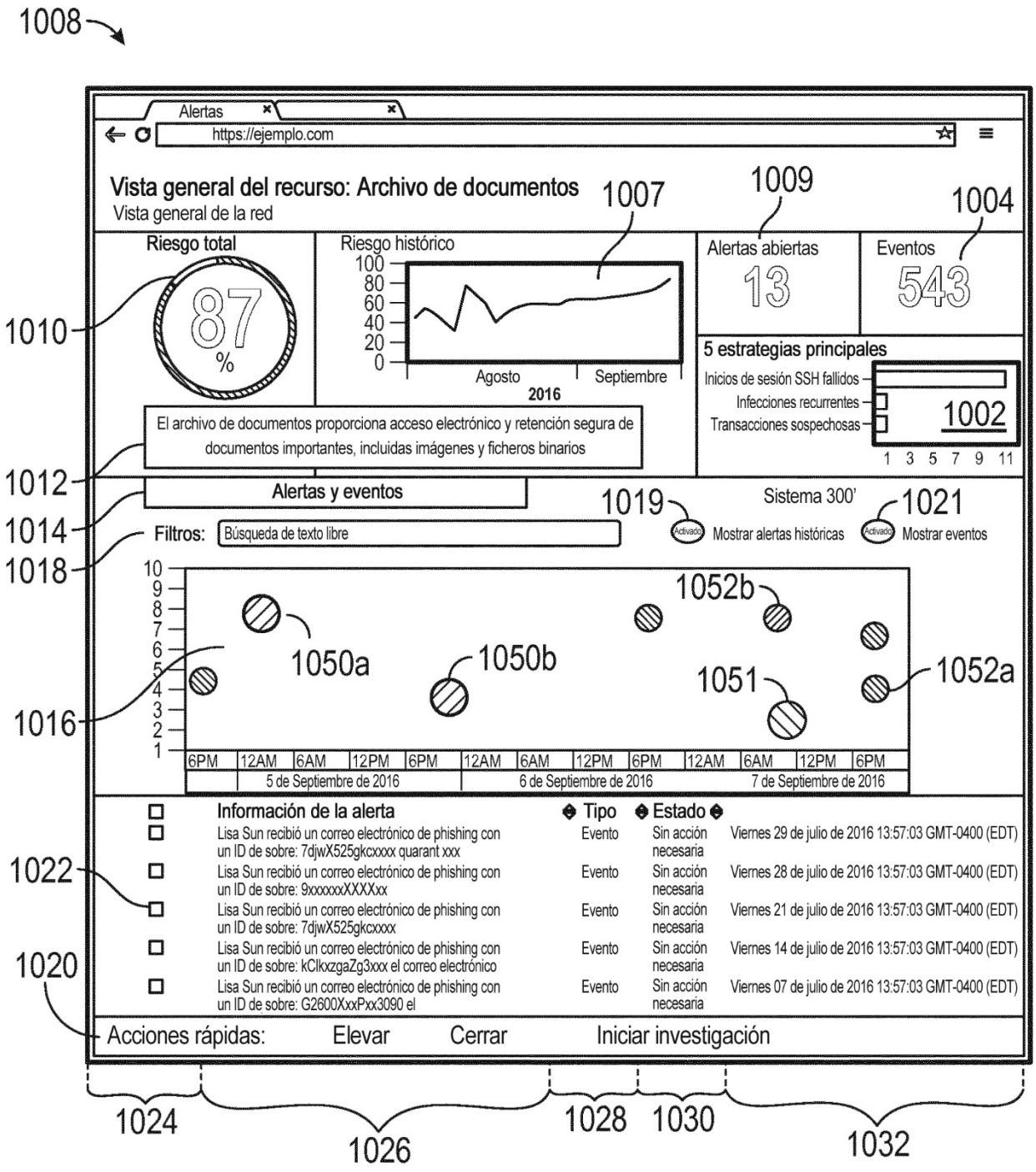

1008
Alertas
https://ejemplo.com
Vista general del recurso: Archivo de documentos
Vista general de la red
1007
1009
1004
Riesgo total
87
%
1010
Riesgo histórico
100
80
60
40
20
0
Agosto
Septiembre
2016
Alertas abiertas
13
Eventos
543
5 estrategias principales
Inicios de sesión SSH fallidos
Infecciones recurrentes
Transacciones sospechosas
1002
1 3 5 7 9 11
El archivo de documentos proporciona acceso electrónico y retención segura de documentos importantes, incluidas imágenes y ficheros binarios
1012
Alertas y eventos
1014
Filtros:
Búsqueda de texto libre
1018
1019
Activado
Mostrar alertas históricas
Sistema 300'
1021
Activado
Mostrar eventos
10
9
8
7
6
5
4
3
2
1
1016
1050a
1050b
1052b
1051
1052a
6PM 12AM 6AM 12PM 6PM 12AM 6AM 12PM 6PM 12AM 6AM 12PM 6PM
5 de Septiembre de 2016
6 de Septiembre de 2016
7 de Septiembre de 2016
Información de la alerta
Tipo
Estado
1022
