

Solución para la detección del Fraude Informático.

A nombre de nuestra representada, **Locum Software**, especialistas en soluciones de seguridad, deseamos presentar **inSIGHT**, la solución para la detección de fraude.

El desafío

A medida que más y más casos, de alto perfil, de fraudes internos corporativos han salido a la luz, hay una mayor conciencia de la amenaza interna hacia los activos de la empresa procedente de empleados de la empresa, en contraposición de amenazas externas. Esta amenaza interna proviene principalmente de personas que tienen acceso autorizado y que son capaces de manipular los sistemas internos para obtener beneficios personales. En la medida que estas personas utilizan los mismos comandos de usuario tanto para perpetrar sus planes ilegales, como para realizar su trabajo del día a día, es muy difícil de detectar los infiltrados maliciosos de la gran mayoría de empleados honestos e inocentes.

Las organizaciones que dependen de sistemas legados para sus procesos de negocio, puede enfrentar el duro desafío de proteger las aplicaciones que no fueron diseñados con los mecanismos de control necesarios para el entorno abierto de hoy y las regulaciones de privacidad. Estas regulaciones (FSA, PCI, GLBA, HIPAA y otros) requieren que las organizaciones mantengan registro de auditoría de los accesos de los usuarios a los datos confidenciales de clientes, incluyendo las transacciones de actualización y consultas. La pistas de auditoría deben contener información detallada, incluyendo los datos específicos del cliente que se ha accedido, por cual el usuario, cuándo y desde dónde. El desarrollo de una solución interna con estos requisitos puede implicar un tremendo esfuerzo, ya que puede ser necesario cambiar miles de los programas de aplicación de la organización.

Solución de **inSIGHT** brindada por Locum

Locum presenta el avance de **inSIGHT x** en la detección y prevención de amenazas internas. **inSIGHT** brinda un sistema de vigilancia de primera calidad en su tipo, que trabaja a través de las distintas plataformas que brinda una visibilidad, sin precedentes, de la actividad del usuario final en las plataformas Unisys y demás plataformas de toda la empresa. La solución **inSIGHT** proporciona una infraestructura fundamental para la lucha contra el fraude interno y la fuga de información, haciendo que los usuarios autorizados rindan cuentas por sus acciones. Intellinx es el único producto actual en el mercado que ofrece lo siguiente:

Visibilidad sin precedentes de la actividad del usuario final – Se brinda visibilidad completa de la actividad del usuario final la cual dispone de reproducción visual de cada pantalla y tecla y mensajes cliente / servidor en todas las aplicaciones y en todas las plataformas principales. Todas las acciones son visibles, incluyendo la actualización y las acciones de sólo lectura. Todos los tipos de usuarios finales son rastreados incluyendo

usuarios privilegiados como los administradores de sistemas y administradores de bases de datos que pueden poseer un riesgo más alto, ya que tienen mayores niveles de autorización.

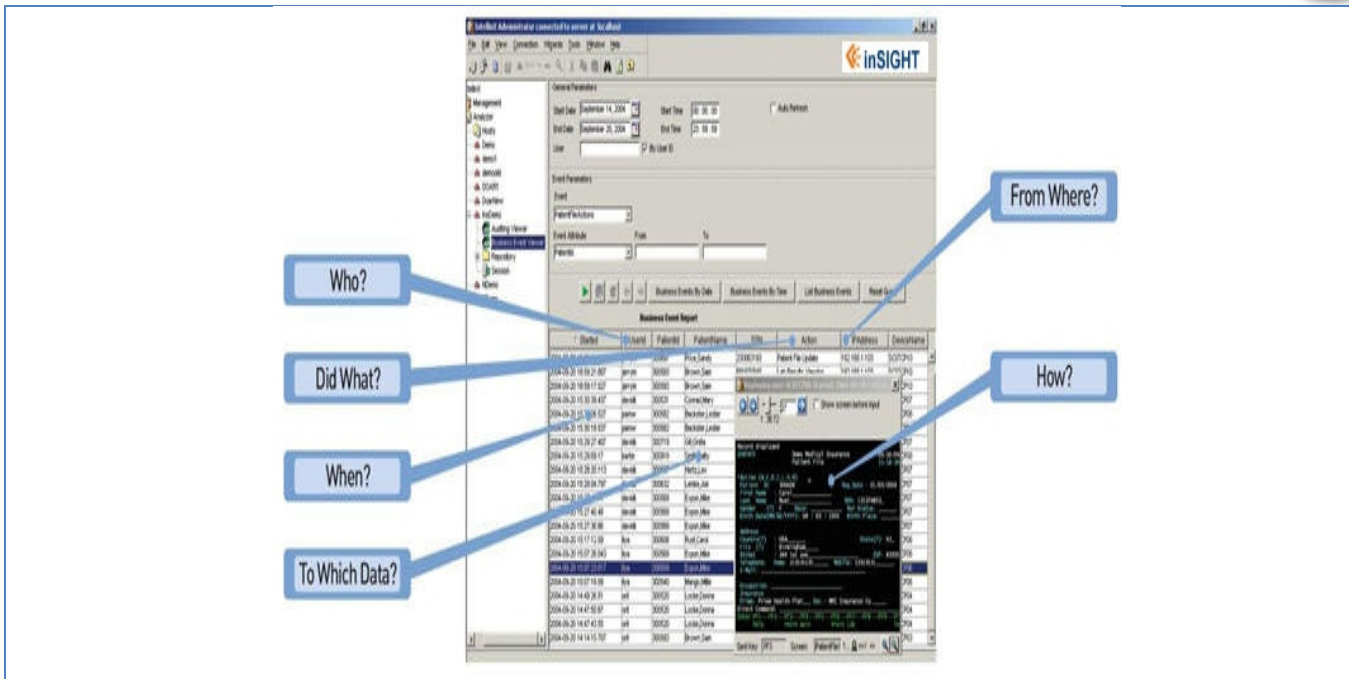
Seguimiento completo de pistas de auditoría - inSIGHT registra la actividad completa 24x7 del usuario, lo que es fundamental para llamar a cuentas a los usuarios finales por sus acciones. Independientemente de si las reglas de detección adecuadas están en su lugar en el momento de un evento, la repetición después del evento permite la investigación forense en un momento posterior.

