LIBRO BLANCO | MARZO DE 2017

Seguridad de los datos empresariales: conceptos básicos del análisis del comportamiento de los usuarios

Índice

Resumen ejecutivo

En la actualidad, los titulares están repletos de informes sobre ciberataques y, aunque la mayoría de los ataques más notorios (como las importantes infracciones en J. P. Morgan, Anthem y Slack) se perpetraron desde el exterior de las organizaciones perjudicadas, los robos y el uso indebido de los datos por parte de los usuarios con privilegios están en alza.

De hecho, el 69 % de los profesionales en materia de seguridad empresarial afirmó haber sufrido un robo o caso de corrupción de la información empresarial de manos de empleados internos de confianza.[1] Asimismo, se dan casos en los que los contratistas, proveedores o partners externos que colaboran con empresas han llevado a cabo infracciones en la red, tanto de forma malintencionada como involuntaria.

Si hemos aprendido algo de este tipo de eventos, es que proteger el acceso con privilegios sigue siendo una preocupación urgente para empresas de todos los tamaños. Sin embargo, a pesar de esta toma de conciencia y del exceso de productos de seguridad disponibles, muchos sistemas de TI aún son vulnerables a los ataques.

El problema reside en que los controles de gestión de identidades y accesos (IAM, por sus siglas en inglés) tradicionales, aunque amplios, son estáticos: una vez que los usuarios malintencionados obtienen acceso, pueden aprovecharse del sistema hasta donde se lo permitan los privilegios establecidos de la cuenta.

No obstante, si las empresas adoptan un enfoque respecto a la seguridad que esté centrado en las identidades y que aúne los análisis del comportamiento de los usuarios y la detección de anomalías en un modelo de aprendizaje automático, podrán detectar rápidamente la actividad que entrañe riesgos y activar de forma automática controles de mitigación para limitar el perjuicio a la empresa.

CA Threat Analytics

CA Threat Analytics protege los datos empresariales del mismo modo que las tarjetas de crédito protegen el dinero. Aunque estas palabras traen a la mente las ideas correctas (monitorización continua y uso de análisis para determinar el riesgo y prevenir que los “malos” roben activos), no ofrecen mucha información sobre cómo se lleva a cabo. En este libro blanco, se describe de qué modo CA Threat Analytics protege los datos empresariales mediante dos funciones relacionadas: el análisis del comportamiento de los usuarios y la mitigación automatizada.

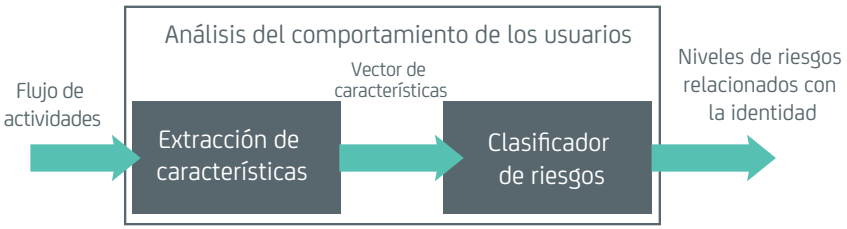
Mediante el análisis del comportamiento de los usuarios, la empresa puede evaluar constantemente el riesgo y detectar con rapidez actividades maliciosas. Como entrada, los análisis del comportamiento de los usuarios toman un flujo de datos sobre cómo interactúa una identidad específica, o un grupo de identidades, con los servicios o aplicaciones, y después generan un nivel de riesgo asociado a cada identidad empresarial.

Por su parte, la mitigación automatizada permite a las empresas realizar una serie de pasos de manera automática para mitigar el riesgo y frustrar las actividades maliciosas detectadas. Asimismo, esta característica cambia la forma de controlar el acceso de las identidades individuales en función del resultado relativo al riesgo obtenido a partir del análisis del comportamiento de los usuarios. Un ejemplo sencillo de mitigación automatizada sería bloquear automáticamente el acceso de identidades de alto riesgo a aplicaciones o repositorios de datos con información especialmente confidencial.

Aunque tanto el análisis del comportamiento de los usuarios como la mitigación automatizada constituyen elementos esenciales del funcionamiento de CA Threat Analytics, el objetivo de este libro blanco es centrarse en el análisis del comportamiento de los usuarios. A lo largo de las siguientes secciones, la función de análisis del comportamiento de los usuarios descrita en los párrafos anteriores se desglosará en las distintas partes que la conforman. Después, dichas partes se detallarán por separado. En aras de la sencillez, el análisis girará en un primer momento en torno a la protección de una sola identidad en un solo servicio. Tras explicar los aspectos básicos de las técnicas utilizadas, se debatirá cómo se pueden mejorar estas ideas al trabajar con una comunidad de identidades en varios servicios.