Lisa Sun recibió un correo electrónico de phishing con un ID de sobre: 7djwX525gkcxxxx quarant xxx
Evento
Sin acción necesaria
Viernes 29 de julio de 2016 13:57:03 GMT-0400 (EDT)
Lisa Sun recibió un correo electrónico de phishing con un ID de sobre: 9xxxxxxXXXXxx
Evento
Sin acción necesaria
Viernes 28 de julio de 2016 13:57:03 GMT-0400 (EDT)
Lisa Sun recibió un correo electrónico de phishing con un ID de sobre: 7djwX525gkcxxxx
Evento
Sin acción necesaria
Viernes 21 de julio de 2016 13:57:03 GMT-0400 (EDT)
Lisa Sun recibió un correo electrónico de phishing con un ID de sobre: kClkxzgaZg3xxx el correo electrónico
Evento
Sin acción necesaria
Viernes 14 de julio de 2016 13:57:03 GMT-0400 (EDT)
Lisa Sun recibió un correo electrónico de phishing con un ID de sobre: G2600XxxPxx3090 el
Evento
Sin acción necesaria
Viernes 07 de julio de 2016 13:57:03 GMT-0400 (EDT)
1020
Acciones rápidas:
Elevar
Cerrar
Iniciar investigación
1024
1026
1028
1030
1032

