Renfe: análisis de información con visión global

Cuando ha sucedido una crisis, se habla mucho de trazabilidad completa, de tener toda la información, saber qué ha ocurrido, cómo ha reaccionado cada pieza involucrada… Pero es necesario ofrecer evidencias irrefutables sobre la actividad deseada, tener integridad de los datos monitorizados, y poder acortar los tiempos de investigación. Para ello se deben poder generar alertas con enlace directo a los datos, pudiendo contrastar esa información con evidencias reales. Es decir poder grabar y reproducir la actividad deseada de forma integral.

Francisco Lázaro Anguis / Paloma García Piserra

En la película "En el punto de mira", ocho desconocidos, cada uno con un punto de vista diferente, intentan descubrir qué pasó realmente tras un intento de asesinato al presidente de los Estados Unidos. Cuando el presidente recibe un disparo poco después de llegar a España, surge el caos y las vidas de distintas personas coinciden en la caza del asesino. Esta investigación está llena de tramas opuestas, análisis contradictorios, informaciones dispares, ya que los puntos de vista individuales no contemplan todo lo sucedido. A medida que ellos y otros van dando a conocer sus historias, las piezas del puzle empiezan a encajar, y se hará evidente que hay motivaciones mucho más oscuras de lo que parece a simple vista.

Cada testigo conoce una parte de la verdad, pero si solo se tuviera en consideración "su verdad", obtendríamos conclusiones erróneas. Por ello, tras un incidente de seguridad, y para lo que llamamos "lecciones aprendidas", se requiere un "testigo" omnipresente en todas las partes del puzle, que cuente verazmente lo que ha visto, o mejor dicho, que tenga la capacidad de recopilar, analizar y presentar la información de una forma fehaciente.

Trazabilidad

¿Por qué es importante tener una solución que encaje las piezas del puzle en un momento de crisis? La clave es poder obtener una trazabilidad completa de todos los sucesos. Que cada "personaje" cuente su versión de forma independiente no es suficiente para resolver el caso.

Con la intención de estandarizar procedimientos, o mejorarlos, o con el fin de tener un análisis forense certero, es necesario tener una visión global (lo que ha hecho cada parte y resultado de esa acción), permitiendo coordinar la información, aunque esta se obtenga a través de medios dispares. La prioridad es precisamente la necesidad de conocer qué ha pasado, cuándo y dónde.

Grabación de video de sesiones

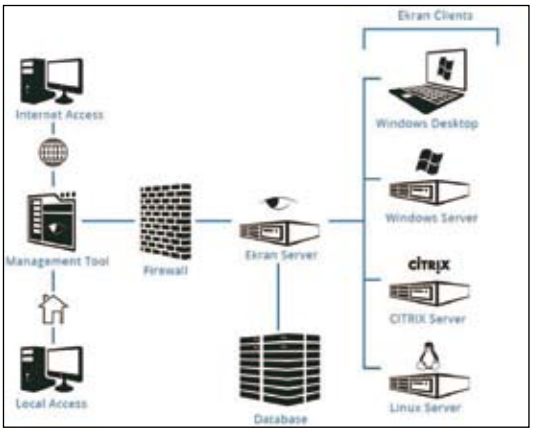
Bajo esas premisas, **Renfe** utiliza **Ekran** para tener una visión global de todo lo sucedido en los equipos que conforman el grupo de respuesta y así poder responder de una forma completa ante incidencias de seguridad. La solución de Ekran permite a Renfe saber cómo se han desarrollado los sucesos y qué reacción ha habido ante ellos. Con dicho fin, se decide instalar la solución Ekran, ya que proporciona una grabación de video de todas las sesiones de los servidores, así como de las sesiones locales y remotas de las Workstation en la red corporativa.

Cuando se evalúan las posibles opciones para conseguir juntar toda la información que se necesitaba y poder gestionarla y analizarla desde un único punto, se observó que Ekran cumplía técnicamente con todos los requisitos que se necesitaban para ese proceso. Esta propuesta tecnológica permite generar alertas en tiempo real con enlace directo al video correspondiente, proporcionan una monitorización más proactiva y la coordinación de los diferentes grupos dentro de Sistemas de la Información. De esta manera, queda evidencia de las acciones realizadas por los diferentes grupos críticos. Todo se visualiza y se gestiona desde un único punto, agrupando todas las piezas para conseguir el objetivo.

Renfe utiliza Ekran para tener una visión global de todo lo sucedido en los equipos que conforman el grupo de respuesta y así poder responder de una forma completa ante incidencias de seguridad.

Ekran es una herramienta fácil de instalar y utilizar, y a través de ella se obtiene una trazabilidad completa, proporcionando un considerable ahorro de tiempo, ya que permite visualizar a través de filtros sólo los eventos clave que se deseen. Facilita, además, el cumplimiento normativo como por ejemplo de PCI y de la LOPD.

Cuando hablamos de que es necesario juntar todas las piezas del puzle de forma correcta, además de tener un único punto desde donde se gestione todo, es necesario disponer de un equipo de personas experimentadas, preparadas para resolver todas las incidencias que puedan encontrar en el camino. El equipo humano de Renfe junto con el de **Consist** han aunado esfuerzos para conseguir dicho fin de forma rápida y eficaz. ■



Francisco Lázaro Anguis
CISO
RENFE

Paloma García Piserra
Country Manager
CONSIST ESPAÑA