

REIVINDICACIONES

1. Un método (500) para detectar ámbitos comprometidos en un servicio en línea (110), que comprende:

recibir (510) resultados de detección de comportamientos que ocurren en los dispositivos dentro del servicio en línea (110);

puntuar (520) los resultados de detección basándose en cómo los comportamientos anómalos asociados están dentro del servicio en línea (110), en donde los resultados de detección son puntuados con base en una proporción entre un recuento de subpoblación y un recuento de población para el comportamiento dentro del servicio en línea (110);

excluir los resultados de detección puntuados que tienen uno o más de un recuento de subpoblación y un recuento de población para el comportamiento por debajo de uno o más de un umbral de subpoblación y un umbral de población, respectivamente;

organizar (530) los resultados de detección puntuados restantes de acuerdo con los ámbitos;

aplicar (540) la lógica de detección de señales múltiples a un ámbito determinado para producir una puntuación de confianza que indica si el ámbito determinado está comprometido;

determinar (550) si desea presentar una alerta de si el ámbito determinado está comprometido con base en la comparación de la puntuación de confianza con un umbral de alerta; y

en respuesta a la determinación de que la alerta se va a presentar del ámbito determinado que está comprometido, generar y transmitir la alerta (560).

2. El método (500) de acuerdo con la reivindicación 1, en donde el ámbito determinado está asociado con un dispositivo determinado o una cuenta de usuario dada en el servicio en línea (110).

3. El método (500) de acuerdo con la reivindicación 1, en donde la puntuación (520) de los resultados de detección además comprende:

calcular (600) un identificador para un determinado resultado de detección;

recuperar (620) una cuenta de agregado para el resultado de detección dado;

incrementar (630) los recuentos de población agregados para el resultado de detección dado;

calcular (640) una puntuación de anomalía para el resultado de detección dado basándose en los recuentos de población agregados; y

asociar la puntuación de anomalía con el resultado de detección dado para producir un resultado de detección puntuado.

4. El método (500) de acuerdo con la reivindicación 3, en donde los recuentos de población de agregado incluyen:

un recuento de población sin procesar, que se incrementa para cada resultado de detección observado; y

al menos un recuento de subpoblación, que se incrementa para cada resultado de detección observado que incluye una característica que define una subpoblación de resultados de detección.

5. El método (500) de acuerdo con la reivindicación 3, en donde el identificador incluye al menos un campo del resultado de detección dado, que incluye:

- un papel para un dispositivo dado asociado con el resultado de detección dado;
- un usuario asociado con el resultado de detección dado;
- una clase de comportamiento asociado con el resultado de detección dado; y
- una marca de tiempo.

6. El método (500) de acuerdo con la reivindicación 1, en donde la organización (530) de los resultados de detección puntuados de acuerdo con los ámbitos además comprende:

recibir una definición de ámbito identificando una característica a través de la cual se dividen los resultados de detección;

recibir una ventana de tiempo a través de la cual los resultados de detección se van a analizar;
y

dividir los resultados de detección que se observaron dentro de la ventana de tiempo en los ámbitos de acuerdo con los valores de la característica identificada incluidos en los resultados de detección.

7. El método (500) de acuerdo con la reivindicación 6, en donde la característica especifica valores para:

- Identificadores de dispositivos;
- cuentas de usuario; e
- Identificadores de procesos.

8. El método (500) de acuerdo con la reivindicación 1, en donde los resultados de detección desde una ventana de tiempo más pequeña, que comprende varios minutos de resultados de detección y una ventana de tiempo más grande, que comprende varios días de resultados de detección, se incluyen en los ámbitos.

9. El método (500) de acuerdo con la reivindicación 1, en donde la aplicación (540) de lógica de detección de señales múltiples al ámbito determinado para producir la puntuación de confianza además comprende:

- seleccionar (710) un modelo predictivo;
- extraer (720) características de los resultados de detección;
- puntuar (730) las características para la conversión en características valoradas numéricamente; y

proporcionar (740) las características del modelo predictivo para generar la puntuación de confianza.

10. El método (500) de acuerdo con la reivindicación 9, en donde el modelo predictivo se genera y selecciona en función de un proceso de aprendizaje continuo de máquina.

11. Un sistema que incluye un procesador (802; 906) y un dispositivo de almacenamiento de memoria (804; 962) que almacena instrucciones que cuando se ejecutan por el procesador ofrecen detectar ámbitos comprometidos en un servicio en línea (110), que comprende:

un calificador de anomalía de firma, configurado para:

recibir un determinado resultado de detección de un evento observado que ocurre en el servicio en línea (110);

determinar el grado al cual un comportamiento asociado con el determinado resultado de detección ha sido anteriormente observado que ocurre en el servicio en línea (110) al determinar un recuento de subpoblación y un recuento de población para el comportamiento en el servicio en línea (110);

producir una puntuación de anomalía que será asociada con el resultado de detección dado basándose en una proporción entre un recuento de subpoblación y un recuento de población para el comportamiento; y

determinar que el recuento de subpoblación y el recuento de población para el comportamiento está por encima de un umbral de subpoblación y un umbral de población, respectivamente; y

un detector de señales múltiples en comunicación con el calificador de anomalía de firma, configurado para:

recibir uno o más resultados de detección que comparten un ámbito en el servicio en línea (110) con el resultado de detección dado;

recibir, del calificador de anomalía de firma, la puntuación de anomalía asociada con el resultado de detección;

extraer las características del resultado de detección dado y de uno o más resultados de detección que comparten el ámbito, las características incluyendo la puntuación de anomalía; y

generar una puntuación de confianza basándose en las características extraídas de si el ámbito está comprometido.