FIG. 6

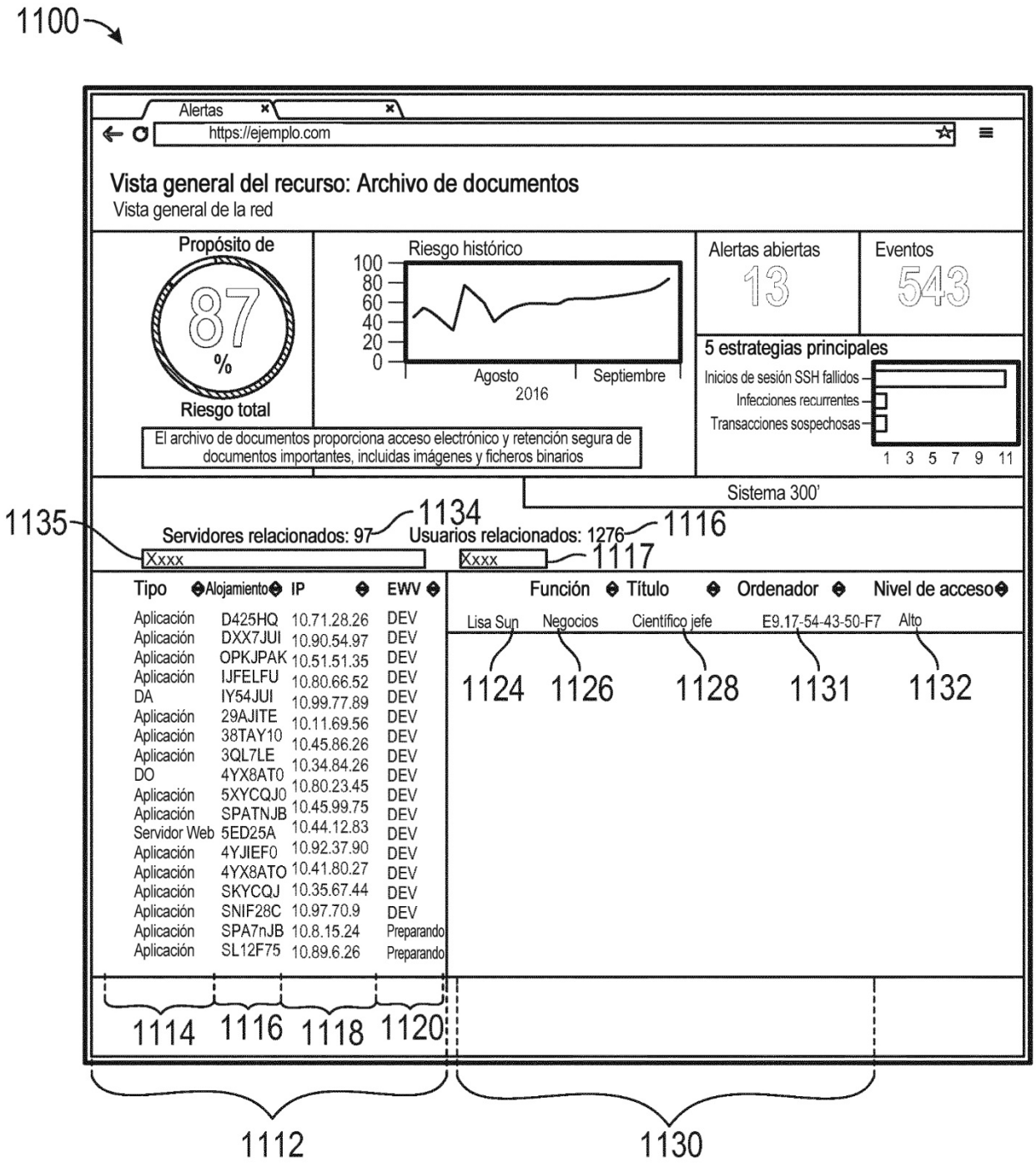

1100
Alertas
https://ejemplo.com
Vista general del recurso: Archivo de documentos
Vista general de la red
Propósito de
87
%
Riesgo total
Riesgo histórico
100
80
60
40
20
0
Agosto
Septiembre
2016
Alertas abiertas
13
Eventos
543
5 estrategias principales
Inicios de sesión SSH fallidos
Infecciones recurrentes
Transacciones sospechosas
1 3 5 7 9 11
El archivo de documentos proporciona acceso electrónico y retención segura de documentos importantes, incluidas imágenes y ficheros binarios
Sistema 300'
1135
Servidores relacionados: 97
1134
Usuarios relacionados: 1276
1116
Xxxx
Xxxx
1117
Tipo
Alojamiento
IP
EWV
Función
Título
Ordenador
Nivel de acceso
Aplicación D425HQ 10.71.28.26 DEV
Aplicación DXX7JUI 10.90.54.97 DEV
Aplicación OPKJPAK 10.51.51.35 DEV
Aplicación IJFELFU 10.80.66.52 DEV
DA IY54JUI 10.99.77.89 DEV
Aplicación 29AJITE 10.11.69.56 DEV
Aplicación 38TAY10 10.45.86.26 DEV
Aplicación 3QL7LE 10.34.84.26 DEV
DO 4YX8AT0 10.80.23.45 DEV
Aplicación 5XYCQJ0 10.45.99.75 DEV
Aplicación SPATNJB 10.44.12.83 DEV
Servidor Web 5ED25A 10.92.37.90 DEV
Aplicación 4YJIEF0 10.41.80.27 DEV
Aplicación 4YX8ATO 10.35.67.44 DEV
Aplicación SKYCQJ 10.97.70.9 DEV
Aplicación SNIF28C 10.8.15.24 Preparando
Aplicación SPA7nJB 10.89.6.26 Preparando
Aplicación SL12F75
Lisa Sun
Negocios
Científico jefe
E9.17-54-43-50-F7
Alto
1124
1126
1128
1131
1132
1114
1116
1118
1120
1112
1130

