



Principales aportaciones del proyecto

- Permite a Iberdrola reaccionar inmediata y eficazmente frente a ataques y situaciones anómalas desde un punto de vista global
- Supone una mejora muy significativa en la capacidad de Iberdrola para filtrar y correlar los más de 15 millones de eventos de seguridad que se producen diariamente y los reduce a muy pocas alarmas críticas.
- Facilita a Iberdrola una visión clara de su exposición a amenazas, imprescindible para la gestión de riesgos.

Con una historia de 100 años, Iberdrola presta servicio a más de 16 millones de clientes – incluyendo nueve millones sólo en España. Es la compañía líder mundial en energía eólica y uno de los principales operadores en el sector de energías renovables.

Desde hace tiempo, Iberdrola tiene un fuerte compromiso con la promoción y adopción de las mejores prácticas de calidad y buena gestión corporativa en todas sus operaciones. La reciente consolidación y gestión eficiente de su infraestructura de seguridad lógica a través de la implementación del SIM ArcSight ha supuesto un paso adelante en su programa estratégico de calidad y gestión corporativa.

El desafío de Iberdrola

Con múltiples unidades de negocio y prestando servicios a millones de clientes en diferentes entornos en todo el mundo, Iberdrola se enfrentaba a un desafío común a todas las corporaciones de su tamaño, esto es, el manejo e

CASO DE ÉXITO: IBERDROLA

Javier García Carmona

DIRECTOR DE SEGURIDAD LÓGICA.
IBERDROLA S.A.



“La herramienta SIM ArcSight ha tenido un impacto inmediato en nuestro negocio, fortaleciendo enormemente nuestra red frente a amenazas externas e internas. Adicionalmente, y gracias a la identificación, correlación y priorización de eventos de seguridad, ArcSight ha mejorado la eficiencia de nuestra organización, eliminando falsos positivos y minimizando el número de alarmas críticas”

interpretación del volumen de información de seguridad generado por infinidad de dispositivos en toda su red.

En este contexto, Iberdrola requería una clarificación completa de su entorno de seguridad para evaluar y reducir su exposición al riesgo mediante la reacción inmediata frente a ataques o

situaciones anómalas, mejorando también el control y eficiencia de sus políticas y dispositivos de seguridad. Además, y de acuerdo con su compromiso con la calidad y las mejores prácticas de gestión, Iberdrola también exigía que este proyecto sirviera como base para el desarrollo de un cuadro de

SEGURIDAD LÓGICA: COMPLEJIDAD CRECIENTE

Métrica	2002	2005
Estrategia	Defensa perimetral	Defensa global (También Amenazas internas)
Herramientas en uso	Decenas	Miles
Alcance	Capa de red	Stack completo
Eventos / Día	50,000	50,000,000
Almacenamiento de datos	Centralizado	Distribuido y fragmentado
Conocimiento Necesario	Limitado (FW, VPN, AV)	Amplio (Aplicaciones, BD, S/O, Compliance)
Activos en Riesgo	Conocidos y limitados	Ilimitados y desconocidos
Cobertura Geográfica	Oficinas centrales	Distribuido globalmente
Toma de Decisiones	Sólo IT	IT, CFO y responsables de negocio
Usuarios primarios	► Administradores IT (Tiempo parcial)	► Analistas de seguridad (24x7) ► Auditoría y Compliance
Objetivos y metas	► Informes mensuales ► Investigaciones Ad-hoc	► Protección global en tiempo real ► Informes de compliance ► Gestión de riesgo ► Respuesta a incidentes ► Análisis forense ► Cuadro de mandos



IBERDROLA

mandos para la evaluación del rendimiento y la calidad de gestión.

