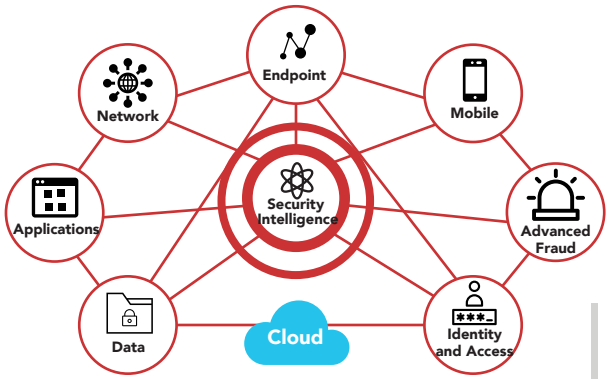
IBM Security QRadar

- ¿Relaciona los eventos de seguridad de diferentes plataformas en tiempo real para detectar amenazas?
- ¿Conoce los usuarios y los dispositivos más riesgosos o vulnerables?
- ¿Sabe qué incidentes de seguridad tiene en este momento?



Puntos Destacados

- Colección unificada, acumulación y análisis en **tiempo real** de logs aplicativos, eventos de seguridad, datos de vulnerabilidades, archivos de configuración y **flujos de red**, entre otros.
- Una plataforma común para búsquedas de eventos de seguridad, filtrado, detección de amenazas y generación de **informes.**
- Una interfaz de usuario única para toda la administración de logs, vulnerabilidades y priorización de riesgos, detección de incidentes y análisis forense.
- Detección avanzada de incidentes de seguridad que reduce el número de falsos positivos y detecta amenazas que otras soluciones no detectan.
- La **arquitectura distribuida** en diferentes appliances se **escala** para proporcionar inteligencia de seguridad a cualquier red empresarial desde medianas a las mayores organizaciones del mundo.

Los productos de la plataforma de Inteligencia de Seguridad QRadar proporcionan una arquitectura para integración de información de seguridad y administración de eventos **(SIEM)**, administración de logs, detección de **anomalías**, administración de **configuración de dispositivos**, gestión de **vulnerabilidades** y análisis **forense**. Estos productos ofrecen detección avanzada de amenazas, mayor facilidad de uso y menor costo total de propiedad (cost of ownership).

Construida sobre tres pilares de inteligencia, integración y automatización, la solución IBM Security QRadar aborda el problema de **centralizar y correlacionar** grandes cantidades de información generadas por dispositivos de red, sistemas de seguridad, aplicaciones y hosts dentro de la red. Esto resuelve un reto para las compañías y organizaciones de todos los tamaños, que deben recopilar estos datos para **cumplimiento de políticas** internas y externas. Además, permite mayor visibilidad en la red usando técnicas avanzadas de detección de anomalías de comportamiento.

QRadar User Behavior Analysis monitorea las actividades de personal interno de confianza, detectando actividades sospechosas que indiquen **ataques internos,** incluyendo escalamiento de privilegios y filtración de información sensible fuera de la organización.

Contáctenos:

info@xelere.com
xelere.com
(+54 11) 5353-8300
XelereSA Xelere

xelere Making IT better

IBM Silver Business Partner