Ciber Fraude y la Gestión de Riesgos.

Intellinx Digital banking

OPTARIS

Tabla de Contenidos.

El Desafío del Ciber Fraude

El número de ataques cibernéticos de fraude y los costos resultantes están por las nubes.

Los atacantes, ya sea dentro o fuera de la organización, están utilizando técnicas más sofisticadas para acceder a información crítica. Además, las tácticas de fraude que se utilizan son más difíciles de identificar para los sistemas de seguridad tradicionales. En orden de proteger tanto a los datos corporativos como al de los clientes, quienes toman las decisiones deben reconsiderar la modalidad para la detección de fraudes y la seguridad cibernética. Las instituciones financieras necesitan la completa visibilidad del comportamiento de los usuarios. Sin ella se está perdiendo una línea fundamental de defensa.

Usted es productivo tanto como sus herramientas le permitan serlo.

Las soluciones tradicionales y rígidas carecen de la sofisticación técnica para protegerse de la gran cantidad de estafadores que están en constante evolución de sus métodos delictivos. A menos que usted se adapte, su empresa está en riesgo.

- Obtener una visión completa del comportamiento de los usuarios dentro de los sistemas.
- Usar alertas instantáneas para detener el fraude en tiempo real.
- Contar con total captura, auditoría y análisis de los datos.

El Desafío del Ciber Fraude

Reconsiderar la estrategia del ciber fraude.

La clave para proteger su institución financiera está en la estrategia que define las herramientas que usted empleará. Más que en recopilar y analizar, tiene que estar equipado con la visibilidad e inteligencia necesaria para poder actuar.

Las tecnologías de Intellinx para Ciber Fraude y Riesgo proveen herramientas de vanguardia para supervisar y analizar de forma no invasiva la actividad de los usuarios, brindar alertas y resolver el fraude anticipadamente. Desde visualizar todo desde un mismo tablero de control y que va más allá de los archivos de registro – Logs – al capturar la actividad del comportamiento del usuario como el de los atacantes, ayudando a reducir el fraude y brindar rápidamente las garantías de cumplimiento de las normativas.

20,8 millones es el costo medio de violación de datos en las organizaciones financieras.

(US Dept of Justice, 2013).

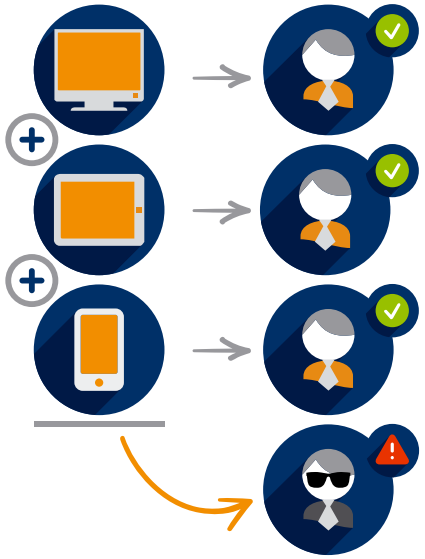
Supervisión del comportamiento del usuario

Usted no puede detener el fraude si no conoce lo que sus usuarios hacen.

La mayoría de las inversiones en seguridad protegen a las instituciones financieras del malware, así como los riesgos de acceso no autorizado, pero esto no es suficiente. Muchas instituciones financieras tienen una imagen incompleta de lo que sus usuarios autorizados están haciendo, creando un punto crítico cuando se trata de detectar y detener el fraude.

El seguimiento de las actividades no es suficiente. Realice también el seguimiento del comportamiento.

La actividad de un usuario puede parecer normal en un sistema, pero es anormal en otro. ¿Cómo se puede saber la diferencia? A través de la tecnología de canales cruzados que analizan los patrones de comportamiento en las redes y aplicaciones, pueden ayudar a detectar y detener la actividad sospechosa en tiempo real.



- Analice el comportamiento integral en lugar de transacciones individuales.
- Actúe ante las actividades sospechosas antes del que daño este hecho.
- Incremente la seguridad de la organización con una visibilidad centralizada.

