RESUMEN DEL PRODUCTO

Network Monitor

LogRhythm

Una auténtica inteligencia de seguridad empresarial requiere conocimiento en tiempo real y comprensión de todos los datos que atraviesan la red. LogRhythm Network Monitor proporciona conocimiento en el nivel de aplicaciones y detalles completos de las sesiones de red, aportando así visibilidad sobre toda la red de la empresa. Al aportar un conjunto detallado de metadatos con completas posibilidades de búsqueda, Network Monitor proporciona un acceso rápido a pruebas forenses altamente valiosas, ofreciendo así una comprensión rápida y profunda de la actividad de la red. Además, la capacidad de Network Monitor para realizar una captura completa de los paquetes permite el acceso a los detalles de los paquetes en bruto de cada sesión como información forense adicional.

LogRhythm Network Monitor proporciona una visibilidad crítica a la hora de detectar y responder a las amenazas avanzadas de nuestro tiempo. Permite a las organizaciones:

- Referenciar el comportamiento de la red para detectar inmediatamente cualquier actividad anormal
- Detectar la actividad de aplicaciones no autorizada o sospechosa
- Agilizar las investigaciones forenses de la red
- Realizar una captura completa de los paquetes de las sesiones para un análisis forense avanzado
- Prevenir la pérdida de datos sensibles
- Monitorizar el consumo de ancho de banda de las aplicaciones

Identificación de la aplicación real: identifica más de 1700 aplicaciones para un análisis en profundidad, mediante la inspección profunda de los paquetes y la aplicación de múltiples métodos de clasificación para determinar la identidad real de la aplicación. La ID de la aplicación real proporciona la visibilidad necesaria para detectar actividades críticas tales como transmisiones sospechosas de datos, vulneraciones de las normas de uso de la red y ataques avanzados.

SmartFlow™: aporta un conjunto detallado de metadatos de paquetes derivados de cada sesión de red, de acuerdo con el tipo de aplicación utilizado. El alto grado de detalle disponible en SmartFlow™, que cataloga cada una de las sesiones de la red, proporciona una comprensión profunda de la actividad de red de una aplicación en un formato rápidamente accesible.

Búsqueda no estructurada, análisis potente: proporciona un acceso rápido a los detalles de SmartFlow™ a través de un potente motor de búsqueda parecido a Google que agiliza y simplifica las investigaciones forenses de la red. Los resultados se presentan en visualizaciones altamente informativas y formatos personalizados, lo que permite un análisis instantáneo de los datos de los paquetes de red.

Captura completa de los paquetes de las sesiones: captura los encabezados y contenidos de los paquetes completos de los niveles 2 a 7 de cada sesión, para disponer de un registro completo de la actividad de la red. Toda la información se organiza por sesiones, para ofrecer un contexto global de las comunicaciones de cada aplicación y las transmisiones de contenidos a través de la red.

SmartCapture™: proporciona una captura completa de los paquetes sin las grandes necesidades de almacenamiento de las soluciones tradicionales, gracias a que conserva solo las sesiones de interés.

Integración de análisis de seguridad: proporciona un flujo de datos de SmartFlow™ detallados y en tiempo real a las soluciones de análisis de seguridad de LogRhythm, de terceros o propias de la empresa.

Análisis de seguridad LogRhythm

LogRhythm Network Monitor puede implementarse por sí solo o como un componente totalmente integrado del galardonado SIEM de LogRhythm, para aportar un análisis de seguridad insuperable de todas las actividades de la red. La plataforma integrada contiene:

- Análisis de seguridad en tiempo real de todos los datos forenses para reconocer eventos altamente relevantes en:
  - Datos de bitácoras y auditoría de toda la red
  - Actividad de equipos anfitriones recopilada independientemente a través de LogRhythm System Monitor
  - Actividad de red recopilada independientemente a través de LogRhythm Network Monitor
- Capacidades llave en mano completas para NBAD (Network Behavior Anomaly Detection, detección de anomalías de comportamiento de la red)
- Potente búsqueda de visualización, con profundización, pivotado y correlación, para agilizar las investigaciones
- Inicio de la captura completa de paquetes de sesiones mediante SmartCapture™ de Network Monitor en respuesta a actividades de alta prioridad reconocidas por el SIEM.

