McAfee Advanced Correlation Engine

Detecte las amenazas que afectan a lo que más valora

Las sutiles amenazas actuales desafían la detección de amenazas basada en reglas. Despliegue la solución McAfee® Advanced Correlation Engine con McAfee Enterprise Security Manager para identificar y calificar en tiempo real los eventos de amenazas, usando simultáneamente la lógica basada en reglas y basada en riesgos. Bastará con indicarle a McAfee Advanced Correlation Engine qué desea supervisar —usuarios o grupos, aplicaciones, servidores específicos o subredes— para que la solución envíe alertas en caso de que algún activo se vea amenazado. Los registros de auditoría y las reproducciones de datos históricos facilitan los análisis forenses, el cumplimiento de normativas y la configuración de las reglas.

La solución McAfee Advanced Correlation Engine complementa la correlación de incidentes de McAfee Enterprise Security Manager con dos motores de correlación dedicados y un rendimiento creado ex profeso:

- Un motor de detección de riesgos que genera una calificación de riesgo mediante la correlación sin reglas.
- Un motor de detección de amenazas que detecta las amenazas mediante la correlación de eventos tradicional, basada en reglas.

La solución independiente McAfee Advanced Correlation Engine proporciona la capacidad de procesamiento necesaria para llevar a cabo esta completa correlación en toda su empresa. Su motor de datos se escala para adaptarse incluso a las redes de mayor tamaño.

Detección de amenazas en tiempo real y pasadas

McAfee Advanced Correlation Engine se puede desplegar en modo de tiempo real o histórico. En el modo de tiempo real, la solución McAfee Advanced Correlation Engine analiza los eventos a medida que se recopilan con el fin de detectar inmediatamente el riesgo y las amenazas:

- Correlación de datos de eventos en tiempo real basada en reglas, para detectar las amenazas en el momento en el que se producen.
- Correlación de datos de eventos en tiempo real sin reglas, para detectar las amenazas a medida que avanzan.

En el modo histórico, los datos obtenidos se pueden "reproducir" mediante los dos motores de correlación, para facilitar la detección de amenazas y riesgos

Principales ventajas

- Simplifica el inicio: sin actualizaciones de reglas, configuración de firmas ni ninguna otra engorrosa tarea.
- Alerta si las amenazas se dirigen a usuarios, activos, aplicaciones y actividades prioritarios.
- Califica con precisión gracias a la correlación simultánea basada en reglas y sin reglas.
- Permite comprobar si hay nuevos ataques y vulnerabilidades usando su historial como referencia, con el fin de detectar incidentes ocurridos en el pasado.
- Añade recursos especializados de correlación y procesamiento a McAfee Enterprise Security Manager.
- Disponible tanto en despliegues basados en dispositivos como virtuales.

recurrentes. Cuando se descubre un ataque "zero-day", la solución McAfee Advanced Correlation Engine examina los registros históricos con el fin de determinar si la empresa ya se había expuesto a ese ataque en el pasado, para la detección de amenazas "sub zero-day".

Rendimiento dedicado cuando se necesita

La solución McAfee Advanced Correlation Engine es un dispositivo totalmente independiente u oferta virtual, por lo que no afecta en absoluto al rendimiento de McAfee Enterprise Security Manager en cuanto a recopilación y gestión de eventos. Puede hacer un uso completo de todas las funciones de las aplicaciones de McAfee Advanced Correlation Engine sin afectar a su utilidad McAfee Enterprise Security Manager y aprovechándola al máximo.

Correlación de eventos basada en reglas

La correlación basada en reglas emplea la lógica de correlación tradicional para analizar la información recopilada en tiempo real. Todos los registros, eventos y flujos de las redes se correlacionan —junto a la información de contexto, como la identidad, funciones, vulnerabilidades, etc.— para detectar patrones indicativos de amenazas importantes. Si bien todas las soluciones de McAfee Enterprise Security Manager ofrecen ya correlación basada en reglas en toda la red, la solución McAfee Advanced Correlation Engine proporciona un recurso dedicado para correlacionar incluso mayores volúmenes de datos, ya sea como complemento a las iniciativas de correlación existentes o asumiéndolas totalmente.

Correlación de calificaciones de riesgos sin reglas

Aunque la correlación basada en reglas es una función necesaria y de gran valor en cualquier sistema de administración de información y eventos de seguridad (SIEM), estos sistemas solo pueden detectar patrones de amenazas conocidos, lo que requiere constantemente el ajuste de las firmas y las actualizaciones para ser eficaces. La respuesta es complementar la correlación de eventos tradicional con tecnología de correlación "sin reglas". En los sistemas de correlación sin reglas, las firmas de detección se sustituyen por una sencilla configuración que se realiza una vez: basta con indicar a la solución McAfee Advanced Correlation Engine qué es importante para su empresa. Puede ser un servicio o una aplicación determinados, un grupo de usuarios o tipos concretos de datos.