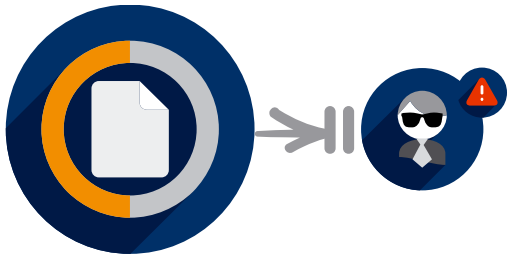
Supervisión del comportamiento del usuario

Los archivos de Log no son suficientes.

Los registros de auditoría – logs – generados por el sistema son costosos, requieren mucho tiempo para analizarlos y sólo cuentan una parte de la historia, a menudo demasiado tarde. Este desafío puede ser aliviado a través de la inversión de un sistema central de registro.

Proteja su institución financiera con una "cámara virtual de vigilancia."

El monitoreo del comportamiento de los usuarios de Intellinx es una solución no invasiva que escucha el tráfico de red entre los usuarios, los sistemas y las aplicaciones y analiza los intercambios de información en tiempo real y la reconstrucción de las sesiones de usuario en forma completa.
Es como tener una cámara de vigilancia que proporciona la reproducción, pantalla por pantalla, de lo que los usuarios ven y hacen a través de los sistemas y las aplicaciones. La solución lo hará sin impacto en la red y en el rendimiento del sistema.



49%: Es el porciento de encuestados, quienes coincidieron en que la recopilación y análisis de los registros logs, no son eficaces para identificar a los usuarios de aplicaciones, en el mal uso de información crítica o confidencial.

(Ponemon Institute, LLC. Lo que usted no sabe le hará daño: Un Estudio del Riesgo de acceso a la aplicación y uso, 2015).

Supervisión del comportamiento del usuario

Como trabaja:

El monitoreo del comportamiento del usuario de Intellinx incorpora una tecnología especial para marcar la actividad inusual de los usuarios autorizados. Por ejemplo, si un empleado tiene acceso a archivos no relacionados con su trabajo, múltiples veces dentro de un período determinado.

Los investigadores pueden reproducir todas las interacciones del empleado - cada pantalla y cada clic - para detectar la actividad potencialmente fraudulenta.

Las características incluyen:

Alertas en tiempo real e Investigación de alertas y casos:
Investigar las alertas y documentar los comportamientos sospechosos, en tiempo real

Función de informes de gran alcance:
Genera reportes para cualquier tipo de acceso, el cual puede ser filtrado y ordenado

Análisis de los enlaces:
Permite mostrar visualmente las relaciones entre los usuarios (empleados, clientes, cuentas y otros), con los sistemas y datos.
Las entidades fraudulentas, o aquellas bajo investigación, son resaltadas para permitir un posterior examen más detallado.

Reproducción pantalla por pantalla:
Para comprender plenamente todo lo que el usuario hizo y vio en su operatoria con los sistemas y aplicaciones, a través del tiempo, los investigadores pueden reproducir la actividad del usuario y analizar el comportamiento, pantalla a pantalla.

Búsqueda de la actividad del usuario a través de múltiples plataformas:
Permite realizar una búsqueda similar a Google sobre el contenido de todas las pantallas de los usuarios que acceden a través de sistemas dispares en un intervalo de tiempo dado, para encontrar, por ejemplo, a todos los usuarios que han accedido a una cuenta específica del cliente en un plazo de tiempo determinado.

Enterprise Case Manager

El tiempo es esencial.

Detener el fraude en tiempo real es un desafío cuando se está basando solo en el análisis y en la revisión manual del archivo de log.

Hoy la tecnología no logra alcanzar el ritmo de los cambios.

Mientras que el fraude que se comete es cada vez más dinámico y sofisticado, la mayoría de las soluciones tradicionales no son capaces de seguir el ritmo de los cambios en los variados tipos de amenazas ni proporcionan la agilidad necesaria para realizar las investigaciones en tiempo real.

Enterprise Case Manager

Una protección limitada lo deja vulnerable.

