LA PLATAFORMA PARA EL ANÁLISIS DE LA SEGURIDAD

LogRhythm™

La protección frente a un actual panorama de amenazas en rápida evolución requiere una amplia y profunda visibilidad de todo el entorno de sistemas. Las amenazas y los riesgos llegan desde numerosos ángulos y las pruebas de su existencia pueden hallarse en las bitácoras y los datos de máquinas ya existentes. Una visibilidad más profunda y esencial se obtiene a través de la monitorización forense específica de los equipos anfitriones y las redes. Si esta premisa se aplica a múltiples técnicas analíticas automatizadas, las amenazas y los riesgos se ponen de manifiesto en una medida sin precedentes.

LogRhythm combina de forma única el SIEM de categoría empresarial, Administración de Bitácoras, Monitorización de Integridad de Archivos y análisis automatizado, además del análisis forense de los equipos anfitriones y las redes, con el análisis forense de equipos anfitriones y redes, en una plataforma de seguridad totalmente integrada. La solución LogRhythm proporciona una visibilidad profunda de amenazas y riesgos que de lo contrario permanecerían ocultas a las organizaciones. Diseñado para ayudar a prevenir las intrusiones antes de que se produzcan, el análisis de seguridad de LogRhythm detecta fiablemente una amplia variedad de indicadores de peligro tempranos, lo que permite una respuesta y una mitigación rápidas. La profunda visibilidad y comprensión aportada por el análisis de seguridad de LogRhythm aporta una nueva fuerza a las empresas para proteger sus redes y cumplir con las exigencias de la normativa.

Un estándar superior en el SIEM y los análisis de seguridad

LogRhythm aporta una nueva generación de capacidades para la detección, la defensa y la respuesta ante las amenazas cibernéticas y sus riesgos asociados. La plataforma de análisis de seguridad de LogRhythm aporta:

- SIEM y Administración de Bitácoras de próxima generación
- Análisis Forense de Equipos Anfitriones y Monitorización de Integridad de Archivos
- Análisis forense de la red con ID de aplicaciones y captura completa de paquetes
- Análisis automatizado de última generación
  - Correlación avanzada y reconocimiento de patrones
  - Detección multidimensional de anomalías de comportamiento de usuarios/equipos anfitriones/redes
- Búsqueda rápida e inteligente
- Análisis de grandes conjuntos de datos con análisis visual y pivotado, y desglosamiento
- Respuesta automática vinculada a flujos de trabajo con LogRhythm Smart**Response**™
- Administración integrada de casos

El análisis de la totalidad de bitácoras y datos de máquinas disponibles y la combinación con una visibilidad forense profunda a los niveles del equipo anfitrión y de red aporta una auténtica visibilidad. Esta visión se aprovecha del AI Engine, nuestra tecnología patentada de análisis automatizado, para proporcionar un análisis continuo y automatizado de toda la actividad observada dentro del entorno. AI Engine aporta una nueva fuerza a las organizaciones para identificar amenazas y riesgos que antes se pasaban por alto. Su arquitectura integrada garantiza que, tan pronto como se detecte una amenaza, los clientes puedan acceder rápidamente a una visión global de la actividad, lo que permite una excepcional inteligencia de seguridad y una respuesta rápida. LogRhythm Security Analytics proporciona exclusivas capacidades de inteligencia susceptible de actuación y respuesta a incidentes para responder a los ciberataques más sofisticados de nuestros días.

Rápida rentabilización

Si está protegiendo una pequeña red empresarial o gestionando un centro de operaciones de seguridad (SOC) de alcance mundial, una rápida rentabilización y el coste total de propiedad son importantes. La arquitectura integrada de LogRhythm, combinada con nuestro énfasis en la facilidad de uso, ayuda a los clientes a aprovechar rápidamente sus potentes capacidades, pero también a mantener controlados sus costes a largo plazo. Nos preciamos de transformar problemas difíciles en soluciones sencillas y fáciles de usar.

LogRhythm Labs™ ofrece capacidades críticas llave en mano que se alinean con las implementaciones de los clientes para alcanzar sus objetivos empresariales. La extensa base de conocimientos de LogRhythm, suministrada automáticamente y actualizada permanentemente con la información más actual sobre investigación de amenazas y cumplimiento normativo, permite a los clientes pertrecharse rápidamente contra las amenazas emergentes, a la vez que se mantienen al día sobre los requisitos de cumplimiento normativo y auditoría. La base de conocimientos contiene:

