Hacer operativa la información sobre amenazas

Detrás de casi todas las alertas legítimas que recibe su departamento de seguridad de TI hay un adversario que utiliza múltiples técnicas de ataque para introducirse en su infraestructura y comprometer sus datos y sistemas fundamentales. Los ataques selectivos actuales se desarrollan en varias etapas que componen la cadena del ciberataque: reconocimiento, búsqueda de vulnerabilidades, aprovechamiento y, por último, filtración de datos empresariales valiosos.

Los analistas de seguridad conocen perfectamente estas técnicas y emplean la inteligencia (información) sobre amenazas para deducir cuáles son los métodos de ataque empleados y las motivaciones. Esto les permite detectar y neutralizar amenazas avanzadas, aplicar las medidas de corrección adecuadas y estar mejor preparados para cuando vuelva a sonar la alarma de seguridad. Sin embargo, muy a menudo carecen de visibilidad de determinados sistemas o bien están desbordados por una enorme cantidad de datos sin los correspondientes análisis. Según el estudio del SANS Institute *Who's Using Cyberthreat Intelligence and How?* (¿Quién utiliza la inteligencia sobre ciberamenazas y cómo?), "... solo el 11,9 % de los entrevistados consigue reunir información de amenazas de casi todas las fuentes y únicamente el 8,8 % tiene una perspectiva completa para combinar eventos con indicadores de peligro[1]".

En un informe reciente, Forrester señala que el 77 % de los responsables de la toma de decisiones de empresas norteamericanas y europeas considera prioritario mejorar las funciones de inteligencia sobre amenazas[2]. Gracias a la inteligencia sobre amenazas, los profesionales de la seguridad están sobre aviso si hay ciberdelincuentes que pretenden dirigir sus ataques contra su región, su sector o incluso sus empresas específicas, de manera que cuentan con tiempo para actuar. Sin embargo, a pesar de esto, la seguridad de TI sigue enfrentándose a dificultades importantes:

- Cómo recopilar inteligencia sobre amenazas de fuentes externas e internas.
- Cómo correlacionar los datos y establecer prioridades entre los riesgos.
- Cómo distribuir inteligencia a los controles de seguridad de varios proveedores en toda la empresa.
- Cómo obtener más visibilidad del panorama de TI para poner en marcha medidas apropiadas e inmediatas.

Las empresas modernas necesitan una arquitectura abierta e integrada que facilite la adopción de la inteligencia sobre amenazas y les permita disfrutar de sus ventajas: desde recopilar datos básicos sobre amenazas para análisis forenses hasta utilizarlos para enriquecer los análisis de las soluciones SIEM. En otras palabras, los usuarios necesitan sacar provecho de la inteligencia sobre amenazas mediante procesos automatizados que ayuden a analizarla, digerirla y administrarla.

Las nuevas amenazas exigen un nuevo enfoque de la inteligencia sobre amenazas

Ante el crecimiento de la complejidad, precisión y volumen de los ataques, el enfoque utilizado hasta ahora para tratar la inteligencia sobre amenazas ya no es válido. Investigar ataques selectivos no es tarea fácil. El dinamismo de los agresores, la mayor variedad y disponibilidad de fuentes locales y mundiales de inteligencia sobre amenazas, y la diversidad de los datos pueden dificultar más que nunca la agregación y digestión de esta información en el centro de operaciones de seguridad (SOC).

Los entornos con soluciones de distintos proveedores, habituales en la mayoría de las empresas, incrementan las dificultades para compartir datos de eventos y garantizar su visibilidad en toda la organización. Como señala Gartner en su informe *Technology Overview for Threat Intelligence Platforms* (Descripción de la tecnología de las plataformas de inteligencia sobre amenazas), "la incapacidad de las organizaciones para compartir la inteligencia sobre amenazas es una ventaja para los ciberdelincuentes. Compartir la inteligencia sobre amenazas tiene un efecto multiplicador y se está convirtiendo en un elemento clave para seguir el ritmo del creciente número de ciberdelincuentes y ataques"[3].