Una solución que no protege a toda su empresa, aumentará su exposición al fraude. Asegurarse de que su organización cumple con las regulaciones gubernamentales y registra los Informes de Actividades Sospechosas (SAR), de manera oportuna, debe ser un requisito mínimo para usted.

Proteja su institución financiera con un sistema de gestión de casos de punta a punta.

Intellinx Enterprise Case Manager es un administrador de casos que potencia a los investigadores con un sistema escalable y abarcativo a toda la compañía. Permite el manejo de alertas y casos que reducen el riesgo financiero y ayudan al cumplimiento de las normativas a bajo costo. Es una solución fácil de implementar y configurar.

54%: de las compañías declara tener inconvenientes en detectar actividades ilegales o inadecuadas de los usuarios en tiempo real.
(Ponemon Institute, LLC, Lo que usted no sabe le hará daño: Un Estudio del Riesgo de acceso a la aplicación y uso, 2015)

- Dar a los investigadores una consola centralizada para gestionar todos los casos.
- Proporcionar mayor velocidad a los tiempos de investigación y aumentar la productividad.
- Estimar fácilmente el impacto financiero de las actividades sospechosas.

Enterprise Case Manager

Como trabaja:

Intellinx Enterprise Case Manager detecta las actividades sospechosas y provee la visibilidad de gestión necesaria para apoyar la gestión de casos sospechosos de fraude que efectan el normal desenvolvimiento de los negocios.

Identifica automáticamente los casos en que debe presentarse un reporte SAR y generarlo en el formato requerido por el FINCEN/UIF en forma electrónica. El sistema da a los investigadores todas las herramientas e información necesaria para manejar y resolver el caso sin agotar los recursos de sus equipos de fraude y cumplimiento.

Las características incluyen:

Gestión integral de casos:
En el caso de una señal de alerta, la plataforma reúne toda la información necesaria de las fuentes pertinentes. Desde el tablero de control, proporciona a los investigadores una visión transversal de los canales de actividades sospechosas.

Sistema único de registro:
Debido a que está conectado a todos los sistemas y fuentes de datos corporativos relevantes, Enterprise Case Manager reduce la redundancia y proporciona una única fuente de datos para los investigadores.

Calculadora de impacto financiero:
Mirando hacia la exposición financiera, la pérdida anticipada, y el cargo del recupero, Enterprise Case Manager calcula automáticamente el riesgo financiero de las actividades sospechosas y sospechas de fraude.

Totalmente adaptable:
Enterprise Case Manager ayuda a los departamentos de cumplimiento a gestionar la carga de trabajo y optimizar la productividad. Es completamente escalable, con informes pre configurados, tableros de control y flujos de trabajo, que eliminan la necesidad de programación o soporte de TI.

Suite de Reportes adaptables:
Con la identificación automática de la necesidad de presentar un reporte SAR, Enterprise Case Manager mejora el cumplimiento de las regulaciones gubernamentales y asistencias en su creación, por ejemplo, a todos los usuarios que han accedido a una cuenta específica del cliente en un plazo de tiempo determinado.

Enterprise Case Manager automáticamente:

- Notifica cuando se requiere un reporte SAR.
- Alerta cuando se llega a una fecha límite.
- Genera los plazos de vencimiento, lo que reduce las posibilidades de que, con vistas a la presentación de un SAR se llegue demasiado tarde.

Fraude Interno

La fuga de información pone en peligro las relaciones.

La incapacidad de controlar con eficacia exactamente lo que están haciendo los usuarios, puede abrir las puertas a la fuga de datos, produciendo pérdida de reputación y valor para los accionistas.

Invertir en una solución verdadera de fraude, punta a punta.

Intellinx con su tecnología para Fraude interno proporciona un nivel de conocimiento sin igual: una visibilidad completa del comportamiento de los usuarios. Esto no sólo ayuda a detener el fraude con sus pistas, sino que tiene el poder de disuadir a los posibles defraudadores, al detectar actividades y comportamiento inusuales, así como generar responsabilidad total en los empleados.

Fraude Interno

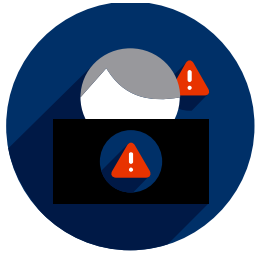
Detenga ahora las actividades internas maliciosas.

