

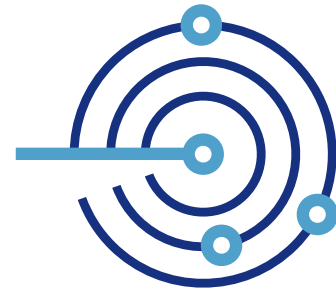
Solucion SIEM QRadar Interside



- + Interside Holding, proveedor experto de soluciones y servicios en el ámbito de las Tecnologías de Información y Comunicaciones (TIC), con una sólida base formativa y vasta experiencia profesional. La apropiada configuración de esta herramienta, realizada por Interside Holding, permite a nuestros clientes identificar y prevenir eventuales amenazas tanto externas como internas, asegurando la operación y la reputación de la organización.

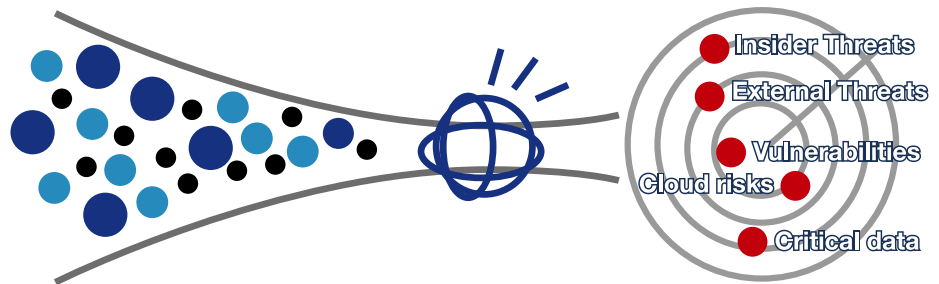
Sistema SIEM QRadar

- + La plataforma QRadar permite disponer de vistas de ataques en tiempo real, priorización en función del negocio y análisis cognitivo, el que facilita la etapa de triage o discriminación entre distintos tipos de alerta. Estas funciones avanzadas se diferencian de un SIEM tradicional (Security Information and event management) el que solo correlaciona eventos sin hacer una inspección en profundidad de los resultados de estas operaciones.



Bondades de QRadar

- + Efectiva detección y respuesta a amenazas de manera veloz, exacta y fundamentada.
- + Rápido despliegue.
- + Rápida incorporación de nuevas fuentes.
Correlación y analítica automatizada.
- + Analítica personalizada para la caza de amenazas.
- + Seguridad cognitiva aplicada.
- + Remediación y orquestación automatizada.



Solucion SIEM QRadar Interside

Implementación QRadar

- ⊕ La arquitectura global del sistema es mostrada en la siguiente figura. El componente Collector es el encargado de recoger la información relevante de la red del cliente. El resto de los componentes se alberga en nuestro SOC, en modalidad multi tenant, a fin de poder ofrecer servicio MSSP.

