

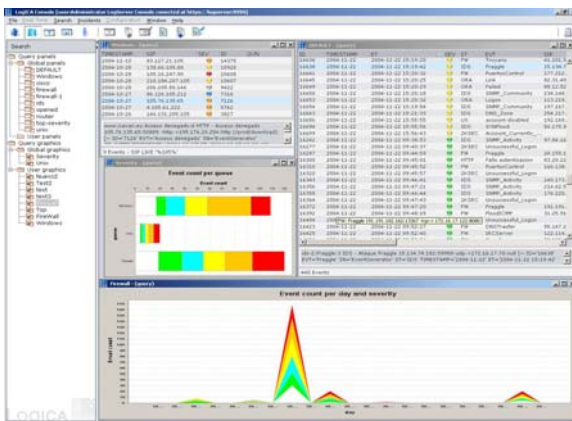


Monitorización y Gestión de la Seguridad

LogICA™ facilita la recolección, el análisis, la generación de informes, y el almacenamiento de manera segura terabytes de Logs críticos y de datos de los Eventos, que simplifican el cumplimiento de requerimientos legales y mejoran la seguridad de la organización

LogICA

Los módulos principales de LogICA™ son LogServer™ y LogAgent™



Módulo Tiempo Real

Monitorización y correlación de la seguridad de eventos en tiempo real a través de consola gráfica. LogICA incorpora un editor de reglas sencillo e intuitivo para la generación de reglas de correlación.

Módulo Forense

Cualquier fuente de Log, independientemente del sistema o aplicación se recoge y centraliza en un sistema securizado, dando lugar a una estructura de Logs segura, sencilla de analizar y que incorpora gestión de evidencias.

Informes y Consultas

A partir de la información recogida con los módulos de de Tiempo Real y forense, se genera información estadística para obtener unas bandas de normalidad que permitan conocer el estado de la seguridad y los puntos débiles de la misma.

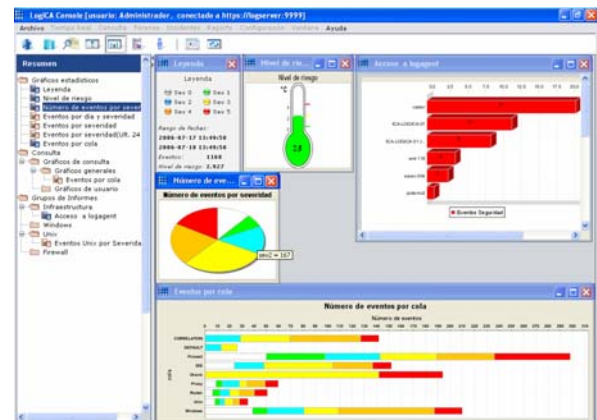
Agentes

Módulo de monitorización y recolección de Logs que puede trabajar tando de forma local como remota.

Inventario de Activos

Orientación a CMDB (ITIL) para el registro de ítems de configuración y los procesos asociados a su gestión.

Importación, exportación de información de activos. Alta manual de Activos, consulta de activos y Autodescubrimiento de activos.



Vulnerabilidades

Descubrimiento de vulnerabilidades de activos. Consulta a BD de vulnerabilidades para ver estado de activos, Búsquedas multicriterio y exportación de resultados a formatos HTML, PDF y XML para integración con otras herramientas

Fraude Interno

Mediante la correlación de eventos es posible detectar accesos realizados por usuarios autorizados bajo patrones de utilización no convencionales.

Vigilancia de configuraciones

Esta funcionalidad permite el control de cambios de los ficheros de configuración de sistemas y aplicaciones.

Cuadro de mando de seguridad

Con la información de seguridad acumulada por LogICA se generan variables estadísticas en el tiempo, que pueden integrarse en un cuadro de mando de seguridad como

indicadores. Estos indicadores facilitan la toma de decisiones de seguridad.

Suite ICA

LogICA, junto con CuadICA forma parte de la Suite ICA para la gestión y análisis de la información de seguridad en las organizaciones.



Principales Características

Centralización de Gestión de Eventos

Monitorización en Tiempo Real

Reportes exhaustivos

Análisis Forense

centraliza la recolección de datos en los logs de la empresa

monitoriza Eventos de seguridad en Tiempo Real

intrusiones, correlación, antivirus y reportes de vulnerabilidades

consulta de datos en los logs para detectar anomalías, y adecuación a requerimientos legales

Especificaciones Técnicas

Producto

Sistema Operativo

Acceso Web

Puertos Necesarios

Bases de Datos Soportadas

LogICA version2 es una solución SIM basada en Linux y Java

Red Hat Enterprise Linux ES 4 kernel 2.6.9

Mozilla Firefox version 2.0 y superior

9999/tcp para EventCollector y 9998/tcp para LogAgent

Oracle, SQL server and MySQL

Fuentes de Eventos Soportadas

Redes

Seguridad

Sistemas

Infraestructura

Firewalls, Routers, Switches...

Control de Acceso, Antivirus, Análisis de Vulnerabilidades, IDS/IPS

Servidores, Clientes, Administración de Sistemas

Base de Datos, Proxies, Servidores de Correo, LDAP, Web, Aplicaciones

• www.grupoica.com • seguridad@grupoica.com

© 2007 I.C.A. Informática y Comunicaciones Avanzadas, S.L.

Todos los nombres y logotipos son marcas de propiedad o de servicios de sus propietarios



Para todos los procesos de consultoría de seguridad