Pero compartir la inteligencia sobre amenazas no constituye necesariamente en sí misma una medida preventiva y correctiva sostenible. Es fácil que los analistas de seguridad se vean desbordados por una ingente cantidad de información. Normalmente, los equipos de seguridad están inmersos en un proceso agotador (véase la figura 1) que consiste en analizar manualmente millones de eventos de seguridad y archivos sospechosos con el fin de articular multitud de datos e intentar reconstruir el ataque selectivo.

"Para nuestra infraestructura de seguridad, necesitábamos mucho más que un proveedor de tecnología. Era absolutamente fundamental establecer una relación con un partner que nos ayudara a hacer frente a la diversidad de requisitos de los clientes y a un panorama de amenazas en constante evolución. McAfee ofrece esa alianza; la información de seguridad que recibimos constantemente de las soluciones de McAfee es crucial para mantener las operaciones de nuestra empresa en la vanguardia".

—Anurana Saluja
CISO y Vicepresidente de Seguridad de la Información
Sutherland Global Services

A la larga, esto afecta a la exhaustividad y la agilidad de la respuesta a las amenazas. Mucho antes de llegar a comprender las amenazas, los equipos de seguridad se empeñan en contener cuanto antes los ataques. En un reciente estudio de Intel Security (ahora McAfee): *When Minutes Count, 2014* (Cuando los minutos cuentan, 2014), menos del 25 % de los encuestados manifestaron que podían detectar un ataque en cuestión de minutos[4].

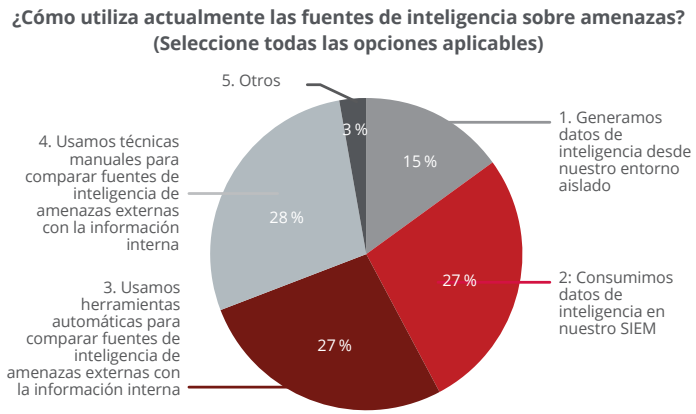

Figura 1. Según una encuesta de Intel Security (ahora McAfee) realizada en BlackHat 2015, un gran número de usuarios siguen utilizando técnicas manuales para comparar la inteligencia externa sobre amenazas con la interna.

Operatividad de la inteligencia sobre amenazas

Para detectar y corregir las amenazas mediante el empleo de la inteligencia no basta con importar manualmente a una tabla de vigilancia SIEM las direcciones IP de los agresores que han sido publicadas en un sitio web abierto una vez por semana.

Es fundamental ingerir la inteligencia sobre amenazas en tiempo real y correlacionar todas las facetas de un ataque, incluidos sus métodos y campañas mundiales, para que las empresas puedan prever hasta las amenazas más sigilosas y con mayor capacidad de adaptación. Los SOC empresariales necesitan un modo de "hacer operativa la inteligencia sobre amenazas" para obtener una visión completa de los ataques que afectan a su entorno. Deben saber cómo cribar la enorme cantidad de datos para analizar, correlacionar y establecer prioridades en la inteligencia sobre amenazas y así determinar qué es relevante para su sector, su geografía y su organización. Además, necesitan conocer los ataques específicos que podrían tener lugar en la actualidad, así como las tendencias que sugieren los datos históricos de eventos de seguridad. Como destaca Forrester, es imprescindible que la inteligencia sobre amenazas sea operativa, ya que el 75 % de los ataques se propaga de una víctima a la siguiente en menos de 24 horas. Las empresas deben reducir la diferencia entre "la velocidad para compartir y la velocidad del ataque"[5].