Distinguir entre las actividades maliciosas, negligentes y normales cuando cada empleado utiliza los mismos comandos legítimos del sistema es realmente un proceso complejo.

Una solución anti fraude no debe ser unidimensional.

Realizar un seguimiento a través de sistemas dispares para determinar un comportamiento fraudulento es muy difícil de hacer, por esta razón simplemente no puede depender de una imagen parcial de la actividad del usuario.

- Eliminar las revisiones de los informes de registros -Logs- que son muy consumidores de tiempo.
- Responder inmediatamente a nuevas amenazas.
- Mantener la completa visibilidad del usuario interno



78% del fraude ocupacional es realizado por o con empleados.

$3.7 mil millones: Pérdida global de fraudes internos en 2014.

(Association of Certified Fraud Examiners (ACFE), 2014 Report to the Nations on Occupational Fraud and Abuse. (http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf)

www.optaris.com

hola@optaris.com

Fraude Interno

Como trabaja:

Usando el conocimiento de más de 200 implementaciones y la experiencia del personal de Intellinx, la biblioteca de reglas pre-empaquetadas que ha sido refinada para detectar anomalías en los patrones de trabajo y de datos.

Es fácil de configurar, y las reglas son fácilmente configurables para los escenarios de riesgo específicos de su organización.

Ejemplos de reglas:

Regla:
Fuga de información crítica

Alerta:
El usuario ejecuta consultas sobre cuentas o datos de cliente que superan el promedio esperado

Regla:
Malversación

Alerta:
Se intentan ejecutar transacciones monetarias de cierta categoría con un gran monto total

Regla:
Violación de políticas

Alerta:
Se detecta la creación de múltiples cuentas con saldos bajos o nulos.

Fraude con cheques

Los esquemas de fraude están en aumentos.

A pesar de los controles de verificación en el sector bancario, las pérdidas atribuidas a los fraudes con cheques siguen estando entre las más altas de cualquier tipo de fraude.

Los sistemas rígidos carecen de flexibilidad.

Los estafadores están utilizando nuevos y sofisticados métodos, a través de múltiples canales y tecnologías de última generación. Su solución de riesgos debe ser sofisticada y ágil para detenerlos.

Fraude con cheques

Proteja su entidad financiera con el control total del riesgo y protección contra el robo.

A pesar de los controles de verificación en el sector bancario, las pérdidas atribuidas a los fraudes con cheques siguen estando entre las más altas de cualquier tipo de fraude.

Funcionalidades adicionales.

Los estafadores están utilizando nuevos y sofisticados métodos, a través de múltiples canales y tecnologías de punta. Vuestra solución de riesgos debe ser, por lo tanto sofisticado y ágil

Perfila las cuentas de los clientes para detectar desviaciones y actividades sospechosas.

Evalúa todas las posibles conexiones entre las cuentas y clientes.

Reduce falsos positivos utilizando modelos predictivos.

Recolecta y almacena gran cantidad de datos en una única fuente para los investigadores.

Registra toda la actividad a través de múltiples cuentas de un mismo cliente

De las organizaciones que fueron víctimas de fraude o atentaron fraude, el 82% fueron a través de cheques.
(2014 AFP Payments Fraud and Control Survey)

- Detecta y responde a una gran variedad de esquemas de fraude con cheques.
- Gana visibilidad por su actividad entre las cuentas y con las conexiones entre cuentas y clientes.
- Fácil integración con las imágenes de cheques, el procesamiento de ítems y los sistemas DDA (Débito Directo Autorizado).

www.optaris.com

hola@optaris.com

Fraude con cheques

Como trabaja:

A cada transacción se le asigna un puntaje de riesgo, usando reglas y perfiles de usuario. Si el puntaje supera determinado umbral, le avisa a un administrador para que tome la decisión de pagar o no.

Captura una gran cantidad de información, incluyendo imágenes de frente y reverso del cheque y cuando se dispara una alerta, se lo presenta y muestra al investigador.
Todas las alertas son guardadas en el Centro de Investigación para asegurar que se tomen decisiones rápidas y se realicen los procesos de investigación.