FIG. 7

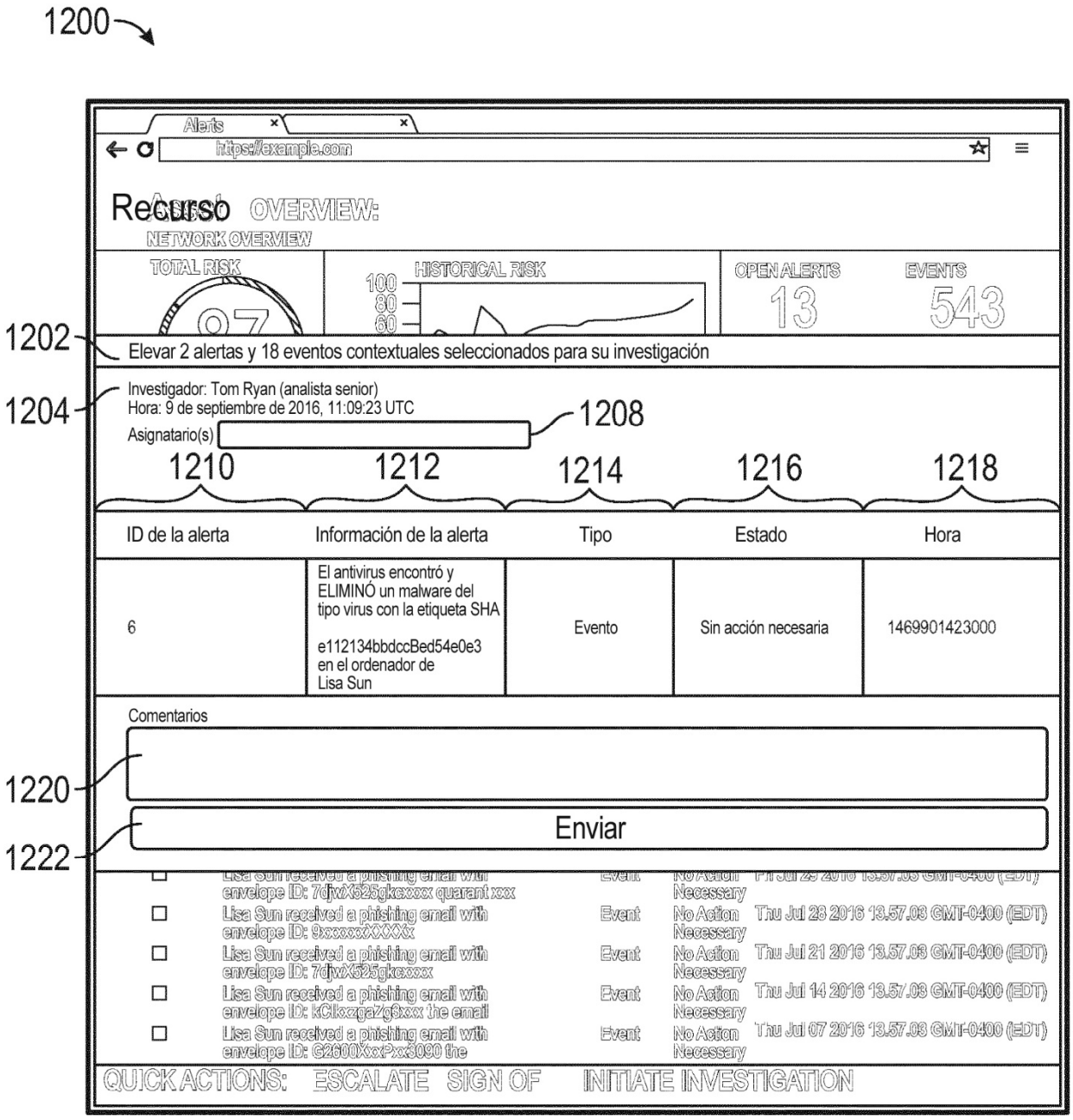

1200
Alerts
https://example.com
Recurso OVERVIEW:
NETWORK OVERVIEW
TOTAL RISK
07
HISTORICAL RISK
100
80
60
OPEN ALERTS
13
EVENTS
543
1202
Elevar 2 alertas y 18 eventos contextuales seleccionados para su investigación
1204
Investigador: Tom Ryan (analista senior)
Hora: 9 de septiembre de 2016, 11:09:23 UTC
Asignatario(s)
1208
1210
1212
1214
1216
1218
ID de la alerta
Información de la alerta
Tipo
Estado
Hora
6
El antivirus encontró y ELIMINÓ un malware del tipo virus con la etiqueta SHA e112134bbdccBed54e0e3 en el ordenador de Lisa Sun
Evento
Sin acción necesaria
1469901423000
Comentarios
1220
Enviar
1222
Lisa Sun received a phishing email with envelope ID: 7djwX525gkexxxx quarant xxx
Event
No Action Necessary
Lisa Sun received a phishing email with envelope ID: 9xxxxxXXXXx
Event
No Action Necessary
Thu Jul 28 2016 13.57.08 GMT-0400 (EDT)
Lisa Sun received a phishing email with envelope ID: 7djwX525gkexxxx
Event
No Action Necessary
Thu Jul 21 2016 13.57.08 GMT-0400 (EDT)
Lisa Sun received a phishing email with envelope ID: kCIkxzgaZg9xxx the email
Event
No Action Necessary
Thu Jul 14 2016 13.57.08 GMT-0400 (EDT)
Lisa Sun received a phishing email with envelope ID: G2600XxxPxx3090 the
Event
No Action Necessary
Thu Jul 07 2016 13.57.08 GMT-0400 (EDT)
QUICK ACTIONS: ESCALATE SIGN OF INITIATE INVESTIGATION