Supervisión y alertas en tiempo real

A continuación, la solución McAfee Advanced Correlation Engine comienza a supervisar toda la actividad relacionada con esos elementos, para generar una calificación de riesgos dinámica que aumenta o disminuye según la actividad en tiempo real. Cuando una calificación de riesgos supera un cierto nivel, se genera un evento en la solución McAfee Advanced Correlation Engine. Este evento puede utilizarse para alertar a un analista de seguridad de que han aumentado las condiciones para que se produzca una amenaza, o puede ser usado por el motor de correlación basado en reglas como condición de un incidente mayor. La solución McAfee Advanced Correlation Engine mantiene una completa pista de auditoría de la calificación de riesgos que permite analizar e investigar en detalle las condiciones de las amenazas a lo largo del tiempo.

Casos prácticos

Configuración del riesgo en la empresa

La solución McAfee Advanced Correlation Engine ofrece una plataforma para configurar de forma eficaz el riesgo en su empresa. El acceso a documentos muy confidenciales por parte de empleados con un alto nivel de derechos puede implicar un riesgo para una empresa de defensa, mientras que una filtración de registros de pacientes famosos a los que se les ha diagnosticado una enfermedad grave puede provocar riesgos en un hospital. La solución McAfee Advanced Correlation Engine ofrece un medio perfecto para adaptar los riesgos para su empresa. Para ello se califican los atributos que importan, generando una línea de base y enviando notificaciones cuando se superan los umbrales normales.

Evaluaciones de riesgos proactivas con datos críticos

La solución McAfee Advanced Correlation Engine supervisa los datos en tiempo real, lo que le permite utilizar simultáneamente los dos motores de correlación para detectar riesgos y amenazas antes de que se produzcan. Las calificaciones de riesgos se pueden utilizar dentro de la lógica de correlación tradicional. Por ejemplo, una firma de detección de amenazas tradicional basada en firmas podría ser "un evento de malware que se produce después de un inicio de sesión por fuerza bruta". Normalmente, cuando se activa esta firma ya ha ocurrido un evento. Sin embargo, con la solución McAfee Advanced Correlation Engine puede incorporar un factor de riesgo, como por ejemplo, un incremento del 20 % de la calificación de riesgo tras un inicio de sesión por fuerza bruta. Cuando se detecta este evento, la solución McAfee Advanced Correlation Engine puede proporcionar una alerta proactiva de incidente inminente, lo que facilita la intervención antes de que se haya causado el daño.

Evaluación de amenazas recurrentes

No es raro identificar una amenaza o descubrir una fuga y no saber cuánto tiempo lleva activa. Con la solución McAfee Advanced Correlation Engine en modo histórico, se pueden reproducir los conjuntos de datos históricos configurados, mediante los motores de correlación tradicional y sin reglas.

Al determinar cuándo se materializó por primera vez una amenaza, es mucho más probable que se pueda identificar la causa principal.

Modos de funcionamiento

Modo de correlación en tiempo real:

- Correlación de datos de eventos en tiempo real basada en reglas, para detectar las amenazas en el momento en el que se producen.
- Correlación de datos de eventos en tiempo real sin reglas para detectar las amenazas a medida que avanzan.

Modo de correlación histórica:

- Correlación de datos de eventos históricos basada en reglas, para la detección continua de amenazas.
- Correlación de datos de eventos históricos sin reglas, para la evaluación continua de amenazas.

Capacidad de correlación

- Correlación simultánea basada en reglas y sin reglas.
- Correlaciona datos de cualquier fuente de información compatible.
- Correlaciona datos entre redes y recopiladores distribuidos.
- Incluye cientos de reglas de correlación de eventos predefinidas.
- Incluye un editor de configuración para la correlación sin reglas.
- Incluye una sencilla interfaz de edición de reglas de correlación de eventos para personalizar las reglas o crear reglas nuevas.

Figura 1. La correlación basada en riesgos le ayuda a detectar las amenazas que se ciernen sobre los activos prioritarios.

Más información

Para obtener más información, visite **www.mcafee.com/mx/products/siem/index.aspx**.

McAfee
Together is power.

Av. Paseo de la Reforma No.342 Piso 25
Colonia Juárez, México DF
C.P. 06600
+52-55-50890250
www.mcafee.com/mx

41606ds_adv-corr-engine_1112B
NOVIEMBRE DE 2012