Modelo de seguridad gestionada basada en eventos de Gobierno de Aragón

Andoni Valverde, Responsable Implantación Productos Propios, zona Norte de S21sec.

Robero Acero, Responsable de Gestión de Seguridad de Aragonesa de Servicios Telemáticos (AST).

Resumen

Transcurrido un año desde que S21sec y Aragonesa de Servicios Telemáticos (AST) – entidad responsable de la provisión de infraestructuras y servicios telemáticos de Gobierno de Aragón – emprendieran el proyecto para la monitorización y gestión de la seguridad de sus servicios e infraestructuras TI, este artículo describe la evolución del proyecto y recoge los resultados que, a día de hoy, permite a AST el disponer de un equipo especializado en seguridad como es S21sec, que monitoriza y analiza los sucesos y tendencias de la organización activamente, lo que se traduce en respuestas y acciones de mejora continua, y cuyo objetivo es el de proporcionar un mayor nivel de seguridad en beneficio de la calidad de los servicios provistos por AST.

El modelo desarrollado garantiza un servicio integral de **seguridad gestionada basada en eventos** con capacidad de reducir los tiempos de detección de incidentes y la gestión inmediata para su neutralización. La solución es posible gracias a Bitacora Log Management, que actúa como plataforma integral de recolección, análisis y explotación de logs y a los servicios de monitorización y operación de los dispositivos de seguridad ofrecidos en 24 x 7.

Aragonesa de Servicios Telemáticos

Aragonesa de Servicios Telemáticos es la entidad de derecho público que, desde su puesta en marcha en 2002, participa activamente en la cadena de prestación de servicios y soluciones en Tecnologías de la Información y la Comunicación (TIC) al Gobierno de Aragón. Este modelo presenta importantes beneficios a la Administración Pública, así como al territorio y al ciudadano: optimización del uso de infraestructuras y servicios; homogeneidad, compatibilidad e interoperabilidad de soluciones; facilita la focalización en su actividad principal (servicios públicos, sanitarios, educativos, etc.); mayor extensión territorial de los servicios; más puntos de acceso a los servicios, etc.

En los últimos años, Gobierno de Aragón y AST se han posicionado a la vanguardia autonómica en innovación TIC. En mayo de 2009 se inauguró el Centro de Servicios Informáticos (CSI), así como el modelo de gestión de servicios e infraestructuras

global. Ese mismo año, de la mano de S21sec, aborda el proyecto de seguridad integral de la actividad de negocio, con el despliegue de Bitacora Log Management y los servicios 24x7 de monitorización y gestión de dispositivos que operan de forma conjunta.

Seguridad para los servicios críticos

AST provee de infraestructuras y servicios telemáticos a todos los Departamentos y Organismos de la Administración de la Comunidad Autónoma de Aragón. Los servicios internos y públicos prestados a día de hoy, su evolución, complejidad, así como la previsión de crecimiento, requieren un elevado número de sistemas de información altamente heterogéneos que deben ser gestionados y administrados en conjunto.

La existencia de servicios de carácter crítico, como por ejemplo, diversos servicios sanitarios o la e-Administración, están sujetos a requerimientos legales específicos, cuya existencia marcan las necesidades de desarrollo en cuanto a generación, protección y disponibilidad de los registros de actividad que deban proveer las aplicaciones de los sistemas utilizados.

Además, la evolución de ataques, riesgos y nuevas amenazas procedentes de Internet y de dentro de las grandes redes, hace necesaria una gestión eficiente de la seguridad de la red y de los sistemas corporativos.

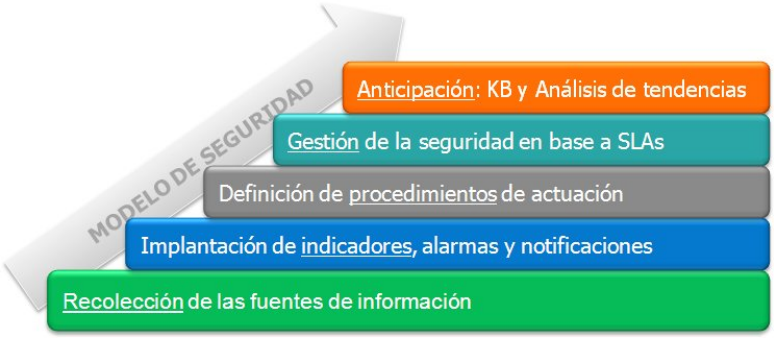
El alcance de la solución comprende todos los componentes tecnológicos de Gobierno de Aragón (sistemas, dispositivos de comunicaciones, aplicaciones, aplicaciones de desarrollo interno, etc.) en su arquitectura distribuida en varios CPDs.

