McAfee Advanced Correlation Engine

Detección de amenazas basada en sus activos prioritarios

En la actualidad, las amenazas han alcanzado tal nivel de sofisticación que desafían a los sistemas de detección de amenazas clásicos, basados en reglas. Despliegue la solución McAfee® Advanced Correlation Engine con McAfee Enterprise Security Manager para identificar y calificar los eventos de amenazas en tiempo real, mediante una lógica basada tanto en reglas como en riesgos. Basta con definir en McAfee Advanced Correlation Engine los activos que considera más importantes (usuarios o grupos, aplicaciones, servidores específicos o subredes) y la solución le alertará cuando el activo esté amenazado. Las pistas de auditoria y la simulación de datos históricos le permiten llevar a cabo análisis forenses, optimizar las reglas y garantizar el cumplimiento de normativas.

Ventajas principales

- Simplificación de la puesta en marcha: sin actualizaciones de reglas, ajuste de firmas o cualquier otra dificultad
- Generación de alertas si las amenazas tienen como objetivo los usuarios, activos, aplicaciones y actividades consideradas prioritarias
- Asignación de una calificación precisa gracias a la correlación simultánea con y sin reglas
- Comparación de los nuevos ataques y vulnerabilidades con su historial para identificar eventos pasados
- Incorporación de recursos de correlación y proceso especializados a McAfee Enterprise Security Manager
- Despliegue disponible como dispositivo físico o virtual

La solución McAfee Advanced Correlation Engine complementa la correlación de eventos de McAfee Enterprise Security Manager con dos motores de correlación dedicados y con funciones específicas:

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

La solución independiente McAfee Advanced Correlation Engine proporciona la potencia de proceso necesaria para poder llevar a cabo la correlación completa de eventos en toda la empresa. Su motor de proceso de datos se amplía para adaptarse incluso a las redes de mayor tamaño.

Detección de amenazas histórica y en tiempo real

La solución McAfee Advanced Correlation Engine puede desplegarse en modo de tiempo real o en modo histórico. En modo de tiempo real, analiza los eventos en el momento que se recopilan para conseguir la detección inmediata de amenazas y riesgos.

- Correlación de los datos, basada en reglas y en tiempo real, para detectar las amenazas a medida que aparecen.
- Correlación de los datos, sin reglas y en tiempo real, para detectar las amenazas a medida que se desarrollan.

En modo histórico, los datos recopilados pueden “reproducirse” a través de ambos motores para una detección recursiva de riesgos y amenazas. Cuando se descubren ataques de tipo zero-day, la solución McAfee Advanced Correlation Engine puede

intel Security

examinar los datos históricos para determinar si su empresa ha estado expuesta a este ataque en el pasado, con el fin de detectar de amenazas que se manifiestan antes de su identificación formal.

Impacto cero en el rendimiento

El hecho de que la solución McAfee Advanced Correlation Engine se ofrezca como dispositivo independiente o como dispositivo virtual le permite no tener absolutamente ningún impacto en el rendimiento de McAfee Enterprise Security Manager en lo que se refiere a la recopilación de datos y administración de eventos. Puede disfrutar plenamente de todas las funciones de las aplicaciones de McAfee Advanced Correlation Engine y, al mismo tiempo, aprovechar al máximo la utilidad McAfee Enterprise Security Manager.

Correlación de eventos basada en reglas

La correlación de eventos basada en reglas utiliza la lógica de correlación tradicional para analizar la información recopilada en tiempo real. Todos los registros, eventos y flujos de red se correlacionan con otros tipos de información contextual, como la identidad, las funciones, las vulnerabilidades y otros datos, para detectar patrones de comportamiento que indiquen amenazas más virulentas. Aunque todas las soluciones McAfee Enterprise Security Manager ya admiten la correlación basada en reglas en toda la red, McAfee Advanced Correlation Engine proporciona un recurso de proceso dedicado, capaz de correlacionar volúmenes de datos incluso mayores, complementando los procesos de correlación existentes o encargándose por completo de esta tarea.

Correlación con calificación de riesgo sin reglas

Aunque la correlación basada en reglas es una función necesaria e indispensable de cualquier sistema de administración de eventos e información de seguridad (SIEM) tradicional, dichos sistemas únicamente pueden detectar patrones de amenazas conocidos que, para ser eficaces, precisan ajustes y actualizaciones de firmas constantes. La solución consiste en completar la correlación de eventos tradicional con la tecnología de correlación “sin reglas”.