Aprovechamiento de la arquitectura integrada de McAfee

McAfee ofrece una plataforma unificada de colaboración con todos los componentes necesarios para hacer operativa la inteligencia sobre amenazas —incluida la procedente de fuentes mundiales—, crear información local, compartir la información en toda la infraestructura de TI, administrar la información y los eventos de seguridad, y proporcionar una protección automatizada y adaptable.

RESUMEN DE LA SOLUCIÓN

Requisitos de la inteligencia sobre amenazas	McAfee® Threat Intelligence Exchange	McAfee Advanced Threat Defense	McAfee Enterprise Security Manager	McAfee Global Threat Intelligence
Reunir inteligencia sobre amenazas de fuentes externas	Importa datos de STIX, McAfee® Global Threat Intelligence (McAfee GTI) y VirusTotal	Importa datos de McAfee GTI	Importa datos de McAfee GTI, TAXII/STIX e información de amenazas HTTP a través del gestor de ciberamenazas McAfee Enterprise Security Manager	McAfee GTI reúne inteligencia de amenazas de múltiples partners de la Cyber Threat Alliance y fuentes públicas. McAfee GTI extrae inteligencia sobre amenazas de millones de sensores de productos de McAfee desplegados por los clientes, como las soluciones para endpoints, la Web y el correo electrónico, los sistemas de prevención de intrusiones para red (IPS) y los dispositivos firewall.
Reunir inteligencia sobre amenazas interna	Recoge muestras de McAfee VirusScan®, McAfee Application Control, McAfee Web Gateway, McAfee Advanced Threat Defense y McAfee Enterprise Security Manager, y de productos de otros proveedores que envían información a través de Data Exchange Layer	Recibe archivos de muestra de McAfee Threat Intelligence Exchange o de la red para detonar su carga útil	A través de STIX/TAXII y Data Exchange Layer	
Generar inteligencia sobre amenazas local	Registra incidentes de archivos sospechosos y crea una base de datos local que indica el primer contacto y la trayectoria de las amenazas	Disecciona y califica el malware como tal, genera inteligencia sobre amenazas local y la distribuye a través de Data Exchange Layer o como una API con formato STIX	Crea listas de vigilancia, informes y vistas de amenazas basándose en eventos correlacionados	
Distribuir la inteligencia sobre amenazas a todos los controles de seguridad	A través de Data Exchange Layer	A través de Data Exchange Layer y la API del producto	A través de Data Exchange Layer, la API del producto y la integración de secuencias de comandos	McAfee GTI se integra en numerosos productos de McAfee, como McAfee Web Gateway, McAfee Enterprise Security Manager y las soluciones para endpoints de McAfee

Requisitos de la inteligencia sobre amenazas	McAfee® Threat Intelligence Exchange	McAfee Advanced Threat Defense	McAfee Enterprise Security Manager	McAfee Global Threat Intelligence
Ofrecer visibilidad de la información sobre amenazas recopilada	A través de los paneles de McAfee Threat Intelligence Exchange	A través de informes	A través de paneles, vistas e informes suministrados en paquetes de contenido o generados por el cliente	A través de McAfee Threat Center y del informe trimestral de McAfee sobre amenazas

Tabla 1. Plataforma integrada de inteligencia sobre amenazas de McAfee

Ingesta, análisis y propagación de información

McAfee Global Threat Intelligence

Un buen punto de partida para empezar a construir su plataforma integrada de inteligencia sobre amenazas es McAfee Global Threat Intelligence (McAfee GTI), un servicio exhaustivo de reputación en tiempo real basado en la nube que se integra plenamente en los productos de McAfee y les permite bloquear con rapidez las ciberamenazas en todos los vectores: archivos, Web, mensajería y la red. McAfee GTI asigna puntuaciones de reputación a miles de millones de archivos, URL, dominios y direcciones IP en función de datos de amenazas obtenidos de diversas fuentes: millones de sensores que analiza y supervisa McAfee Labs desplegados por todo el mundo, información sobre amenazas de partners de investigación y la Cyber Threat Alliance, así como información multivectorial de los datos de amenazas de la Web, el correo electrónico y la red. Apoyándose en información sobre amenazas relevante y de alta calidad, McAfee GTI ofrece asesoramiento riguroso sobre los riesgos, lo que facilita la toma de decisiones fundamentadas sobre las políticas de seguridad y permite que los controles bloqueen, limpien o autoricen, según corresponda.