> “Las capacidades de NBAD llave en mano nos permiten detectar e investigar el tráfico sospechoso para identificar toda una variedad de problemas, desde la presencia de malware hasta un consumo excesivo de ancho de banda por las videoconferencias.”
>
> ***Vaughn Adams*** Director sénior de sistemas, InterDigital.

Network Monitor en acción

LogRhythm Network Monitor responde a casos de uso del mundo real para resolver cuestiones críticas para la seguridad y arrojar luz sobre las anomalías de la red y las actividades inadecuadas de los usuarios. Si le preocupan el malware personalizado, el espionaje entre naciones o el uso indebido rutinario de la red, LogRhythm le proporciona la visión profunda que necesita para detectar toda una variedad de amenazas, a la vez que le permite una respuesta más eficiente e informada.

Sustracción de datos

El reconocimiento rápido de los eventos relevantes que rodean a una intrusión puede ayudarle a reducir la exposición y el coste del remedio.

1. El panel de control de Network Monitor arroja luz sobre las sesiones SSH de larga duración.
2. Los detalles de SmartFlow™ de Network Monitor revelan el uso de SSH para un acceso de túnel al equipo anfitrión, lo que proporciona un acceso remoto al sistema.
3. Ahora es posible tomar medidas adicionales para proteger los equipos anfitriones atacados y para denegar el acceso del sistema atacante a la red.

Detección de botnets

Las actuales devoluciones de llamada de botnet utilizan puertos estándar y posiblemente aplicaciones legítimas para disimular su tráfico y evitar la detección.

1. Network Monitor observa el tráfico distintos al HTTP en el puerto 80 e identifica la aplicación real o expone los encabezados alterados de los paquetes HTTP.
2. La captura completa de los paquetes de la sesión revela contenidos adicionales no identificados por las herramientas de seguridad tradicionales, lo que permite un análisis posterior y la verificación de las amenazas identificadas.

> "Con Network Monitor hemos mejorado radicalmente nuestras capacidades de defensa, detección y respuesta en múltiples entornos de datos seguros."
>
> *Erin Osminer*
> Ingeniero de redes
> StoneRiver

Uso inadecuado de la red

Cuando no se dispone de datos de inteligencia más allá de lo que proporcionan los datos de flujo tradicionales, resulta difícil diferenciar entre una actividad legítima y un comportamiento sospechoso.

1. El análisis de flujos tradicional identifica el uso excesivo de ancho de banda desde un sitio web a través de HTTP, pero no proporciona información adicional.
2. Network Monitor deriva unos extensos metadatos de la sesión de red para identificar detalles tales como la presencia de una gran descarga de archivos, el URL de origen o de destino y los nombres de los archivos transmitidos.
3. El acceso rápido a los detalles de SmartFlow™ a través de la intuitiva búsqueda de Network Monitor permite identificar rápidamente la actividad inadecuada, tal como la transferencia de material protegido por copyright o el uso de una aplicación de intercambio en la nube no aprobada.

Implementación

Network Monitor emplea una IU simple e intuitiva basada en la web para gestionar la instalación y las actualizaciones. Se implementa fuera de banda mediante TAP, SPAN o integración con soluciones de agente de paquetes de red de otros desarrolladores. Network Monitor comienza inmediatamente a analizar y reconocer el tráfico y ofrece una búsqueda en tiempo real parecida a Google en todos los metadatos y capturas de paquetes, además de reenviar opcionalmente el SmartFlow™ de nivel 7 al SIEM u otras soluciones para su análisis adicional.

LÍNEA DE APARATOS	PROCESAMIENTO MÁX.	CPU	MEMORIA	ALMACE-NAMIENTO	CHASIS	ALIMENTACIÓN	ETHERNET	MEDIDAS	PESO
LR-NM3330	500 Mbps	2,1 GHz	64 GB	2 TB	1U	100-240 V	4 X 1 GB	AL. 4,28 X AN. 48,24 X PROF. 67,73 CM	19,3 kg
LR-NM3350	1 Gbps	2,1 GHz	64 GB	2 TB	1U	100-240 V	4 X 1 GB	AL. 4,28 X AN. 48,24 X PROF. 67,73 CM	19,3 kg

Disponemos de opciones de DAS adicionales que aportan una capacidad ampliada para el almacenamiento de datos de SmartFlow™ y capturas de paquetes en bruto. Network Monitor también admite el traslado de las capturas de paquetes a SAN o un almacenamiento alternativo para su retención a largo plazo.