Conceptos básicos

Desde el punto de vista conceptual, la función de análisis del comportamiento de los usuarios está formada por dos componentes: la extracción de características y el clasificador de riesgos.



El componente de extracción de características procesa un flujo de actividades y extrae un conjunto de características pertinentes, que son propias de una identidad individual que se ha observado durante un tiempo. Por ejemplo:

- La identidad utiliza un dispositivo móvil desconocido.
- La identidad trabaja en una ubicación remota.
- La identidad proviene de una dirección IP sospechosa.
- La identidad es miembro de un grupo con privilegios.
- La identidad utilizó el servicio X fuera de las horas de trabajo habituales.

La extracción de características es más complicada de lo que parece, ya que no solo consiste en extraer las características de una transacción en curso. A pesar de que el flujo de actividades se recibe como una secuencia de eventos separados, la información entrante real es el flujo de actividades completo, desde que se inició. De este modo, se puede entender el uso y el comportamiento de cada identidad en su conjunto. Sin examinar la totalidad del historial de actividades, se vería obligado a evaluar el riesgo en función, únicamente, de cada evento separado de forma individual.

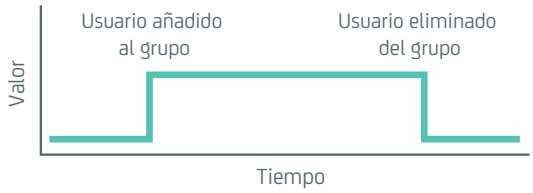
Si tomamos como ejemplo las características enumeradas, ¿qué significan las horas habituales de trabajo en el contexto de un solo evento? Con el fin de que CA Threat Analytics pueda utilizar importantes características como esta, debe calcular y emplear también la información relativa a los datos históricos.

Al examinar el flujo de actividades completo, CA Threat Analytics proporciona a la empresa una cantidad considerablemente mayor de información que la que antes tenía a su disposición para evaluar los riesgos y detectar actividades maliciosas. Ahora la empresa puede evaluar el riesgo en función de las actividades pasadas y la información concreta de cada identidad. Esta ventaja se logra a cambio de procesar un gran volumen de datos, muchos de los cuales son redundantes. Afortunadamente, gracias a la extracción de características, la dimensión de los datos se reduce, pues se eliminan o agregan datos repetidos mientras se destaca la información que necesita el segundo componente de la función de análisis del comportamiento de los usuarios: el clasificador de riesgos.

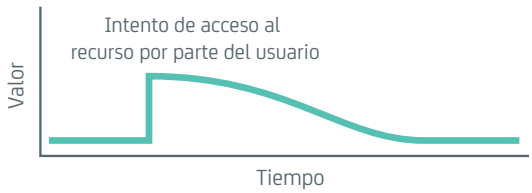
Determinación del valor en el contexto del tiempo

Antes de continuar, cabe destacar un interesante detalle de las características que se observan a lo largo del tiempo. Dado que estas se modifican al recibir las actividades, desde un punto de vista técnico, tienen un carácter diacrónico, lo que simplemente significa que los valores cambian a lo largo del tiempo. Al observar una característica, CA Threat Analytics modeliza la observación como una función de tiempo. En otras palabras, si una actividad entrante provoca que se active una característica, el "valor" de esta puede encontrarse en su máximo nivel en el momento de esa actividad y cambiar a medida que el tiempo avanza.

La forma real en la que el valor cambia varía enormemente en función de la característica que se haya extraído. Algunas son completamente binarias, por lo que cuando se observa una característica, esta permanece en su valor más alto hasta que algún evento la mitiga, como se muestra a continuación.



Por ejemplo, la pertenencia a un grupo confidencial. Esa característica se valora en su totalidad durante todo el tiempo que la identidad permanece asociada al grupo. Otras características se modelizan como líneas descendentes. Cuando se observa una característica de este tipo, el valor se encuentra en el valor más alto y disminuye a lo largo del tiempo, como se muestra a continuación.



Por ejemplo, cuando un usuario intenta acceder a un recurso para el que no tiene permiso. Aunque hoy esa característica es pertinente para calcular el nivel de riesgo de una identidad, dicha pertinencia se reduce en gran medida pasada una semana e incluso más pasado un mes. Al disminuir el valor de las características con el paso del tiempo, CA Threat Analytics garantiza que estas contribuyan a la hora de establecer un nivel de riesgo de la forma más adecuada.

