xelere

Making IT better

Security Analytics

Servicios Integrales de implementación y gestión

Las soluciones SIEM (Security Information & Event Management) bien utilizadas, brindan datos e información muy valiosa para mejorar el nivel de seguridad y proteger los activos de información de su organización.

La promesa de las distintas soluciones disponibles en el mercado pasa por facilitar el trabajo de los analistas de seguridad, ahorrando tiempo de análisis de información de diversas fuentes y abriendo el camino a las capacidades de prevención, detección y resolución de incidentes de seguridad.

Sin embargo, en general las organizaciones no explotan todo el potencial de las soluciones SIEM:

- Implementación de casos de uso que respondan a las necesidades de la organización
- Generación de valor y colaboración con otras áreas además de auditoría y seguridad
- Detección temprana de incidentes
- Automatización de tareas y visualización en tiempo real del estado de la seguridad

En Xelere ofrecemos servicios que le permiten superar estos desafíos, a través de la combinación de nuestra experiencia y el respaldo de **IBM Security QRadar**, reconocida como solución SIEM líder del mercado:

	Proyecto de Implementación	Soporte y Optimización	Administración y soporte	Gestión Local	Gestión Remota
Provisión de solución	●				
Implementación	●				
Soporte Nivel 1		●	●	●	●
Soporte Nivel 2				●	●
Mantenimiento		soporte	●	●	●
Administración			●	●	●
Monitoreo on-premise				●	
Monitoreo remoto					●
Definición de casos de uso y optimización de reglas	● (*)	soporte	●	●	●
Generación de informes y dashboards	● (*)	soporte	●	●	●
Integraciones	● (*)	soporte	●	●	●
Consultoría / Asesoramiento	opcional	opcional	opcional	opcional	opcional
Guardia Pasiva		opcional	opcional	opcional	opcional
Duración	2 a 6 meses según alcance y envergadura del proyecto	24/32 horas mensuales - contrato anual	80 horas mensuales (mínimo) - contrato anual	1 especialista dedicado	1 especialista dedicado

(*)Según definido en el alcance del proyecto

Provisión de la solución

La solución IBM Security QRadar cuenta con la posibilidad de implementarse como solución on-premise o servicio mensual en la nube. Dentro de nuestros servicios, ofrecemos la posibilidad de realizar pruebas, definir la arquitectura que mejor se adapte a sus necesidades y su posterior venta.

Implementación

Xelere cuenta con profesionales certificados por IBM Security para la implementación y configuración de la solución QRadar. Dimensionaremos el proyecto de implementación en función de las necesidades de su organización.

Soporte Nivel 1

Con el soporte de primer nivel Xelere se constituye como primer punto de contacto ante errores o problemas.
Para su resolución se procede a la creación y seguimiento de tickets de soporte de IBM.

Soporte Nivel 2

El team de profesionales de Xelere tiene la capacidad de resolver problemas conocidos y recomendar configuraciones sin la necesidad de recurrir en primera instancia al soporte de IBM.
De ser necesario, gestionarán el ticket con IBM, y realizarán su seguimiento y todas las tareas para su resolución.

Mantenimiento

Las tareas de mantenimiento preventivo y actualizaciones permiten que la solución SIEM esté siempre actualizada y funcionando al 100% de su capacidad.

Administración

Este servicio contempla todas las tareas operativas que permiten asegurar el correcto funcionamiento de la solución. Por ejemplo, administración de usuarios y perfiles, backups, monitoreo y tuning de variables de performance, etc.

Monitoreo on-premise o remoto

Servicio de monitoreo de los eventos, alarmas y ofensas generados por la solución. Derivación y seguimiento de los incidentes. En la modalidad on-premise, los consultores de SIEM realizan sus tareas en las oficinas del cliente, mientras que en la modalidad remota se realizará desde el centro de control de Xelere.

Capacitación

Contamos con distintos planes de capacitación orientados a los diferentes usuarios de la plataforma: usuarios finales, operadores y administradores.

Definición de casos de uso y optimización de reglas

La definición de casos de uso es indispensable para aprovechar al máximo las capacidades de una solución SIEM. Nuestros servicios de consultoría se enfocan en identificar y definir casos de uso que respondan tanto a las necesidades de la organización como a las tendencias en el ámbito de la seguridad.

Generación de informes y dashboards

Este servicio se enfoca en generar y actualizar la definición de informes tanto a demanda como programados con el objetivo de responder a los requerimientos de información de la organización (auditoría interna, externa, gestión operativa, etc). Los dashboards permitirán visualizar representaciones online de la información contenida en la solución.

Integraciones

Las soluciones SIEM deben recibir información de diferentes dispositivos, herramientas y aplicaciones. Durante la implementación y evolución de la solución se integrarán todas estas fuentes de datos para enriquecer la capacidad de intepretación, correlación y visualización de la información.

Consultoría / asesoramiento

Servicio opcional de alto nivel para la mejora de controles, definición de los procedimientos de respuesta, identificación de acciones para agregar valor a otras áreas de la organización.

Guardia Pasiva

El servicio de guardia pasiva complementa los servicios contratados para aquellas organizaciones que necesiten una cobertura 7x24.