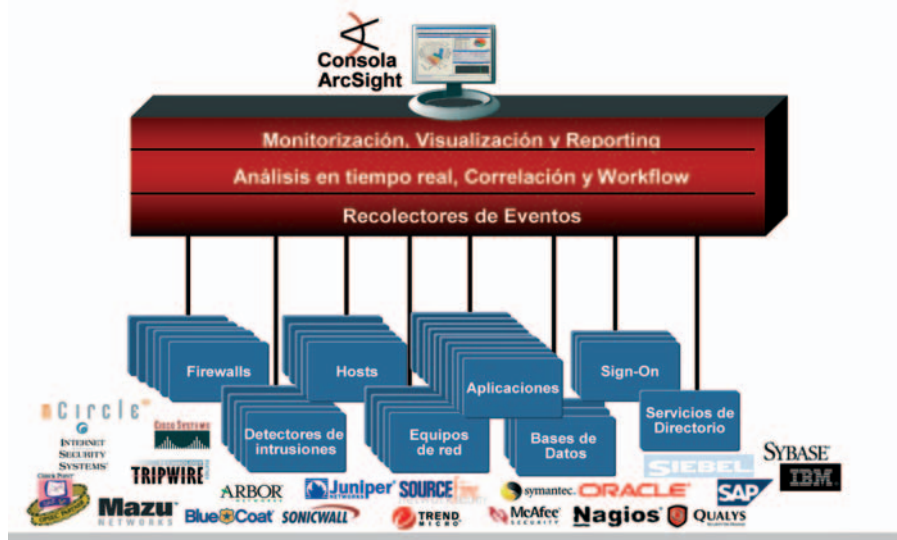
En la situación de partida, los millones de eventos de seguridad generados por sus sistemas cada día suponían un desafío muy considerable para Iberdrola a la hora de filtrar y correlar esa información. Este hecho estaba teniendo un impacto negativo en la eficiencia de sus sistemas de seguridad lógica y costaba cientos de horas/hombre de trabajo innecesario y de bajo nivel para el personal.

Iberdrola entendió que en esta situación necesitaba un sistema de gestión de seguridad corporativa de primer nivel para alcanzar sus objetivos estratégicos de negocio e incrementar la eficiencia de sus sistemas.

El equipo de Iberdrola investigó inicialmente nueve tecnologías que representaban la oferta existente en el mercado. Después de un proceso exhaustivo, Iberdrola seleccionó a ArcSight y a otro fabricante para realizar pilotos, basándose en criterios como, funcionalidad, estabilidad, escalabilidad, facilidad de integración, capacidad técnica del integrador, roadmap del fabricante y coste total de propiedad (TCO). Finalmente, y después de realizar en pocos días un piloto particularmente exigente, ArcSight fue la tecnología seleccionada.

«Hemos seleccionado a ArcSight como proveedor por dos sencillas razones», afirma Javier García Carmona, Director de Seguridad Lógica de Iberdrola. «Primero, nos parece claro que ArcSight ha desarrollado la solución SIM más completa del mercado para grandes entidades y corporaciones. Segundo, nos convenció la capaci-

Un solo punto para consolidar toda la información



dad técnica y el grado de especialización de Breyer, el partner integrador».

La solución de ArcSight

La solución de ArcSight satisfizo los criterios específicos de selección de Iberdrola. El proyecto ha permitido la captura y consolidación de toda la información de seguridad generada en la

La característica diferenciadora que llevó a Iberdrola a seleccionar la solución de ArcSight fue el amplio abanico de capacidades que ofrecía para resolver las complejas necesidades de su negocio. «No era tan importante que la herramienta puntuara un diez sobre diez en uno o dos aspectos, pero resultaba vital que no puntuara menos de ocho en cada criterio de evaluación», añade García Carmona. «Eso es exactamente lo que hizo el SIM de ArcSight».

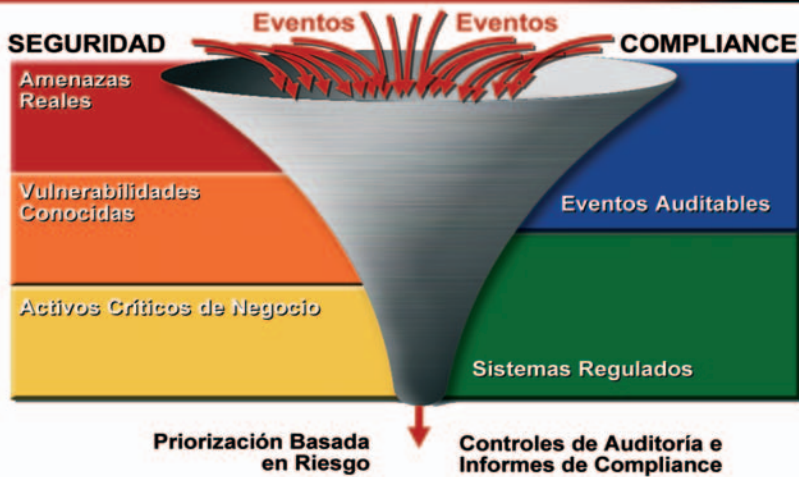
Iberdrola compró la primera de sus 1.200 licencias en Diciembre del 2004, después de la realización con éxito del piloto. «Era esencial tener una base sólida, y el trabajo más pesado era el análisis a alto nivel del volumen y la estructura de la información que debíamos consolidar. Además teníamos que integrar sin traumas el SIM de ArcSight dentro de los sistemas, aplicaciones e infraestructura ya existentes en Iberdrola. Por último hay que tener en cuenta que el nivel de exigencia de Iberdrola en cuanto a metodología, documentación y calidad del proyecto es extremadamente alto,» afirma José Manuel Bermúdez, Consejero Delegado de Breyer, partner certificado de