El clasificador de riesgos

El clasificador de riesgos es una función de análisis que divide el vector de características en tres niveles de riesgo separados:

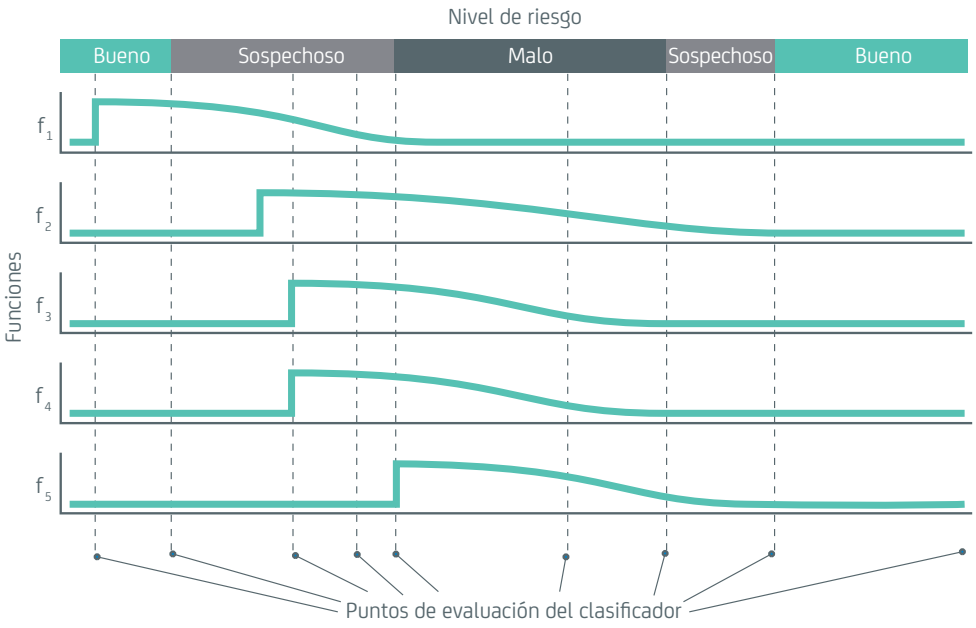
- **Bueno**: el riesgo de la identidad es mínimo.
- **Sospechoso**: la identidad se ha asociado a eventos o actividades que suponen un riesgo, pero dicho riesgo no requiere acciones inmediatas. El sistema monitorizará esta identidad de forma más atenta y podrá iniciar un conjunto de mitigaciones automatizadas, según la política de la empresa.
- **Malo**: la identidad se considera un alto riesgo y requiere atención inmediata. Este sistema iniciará una mitigación automatizada y enviará alertas, según la política de la empresa.

Las funciones del clasificador de riesgos toman como datos de entrada un vector de valores de características y como datos de salida, genera una de las clases separadas indicadas previamente.

$$\text{Clasificador}(\text{características}(t)) \longmapsto \{\text{bueno, sospechoso, malo}\}$$

Tal como se ha indicado en los párrafos anteriores, las características son en sí una función de tiempo, por lo que el clasificador de riesgos también funciona en el dominio del tiempo. Se recurre al clasificador de riesgos en puntos de decisión clave; por lo general, como respuesta a cambios significativos en los valores del vector de características. Independientemente de si el clasificador de riesgos calcula el nivel de riesgo de un momento dado, todas las funciones de las características de esa identidad o entidad se evalúan en ese momento. El conjunto completo de las características activas de la entidad en ese momento compone el vector de características real que se introduce en el clasificador de riesgos y se utiliza para determinar el riesgo.

En la siguiente ilustración, se muestran los puntos separados en los que el clasificador de riesgos probablemente realizaría la evaluación. Como se indica, las evaluaciones se producen cuando el valor de una característica aumenta o cuando desciende por debajo de un umbral. Los valores transferidos al clasificador de riesgos se corresponden con el valor de cada característica en el momento en el que se activa su evaluación (reflejado en las líneas verticales). Por supuesto, no todas las ejecuciones del clasificador de riesgos dan lugar a un nuevo nivel de riesgo. En la práctica, existen muchos más puntos de evaluación que los dibujados y que equivalen a los cambios del valor de la característica, la actividad del sistema y la inteligencia de amenazas. En general, el clasificador de riesgos se activa en cualquier momento en el que exista la posibilidad de que se produzca un cambio de nivel de riesgo.