Búsqueda a través de todas las plataformas incluyendo plataformas Legadas - inSIGHT proporciona una solución única para el seguimiento de la actividad del usuario en todas las plataformas importantes, como Unisys, IBM y los sistemas Windows, Web, MQ y aplicaciones Cliente / Servidor. Asimismo, da seguimiento de la actividad de la red dentro de LINC / EAE / ABS y permite buscar, desde una sola búsqueda simple, cualquier valor específico que sea mostrado en cualquier pantalla de usuario a través de múltiples plataformas. Las reglas de **inSIGHT** dan seguimiento de los procesos multi-plataforma del negocios. Por ejemplo, un proceso de negocio seguido por **inSIGHT** puede comenzar en un equipo Unisys, continuar en una aplicación cliente-servidor y finalizar en la web.

Seguimiento del comportamiento de los usuarios al nivel de aplicación - inSIGHT es la única solución en el mercado que analiza la actividad del usuario a nivel de pantalla de la aplicación, en lugar de a nivel de red o base de datos. Las reglas de **inSIGHT** permiten el seguimiento de todas las pulsaciones de teclado del usuario y el flujo de pantallas accedido por el usuario, detectando los procesos de negocio relevantes, incluyendo cada valor del campo accedido o actualizado. Esta información se correlaciona en tiempo real con la actividad de otros usuarios finales, con la actividad anterior y otros tipos de información generando alertas por el comportamiento sospechoso en tiempo casi real.

inSIGHT : Instale y Use.

inSIGHT proporciona un excepcional valor de negocio de manera inmediata. Una vez que termina la instalación (que suele durar unas pocas horas), **inSIGHT** comienza a capturar toda la actividad de los usuarios de toda la empresa, permitiendo a los auditores internos llevar a cabo investigaciones exhaustivas con repetición visual completa. Los Agentes de seguridad inmediatamente pueden realizar búsquedas tipo Google para todas las pantallas de usuario en las que los valores específicos aparecieron durante un plazo específico en cualquier aplicación a través de todas las plataformas principales de la empresa. Las Organizaciones se comienzan a beneficiar de **inSIGHT** sin demora, sin necesidad de una integración con ninguno de los sistemas de la organización que toma mucho tiempo o las configuraciones relacionadas con la aplicación.



Sin riesgo al implementar

La tecnología sin agentes de **inSIGHT**, pendiente de patente, intercepta la comunicación entre usuarios finales y los servidores de la empresa por medio de “sniffing” en las transmisiones de red a través de los conmutadores de red. Por lo tanto, Intellinx no afectan al rendimiento de hosts o redes de ninguna manera.

La arquitectura de **inSIGHT** es flexible y escalable, proporcionando una solución rentable a las organizaciones con 500 a más de 100.000 usuarios.

No hay necesidad de instalar ningún software o hardware en el host o clientes.

Los archivos de grabación son

cifrados y firmados digitalmente, por lo que son potencialmente admisibles en los tribunales.

Las organizaciones se benefician del proceso de instalación rápida, sin riesgo para las operaciones de TI en curso.

inSIGHT da seguimiento de la actividad del usuario en todas las principales plataformas, incluyendo Unisys T27, mainframe de IBM, cliente / servidor, Web y más:

IBM Mainframe screen protocol
- 3270 on SNA, TCP/IP
(TN3270) and Enterprise
Extender.

IBM iSeries screen protocol -
 5250 on SNA, TCP/IP
 (TN5250), and MPTN.
 Client/Server messages -
 TCP/IP, MQ Series, MSMQ, IBM
 mainframe SNA LU0 and LU6.2,
 SMB
 HTTP, HTTPS
 VT100 and other VT flavors
 SSH

Text
 and binary files, log files,
 database tables, XML and CSV
 files

Las grabaciones se almacenan en
 formato altamente condensada, lo
 que permite el monitoreo de decenas
 de miles de usuarios finales dentro de un
 organización sin gran impacto en el
 espacio en disco.