McAfee Enterprise Security Manager

McAfee Enterprise Security Manager (SIEM) da un paso más en la ingesta y el análisis de la información sobre amenazas, ya que centraliza la consolidación, el análisis y la actuación para todo tipo de inteligencia sobre amenazas. Con esta panorámica de 360 grados se puede disfrutar de plena visibilidad y conocimiento de la situación, lo que agiliza la detección y la respuesta ante los ataques selectivos. Su avanzado sistema de administración de datos está expresamente diseñado para almacenar y asimilar grandes volúmenes de datos contextuales en tiempo real.

McAfee Enterprise Security Manager reúne datos de actividades y eventos de todos los sistemas, bases de datos, redes y aplicaciones. También importa información sobre amenazas de fuentes de todo el mundo y la admite en formatos y tipos de transporte estándar, como Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Indicator Information (TAXII) y Cybox, que normalmente publican comunidades o grupos del sector como el Financial Services Information Sharing and Analysis Center (FS-ISAC).

Utilizando análisis avanzados traduce la información reunida en datos comprensibles y prácticos de seguridad.

Y sobre todo, proporciona más visibilidad de las amenazas emergentes mediante vistas en tiempo real y acceso a información histórica de seguridad. De este modo es posible investigar retrocediendo en el tiempo para comprender la prevalencia y los patrones de un ataque, así como crear listas de vigilancia automatizadas que permitan detectar la aparición o reaparición de eventos en el futuro. Al incrementar la sensibilidad del sistema ante eventos maliciosos conocidos, aumenta su capacidad para detectar actividades y patrones de actividad sospechosos en varias etapas de la cadena de ataque y después establecer las prioridades de respuesta.

Figura 2. Vista de McAfee GTI.

McAfee GTI for Enterprise Security Manager permite aprovechar las potentes funciones de investigación de McAfee Labs para supervisar la seguridad empresarial. La abundante información que aporta McAfee GTI, actualizada constantemente, mejora el conocimiento de la situación, ya que permite detectar rápidamente eventos relacionados con comunicaciones con IP sospechosas o maliciosas, y permite a los administradores de la seguridad determinar qué hosts de la empresa se han comunicado o se comunican actualmente con ciberdelincuentes conocidos.

McAfee Threat Intelligence Exchange

Un tercer componente que puede añadir para crear un ecosistema integrado de inteligencia sobre amenazas es McAfee Threat Intelligence Exchange, que agrupa y comparte inteligencia sobre reputación de archivos con toda la infraestructura de seguridad. McAfee Threat Intelligence Exchange recibe información sobre amenazas de McAfee GTI, importaciones de archivos de STIX, datos de McAfee Enterprise Security Manager e información de endpoints, control de aplicaciones, dispositivos móviles, gateways, centros de datos y tecnologías de análisis en entornos aislados de soluciones de McAfee y de otros proveedores.

Mediante la recopilación de datos de todos los puntos de la infraestructura, ofrece información sobre amenazas que quizá se encuentren solo en su entorno, como es el caso en muchos ataques selectivos. A su vez, la información de reputación de archivos se comparte al instante en todo el ecosistema con todos los productos y soluciones conectados a McAfee Threat Intelligence Exchange a través de Data Exchange Layer (DXL). Por ejemplo, si McAfee Threat Intelligence Exchange distribuye información sobre un ejecutable malicioso, McAfee Data Loss Prevention la recibe a través de DXL y empieza a supervisar si ese ejecutable accede a algún archivo confidencial.

Los datos de amenazas compartidos a través de DXL incluyen reputación de archivos, clasificaciones de datos, integridad de aplicaciones y datos contextuales

¿Qué es la Cyber Threat Alliance?

