McAfee Global Threat Intelligence for Enterprise Security Manager

Incorpore la capacidad de McAfee® Labs al conocimiento de la situación.

McAfee® Global Threat Intelligence for Enterprise Security Manager permite aprovechar los activos de McAfee Labs en la supervisión de la seguridad en la empresa. Por primera vez, la información de reputaciones de IP —que recopila McAfee Labs a través de sus más de 100 millones de sensores de amenazas repartidos por todo el mundo— está ya disponible para su uso en una solución de administración de eventos e información de seguridad (SIEM). Esta rica fuente de información para McAfee Enterprise Security Manager, que se actualiza constantemente, mejora el conocimiento del contexto, ya que permite descubrir rápidamente los eventos en los que participan comunicaciones con direcciones IP sospechosas o maliciosas. De esta forma, los administradores de seguridad pueden determinar qué hosts se han comunicado o se están comunicando con sistemas maliciosos, así como identificar las condiciones en las que dichos sistemas originan la actividad de una amenaza.

La necesidad de un contexto externo

Los incidentes de seguridad aportan datos sobre toda la actividad relacionada con la seguridad que se desarrolla en un momento dado. Si bien es cierto que las soluciones SIEM permiten correlacionar estos incidentes, dejan algunas preguntas sin respuesta para el operador: ¿Es esta actividad aceptable? ¿Cómo sé qué es más urgente? ¿Cómo detecto aquellos ataques sofisticados que pasan más desapercibidos? Si multiplicamos estas preguntas por los eventos cotidianos de una empresa típica —más de 250 000 millones— es evidente que la detección de patrones conocidos, factor en el que se basan las soluciones SIEM tradicionales, es solo la punta del iceberg de la supervisión de la seguridad. Uno de los elementos más importantes del contexto de las amenazas es la reputación de los sistemas externos. Hasta ahora, disponer de este conocimiento claro de los incidentes de seguridad no ha sido posible.

Principales ventajas

- Aprovechar la información de McAfee Labs en soluciones SIEM.
- Conocer al detalle los riesgos asociados a los eventos.
- Aprovechar la inmensa fuente de información sobre amenazas que ofrece McAfee GTI sin afectar al rendimiento.
- Recibir y procesar automáticamente reputaciones de nuevas fuentes de amenazas en McAfee Enterprise Security Manager.
- Aumentar la precisión en la detección de amenazas, reduciendo también el tiempo de respuesta.
- Identificar rápidamente las vías de ataque y las interacciones en el pasado con ciberdelincuentes conocidos relacionados con ataques de denegación de servicios distribuidos (DDoS) o redes de bots, malware de envío de spam/correo con sondeos de red, presencia de malware, alojamiento de DNS y actividades generadas por ataques de intrusión.

Las soluciones SIEM aprovechan la información de McAfee Labs

McAfee Global Threat Intelligence for Enterprise Security Manager pone los recursos de McAfee Labs directamente al servicio de la supervisión de la seguridad a través de una solución McAfee SIEM de gran velocidad y muy inteligente, diseñada para grandes volúmenes de datos. Este servicio de suscripción opcional proporciona y ajusta de manera continua datos de reputación de más de 140 millones de direcciones IP, incorporando así directamente el contexto de la reputación de los sistemas externos al flujo de eventos de seguridad e identificando rápidamente las interacciones con ciberdelincuentes conocidos, producidas en la actualidad o en el pasado. La reputación de IP de McAfee Global Threat Intelligence se obtiene mediante la correlación de datos sobre amenazas procedentes de todos los principales vectores, con la ayuda de más de 100 millones de sensores globales y más de 500 investigadores.

Ventajas de McAfee Global Threat Intelligence for Enterprise Security Manager

- **Mayor protección para toda la red:** McAfee Global Threat Intelligence for Enterprise Security Manager detecta inmediatamente cuando un nodo de su red se comunica con un sistema malicioso conocido o sospechoso y capta rápidamente la ruta de la amenaza.
- **Prioridades basadas en riesgos:** la reputación de IP se incorpora automáticamente al algoritmo de calificación de riesgos sin reglas de McAfee Enterprise Security Manager, señalando inmediatamente la necesidad de responder.
- **Supervisión continua de amenazas:** McAfee Labs examina constantemente los datos sobre amenazas para detectar los sistemas recién infectados y maliciosos, así como los que se han limpiado, con el fin de ofrecer a las empresas información precisa y actualizada acerca de la situación de las amenazas en el mundo.

Detección de la actividad maliciosa en tiempo real

Con McAfee Global Threat Intelligence for Enterprise Security Manager, las empresas ya pueden conocer la reputación de IP de cualquier evento que se produzca, incluidos los de los distintos firewalls, sistemas de prevención de intrusiones, enrutadores y endpoints. Gracias a la lista de vigilancia dinámica de McAfee Enterprise Security Manager, los eventos se asocian automáticamente con una calificación de reputación de la fuente y el riesgo se ajusta convenientemente. A medida que cambian las amenazas globales, McAfee GTI actualiza McAfee Enterprise Security Manager, de manera que los servidores y sistemas cuenten siempre con la calificación de reputación adecuada. De esta forma, las empresas no solo pueden entender los riesgos, sino que además pueden detectar problemas urgentes en tiempo real, reduciendo el tiempo de respuesta a incidentes y proporcionando un análisis de riesgos de gran precisión.

Descubra lo que no sabía

Una de las ventajas principales de McAfee Enterprise Security Manager es su capacidad para almacenar, recuperar y correlacionar datos históricos de varios años. Ahora, con McAfee GTI, los analistas de seguridad pueden retroceder en el tiempo, para examinar datos de otros años, con el fin de entender las interacciones con los ciberdelincuentes en el pasado. Esto es esencial para detectar ataques que pasan desapercibidos, actividades que se repiten desde redes de bots, secuencias de comandos entre sitios e intentos de inyección SQL.

Reducción del tiempo de respuesta

McAfee GTI se integra perfectamente con los mecanismos de alerta y alarma de McAfee Enterprise Security Manager para garantizar que las interacciones con sistemas maliciosos conocidos reciban la atención que merecen.

Con el respaldo de la base de datos de McAfee, diseñada para grandes volúmenes de datos de seguridad

Se ha hablado mucho sobre el incremento del volumen de los datos y esto afecta a la incorporación de la abundante información de seguridad de McAfee Labs a una solución SIEM. McAfee Enterprise Security Manager es la única solución que permite almacenar, correlacionar y actualizar la enorme cantidad de datos de reputación de IP de McAfee GTI, sin afectar al rendimiento. McAfee Enterprise Security Manager incluye una base de datos propia que no solo elimina la engorrosa tarea de administración de bases de datos para SIEM, sino que además se ha diseñado específicamente para la obtención y el procesamiento masivo de datos de eventos y relacionales a velocidades increíblemente altas. Con McAfee Global Threat Intelligence for Enterprise Security Manager, los clientes tienen la tranquilidad de que la información de McAfee GTI llegará en tiempo real.

Especificaciones

Versiones compatibles
McAfee Enterprise Security Manager 9.4 y McAfee Event Reporter Appliance 9.4

- Red de inteligencia sobre amenazas de McAfee Labs: más de 100 millones de nodos en más de 120 países
- Reputación media de direcciones IP: varía en función del panorama de las amenazas

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