SEGURIDAD INTELIGENTE_

*Seguridad inteligente para detectar, defender y responder frente a amenazas inteligentes y ataques de día cero_*

SEGURIDAD INTELIGENTE_

entel_*CyberSecure*

Plataforma de seguridad inteligente para la protección de infraestructuras críticas

LogRhythm
The Security Intelligence Company

entel_*CyberSecure* con su aliado tecnológico LogRhythm ofrece una nueva generación de Plataformas de Seguridad Inteligente, diseñada para la visibilidad, defensa en profundidad y análisis forense ante fugas de información, especialmente para la protección de infraestructuras críticas y sistemas de ciberdefensa.

entel_*CyberSecure* recomienda la plataforma de seguridad inteligente, que entrega las siguientes ventajas a su infraestructura TIC:

> Next Generation SIEM y gestión de logs
> Módulo de host forensics y monitoreo de archivos integrados
> Módulo de network forensics con identificación de aplicaciones y captura total de paquetes de datos
> Estado del arte en la analítica de máquinas
> Correlación avanzada y reconocimiento de patrones
> Detección de comportamiento anómalo multi-dimensional: User / Host / Network
> Búsqueda rápida e inteligente
> Análisis de grandes volúmenes de datos y en profundidad
> Módulo smartResponse para la generación de workflows de respuestas automáticas
> Administración integrada

Los módulos que conforman la plataforma de LogRhythm han sido construidos para ofrecer la máxima flexibilidad:

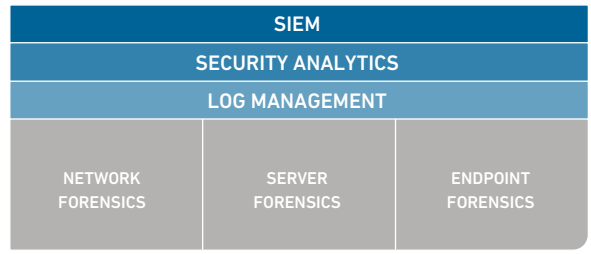
> Platform Manager (PM): Provee de alarmas, notificaciones, gestión de casos e incidencias de seguridad, flujos de aprobación, automatización de respuestas y administración centralizada de despliegue de la plataforma.

> Data Processor (DP): Son módulos distribuidos y de alto rendimiento para el proceso de datos de máquina y datos forenses. Éstos reciben los datos de los Log Collectors y los sensores forenses que permiten al DP transformar los datos en información estructurada y contextualizada. Los DP archivan los datos y distribuyen, tanto el original como la copia procesada, a otros componentes de LogRhythm para el indexado, análisis y alarmado.

> Data Indexer (DX): Provee de un indexado escalable de los datos de los equipos y los datos forenses. Los DX pueden ser clusterizados de forma replicada o no replicada para permitir la alta disponibilidad y mejora del rendimiento. Los datos originales son almacenados al igual que los datos estructurados y no estructurados para las búsquedas y análisis.

> AI Engine (AIE): Es un módulo ampliamente escalable con un motor de análisis patentado para la correlación avanzada y análisis por comportamientos. AI Engine incluye aprendizaje de comportamientos automático, histograma, estadísticas y perfiles de whitelisting (lista blanca). Múltiples AI Engines pueden desplegarse en soporte a un análisis distribuido y balanceo de carga.

> Data Collector (DC): Módulo para la recolección de logs, flujos y datos de equipos. Además, provee de un transporte seguro para las localizaciones remotas, comprimiendo y encriptando los datos antes del envío.



La plataforma LogRhythm también es usada para facilitar el cumplimiento de los mandatos regulatorios, incluyendo PCI DSS (Payment Card Industry Data Security Standard), NERC CIP (Critical Infrastructure Protection) y Sarbanes–Oxley Act (S-OX). LogRhythm posee varias certificaciones y premios a nivel internacional, destacándose las certificaciones: CoN US Army, FIPS 140-2, EAL2 y ONC Certfied Hit.