En los sistemas de correlación sin reglas, las firmas de detección se sustituyen por una configuración simple y única: sencillamente indíquele a la solución McAfee Advanced Correlation Engine lo que es importante para su empresa. Podría tratarse de un servicio o de una aplicación concreta, un grupo de usuarios o incluso tipos de datos específicos.

Seguimiento y alertas en tiempo real

La solución McAfee Advanced Correlation Engine inicia entonces el seguimiento de la actividad relacionada con estos recursos y genera una calificación de riesgo dinámica que aumenta o disminuye en función de la actividad en tiempo real. Cuando una calificación de riesgo supera un determinado umbral, McAfee Advanced Correlation Engine genera un evento. Este evento puede utilizarse para advertir a un analista de seguridad del aumento de posibilidades de que aparezcan amenazas, o bien puede utilizarlo el motor de correlación tradicional, basado en reglas, como indicio de un incidente de mayor calado. La solución McAfee Advanced Correlation Engine conserva una pista de auditoría completa de todas las calificaciones de riesgo, lo que permite llevar a cabo análisis e investigaciones en profundidad de los factores de amenazas a lo largo del tiempo.

Casos de uso

Modelización de riesgos de la empresa

La solución McAfee Advanced Correlation Engine proporciona una plataforma de modelización eficaz de los riesgos para su empresa. El acceso a documentos de carácter extremadamente confidencial por parte de empleados con derechos de seguridad elevados puede constituir un riesgo para un organismo de defensa, al mismo nivel que la divulgación de la historia médica de un paciente famoso al que se le ha diagnosticado una enfermedad grave, para un hospital. La solución McAfee Advanced Correlation Engine ofrece una modelización perfecta de los riesgos para las empresas, gracias a la calificación de los criterios pertinentes, lo que permite crear una base de referencia y enviar notificaciones cuando se superan los umbrales considerados como normales.

Evaluación proactiva de riesgos contra los datos críticos

Gracias a que la solución McAfee Advanced Correlation Engine supervisa los datos en tiempo real, pueden utilizarse de forma simultánea ambos motores de correlación para detectar riesgos y amenazas antes de que afecten a sus sistemas. Las calificaciones de riesgo pueden integrarse en la lógica de correlación tradicional. Por ejemplo, una firma de detección de amenazas tradicional (basada en reglas) podría ser "un evento de malware como consecuencia de un ataque de fuerza fruta". Por lo general, cuando se activa esta firma, el evento ya se ha producido. En cambio, gracias a la solución McAfee Advanced Correlation Engine, ahora puede incorporar un factor de riesgo, como en aumento de un 20% en la calificación de riesgo, tras un evento de ataque de fuerza bruta. Una vez detectado este evento, la solución es capaz de generar una alerta proactiva de incidente inminente, permitiendo la intervención antes de que se produzca daño alguno.

Evaluación de amenazas recursiva

Cuando se identifica una amenaza o se descubre una brecha, es lógico preguntarse desde cuándo ha estado ahí. El despliegue de la solución McAfee Advanced Correlation Engine en modo histórico permite volver a analizar los datos histórico en los dos motores de correlación (con y sin reglas).

La identificación del momento exacto de la aparición de una amenaza recién descubierta permite determinar más fácilmente la causa de esta situación.

Modos de funcionamiento

Modo de correlación en tiempo real

- Correlación de los datos, basada en reglas y en tiempo real, para detectar las amenazas a medida que aparecen.
- Correlación de los datos, sin reglas y en tiempo real, para detectar las amenazas a medida que se desarrollan.

Modo de correlación histórico

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

Funciones de correlación

- Correlación simultánea con y sin reglas
- Correlación de datos recopilados de cualquier fuente de datos admitida
- Correlación de datos de redes distribuidas y de recopiladores
- Inclusión de cientos de reglas de correlación de eventos predefinidas
- Editor de configuración para la correlación sin reglas
- Editor de reglas de correlación de eventos con una interfaz gráfica de usuario fácil de utilizar para la personalización o creación de reglas

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

Figura 1. La correlación basada en riesgos ayuda a detectar amenazas inminentes contra activos prioritarios.

McAfee. Part of Intel Security.
6205 Blue Lagoon Drive
Suite 600
Miami, Florida 33126
U.S.A.
www.intelsecurity.com