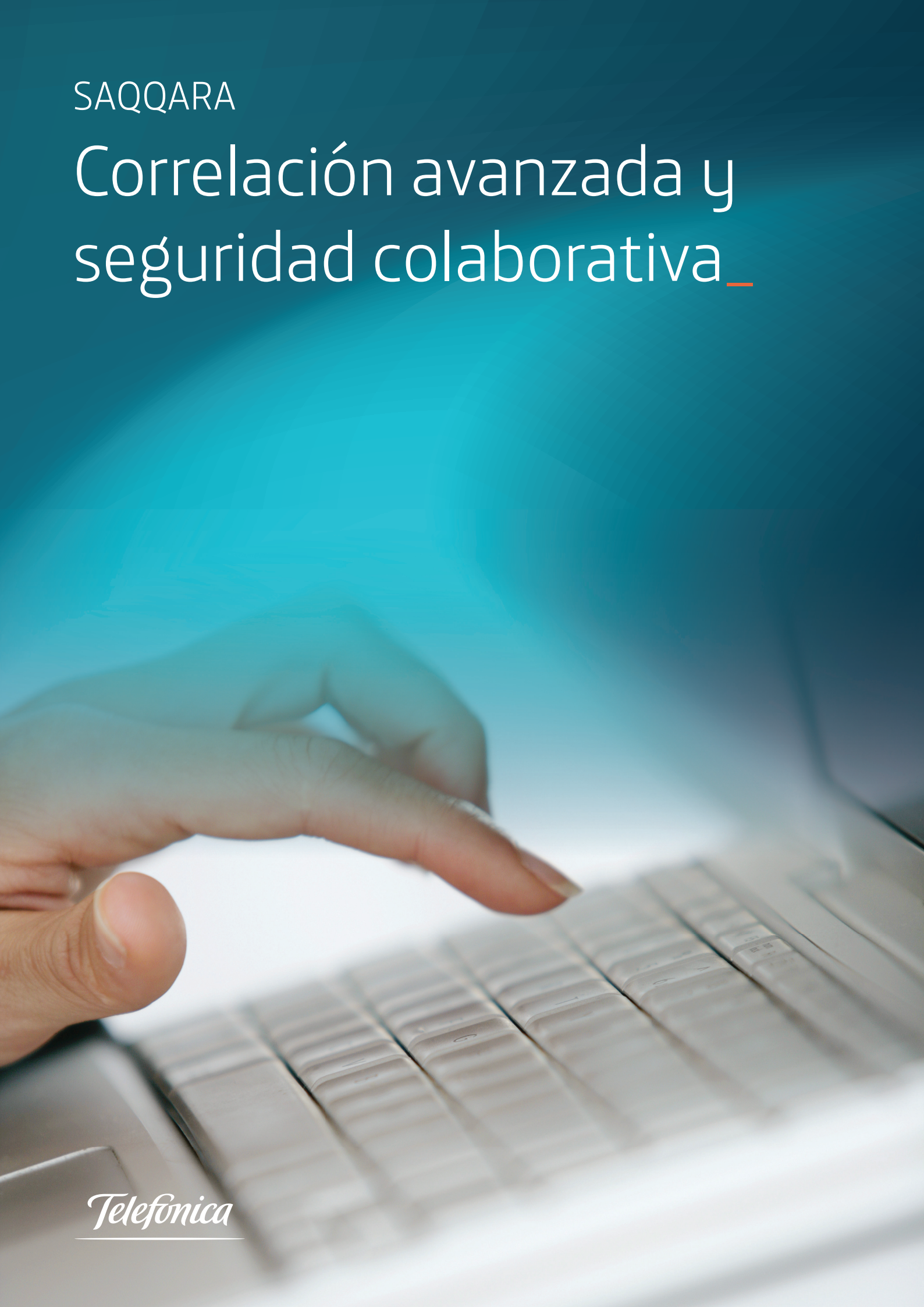
SAQQARA

Correlación avanzada y seguridad colaborativa_



Telefónica

¿Tiene su seguridad 100% garantizada con su SIEM?_

Los SIEMs nos ayudan, pero su dependencia de los eventos y tecnologías, su reducida flexibilidad y la fijación de umbrales nos generan un alto número de falsos negativos y falsos positivos elevando el coste de las operaciones.

Con el objetivo de ampliar las capacidades de análisis y generación de alarmas de los motores de correlación incluidos por los fabricantes de los productos utilizados para prestar el servicio de monitorización de la seguridad, Telefónica ha desarrollado SAQQARA, que ofrece un nivel adicional de análisis de los eventos almacenados por dichos productos. Telefónica utiliza SAQQARA dentro de sus servicios de Seguridad Gestionada.