FIG. 8

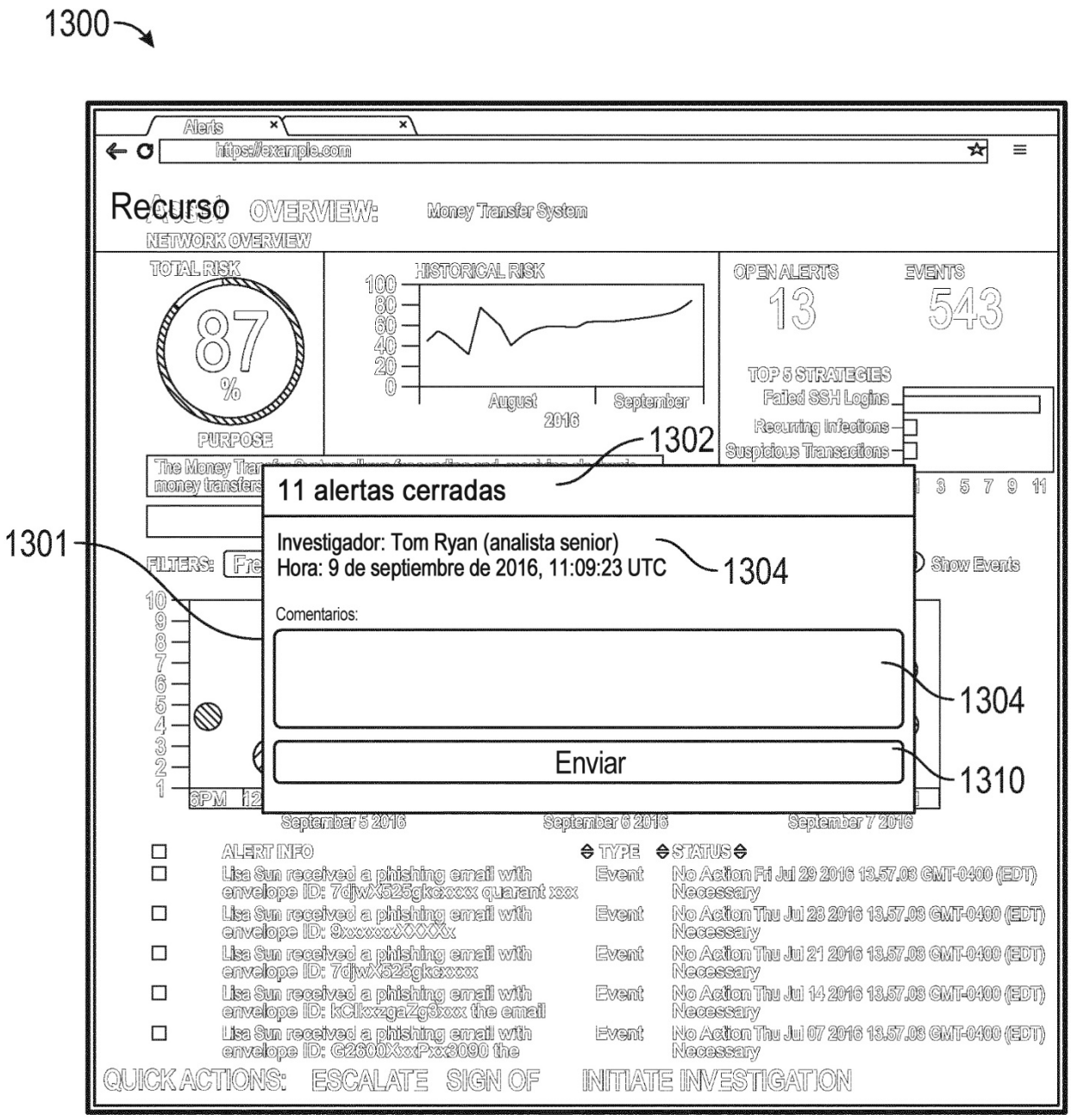

1300
Alerts
https://example.com
Recurso
OVERVIEW:
Money Transfer System
NETWORK OVERVIEW
TOTAL RISK
87
%
PURPOSE
HISTORICAL RISK
100
80
60
40
20
0
August
September
2016
OPEN ALERTS
13
EVENTS
543
TOP 5 STRATEGIES
Failed SSH Logins
Recurring Infections
Suspicious Transactions
1 3 5 7 9 11
1302
11 alertas cerradas
1301
Investigador: Tom Ryan (analista senior)
Hora: 9 de septiembre de 2016, 11:09:23 UTC
1304
Comentarios:
1304
Enviar
1310
FILTERS:
Show Events
10
9
8
7
6
5
4
3
2
1
6PM
September 5 2016
September 6 2016
September 7 2016
ALERT INFO
TYPE
STATUS
Lisa Sun received a phishing email with envelope ID: 7djwX525gkcxxxx quarant xxx
Event
No Action Fri Jul 29 2016 13.57.03 GMT-0400 (EDT) Necessary
Lisa Sun received a phishing email with envelope ID: 9xxxxxXXXXx
Event
No Action Thu Jul 28 2016 13.57.03 GMT-0400 (EDT) Necessary
Lisa Sun received a phishing email with envelope ID: 7djwX525gkcxxxx
Event
No Action Thu Jul 21 2016 13.57.03 GMT-0400 (EDT) Necessary
Lisa Sun received a phishing email with envelope ID: kCIkxzgaZg3xxx the email
Event
No Action Thu Jul 14 2016 13.57.03 GMT-0400 (EDT) Necessary
Lisa Sun received a phishing email with envelope ID: G2600XxxPxx3090 the
Event
No Action Thu Jul 07 2016 13.57.03 GMT-0400 (EDT) Necessary
QUICK ACTIONS: ESCALATE SIGN OF INITIATE INVESTIGATION

