



 CASO DE ÉXITO

Sector Movilidad

01

Introducción

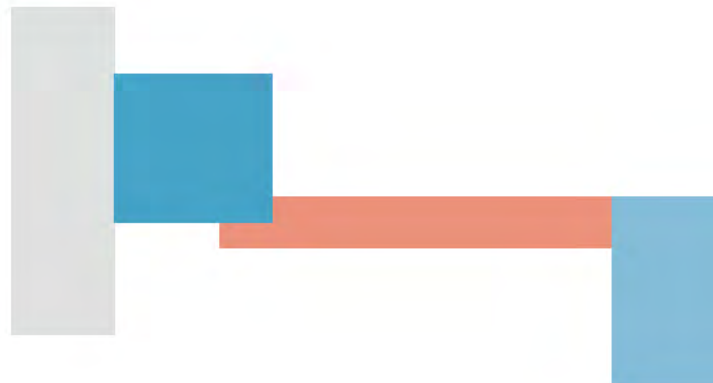
Nuestro cliente es una empresa pública de transporte ferroviario de pasajeros y mercancías; cuenta con más de 5.000 trenes que circulan cada día por el territorio nacional, más de 500 millones de viajeros al año y con cerca de 15.000 empleados.





La organización está constituida como la cabecera de un grupo de 5 sociedades anónimas y se prevé que el año 2023 cierre con unos ingresos de más de 1.332 millones de euros.

Cuentan con un departamento de gerencia de ciberseguridad y privacidad, con una inversión de más de 245 millones de euros en digitalización y ciberseguridad entre los años 2018 y 2023.



02

Problemática/reto



La compañía **dispone de personal especializado** para la operación del centro de operaciones de ciberseguridad de todos los activos de la organización, así como para la información de sus clientes, y **cuentan actualmente con un SIEM** (solución para la Gestión de Información y Eventos de Seguridad) para ello.

El SIEM que tienen desplegado en la compañía, proporciona la debida trazabilidad de acciones de ciberseguridad, para en caso de necesidad interna o ante requerimientos externos, como pueden ser los derivados de acciones judiciales o policiales se pueda aportar la información solicitada.



Sin embargo, **el actual SIEM es insuficiente a las necesidades de la organización y se encuentra totalmente obsoleto.**

Por ese motivo, necesitan desplegar una nueva herramienta, más potente y actualizada, para la **operación y gestión integral continua y en tiempo real de su centro de servicios de ciberseguridad, que permita** identificar tendencias en las alertas, que permitan inferir conclusiones acerca de la postura y estado de la seguridad de la organización, identificando variaciones significativas en el número de alertas que puedan deberse a modificaciones de la política de seguridad de un elemento, cambios de configuración o una mala política de autenticación.



Actuación realizada

S2 Grupo ha llevado a cabo el suministro, despliegue, instalación, puesta en marcha, capacitación y mantenimiento del hardware y software necesarios para la implantación de la **solución SIEM GLORIA**, dimensionada para 70.000 EPS y con una retención de 30 días de logs online y 365 de logs offline.

Se realizó un estudio para el dimensionamiento del hardware necesario para la implantación de Gloria, en función del volumen previsto de EPS que tendrá que soportar la solución, el tamaño medio de los registros y de su periodo de retención.

Se diseñó el **modelo de despliegue más adecuado a la solución propuesta**, estableciendo un modelo a través de Kubernetes que permiten una estabilidad y escalabilidad mayor si fuera necesario. Posteriormente, se aprovisionó y se instaló el Hardware necesario para la implantación de Gloria en las instalaciones del cliente, y se desplegó el nuevo SIEM bajo el modelo definido previamente.

Se realizó una **Instalación y configuración de la plataforma** y se realizaron unas **pruebas de funcionamiento para asegurar su correcto despliegue**. En esas pruebas se verificaron la instalación y la configuración base de la plataforma, verificando la disponibilidad de todos los componentes de la plataforma mediante la utilidad de autodiagnóstico de la solución, la correcta recepción de eventos, la correlación y generación de alertas en la consola de gestión y por último la disponibilidad de los cuadros de mando.

Posteriormente se integraron y calibraron las fuentes requeridas por el cliente, que ascienden a un total de 350. Su integración se realizará a lo largo de los siguientes cinco años.

Por último, y una vez se puso en marcha el servicio, se llevó a cabo **4 cursos de formación de la plataforma** para los usuarios del centro de operaciones de la organización. Esta formación se impartió dos veces de modo que favoreciera la asistencia de todas las personas necesarias de la organización.



04

Beneficios obtenidos

Con la realización de este proyecto el cliente:



Dispone de la solución GLORIA para la operación y gestión **integral continua y en tiempo real para su centro de servicios de ciberseguridad**. Una solución desarrollada de manera conjunta entre S2 Grupo y el CCN, y que se encuentra dentro del catálogo de productos y servicios de seguridad de las tecnologías de la información y comunicación en la **guía CCN-STIC 105** como una solución de **categoría ALTA** según el Esquema Nacional de Seguridad.



Dispone de una plataforma con capacidades de **monitorización de seguridad y recolección**, con una orientación flexible hacia la vigilancia del mundo IP, incluyendo **IoT y el mundo OT en general, inteligencia avanzada** mediante técnicas de correlación compleja de eventos o **análisis de patrones para la identificación de anomalías y gestión de los procesos** ligados al servicio, con una consola única de gestión de alertas e incidentes, que aporta eficiencia y eficacia a su operación.



Cuenta con una solución que irá integrando paulatinamente las fuentes más necesarias por la organización, pudiendo de esta forma, priorizar o no en aquellas fuentes más necesarias en función de las necesidades del momento.



MADRID
BARCELONA
VALENCIA CERT
VALENCIA HQ
SEVILLA
SAN SEBASTIÁN

SANTIAGO DE CHILE
C.D. MÉXICO
BOGOTÁ
LISBOA
RÓTERDAM

Síguenos en:



• @s2grupo

• s2grupo.es