Aumentado la eficiencia y eficacia de la correlación_

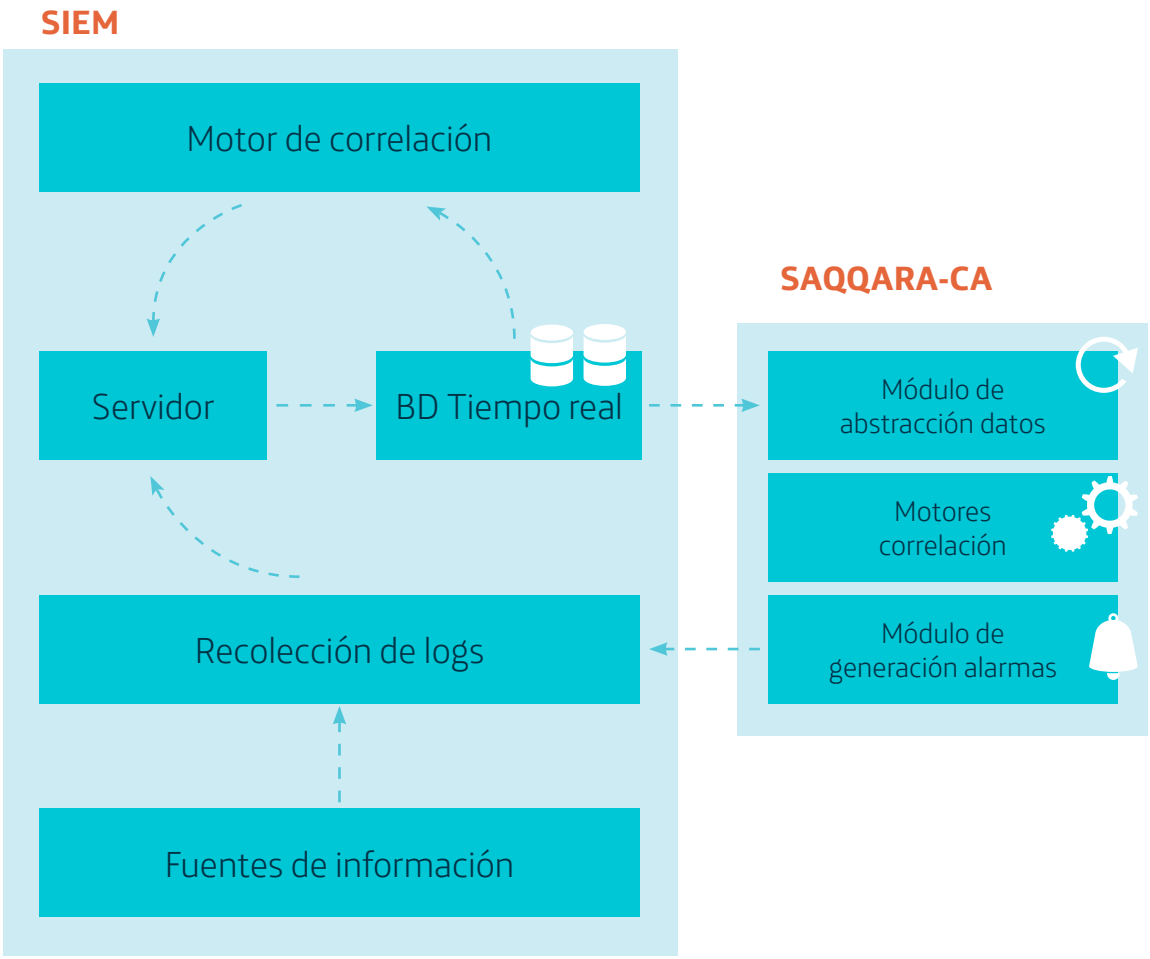
El objetivo principal de SAQQARA es complementar los sistemas de correlación tradicionales ya desplegados e incluidos en las propias herramientas comerciales, realizando un análisis independiente del realizado por el correlador nativo, aumentado la eficiencia y eficacia del servicio en su totalidad al establecer un doble sistema de análisis, independiente el uno del otro, sobre los datos recibidos por el servicio de monitorización.

