RESUMEN DEL PRODUCTO

SmartResponse™

LogRhythm

LogRhythm ofrece Smart**Response**™, una protección inmediata contra amenazas para la seguridad, infracciones a las políticas sobre cumplimiento y problemas operativos. Sus capacidades inteligentes y enfocadas en los procesos brindan a las organizaciones la posibilidad de tomar medidas y responder a cualquier tipo de alarma en forma automática. Smart**Response**™ enfrenta de inmediato problemáticas reales como, por ejemplo, la detección de patrones de comportamiento sospechosos, la infracción de políticas internas o centradas en cumplimiento específicas o el cruce de umbrales de desempeño críticos. LogRhythm garantiza que las respuestas estén basadas en información precisa gracias a un análisis en tiempo real de todos los datos en las entradas en logs, lo que ayuda a reducir tanto la posibilidad de falsos positivos como la demora asociada a una intervención manual.

Un remedio automático a su servicio

Muchas organizaciones consideran que implementar remedios automáticos genera más riesgos que los que debe evitar. Uno de los problemas es que, en general, se trata de un proceso de tipo "todo o nada"; eso quiere decir que las medidas activas se llevan a cabo sin opción de una validación externa. La cantidad de variables asociadas a un evento en particular y los riesgos vinculados con la interrupción errónea de operaciones críticas llevan a que muchas organizaciones se resistan justificadamente a emplear remedios automáticos que vayan más allá de los conectados con los casos más mundanos.

Smart**Response**™ es un producto de LogRhythm diseñado específicamente para que cualquier medida pueda configurarse de manera sencilla para cumplir con las políticas organizacionales importantes y para garantizar que cada respuesta sea la medida correcta a tomar. Trae incorporado un proceso de aprobación opcional que exige hasta tres niveles de autorización antes de llevar a cabo la medida. Eso permite que las organizaciones tengan la posibilidad de revisar los hechos primero, antes de quitar el acceso a la persona equivocada o desactivar por error una aplicación crítica. Además, si se determinó que ese remedio en particular es la medida correcta, la respuesta ya estará puesta en cola para su ejecución inmediata con solo presionar un botón.

Funcionamiento

Una interfaz gráfica de usuario simple y de tipo plug-in permite que los administradores importen cualquier tipo de respuesta basada en secuencias de comandos para que se active si se produce una correlación avanzada de eventos o si se dispara una alarma de eventos. Smart**Response**™ de LogRhythm incluye lo siguiente:

- Requisitos opcionales de hasta tres niveles de autorización
- Respuestas específicas a parámetros de alarma precisos, por ejemplo:
  - Bloqueo de direcciones IP sospechosas
  - Colocación en cuarentena de usuarios invasores específicos
  - Puesta en marcha o detención de determinados procesos en particular
  - Más de 50 campos exclusivos para brindar el máximo nivel de precisión
- Gestión de respuesta ante incidentes con:
  - Estado actual de los remedios
  - Rastreo del destinatario de la alarma
  - Auditoría del proceso de autorización
- Evaluación con un solo clic para validar la secuencia de comandos

SmartResponse™ en acción

LogRhythm Labs proporciona acceso inmediato a secuencias de comandos prácticas diseñadas para abordar problemas organizacionales comunes que estén relacionados con la seguridad, el cumplimiento y las operaciones. Smart**Response**™ puede ejecutar cualquier secuencia de comandos que pueda crear el usuario, con defensas opcionales que exigen hasta tres niveles de autorización antes de llevar a cabo una medida. Algunos ejemplos:

Detección y respuesta ante amenazas avanzadas (externas)

Problema: Es frecuente que el malware intente acceder a un entorno iniciando sesión a múltiples servidores, pasando de un objetivo al siguiente hasta lograr el acceso.

Detección: La generación de perfiles conductuales que LogRhythm realiza automáticamente crea listas blancas de actividades aceptables en cualquier equipo anfitrión. Las alarmas se actualizan de manera dinámica para que ofrezcan respuesta a cualquier tipo de anomalía conductual, por ejemplo, a un intento de conexión desde una ubicación no incluida en la lista blanca.

Smart**Response**™ puede extraer la dirección de IP atacante directamente de la alarma y agregarla a una ACL de firewall, cortando al instante el acceso potencialmente peligroso a su red.

Detección y respuesta ante amenazas avanzadas (internas)

Problema: Los administradores de sistemas tienen la capacidad de acceder y modificar sistemas, además de crear cuentas con privilegios superiores. Eso hace posible que participen de un amplio rango de actividades maliciosas sin ser detectados.

Detección: LogRhythm notifica cuando se crea una cuenta nueva con privilegios superiores o si se realizan modificaciones sospechosas a cuentas con acceso a sistemas críticos.

Smart**Response**™ puede suspender o eliminar en forma automática las cuentas con privilegios creadas o modificadas recientemente, hasta que se verifique que se trata de una actividad legítima.

Automatización y garantía del cumplimiento

Problema: Muchas regulaciones sobre cumplimiento exigen implementar controles estrictos de acceso a datos confidenciales, como las cuentas vinculadas con información médica protegida (PHI) o con tarjetas de crédito.

Detección: Las alarmas de LogRhythm pueden aprovechar las listas blancas con actualización dinámica que indican qué usuarios cuentan con acceso autorizado a recursos críticos o archivos específicos, lo que permite detectar y alertar en tiempo real cuando se infringe una política de acceso.

Smart**Response**™ elimina de inmediato a cualquier usuario culpable de una violación de acceso desde la red, hasta que se investigue el incidente, lo que impone en forma activa la política y protege recursos críticos.

Servicio de inteligencia y optimización de las operaciones

Problema: La detección del momento en que todos los aspectos de un servidor se han reiniciado correctamente después realizar tareas rutinarias de mantenimiento presenta todo un desafío, en especial en el caso de empresas grandes con un gran número de equipos anfitriones distribuidos.

Detección: LogRhythm detecta de manera independiente el momento en que un proceso crítico se detiene o falla su reactivación luego de un evento específico, por ejemplo, un reinicio del sistema.

Smart**Response**™ puede reactivar procesos individuales extrayendo todo tipo de información relevante, como el nombre del proceso y el equipo anfitrión afectado, directamente de la alarma.