La **Cyber Threat Alliance** es un grupo de profesionales de la seguridad de organizaciones que trabajan juntas para compartir inteligencia sobre amenazas y ayudar a mejorar las defensas frente a los agresores en todas las organizaciones miembros y sus clientes. McAfee es uno de los miembros fundadores que han dedicado sus recursos a encontrar las formas más eficaces para compartir datos de amenazas, fomentar la colaboración entre los miembros y lograr un progreso conjunto en la lucha contra los ciberdelincuentes sofisticados.

de usuarios, todo lo cual se comparte con los productos integrados en la estructura de DXL. En DXL puede integrarse cualquier producto o solución; después, este se configura para determinar qué información publica en el sistema, qué información debe buscar y a cuál debe suscribirse.

McAfee Threat Intelligence Exchange trabaja en estrecha colaboración con la solución avanzada de entornos aislados, McAfee Advanced Threat Defense, que suministra datos de análisis de malware a McAfee Threat Intelligence Exchange. Si se determina que un archivo es malicioso, McAfee Threat Intelligence distribuye la información de reputación del archivo a todos los sistemas conectados a través de DXL. Esto también funciona en sentido inverso. Cuando los endpoints con McAfee Threat Intelligence Exchange encuentran archivos con reputación desconocida, los envían a McAfee Advanced Threat Defense para determinar si el objeto es malicioso, lo que elimina los ángulos muertos cuando la carga útil se distribuye fuera de banda. Estos dos productos funcionan juntos para ofrecer una protección automatizada y adaptable frente a las amenazas emergentes. La información sobre los ataques detectados se distribuye en todo el entorno para bloquear la cadena del ciberataque antes de que el daño causado sea mayor.

McAfee Threat Intelligence Exchange facilita una detección de amenazas y una respuesta adaptables, gracias al empleo de la información adquirida en tiempo real en sus soluciones de seguridad para endpoints, gateways, redes y centro de datos. La combinación de datos sobre amenazas globales importados con la información recopilada de forma local, así como la capacidad para compartir dicha información de forma instantánea, permite a sus soluciones de seguridad funcionar como una sola, intercambiando los datos compartidos y actuando en función de ellos.

Interrupción de la cadena del ciberataque

Independientemente de dónde se produzca el primer contacto con un archivo de malware desconocido, una vez detectado todo el entorno conectado recibe la información de inmediato. Cuando McAfee Advanced Threat Defense califica un archivo como malicioso, McAfee Threat Intelligence Exchange pone inmediatamente la información sobre la amenaza a disposición de todos los controles de seguridad de la empresa mediante una actualización de reputación que se distribuye a través de DXL. Por su parte, los gateways con McAfee Threat Intelligence Exchange evitan que el archivo entre en la infraestructura. Al compartir la inteligencia sobre la amenaza de forma coordinada con todos los controles de seguridad, es más fácil interrumpir la cadena del ataque y prevenir daños mayores sin necesidad de ninguna intervención manual.

Digestión y aplicación de la información: detecte con precisión y tome mejores decisiones

Una vez recibidos los datos de amenazas, McAfee Enterprise Security Manager actúa como punto central de visibilidad y correlaciona la información de McAfee GTI, McAfee Threat Intelligence Exchange y los indicadores de peligro con formato STIX/TAXII con los datos de eventos, detectados en tiempo real o históricamente cuando los nodos de la red se comunican con ciberdelincuentes conocidos o dominios sospechosos. El panel de gestión de amenazas ofrece a los analistas una única vista integral