El único requisito que precisa SAQQARA es poder acceder en modo lectura a la base de datos donde el SIEM almacena los eventos de seguridad. Una vez que tiene acceso a esos datos, SAQQARA normaliza de forma dinámica la información y utiliza los múltiples algoritmos implementados para detectar posibles actividades sospechosas. En el caso de detectarse alguna, es notificada al SIEM para que sea reportada como una alarma más y que pueda ser analizada por el operador.

SAQQARA consta de dos módulos, un correlador avanzado, en adelante SAQQARA-CA, y un módulo colaborativo, en adelante SAQQARA-SC, cuyas funcionalidades principales son descritas a continuación.

SAQQARA-CA_

SAQQARA-CA es un módulo de correlación avanzada de eventos de seguridad que, de forma independiente, complementa la funcionalidad de un SIEM con un conjunto de algoritmos de análisis distintos a los utilizados por el propio correlador nativo.



Características

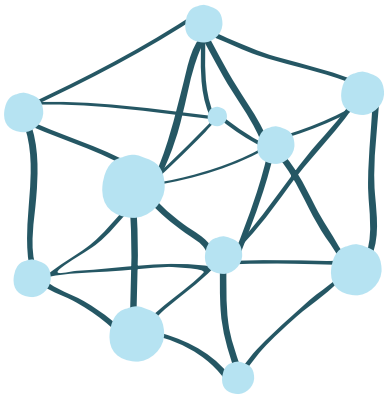
Taxonomía de eventos dinámica

Utilización de una **taxonomía dinámica** que le independiza de eventos específicos. De esta forma, cualquier actualización en alguno de los dispositivos no obliga a revisar la configuración de los motores de correlación. Del mismo modo, eventos con una semántica similar, son analizados de forma homogénea, independientemente del tipo de dispositivo y/o fabricante que lo haya reportado.

Independencia del entorno

Motores de correlación que utilizan algoritmos heurísticos y propietarios, permitiendo la detección amenazas/intrusiones que podrían haber pasado desapercibidas al correlador nativo del SIEM, bien porque no se hubiese actualizado el catálogo de correlaciones implementados, bien porque los eventos no están siendo bien categorizados en las propias sondas.

SAQQARA-CA dispone de **cuatro tipos de algoritmos** de correlación incluidos y configurados por defecto:



- **Redes neuronale**s para la detección de comportamientos que pudiesen implicar una amenaza. Debido a las características intrínsecas de las redes neuronales, estos correladores son los encargados de la detección de comportamientos nuevos o distintos a los que habitualmente son detectados.

- Algoritmo de detección de **comportamientos periódicos**, que permite la detección de actividades que, debido a un reducido número de eventos, podrían haber pasado desapercibidas.

- Detección de **árboles de ataque** basados en la taxonomía dinámica intrínseca de SAQQARA, lo cual permite definir una única política donde analizar comportamientos claramente identificados, como ataques de fuerza bruta o escaneos de red, de forma homogénea, para cualquier tipo de dispositivos que haya generado eventos relacionados con dicho comportamiento.

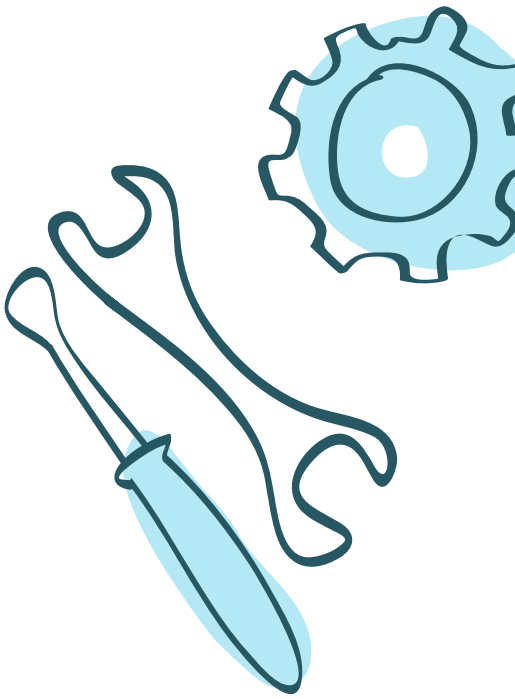
- **Análisis estadístico** del número de eventos reportados por cada dispositivo o sonda, de forma que puedan detectarse desviaciones al comportamiento habitual, así como la caída o falta de eventos por parte de algún dispositivo.