Ejemplos de reglas:

Regla:
Fraude de Depósitos

Alerta:
Un usuario realiza un depósito inusualmente grande en cheques.
Ha habido un monto excesivo de depósitos diarios de cheques.

Regla:
Fraude con cheques de caja

Alerta:
El sistema detecta múltiples operaciones de depósito de cheques con la misma cantidad

Regla:
Giro de Cheques sin Fondo

Alerta:
Se detectan múltiples transacciones de giro de cheques del mismo monto
Se realizan excesivas transacciones de cancelaciones de giro de cheques.

Fraude y Seguridad en la Web

Sin un buen análisis no se podrán detectar las cuentas que están comprometidas.

Muchas soluciones no monitorean todas las capas del tráfico web ni todas las acciones de los usuarios y en última instancia no se puede saber si una cuenta de usuario está comprometida.

Proteger la base de clientes en línea de su institución financiera.

Intellinx Fraude y Seguridad está diseñado para identificar y prevenir el fraude en la plataforma externa, en línea, de su institución. Mediante el control de todo el tráfico web, analiza y alerta a los investigadores sobre las actividades sospechosas, permitiendo esta solución ayudar a detener la actividad fraudulenta. También aprende y se adapta a medida que trabaja en la detección de patrones que son normales para clientes específicos, y anormal para los demás. Ubicado en un esquema centralizado denominado Enterprise Case Manager, los investigadores tienen un único lugar para ir a la información pertinente para cada caso.

Fraude y Seguridad en la Web

El fraude Web plantea una amenaza importante para su institución.

Ya sea con técnicas avanzadas de Troyanos para la inserción de programas maliciosos en las computadoras corporativas o con técnicas de "man in the browser " "hombre en el navegador", los hackers secuestran las credenciales del usuario y cambian los datos enviados al servidor.

Su reputación está en línea.

Los clientes esperan que sus datos sean protegidos y la gestión inadecuada del riesgo puede dejar a su empresa en riesgo de perder dinero y clientes.

Se informó de más de
$ 781 millones
perdidos debido al
fraude Web en 2013.
(FBI, IC3 Report 2013)

- Crea perfiles de comportamiento detalladas para los usuarios de aplicaciones en línea.
- Responde a cambios del "comportamiento normal" en una amplia gama de escenarios.
- Reduce el robo de identidad, la posesión de cuentas, accesos hombre-en-el-navegador y ataques DDoS. (Distributed Denial of Service attacks)

Fraude y Seguridad en la Web

Como trabaja:

Cuando un cliente interactúa con una aplicación online se genera un perfil.

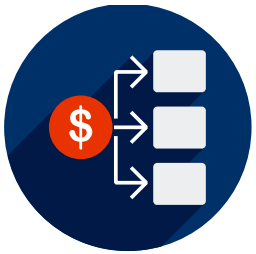
Este perfil identifica y carga patrones, creando una completa pintura de la actividad típica del cliente. Si un cliente interactúa de forma tal que no cumple con esos patrones, entonces se crea un alerta y sus cuentas pueden ser investigadas o suspendidas.

Ejemplos de reglas:

Regla:
Intentos de ingreso

Alerta:
Un cliente intenta identificarse desde ubicaciones diferentes y sospechosas en un tiempo dado.

Un cliente intenta identificarse usando diferentes identificadores de huella digital en un corto período de tiempo.



Regla:
Transacciones de extracción

Alerta:
Una cuenta nueva o cuenta reactivada realiza múltiples transacciones de extracción por un gran monto.

Un cliente intenta realizar una transacción de extracción que se ha marcado como de alto riesgo.

Regla:
Pagos a nuevos beneficiarios

Alerta:
Un cliente intenta realizar una transacción de pagos a varios nuevos beneficiarios en un plazo muy corto de tiempo.

www.optaris.com

hola@optaris.com

Sanciones de No Cumplimiento

Las consecuencias pueden ser muy caras.