**La implementación del SIM
ArcSight ha supuesto un
paso adelante en su
programa estratégico de
calidad y gestión
corporativa**

red global de Iberdrola, haciendo posible el análisis e interpretación en tiempo real de los logs procedentes de dispositivos de comunicaciones y seguridad, sistemas operativos y aplicaciones.



Más allá de la identificación de amenazas: Filtrado, correlación y análisis en tiempo real



ArcSight en España. «El tiempo que invertimos en el análisis, y la flexibilidad y escalabilidad del producto facilitaron una implantación rápida y sin incidentes significativos.»

«La calidad general de la solución de ArcSight y el alto nivel de los ingenieros a cargo de la planificación e implantación no sólo nos permitieron alcanzar nuestros objetivos iniciales, sino que, unidos a la capacidad de integración de ArcSight con multitud de plataformas y entornos heterogéneos, acortaron significativamente los plazos de implantación,» comenta García Carmona.

El Impacto de Arcsight

El SIM de ArcSight provocó un impacto inmediato en el negocio de Iberdrola. La eléctrica ha experimentado una mejora muy significativa en su capacidad para filtrar y correlar el volumen masivo de información que antes suponían un cuello de botella para el departamento de seguridad. Tanto es así que las alarmas críticas son ahora relativamente raras, debido a que ArcSight identifica y prioriza automáticamente los eventos de seguridad, y elimina por tanto el desperdicio de horas/hombre asociados a la investi-

gación de cientos de falsos positivos.

La potencia de la solución ArcSight y el conocimiento y experiencia de Breyer en la implantación de proyectos grandes y técnicamente complejos añadieron valor a lo largo de todo el proyecto. Resultó especialmente llamativa para Iberdrola la rapidez de la implantación y la facilidad de integración dentro de sus entornos tecnológicos.

Sabemos cuál es el coste financiero y de negocio para la organización de un incidente de seguridad detectado demasiado tarde

Adicionalmente, ArcSight ha añadido claridad al entorno de seguridad de Iberdrola hasta un nivel previamente inalcanzable. Sus funcionalidades de consolidación y correlación permiten una comprensión global de la actividad, interna y externa, relacionada con posibles amenazas, midiendo con precisión

la exposición a dichas amenazas y facilitando la ejecución de medidas correctivas.

«Al construir el mapa instantáneo de nuestras vulnerabilidades en toda la red hemos podido emplear nuevos procesos y actividades que reducen significativamente el riesgo de ataque», dice Javier García Carmona. «Esto es fundamental para proteger nuestra red de ataques internos y externos, pero también nos permite reportar ese tipo de actividades, contribuyendo a que las políticas y estándares de calidad de Iberdrola se sitúen entre los más rigurosos de nuestro sector. Además no debemos olvidar que la gestión eficiente de la seguridad es vital en estos tiempos en los que, desafortunadamente, las amenazas terroristas son noticia casi diaria en todo el mundo»

La tecnología de ArcSight ha servido también para liberar al equipo altamente especializado de seguridad lógica de los análisis de bajo nivel y les ha permitido concentrarse en desarrollar nuevos proyectos que realmente añaden valor a la organización – más allá de la tarea de «mantener las luces encendidas»

Aunque la contribución a la mejora en la calidad y el aumento de la eficiencia en la gestión de sistemas son de fundamental importancia para Iberdrola, el Director de Seguridad, García Carmona, tiene muy claro cuál es el beneficio más importante de ArcSight. «Conocemos el TCO de nuestra infraestructura de seguridad y los beneficios que estamos obteniendo de la mejora en nuestra capacidad para gestionar y explotar esos activos. Sin embargo, lo esencial es que sabemos perfectamente cuál es el coste financiero y de negocio para la organización de un incidente de seguridad detectado demasiado tarde. Con 16 millones de clientes a los que atender, simplemente no nos podemos permitir fallos de protección en nuestra red, y por esa razón hemos apostado por ArcSight». ♦