XSECURE

LA SOLUCIÓN DE LOG-MANAGEMENT

LAS EXIGENCIAS DE MERCADO

Las normativas y directrices europeas para la privacy requieren la recogida segura de los datos, su almacenamiento por largos periodos de tiempo y la revisión regular de los ficheros de Log, todo esto es necesario para verificar que se hayan introducido los controles informáticos necesarios para proteger la confidencialidad de datos sensibles, como también la información relacionada a las tarjetas de crédito, los resultados médicos y datos de carácter financiero.

La generación de datos de seguridad produce millones de mensajes cada día, con una sobrecarga de informaciones generadas de diferentes formas, presentadas en mensajes no homogéneos, memorizadas o utilizadas para actividades de reporting en diferentes lugares. En un entorno de este tipo, es muy difícil individuar los eventos que requieren de atención inmediata o cosa más importante cuales de ellos son síntomas de un ataque que pueda paralizar las actividades. También es muy difícil individuar posibles vulnerabilidades que sean causadas por violaciones de seguridad, sobretodo en un entorno configurado de forma no correcta.

Así ocurre que a las empresas se demande continuamente entregar Reports e identificar rápidamente eventuales violaciones de seguridad, por otro lado, las medidas de seguridad preventivas y el responder a las normativas requieren de análisis diarias de informaciones provenientes de diferentes fuentes.

FICHEROS DE LOG

Los ficheros de log contienen información relacionada con la gestión de la seguridad y se generan de diferentes fuentes heterogéneas, entre las cuales están: Sistemas Operativos, Aplicaciones, Nodos de Networking, Firewalls, Sistemas de Intrusión detection y prevention. Muchas organizaciones ignoran los logs hasta que no se verifique un problema de seguridad

LOG MANAGEMENT

La recogida de log, su almacenamiento y el correspondiente análisis son tareas de por si muy complejas y poco atractivas, un normal entorno de elaboración puede generar millones de eventos al día, equivalente a un terabyte de datos en un mes, además, viniendo de fuentes diferentes de logs también sus formatos son heterogéneos. Individuar quien ha asignado privilegios a un usuario, quien ha tenido acceso a los datos, cuando se ha creado un usuario, o cuando se ha cambiado una configuración es una tarea muy laboriosa. Las soluciones de LOG Mamagenemt

Permiten una gran reducción de coses informáticos y una gran reducción de riesgos de incumplimientos para requisitos de normativas.

Gracias a la automatización de la recogida y elaboración de log, evitamos tener que realizar procedimientos manuales caros y poco eficaces, mientras a los datos relevantes para la seguridad se le asigna el nivel correcto de atención. Además como ventaja adicional, existe la posibilidad de proporcionar a los auditores tanto de la empresa, como externos, la información que necesitan en el momento que se demande.

Este tipo de análisis puede ayudad a identificar las causas de las problemáticas y muchas veces ayuda a prevenirlas y no se puede hacer de otra forma sino con las herramientas correctas.

LA SOLUCIÓN: XSECURE

Xech ha realizado XSecure, la solución para ayudar las empresas a alcanzar los objetivos de seguridad y estar alineados con las normativas actuales y futuras.

XSecure, caracterizada por sus rápidos tiempos de implementación, gestiona grandes volúmenes de log, facilita el análisis y creación de reports, simplifica las actividades de auditoria, análisis de seguridad, actividades de alinamiento.

XSecure recoge, filtra, normaliza, archiva y centraliza los log provenientes de fuentes heterogéneas. Permite la correlación de eventos y pone a disposición funcionalidades de búsqueda. Reduce de manera significativa los costes y complejidades de actividades de análisis.

Gracias a las alarmas generadas en caso de violación de las policy definidas por la organización XSecure permite una reacción en tiempo real mientras el enriquecimiento de los reports, disponible de inmediato, aligera las tareas, compleja en si misma, de proveer las pruebas de estar alineados a las normativas.

XSecure garantiza la recogida y la agregación de los datos de log y es capaz de comprimir y archivar los datos de auditoria tanto datos brutos como normalizados. Utilizando las funcionalidades de búsqueda es posible investigar rápidamente las actividades de los usuarios y los accesos a los recursos.

Las funcionalidades

RECOGIDAS DE DATOS

XSecure es capaz de recolectar log de varias fuentes, como sistemas operativos, base de datos, aplicaciones, aparatos de Networking. La arquitectura del producto permite buscar y recolectar de forma distribuida de los log con la escalabilidad necesaria a suporto de grandes volúmenes de diferentes fuentes.

ESCALABILIDAD Y RENDIMIENTO

XSecure se ha desarrollado para comprimir de forma eficiente los log con relación hasta de 10:1, contribuyendo así en reducir los costes del almacenamiento.

ENCRIPTACIÓN Y SIGNATURE

XSecure está desarrollado para encriptar totalmente o en parte los datos recolectados. Además es posible añadir signature con el fin de proteger la información recolectada y verificar si hay modificaciones no autorizadas de los datos archivados.

REPORTS

La implementación de XSecure es muy simple y produce desde el principio ventajas tangibles a través de instrumentos para la búsqueda y análisis, además de reports y query que se pueden utilizar de inmediato.

PERFILACIÓN DE USUARIOS

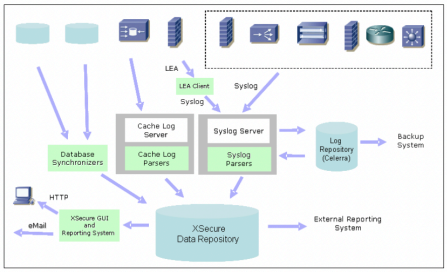
XSecure permite crear perfiles de usuarios de forma que se puedan definir varias tipologías con múltiples posibilidades de análisis de diferentes fuentes.

PLUG-IN

XSecure utiliza las tecnologías que los diferentes sistemas ponen a disposición y permite por lo tanto diferentes tipologías de recolección de log, tanto desde agents como agent-less (como por ejemplo syslog) , no se necesita instalar ningún tipo de software dentro de los sistemas desde los cuales se quiere recolectar los log. Con la modalidad agent es posible instalar software propietarios muy eficientes que recolectan la información y la envían al sistema

FILTROS

Los plug-in tienen la posibilidad de configurar filtros para recolectar y enviar a XSecure exclusivamente la información que se considera importante con el fin de no saturar las infraestructuras de Networking.



ALARMAS

XSecure permite la activación de alarmas que avisan de condiciones particulares.
Además permite verificar que las fuentes estén realmente transmitiendo la información, y avisa de posibles anomalías. Es posible configurar diferentes canales (e-mail, sms, …) para señalar los eventos.

WEB-BASED

XSecure es una solución web-based que permite no solamente la consulta de datos recolectados y la producción y distribución de informes adecuados, sino que también la configuración de las fuentes y de los datos que hay que recolectar.

XECH S.r.l.
via Cesare Ajraghi 30 - 20156 Milano
Tel: +39 0239219548 | Fax: +39 02700403123
P.IVA e C.F. 04029390962