El modelo de seguridad

Bitacora Log Management es la plataforma que permite recolectar y analizar cualquier tipo de evento, posibilitando el empleo de los logs de auditoría como posibles evidencias en un proceso judicial. Bitacora Log Management está certificado por Common Criteria, estándar en seguridad que en España otorga el Centro Criptológico Nacional (CCN), dependiente del Centro Nacional de Inteligencia del Ministerio de Defensa Español.

Los servicios de seguridad gestionada de S21sec se ofrecen ininterrumpidamente las 24 horas del día desde el Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés) y cuentan con la combinación de recursos humanos, procesos, inteligencia (información) y tecnología para la gestión de riesgos de seguridad y la monitorización y mitigación de los efectos de las amenazas de seguridad. La

plataforma para la gestión de la seguridad, actúa como punto único de acceso desde el que gestionar todos los aspectos relativos a la seguridad de las organizaciones.

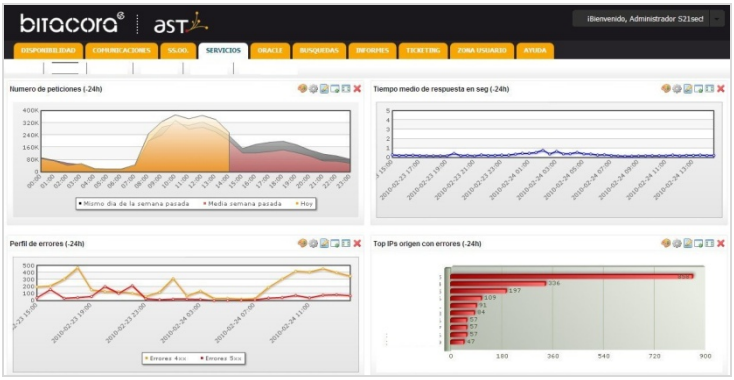


El modelo de seguridad está compuesto por capas donde cada una se sustenta en la anterior siendo la base de todas ellas el almacenamiento y salvaguarda de los logs en texto plano. Las capas intermedias se orientan a la explotación, esto es, el procesamiento de los datos, produciendo así diversos indicadores, informes y la emisión de alarmas. Las capas superiores del modelo representan los procedimientos asociados a las alarmas y los procesos de verificación, contraste e investigación, esto es, la gestión de la seguridad e inteligencia de negocio.

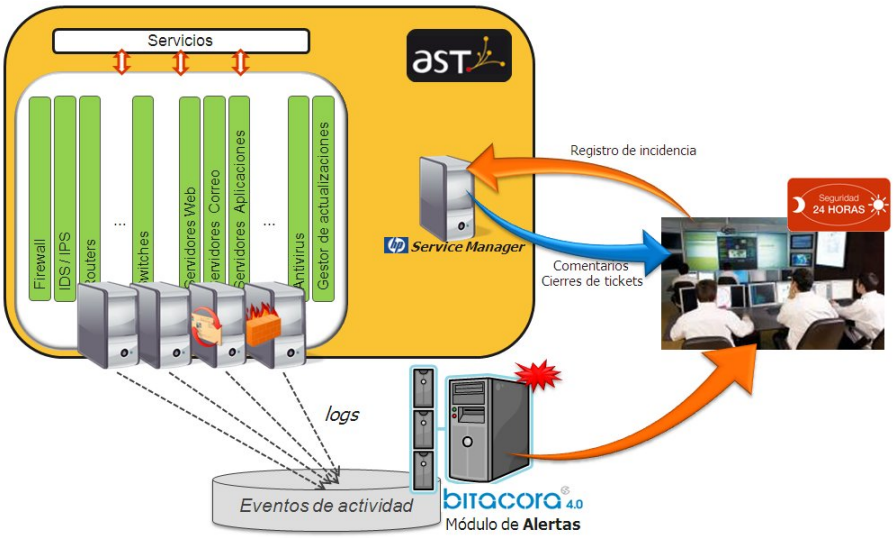
Operativa

AST dispone de un amplio entorno distribuido, por lo que la escalabilidad de la plataforma ha resultado una característica decisiva para lograr un despliegue integral en sus infraestructuras. Se trata de gigabytes de información diarios que son almacenados de forma segura en el sistema de almacenamiento dando lugar a la salvaguarda de la información y contribuyendo al cumplimiento de diversa normativa.