Las multas por no cumplimiento pueden costar millones de dólares.
Las soluciones de detección de sanciones anticuadas no proporcionan el cumplimiento que se necesita para seguir cumpliendo con las leyes contra el lavado de dinero.

Proteja su institución financiera con el cumplimiento, todo en un solo lugar.

Con Intellinx Protección de Cumplimiento, en cada transacción se puede investigar la consolidación de su control tanto de cumplimiento como de fraude, en cualquier número de listas de sanciones, incluidas las listas blancas, listas negras y listas provistas por el cliente.

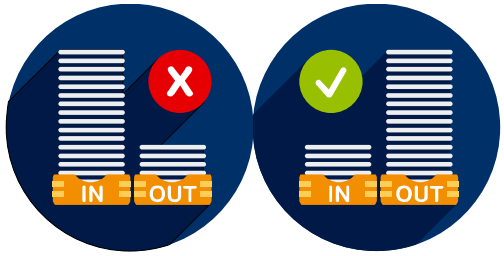
Sanciones de No Cumplimiento

Detectar violaciones es un proceso de dos pasos.

Después de asegurarse que su lista de sanciones esté actualizada, usted debe encargarse y administrar la infraestructura para poder monitorear las transacciones del día a día, en tiempo real. Estas dos medidas por sí solas insumen mucho tiempo y las investigaciones sobre violación toman infinitamente más recursos.

Los falsos positivos ponen en tensión a los escasos recursos.

Usted no debería gastar su tiempo en investigar falsos positivos. Con poco margen para el error y plazos que cumplir, hacen que las soluciones tradicionales no brinden gran ahorro de tiempo ni dinero y sean serios desafíos cuando se encuentran en situación de cada potencial violación.



- Manténgase en cumpliendo de las leyes contra el lavado de dinero.
- Manténgase actualizado con el acceso a más de 100 listas de sanciones a nivel mundial.
- Encuentre los relacionamientos entre individuos y grupos.

Sanciones de No Cumplimiento

Como trabaja:

A medida que va monitoreando las transacciones, van apareciendo alertas rojas en un tablero central de control para una fácil revisión y rápida acción. El investigador está equipado con las marcas y cualquier otra información relevante para realizar el due diligence y asegurar el cumplimiento con las leyes de antilavado de dinero. Mediante la introducción de una lista personalizada de falsos positivos, se puede minimizar el tiempo insumido en investigar los falsos positivos.

Ingresando una lista personalizada de falsos positivos, se pueden minimizar los tiempos que consume la investigación de falsos positivos.

Incluye las siguientes características:

Monitoreo de Transacciones:
Una vez que el registro de pago es enviado, se lo verifica con sus listas seleccionadas de sanciones.

Precisión en la Verificación:
Usted puede controlar el nivel de precisión requerida para que una correspondencia dispare una marca. Si define el 100% solo responderá a equivalencias exactas, mientras que con porcentajes mas reducidos podrá escalarlos a las definiciones de los usuarios.

Lista de Buena Gente:
Luego de haber sido identificados los nuevos falsos positivos, Usted puede mover el nombre a una lista para prevenir que sea marcado nuevamente.

Control inteligente de palabra:
A fin de poder comparar las transacciones con los variados campos de las listas, la solución utiliza el algoritmo de Distancia de Levenshtein

Chequeo Duplicado:
A medida que se van chequeando las transacciones con las listas de sanciones, también va informando sobre cualquier transacción duplicada que contenga la misma información basada en datos claves de la transacción.

Administración de listas:
Si bien la solución mantiene listas pre-configuradas, Usted puede agregar sus propias listas negras o blancas. Estas listas se van actualizando constantemente para asegurar que esté disponible la información mas reciente de las sanciones.

Casos de Estudio

Un grupo de ahorro e inversión de larga trayectoria internacional, con más de 12 millones de clientes y 55.000 empleados en todo el mundo,

implementó Intellinx Ciber Fraude y Gestión de Riesgos para bancos para ayudar en la protección contra el fraude de información privilegiada. Sólo cinco meses después, el sistema había impedido un estimado de $ 2 millones de dólares de pérdidas por parte de una banda de crimen interno que tenía la intención de robar fondos de la compañía. Esto sin tener en cuenta el costo asociado del impacto negativo que se habría provocado en su reputación.

