McAfee Threat Intelligence Exchange

Información sobre amenazas compartida entre soluciones de seguridad

McAfee® Threat Intelligence Exchange actúa como agente de reputación para permitir la detección y respuesta a amenazas adaptable. Combina inteligencia local de las soluciones de seguridad de su empresa, con datos sobre amenazas globales, externos, y comparte esta inteligencia colectiva con todo su ecosistema de seguridad, lo que permite a las soluciones intercambiar información y actuar en función de la inteligencia compartida.

Cree un ecosistema de inteligencia sobre amenazas colaborativo

Un agente de reputación, McAfee Threat Intelligence Exchange, combina inteligencia sobre amenazas de fuentes globales importadas, como McAfee Global Threat Intelligence (McAfee GTI) e información sobre amenazas de terceros (como VirusTotal) con inteligencia de fuentes locales, como los endpoints, los gateways y las soluciones de análisis avanzado. Gracias al uso de Data Exchange Layer (DXL), comparte de manera instantánea esta inteligencia colectiva con todo su ecosistema de seguridad, lo que permite a las soluciones de seguridad funcionar al unísono para mejorar la protección en toda la empresa.

La simplicidad de la integración, basada en DXL, reduce de manera importante los costos operativos y de implementación de varias integraciones de interfaces de programación de aplicaciones (API) directas y proporciona una seguridad, eficacia operativa y efectividad incomparables. Diseñada como plataforma abierta, DXL permite incorporar de manera dinámica al ecosistema McAfee Threat Intelligence Exchange todas las soluciones de seguridad, incluidas las de terceros.

Adáptese e inmunícese frente a las amenazas

Cada vez que se comparte información, sea cual sea la ubicación de la red, mejora su situación en la batalla que se libra contra los ataques selectivos. Estas amenazas son ataques diseñados con precisión milimétrica, por lo que las empresas requieren un sistema de vigilancia local para descubrir las tendencias generales y las agresiones dirigidas exclusivamente a ellas. Los datos contextuales locales obtenidos del intercambio, combinados con la información global sobre amenazas, permiten tomar mejores decisiones sobre archivos desconocidos hasta el momento, lo que agiliza la detección y la protección.

Ventajas principales

- La protección adaptable contra amenazas reduce a milisegundos el intervalo de días, semanas y meses que suele haber entre la detección y la contención de los ataques selectivos avanzados.
- La información colectiva sobre amenazas se genera a partir de fuentes de datos globales y se combina con información sobre amenazas local.
- La información de seguridad relevante se comparte en tiempo real entre soluciones de seguridad para endpoints, gateways, redes y centros de datos.
- Podrá decidir qué hacer con archivos nunca vistos anteriormente en función del contexto de los endpoints (atributos de archivo, proceso y entorno) con la información colectiva sobre amenazas.

Cuando se encuentra un archivo sin identificar en algún punto de su red, se contacta con el servicio McAfee Threat Intelligence Exchange para determinar si existe información de reputación del mismo. También se guardan metadatos descriptivos, como la prevalencia empresarial y la antigüedad, en la información colectiva recopilada. Además de solicitar reputaciones, las soluciones de seguridad integradas también pueden aportar actualizaciones de reputación a McAfee Threat Intelligence Exchange en función de los resultados locales. Las reputaciones actualizadas se distribuyen entonces a todos los sistemas en tiempo real. Esta información local sobre amenazas se almacena para el futuro, lo que significa que si se vuelven a detectar en otro dispositivo o servidor, ya no serán archivos desconocidos, y el ataque será detectado inmediatamente.

McAfee Threat Intelligence Exchange hace posible que los administradores personalicen fácilmente la información integral sobre amenazas. Podrán reunir, omitir, aumentar y adaptar la información para personalizar la protección de sus entornos y organizaciones. Esta información adaptada y con prioridades asignadas localmente proporciona una respuesta instantánea en caso de detecciones en el futuro.

Los puntos de aplicación mejoran la protección

Las soluciones integradas a través de la red —desde el endpoint al perímetro de la red— aplican las directivas en función de la reputación disponible, los metadatos o una combinación de puntos de datos. Una solución muy integrada, McAfee Endpoint Security, aprovecha la inteligencia local combinada (metadatos de archivos, como la prevalencia empresarial y la antigüedad, junto con la reputación local suministrada desde otros componentes de seguridad) y la inteligencia sobre amenazas global disponible, para tomar decisiones precisas. Por ejemplo, una aplicación personalizada sin reputación global, pero con alta prevalencia empresarial no generaría una reputación combinada maliciosa y probablemente se permitiría su ejecución. Por otro lado, un archivo desconocido hasta ahora en la empresa, sin reputación global ni local y empaquetado de manera sospechosa, generaría probablemente un nivel de confianza bajo, y se iniciaría un posible bloqueo o se requeriría una investigación más profunda a través de otros motores de McAfee Endpoint Security o análisis en entorno aislado a través de McAfee Advanced Threat Defense o McAfee Cloud Threat Detection.

Real Protect, la funcionalidad de aprendizaje automático de McAfee Endpoint Security, y la Contención dinámica de aplicaciones mejoran todavía más la detección y la protección. Real Protect busca en la nube la inteligencia sobre amenazas más reciente con análisis antes y después de la ejecución, mientras que la Contención dinámica de aplicaciones impide la actividad maliciosa en el endpoint, protegiendo la primera máquina expuesta a una nueva amenaza, mientras se lleva a cabo un análisis más profundo.

Ventajas principales (continuación)

- La integración se simplifica a través de DXL. Se reducen los costos operativos gracias a la conexión de soluciones de seguridad de McAfee con otras propiedad de terceros a fin de aplicar su información sobre amenazas en tiempo real.

Los ataques avanzados son un problema del mundo real

Diseñados para eludir los radares y establecer su presencia a largo plazo, los ataques selectivos avanzados continúan asediando a las empresas y filtrando datos de alto valor. Según datos recientemente publicados como parte del informe sobre investigaciones sobre amenazas de Verizon de 2015 *(Verizon 2015 Data Breach and Investigations Report)* entre el 70 y el 90 % de las muestras de malware son exclusivas para una sola empresa, lo que indica que la detección de indicadores de amenazas exclusivos es el mayor de los retos actuales[1].

Para obtener más información, visite **www.mcafee.com/mx/products/threat-intelligence-exchange.aspx**.

Benefíciese de la colaboración

Análisis de amenazas avanzadas

Si se requiere más información sobre un archivo, puede enviarse automáticamente desde McAfee Threat Intelligence Exchange a soluciones de análisis avanzado de McAfee (como McAfee Advanced Threat Defense o McAfee Cloud Threat Detection) para obtener información instantánea sobre las nuevas amenazas potenciales y determinar la reputación del archivo concreto. Todo ello está automatizado y se documenta y comparte colectivamente a través de DXL a fin de proteger todo su ecosistema de seguridad.

Gestión de incidentes de seguridad

McAfee Enterprise Security Manager le permite investigar más a fondo los indicadores de riesgo que detecta McAfee Threat Intelligence Exchange. El acceso a la información de seguridad histórica y la posibilidad de crear listas de seguimiento automatizadas incrementan la eficacia de la seguridad en las empresas.

1. http://www.verizonenterprise.com/DBIR/2015/

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