FIG. 9

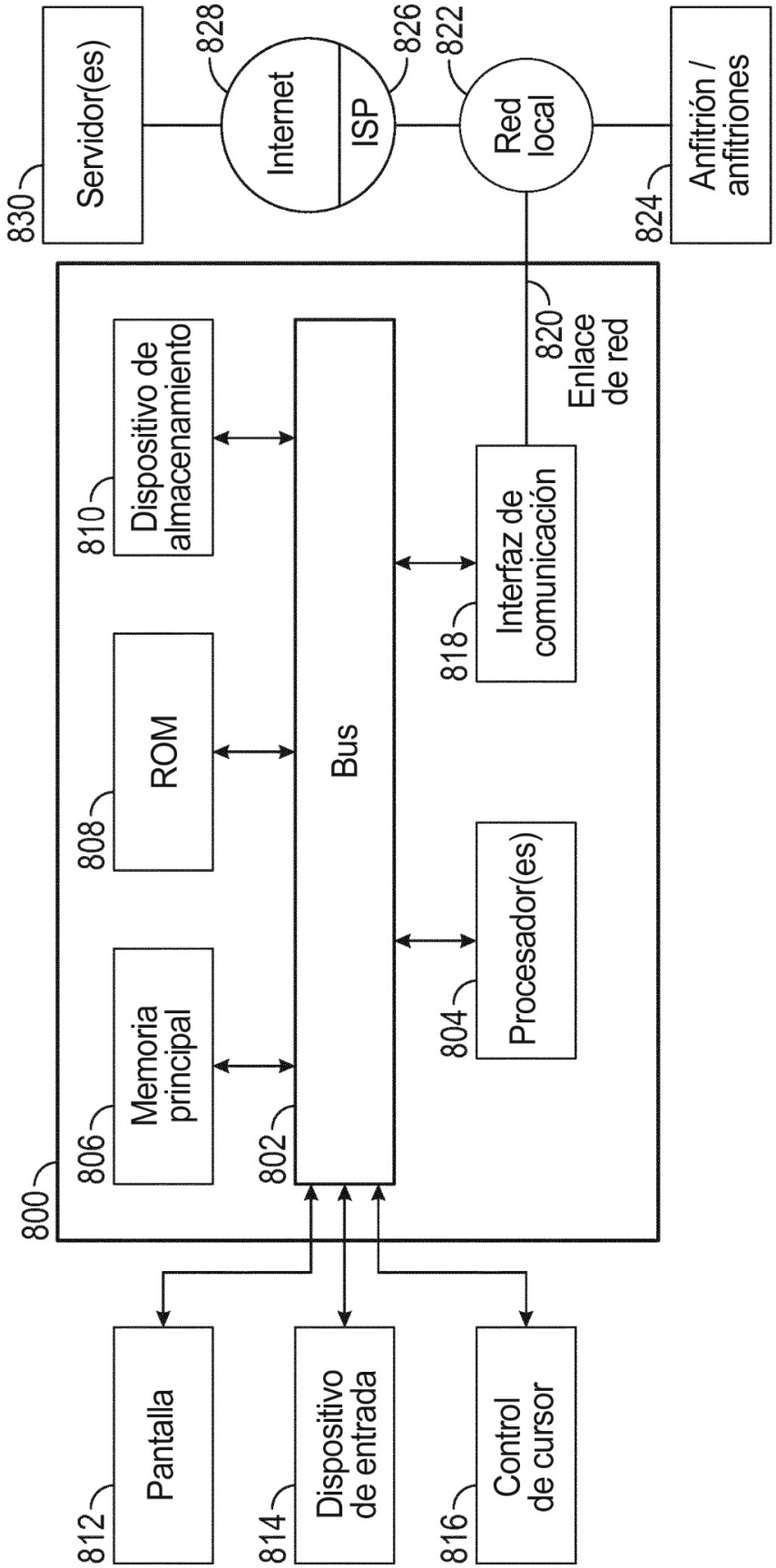

Servidor(es)
830
828
Internet
ISP
826
822
Red local
Anfitrión / anfitriones
824
820
Enlace de red
Dispositivo de almacenamiento
810
ROM
808
Memoria principal
806
Bus
802
Interfaz de comunicación
818
Procesador(es)
804
800
Pantalla
812
Dispositivo de entrada
814
Control de cursor
816

FIG. 10