Funcionalidades para evitar la generación de alarmas duplicadas:

- En el caso de que el correlador nativo del SIEM haya generado una alarma para la misma IP recientemente SAQQARA-CA no genera ninguna alarma para dicha IP, evitando la duplicación de la alarma.
- Si se detecta una alarma generada por SAQQARA-CA de forma repetitiva, se incluye a dicha IP es una lista blanca temporal de tal forma que se evita la generación continua de dicha alarma.

Ambas funcionalidades pueden habilitarse/deshabilitarse según las necesidades de cada entorno.

- El tiempo entre cada análisis realizado por los distintos correladores de SAQQARA-CA es por defecto de 10 minutos, salvo el correlador periódico que se ejecuta cada hora.
- SAQQARA-CA permite incluir en el análisis cualquier tipo de información que pueda ser obtenida de cualquier base de datos externa mediante una consulta SQL.

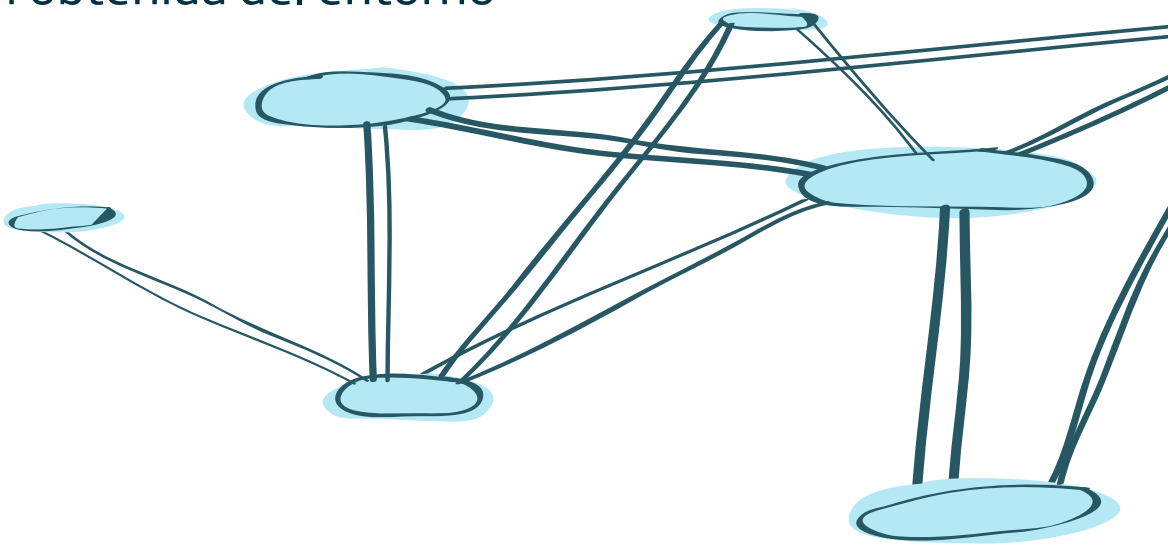


Principales Características_

- Soporte Multifabricante
- Tiempo cuasi real
- Tiempos de implantación y mantenimiento reducidos
- Fácil adaptación al entorno

SAQQARA-SC

SAQQARA-SC completa la funcionalidad ofrecida por SAQQARA-CA mediante el acceso a la red colaborativa de Telefónica que permite ampliar el análisis local realizado por SAQQARA-CA con información obtenida del entorno colaborativo.



Características

- Actualización en tiempo real de una lista negra de IPs que están atacando a los distintos servidores integrados en la red colaborativa. Dicha red colaborativa está compuesta tanto por información de otros clientes del servicio como de entornos propios de Telefónica. Dicha lista negra permite ajustar la fiabilidad de una alarma en tiempo real, forzando el análisis de cualquier IP que se incorpore a dicha lista negra en todos los SAQQARA-CA.
- En ningún momento se intercambia información interna de cliente, únicamente información de IPs públicas y el patrón interno utilizado por SAQQARA, que consta de una serie de enteros y booleanos que identifican el tipo de actividad detectada, pero nunca datos concretos ni información asociada.
- Correlación colaborativa: En el caso de que un nodo de SAQQARA-CA no tenga suficiente información para decidir si un tipo de actividad detectada corresponde con una amenaza o no, realiza una petición al entorno colaborativo para recopilar toda la información que el resto de SAQQARA-CAs puedan tener, realizando un análisis global para dicha IP.
- SAQQARA-SC no requiere ningún tipo de mantenimiento ni configuración adicional, siendo un módulo 100% desatendido y que es actualizado con cada nueva actualización.

Elevada fiabilidad

Detección de amenazas distribuidas

Integración de otras fuentes de información.