TrackerIQ

Preguntas frecuentes

¿QUÉ es TrackerIQ?

TrackerIQ protege a las empresas y organizaciones detectando actividades maliciosas realizadas por empleados y por impostores externos mientras acceden a las aplicaciones empresariales. TrackerIQ es independiente del tipo de Aplicación, y analiza la actividad de los usuarios en y entre diferentes tipos de aplicaciones - SaaS, nube y desarrollo hecho a la medida.

¿Qué problemas resuelve?

El problema que resuelve TrackerIQ es la detección de ataques a los procesos de negocio, para los diferentes tipos de aplicaciones que una compañía tiene implementadas. Estos ataques a las aplicaciones empresariales han sido un desafío sin resolver durante mucho tiempo para las empresas que las utilizan, y están creciendo aún más debido al cambio en todo el mercado, resultante del portado de las Aplicaciones críticas para el negocio a SaaS en la nube. Este cambio, ha ampliado la superficie de ataque de actividades maliciosas, realizadas por impostores y usuarios “de confianza”.

El desafío tecnológico que resuelve TrackerIQ está relacionado con la forma innovadora en que detecta esas actividades maliciosas. Las soluciones actuales de detección de actividades maliciosas en la capa de aplicación se basan en la creación de reglas; sin embargo, las soluciones basadas en reglas solo detectan ataques cuyos patrones de actuación son previamente conocidos, y generan un alto número de falsas alarmas, requiriendo además una constante inversión para crear nuevas reglas y mantener todas las creadas.

TrackerIQ no se basa en la creación de reglas específicas para una determinada aplicación; por el contrario, funciona mediante un Análisis innovador de la actividad de cada usuario, combinado con un exclusivo motor de agrupamiento para detectar con precisión la actividad anómala que refleja actividades maliciosas.

Además, TrackerIQ proporciona herramientas de investigación y respuesta que permiten de una forma muy fácil, una rápida comprensión de la actividad del usuario que ha realizado esa actividad anómala.

¿Qué características únicas ofrece TrackerIQ al mercado?

Precisión sin precedentes en la detección de amenazas internas para empresas, relacionadas con el acceso a Aplicaciones.

TrackerIQ es independiente de la aplicación y se puede implementar para analizar cualquier aplicación, tanto desarrollada a medida como SaaS.

¿Qué deben saber los encargados de tomar decisiones técnicas sobre TrackerIQ?

TrackerIQ es una solución única y probada en el mercado, para la detección de amenazas maliciosas en la capa de aplicaciones. TrackerIQ no requiere el desarrollo o mantenimiento de reglas, y es extremadamente precisa en la detección. Consideremos los tres mensajes tecnológicos más importantes:

1. Analítica del "viaje" del usuario: el seguimiento del "viaje" del usuario permite un nuevo nivel de análisis de la actividad de la aplicación, mucho más preciso y completo que los antiguos basados en reglas y soluciones de modelos estadísticos. La esencia y significado de las actividades que realiza el usuario no es relevante para TrackerIQ, ya que su detección se basa en la pura actividad del usuario. Analizar la secuencia de actividades, en lugar de centrarnos en cada actividad individual, nos permite detectar sesiones anormales con mucha más precisión.
2. La precisión de TrackerIQ es el resultado de un motor de agrupación único que aprende todas las actividades y perfiles de los usuarios. El motor de agrupamiento de TrackerIQ, actúa de forma automática y no supervisada, mediante un algoritmo que aprende los perfiles de cada usuario y los agrupa en sesiones similares. Cada usuario tiene muchos perfiles de actividad y además, múltiples perfiles a través de las diferentes aplicaciones. El motor crea automáticamente perfiles y define comportamientos típicos. Una vez que se definen los comportamientos típicos, comenzamos a verificar cada nueva sesión para ver si en este caso, el comportamiento es típico, o no. Se puede estudiar el comportamiento de esta nueva sesión en comparación con el comportamiento típico del usuario individual, de un grupo de usuarios o de toda la población de la organización.

   Es mucho más difícil para un imitador imitar los perfiles normales de los usuarios, y de la misma forma, los usuarios internos que buscan hacer un mal uso o abuso de una aplicación, eventualmente se desviarán de sus perfiles normales.
3. Detección agnóstica: nuestro modelo es agnóstico al funcionamiento de una aplicación, de modo que puede aplicarse a cualquier tipo de aplicación. Esta característica es fundamental para la detección, ya que cada aplicación tiene un flujo de uso con un formato diferente, y un conjunto diferente de operaciones.