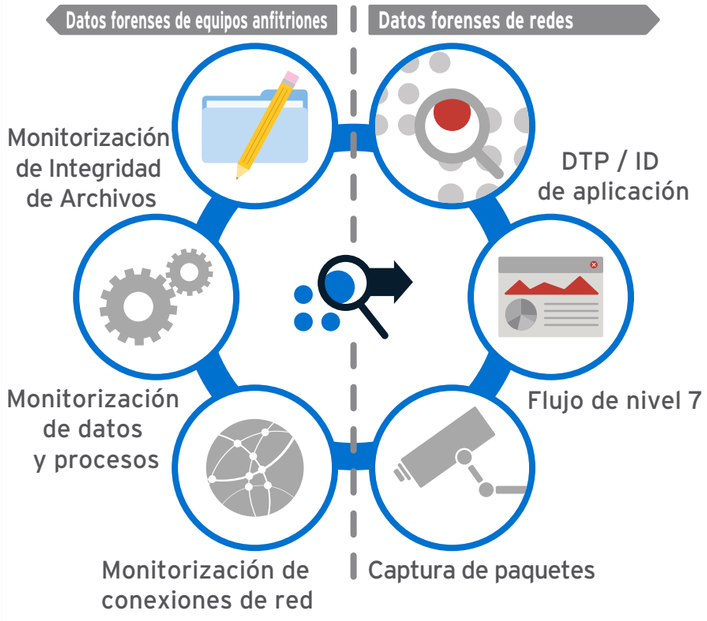
- Reglas de interpretación y normalización de bitácoras para más de 600 sistemas operativos, aplicaciones, bases de datos, aparatos, etc.
- Paquetes de automatización de cumplimiento normativo para una amplia variedad de reglamentos (PCI, SOX, HIPAA, FISMA, GLBA, ISO27001, DODI 8500.1, NERC-CIP, etc.)
- Módulos de análisis de seguridad
  - Monitorización de usuarios privilegiados
  - APT (Advanced Persistent Threat)
  - Defensa de aplicaciones de web
  - Detección de anomalías de comportamiento de usuarios / equipos anfitriones / redes
  - Y muchas otras áreas...

LA PLATAFORMA PARA EL ANÁLISIS DE LA SEGURIDAD

Entrada

RECOPILACIÓN DE DATOS FORENSES

GENERACIÓN DE DATOS FORENSES



LogRhythm Analytics™

PROCESAMIENTO

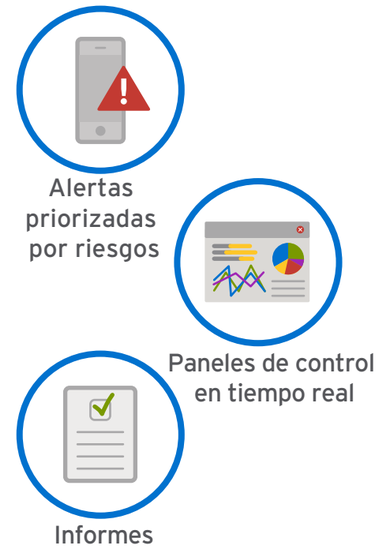
ANÁLISIS EN TIEMPO REAL

ANÁLISIS FORENSE

CIBERDEFENSA ADAPTATIVA

Salida

INTELIGENCIA SUSCEPTIBLE DE ACTUACIÓN



RESPUESTA A INCIDENTES

Opciones de implementación flexibles

Aparatos de alto rendimiento

	TODO EN UNO (XM) (incluye EM, LM, AIE)		ADMINISTRADOR DE EVENTOS DEDICADO (EM) (incluye la licencia de AI Engine)			ADMINISTRADOR DE BITÁCORAS DEDICADO (LM)			AI ENGINE DEDICADO (AIE)			REENVIADOR DE BITÁCORAS DE EMPLAZAMIENTOS (SLF)	NETWORK MONITOR (NM)
Líneas de aparatos	4300	6300	3300 [3]	5300 [4]	6300 [5]	3300	5300	7300	5300	7300	9300	3310	3300
Tasas de archivo máx.	10 000 MPS	25 000 MPS	N/A	N/A	N/A	10 000 MPS	25 000 MPS	50 000 MPS	N/A	N/A	N/A	N/A	N/A
Tasas de procesamiento máx.	1000 MPS	5000 MPS	N/A	N/A	N/A	2000 MPS	5000 MPS	15 000 MPS	5000 MPS	30 000 MPS	75 000 MPS	N/A	1 Gbps

[1] MPS = Mensajes por segundo. [2] Las tasas individuales varían en función del entorno y los requisitos del cliente. [3] Incluye una licencia integrada de AIE para 2000 MPS. [4] Incluye una licencia integrada de AIE para 10 000 MPS. [5] Incluye una licencia integrada de AIE para 20 000 MPS.