01- Captura y Recolección de datos

Las soluciones tradicionales pueden recopilar datos vitales desde los archivos de log y proporcionar análisis de la base de datos, pero no es suficiente. Los archivos de log insumen mucho tiempo de análisis y no proporcionan el nivel de detalle de todas las acciones del usuario, tales como consultas, vistas de pantalla y las operaciones que son necesarias para localizar y detener proactivamente el comportamiento fraudulento.

El enfoque de captura y recopilación de datos de la plataforma es amplia. Todos los datos que se intercambian entre las aplicaciones supervisadas dentro de una red corporativa quedan grabados mediante una tecnología de escucha de red patentada y quedan disponibles para su visualización e investigación en tiempo real. La solución puede capturar datos de texto, archivos binarios, tablas de bases de datos, XML y CSV, consultas de los usuarios, colas de mensajes y otras fuentes datos.

A través del cifrado 128/256 utilizando AES y digitalmente firmado con MD5 y RSA, los datos grabados pueden ser aceptados como pruebas forenses en la corte judicial de EE.UU.

02 - Perfiles y Alertas

Los desafíos que plantea la gestión de perfiles y alertas, implican un eficaz desarrollo del análisis del comportamiento que puede identificar el comportamiento sospechoso, manteniendo baja la tasa de falsos positivos. Las soluciones tradicionales no pueden alertar sobre los diferentes escenarios enfocados al comportamiento y tienden a generar más alertas que las que una empresa puede manejar. La plataforma se va volviendo cada vez más inteligente con el tiempo, para detectar los casos de fraude. Proporciona una mejor visibilidad, generando menos banderas falsas y más verdaderas, resultando alertas mucho mas precisas para los investigadores.

El modelo de datos de la plataforma propuesta es capaz de mantener los datos estáticos y dinámicos relativos a empleados, cuentas y clientes.
Como es sistema genera perfiles para cada usuario o grupo de usuarios, permite discernir y correlacionarse con el motor analítico.

El motor analítico aplica una puntuación de riesgo a los agentes inusuales, genera alertas inmediatas, y limita la tasa de falsos positivos. Las reglas y las puntuaciones pueden ser ajustadas y afinadas para asegurar su éxito continuo.

El perfilado dinámico permite al sistema aprender y adaptarse, ayudando a definir qué actividad es normal y cual es sospechosa.

03 - Investigación y Resolución

Dada la complejidad de los diferentes sistemas, la captura limitada de los registros de log y el número de falsos positivos, los investigadores se encuentran en una posición en donde la investigación es un proceso difícil y costoso.

El Investigation Center es un centro de actividad donde usted puede ejecutar todas las actividades que implican el ciclo de vida de un proceso de investigación. Está compuesto por un conjunto de funciones integradas, cada una de las cuales asiste a los investigadores dentro de las diferentes facetas en la investigación y resolución del fraude.

Alertas y Gestión de casos:

Asiste a los investigadores en la priorización y revisión de las actividades sospechosas de principio a fin.

Capacidad única de reproducción:

Permite a los investigadores ver las pantallas donde la actividad sospechosa ocurre (aunque solo hayan sido miradas), dándole un contexto completo de las acciones ejecutadas.

Actividad de los usuarios en múltiples plataformas:

Permite ejecutar búsquedas estilo Google sobre el contenido de todas las pantallas accedidas por el usuario a través de múltiples plataformas en un tiempo dado, con el propósito de encontrar, por ejemplo, todos los usuarios que accedieron a una cuenta de cliente en un periodo de tiempo específico.

Análisis de enlaces:

Permite visualizar las relaciones entre empleados, clientes, cuentas y otras componentes sensibles.
Las entidades fraudulentas o bajo investigación son resaltadas a los efectos de permitir una mayor claridad y examen sobre las mismas.

Control a través de reglas de negocio:

Permite a los investigadores manejar puntuaciones para reducir el rango de falsos positivos.

Su ventaja,
nuestra
experiencia.

Gracias!

OPTARIS