12. El sistema de acuerdo con la reivindicación 11, en donde el uno o más resultados de detección compartiendo el ámbito en el servicio en línea (110) con el resultado de detección dado son observados dentro de una ventana de tiempo.

13. El sistema de acuerdo con la reivindicación 12, en donde el grado al cual el comportamiento asociado con el resultado de detección dado ha sido observado anteriormente que ocurre en el servicio en línea (110) se basa en ocurrencias durante la ventana de tiempo.

14. El sistema de acuerdo con la reivindicación 11, en donde el grado al cual el comportamiento asociado con el resultado de detección dado ha sido anteriormente observado que ocurre en el servicio en línea (110) se basa en:

un recuento de población sin procesar de los eventos que ocurren en el servicio en línea (110);
y

un recuento de subpoblación sin procesar de un número de ocurrencias del comportamiento en el servicio en línea (110).

15. El sistema de acuerdo con la reivindicación 11, en donde el grado al cual el comportamiento asociado con el resultado de detección dado ha sido anteriormente observado que ocurre en el servicio en línea (110) se basa en:

un recuento de población de ámbito de un número de entidades que comprenden el ámbito del servicio en línea (110); y

un recuento de subpoblación de ámbito de un número de entidades en el ámbito asociado con el comportamiento.

16. El sistema de acuerdo con la reivindicación 15, en donde las entidades que comprenden el ámbito se definen por un analista como uno de los dispositivos dentro del servicio en línea (110) o cuentas de usuario del servicio en línea (110).

17. Un dispositivo de almacenamiento legible por computadora que incluye instrucciones ejecutables por procesador para detectar ámbitos comprometidos en un servicio en línea (110), que comprende:

recibir (510) resultados de detección de comportamientos que ocurren en los dispositivos dentro del servicio en línea (110);

puntuar (520) de los resultados de detección basándose en cómo los comportamientos anómalos están dentro del servicio en línea (110), en donde los resultados de detección son puntuados con base en una proporción entre un recuento de subpoblación y un recuento de población para el comportamiento dentro del servicio en línea (110);

excluir los resultados de detección puntuados que tienen uno o más de un recuento de subpoblación y un recuento de población para el comportamiento por debajo de uno o más de un umbral de subpoblación y un umbral de población, respectivamente;

organizar (530) los resultados de detección puntuados restantes de acuerdo con los ámbitos, en donde un ámbito dado está asociado con un dispositivo dado o una determinada cuenta de usuario en el servicio en línea (110);

aplicar (540) la lógica de detección de señales múltiples al ámbito determinado para producir una puntuación de confianza que indica si el ámbito determinado está comprometido;

determinar (550) si alertar a un analista del ámbito determinado que está comprometido en función de comparar la puntuación de confianza con un umbral de alerta; y

en respuesta a la determinación de que el analista va a ser alertado del ámbito determinado que está comprometido, generar y transmitir una alerta (560).

18. El dispositivo de almacenamiento legible por computadora de acuerdo con la reivindicación 17, en donde la puntuación (520) de los resultados de detección además comprende:
calcular (600) un identificador para un determinado resultado de detección;
recuperar (620) una cuenta de agregado para el resultado de detección dado;
incrementar (630) los recuentos de población agregados para el resultado de detección dado;
calcular (640) una puntuación de anomalía para el resultado de detección dado basándose en los recuentos de población agregados; y
asociar la puntuación de anomalía con el resultado de detección dado para producir un resultado de detección puntuado.

19. El dispositivo de almacenamiento legible por computadora de acuerdo con la reivindicación 17, en donde la organización (530) de los resultados de detección puntuados de acuerdo con los ámbitos además comprende:
recibir una definición de ámbito identificando una característica a través de la cual se dividen los resultados de detección;
recibir una ventana de tiempo a través de la cual los resultados de detección se van a analizar;
y
dividir los resultados de detección que se observaron dentro de la ventana de tiempo en los ámbitos de acuerdo con los valores de la característica identificada incluidos en los resultados de detección.

20. El dispositivo de almacenamiento legible por computadora de acuerdo con la reivindicación 17, en donde la aplicación (540) de lógica de detección de señales múltiples al ámbito determinado para producir la puntuación de confianza además comprende:
seleccionar (710) un modelo predictivo;
extraer (720) características de los resultados de detección;
puntuar (730) las características para la conversión en características valoradas numéricamente; y
proporcionar (740) las características del modelo predictivo para generar la puntuación de confianza.