"Un producto fantástico y una relación de calidad/precio igualmente fantástica. Le otorgamos nuestra calificación **BEST BUY.**"

SC MAGAZINE

"LogRhythm está sobrado de **FLEXIBILIDAD Y FUNCIONES.**"

INFOWORLD

Software | Virtualización

El software de soluciones de LogRhythm puede implementarse fácilmente en hardware proporcionado por el cliente y las principales plataformas de virtualización, tales como:

vmware · Windows Server 2008 Hyper-V · CITRIX XenServer

Servicios de LogRhythm

LogRhythm ofrece soporte y servicios profesionales de categoría mundial con un inigualable énfasis en el suministro de valor y soluciones prácticas. Desde la mayor organización del mundo hasta las PYMEs, LogRhythm se esfuerza sin descanso por maximizar el éxito y la satisfacción de los clientes.

LogRhythm Labs

LogRhythm Labs aporta nueva fuerza a los clientes al actuar como equipo virtual de investigación de las amenazas de seguridad y el cumplimiento normativo; aporta inteligencia llave en mano y conocimientos expertos integrados para una administración avanzada de las amenazas y la automatización y garantía del cumplimiento normativo. El equipo se compone de especialistas dedicados en exclusiva a la seguridad de la información, además de expertos en toda una variedad de temas, tales como la detección de intrusiones, el malware avanzado, la respuesta a incidentes, la auditoría de sistemas y el cumplimiento normativo. Los investigadores de LogRhythm Labs poseen una amplia variedad de certificaciones del sector (p. ej., CISSP, CISA, CEH, etc.) y utilizan una amplia formación continuada y la investigación constante para mantenerse al día con las últimas novedades en amenazas, métodos, cumplimiento normativo y mejores prácticas.

LogRhythm en acción

Detección de malware personalizado con detección de anomalías de comportamiento de los equipos anfitriones

Reto: El malware personalizado vinculado a ataques de día cero se diseña especialmente para eludir las soluciones de seguridad tradicionales, construidas para detectar firmas específicas y comportamientos maliciosos conocidos.

1. LogRhythm genera una referencia del comportamiento «normal» de los equipos anfitriones y crea una lista blanca de actividades de proceso aceptables.
2. La Monitorización de Actividad de Equipos Anfitriones detecta independientemente el inicio de un nuevo proceso.
3. LogRhythm reconoce automáticamente que el nuevo proceso no está en la lista blanca.
4. Los análisis automatizados de LogRhythm contrastan el evento con actividades relacionadas, por ejemplo un tráfico de red anormal, para identificar con exactitud el alto riesgo de la actividad.
5. Se envía una alarma al administrador de seguridad, quien accede fácilmente a los detalles forenses para investigar el caso.

Exposición de credenciales en peligro con detección de anomalías de comportamiento de los usuarios

Reto: A la vista de retos organizativos tales como un personal cada vez más móvil y la adopción acelerada del BYOD, las empresas tienen dificultades para diferenciar entre el comportamiento «normal» y las actividades que indican que las credenciales de un usuario se han visto comprometidas.

1. LogRhythm establece automáticamente un perfil para usuarios específicos, con listas blancas de actividades aceptables y referencias de comportamiento a partir de las actividades observadas entre los usuarios.
2. AI Engine detecta cuando un usuario incurre en una actividad anormal, por ejemplo iniciar una sesión desde un lugar sospechoso o desviarse de la norma de comportamiento, como ocurre al acceder a datos considerablemente distintos o volúmenes de datos y descargas de dichos datos a una aplicación de uso compartido en la nube que no aparece en la lista blanca.
3. SmartResponse™ desactiva automáticamente la cuenta o pone en cola la respuesta para su validación como paso previo a una investigación forense más detallada de las actividades del usuario.

Identificación de filtración de datos con detección de anomalías de comportamiento de la red

Reto: El constante flujo de datos de entrada y salida de las empresas dificulta la detección de las fugas de datos sensibles hacia el exterior de la red de la empresa.

1. Network Monitor proporciona una visibilidad crítica de los puntos de entrada/salida, con datos generados por SmartFlow™ para una profunda visibilidad de los paquetes de cada sesión de red observada y las aplicaciones utilizadas.
2. El análisis automatizado LogRhythm establece diversas referencias de comportamiento a partir de las actividades de red observadas, aprovechando los extensos metadatos de paquetes a través de SmartFlow™.
3. Las anomalías de la red son identificadas y contrastadas con otros datos de bitácoras y máquinas para aportar una visibilidad exacta de las actividades de alto riesgo.
4. SmartCapture™ captura automáticamente todos los paquetes asociados con las sesiones sospechosas, para un análisis forense completo de los paquetes.