¿Quiénes son los competidores más relevantes de TrackerIQ?

TrackerIQ representa una nueva categoría de detección y respuesta ante accesos no deseados a las Aplicaciones. Hasta donde sabemos, no existen competidores que ofrezcan una solución que funcione para todo tipo de Aplicaciones, incluidas las aplicaciones desarrolladas a medida.

Las soluciones basadas en un motor de reglas son, hoy por hoy, la competencia más importante de TrackerIQ, en términos de cuota de mercado. También hemos encontrado algunas soluciones que son específicas de una determinada aplicación, pero como se ha comentado anteriormente, TrackerIQ proporciona una única solución de detección e investigación para TODAS las aplicaciones de la organización, incluidas desarrollos a medida, SaaS y Cloud.

¿Qué diferencia a TrackerIQ de la competencia?

- La detección se basa en el análisis de la actividad del usuario; no hay necesidad de crear reglas, o aprender la lógica de una aplicación.
- Nuestro motor de agrupamiento (pendiente de patente) permite el aprendizaje automático de múltiples perfiles de actividad de cada usuario por sesión.
- Precisión, número de falsos positivos y número de falsos negativos es un criterio importante en una solución de detección.
- TrackerIQ mejora de forma notable la precisión, observando la secuencia de la que forma parte una actividad.
- Conjunto único de herramientas de investigación de la actividad del usuario en función de la información y los conocimientos proporcionados.

¿Qué Casos de Uso son relevantes para TrackerIQ?

Amenazas internas

- Usuarios internos aprovechando sus derechos para acceder a las aplicaciones empresariales para realizar operaciones maliciosas:
  - » Trabajadores descuidados: mal uso de las aplicaciones
  - » Fraude interno / Malversación de fondos accediendo a aplicaciones desarrolladas a medida
  - » Un usuario de la empresa puede robar información para venderla a terceros
  - » Acceder a datos no destinados a ser vistos por ese empleado, de diferentes cuentas, sucursales, países….
  - » Empleado descontento - modificación de datos, cambios o actos maliciosos
  - » Detección de anomalías para terceros que utilizan sus APIs / Banca Abierta
- Las amenazas internas suelen ser mucho más difíciles de detectar porque estas personas conocen su organización bastante bien y tienen acceso a aplicaciones comerciales críticas

El desafío de la suplantación de identidad

- Atacantes que se hacen pasar por usuarios legítimos y realizan actividades maliciosas
  - » Credencial robada o relleno de credenciales
  - » Eludir MFA (Autentificación Multifactor) es complejo pero factible – Ingeniería Social
- Los atacantes se centran en los usuarios privilegiados de las plataformas en la nube y aplicaciones SaaS
  - » Aplicaciones corporativas SaaS – atacantes haciéndose pasar por un empleado/administrador
  - » Plataformas corporativas en la nube: los atacantes se hacen pasar por administradores
  - » Portales orientados al cliente: los atacantes se hacen pasar por un cliente / partner
- Superficie de ataque creciente debido a las transiciones derivadas de la transformación digital
  - » Cambiar de aplicaciones locales a aplicaciones SaaS
  - » El cambio al trabajo remoto (teletrabajo)

Propuesta de Valor de TrackerIQ

www.reveal.security
info@reveal.security

Acerca de RevealSecurity

RevealSecurity monitorea usuarios privilegiados, infiltrados maliciosos e impostores para detectar comportamientos anómalos en aplicaciones y plataformas. Una y otra vez, la investigación acreditada ha encontrado que cuanto más se tarda en detectar una infracción, mayor es su daño. Sin embargo, la mayoría de la detección de infracciones dentro de las aplicaciones aún se basa en reglas, por lo que es costosa e ineficaz debido a una debilitante alta tasa de alertas falsas. La autenticación meticulosa nunca es suficiente, ya que los usuarios que tienen acceso legítimo a la aplicación aún están involucrados en el uso indebido, el abuso y la malicia. RevealSecurity defiende la ubicuidad y la precisión en el mercado de detección de aplicaciones.