La información es procesada para sintetizar los miles de eventos recolectados en indicadores visuales que faciliten la lectura y la comprensión de los datos generados por los sistemas de información y, por tanto, ayudando a la toma de decisiones.



El motor de correlación de Bitacora Log Management analiza en tiempo real toda la información, generando alertas y categorizándolas según su gravedad: cambios de configuración fuera del horario laboral, ataques por fuerza bruta, accesos ilegítimos, escaneo de puertos, spam, propagación de malware, etc. En base a estos valores se propaga la alerta al SOC de S21sec para su correspondiente gestión y resolución.



Según los procedimientos de notificación y actuación definidos conjuntamente entre AST y S21sec, los operadores del SOC actúan según la alerta recibida, activo afectado, franja horaria, umbrales de normalidad, sucesos en otros entornos similares, etc., realizando las acciones pertinentes que van desde la notificación hasta la operación de dispositivos para detener o mitigar un ataque o incidente de mayor gravedad. Todo el proceso, desde la recepción de la alerta, su gestión, así como su cierre, queda debidamente registrado tanto en el sistema de gestión de incidentes y cambios corporativo de AST, como en la plataforma para la gestión de la seguridad de S21sec. Esta operativa es beneficiosa tanto para AST, que le permite conocer el estado de la seguridad actual y disponer de indicadores reales de la gestión que se realiza de la misma, como para S21sec que, a través de la plataforma para la gestión de la seguridad, tiene visibilidad del estado de la seguridad y de los eventos e incidentes en multitud de organizaciones, con el valor añadido de inteligencia de negocio que supone.

Objetivos alcanzados

- Capacitar a AST de un sistema de gestión de logs altamente cualificado para la centralización y explotación de los mismos: Bitacora Log Management recolecta y almacena logs de los sistemas de comunicaciones, servidores y aplicaciones. Provee un mecanismo de acceso a la información basado en perfiles que, interactuando con el mecanismo de LDAP corporativo delega en el mismo el control de acceso. Además, mantiene un control de auditoría interna que registra tanto el acceso a la plataforma como el acceso a la información.
- Dotar a AST de una visión global del estado de la seguridad que ayude en la toma de decisiones: Todos los sistemas considerados críticos disponen de un cuadro de mando de actividad. Los cuadros de mando han resultado de gran utilidad en la detección de malware y usos ilegítimos de los sistemas de información. La visión global en una escala temporal de mayor amplitud se traduce en la generación periódica de informes personalizados que en combinación con los informes emitidos desde el SOC de S21sec, son un fiel reflejo de la actividad en materia de seguridad desempeñada en la organización.
- Dar cumplimiento a requerimientos legales en materia de trazabilidad, salvaguarda y persistencia de la información. Gobierno de Aragón, como administración pública, tiene la obligación de dar cumplimiento a diversa normativa como la Ley de acceso electrónico de los ciudadanos a los servicios públicos, normativa relativa a la protección de datos de carácter personal, o el recientemente publicado Esquema Nacional de Seguridad.
- AST cuenta con el respaldo de un grupo de profesionales que conocen su infraestructura, que la atienden ininterrumpidamente, que tienen capacidad de gestionar sus dispositivos de comunicaciones estructurales y tienen la obligación de informar, reportar y notificar periódicamente de todos los sucesos. Asimismo, este equipo realiza labores de verificación y auditoría con objeto de identificar posibles riesgos potenciales y emitir así las consiguientes recomendaciones. De esta forma, AST logra:
    - Optimizar el tiempo de respuesta ante incidentes de seguridad y gestionarlos en base a procedimientos de notificación y actuación preestablecidos.
    - Gestionar remotamente dispositivos de comunicaciones.
    - Definir un modelo de monitorización y gestión avanzado, en 24 x 7, que se apoye en información proveniente de análisis exhaustivos de los eventos y el sistema de ticketing corporativo.

- Una gestión de la seguridad organizada, activa, de calidad e inmersa en un ciclo continuo de revisión y mejora.