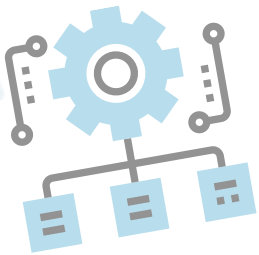
Gestor de logs para responder ante incidentes y amenazas

¿Qué es Gloria?

Gloria es una plataforma para la gestión de incidentes y amenazas de ciberseguridad a través de técnicas de correlación compleja de eventos. Basado en los **sistemas SIEM** (Security Information and Event Management), va un paso más allá de las capacidades de monitorización, almacenamiento e interpretación de los datos relevantes. Así, permite una orientación muy flexible hacia la vigilancia del mundo IP.



¿Por qué usar Gloria?

Ayuda en el procesamiento centralizado de los **grandes volúmenes** de información de eventos de seguridad.

No limita las **capacidades de escalado** cuando se monitoriza un número importante de fuentes.

Soporta un **modelo de correlación distribuida**, en el que los eventos pueden ser recolectados y correlados en origen.

Utiliza solo **alertas previamente correladas** para identificar amenazas que afecten de forma coordinada a varias fuentes.

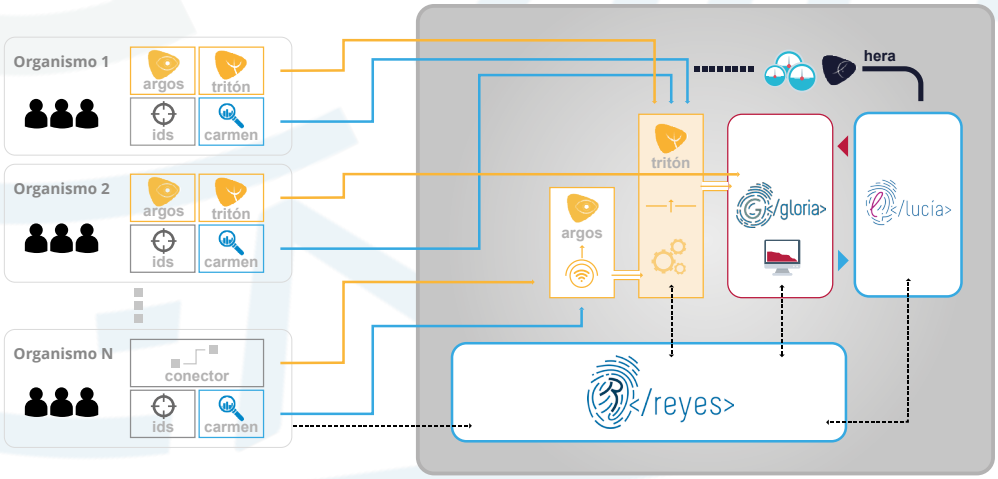
Secciones

- Módulo de vigilancia, monitorización y recolección
- Módulo de inteligencia mediante correlación compleja de eventos
- Módulo de Gestión del Servicio
- Módulo de Dashboarding

¿Cómo funciona?

La solución permite, a través de distintos módulos, las siguientes funcionalidades:

Monitorización de entornos tecnológicos (IT/OT) y recolección de eventos de seguridad. Sistemas de detección de intrusos basados en red (NIDS) y en host (HIDS), sistemas automáticos de análisis de vulnerabilidades, analizadores de tráfico y un conjunto de conectores que permiten obtener los registros o logs de actividad de cualquier sistema o dispositivo del mundo IP.



Inteligencia. A través de técnicas de correlación compleja de eventos, que sirve de base para el desarrollo y parametrización de los mismos.

Gestión del servicio. Con una consola única de gestión de alertas e incidentes, que recoge todas las incidencias o alertas automáticas generadas por el sistema de correlación.

Automatización, orquestación y reducción de tiempos de respuesta. Para la mejora de las técnicas de correlación compleja de eventos se hace especialmente necesaria la integración de las capacidades de SIEM, la notificación de incidentes y la ciberinteligencia. De esta manera, permite la redución del trabajo manual y repetitivo de los operadores/analistas de seguridad en los procesos de detección y respuesta a incidentes.

Integración con otras soluciones CCN-CERT

reyes – Intercambio de información de ciberamenazas

lucía – Gestión de ciberincidentes

carmen – Detección y analisis avanzado de ficheros

gloria

gloria@ccn-cert.cni.es

www.ccn-cert.cni.es

CCN-CERT centro criptológico nacional