Entonces, ¿qué es el clasificador de riesgos propiamente dicho? ¿Cómo convierte un vector de características en un conjunto separado de clases de riesgos? Conviene empezar explicando lo que no es. Los clasificadores de riesgos de CA Threat Analytics no son simples reglas que someten a pruebas características concretas (del tipo "si la característica X está activa, devolver el valor 'malo'"). Esto es un enfoque ingenuo que utilizan muchos productos de seguridad tradicionales y que fracasa estrepitosamente debido a su elevada propensión a generar falsos positivos, a su fragilidad y a la facilidad con la que se puede frustrar su eficacia. Además, no se sirve de la información que resulta primordial tanto para detectar las actividades maliciosas como para que los usuarios legítimos puedan utilizar el sistema.

Las funciones de CA Threat Analytics son mucho más sólidas. El clasificador de riesgos de CA Threat Analytics no examina las características de forma aislada, sino en el contexto del conjunto de características al completo. Con este enfoque, se pueden combinar varias características, que por separado no afectan al nivel de riesgo, para influir de una forma significativa. Es más, CA Threat Analytics incorpora información de los sistemas implementados, como aspectos de los usuarios individuales y los cambios de la comunidad de identidades, con el fin de adecuar las decisiones que toma a lo largo del tiempo. El resultado es un sistema que proporciona la flexibilidad para adaptarse a medida que surgen nuevas amenazas y entornos de implementación.

Comunidades y servicios

Como se ha mencionado en los apartados anteriores, existen varios detalles prácticos que se han simplificado en el análisis precedente. En primer lugar, ¿qué sucede con las comunidades de identidades? Especialmente en el entorno empresarial, hay ciertos aspectos de los grupos de identidades que resultan pertinentes para determinar el nivel de riesgo de una identidad concreta. Por ejemplo:

- Acceder a los recursos con más dispositivos de los habituales en la organización.
- Trabajar fuera de la ubicación de trabajo habitual del grupo.
- Encontrarse en un número indebidamente alto de grupos.

Cada organización establece sus propias líneas de referencia en materia de actividades previstas, que incluyen factores como el número normal de dispositivos asociados a un usuario, las ubicaciones de trabajo de la organización y el número apropiado de grupos. Si se centra en un grupo de identidades en lugar de en las identidades aisladas, puede obtener un alto nivel de estadísticas útiles sobre la comunidad con las que poder contrastar las identidades individuales. Como es natural, esto conlleva un coste. Más que simplemente procesar el flujo de actividades al completo de una identidad, se deben extraer las características de todo el historial de la actividad de la organización en su conjunto.

De modo similar, ampliar los análisis de un solo servicio a un grupo de servicios ofrece una ventaja diferente. Al examinar las acciones que lleva a cabo una identidad en distintos servicios, se pueden extraer las características para crear modelos de patrones de acceso habituales y aplicarlos de forma inteligente para proporcionar seguridad en tales servicios. Con esta información, CA Threat Analytics puede detectar comportamientos anómalos e incoherentes que representan una amenaza para esa identidad o para la empresa.

Conclusión

En este libro blanco, se presenta el modo en que CA Threat Analytics protege los datos empresariales mediante el análisis del comportamiento de los usuarios. Aunque la explicación de las ideas básicas es sencilla, los problemas prácticos relativos a la extracción de características y la clasificación de riesgos van mucho más allá de los aspectos abarcados en este documento. De hecho, muchos de los requisitos del mundo real que orientaron a nuestro equipo ni siquiera se han mencionado, como la posibilidad de tomar decisiones en tiempo real, la garantía de precisión del sistema a lo largo del tiempo y la entrega de información útil verdadera relativa a las decisiones en materia de riesgos a los administradores de los sistemas.

Si le interesa obtener más información sobre estos factores y sobre cómo se puede beneficiar su organización de ellos, consulte: https://www.ca.com/us/products/ca-threat-analytics-for-privileged-access-manager.html

Comuníquese con CA Technologies en ca.com/es

CA Technologies (NASDAQ: CA) crea software que impulsa la transformación de las empresas y les permite aprovechar las oportunidades que brinda la economía de las aplicaciones. El software se encuentra en el corazón de cada empresa, sea cual sea su sector. Desde la planificación hasta la gestión y la seguridad, pasando por el desarrollo, CA trabaja con empresas de todo el mundo para cambiar la forma en que vivimos, realizamos transacciones y nos comunicamos, ya sea a través de la nube pública, la nube privada, plataformas móviles, entornos de mainframe o entornos distribuidos. Para obtener más información, visite **ca.com/es**.

1 Accenture and HfS Research, "The State of Cyber Security and Digital Trust 2016", junio de 2016: https://www.accenture.com/t20160704T014005__w__/us-en/_acnmedia/PDF-23/Accenture-State-Cybersecurity-and-Digital-Trust-2016-Report-June.pdf#zoom=50

CS200-259092