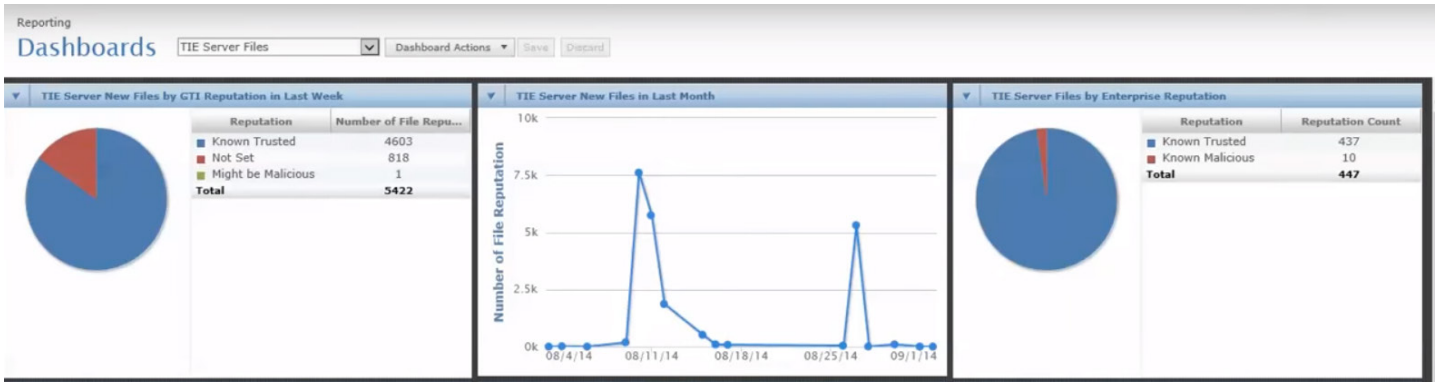

Figura 3. Panel de McAfee Threat Intelligence Exchange.

de los indicadores de amenazas recopilados, las fuentes de la información, la tasa de coincidencia con esos indicadores y detalles en formato legible de los indicadores de peligro.

Utilizando el sistema SIEM de McAfee en combinación con otras herramientas colaborativas de información sobre amenazas, se reducen los gastos de explotación que conlleva la configuración de reglas de correlación, un proceso manual normalmente tedioso. Por ejemplo, los analistas de seguridad pueden revisar directamente la información sobre amenazas recibida en formato legible para el ojo humano, lo que permite comprender mejor las nuevas amenazas detectadas. Y lo que es más importante, las reglas de correlación en tiempo real o históricas pueden incorporar automáticamente la información sobre amenazas recibida, lo que reduce el tiempo necesario para detectar acciones en curso o nuevas agresiones. Los usuarios también pueden seguir el progreso de las amenazas denunciadas en todo el entorno de TI, así como a través de la información contextual de las vistas de alarma, para tomar mejores decisiones con más fundamento. Toda esta información recopilada mejora y agiliza la detección e investigación de ataques selectivos.

Teniendo en cuenta que las amenazas se abren camino rápidamente a través de la infraestructura de TI y que están diseñadas para cambiar con el tiempo, McAfee Enterprise Security Manager puede actualizar periódicamente la información adquirida sobre amenazas, y eliminar los datos antiguos y menos relevantes. Por ejemplo, los servidores de mando y control que han sido retirados o los sitios web saneados con puntuaciones más bajas de reputación maliciosa se eliminan automáticamente para reducir los falsos positivos que puedan distraer al personal de seguridad de perseguir amenazas reales.

Los siguientes productos de McAfee admiten la información sobre amenazas con formato STIX:

- McAfee Threat Intelligence Exchange
- McAfee Advanced Threat Detection
- McAfee Enterprise Security Manager

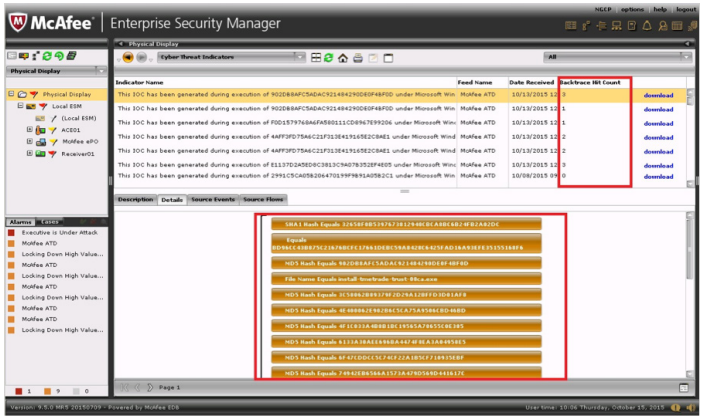

Figura 4. Indicadores de ciberamenazas, número de detecciones de Backtrace y datos de los indicadores de peligro de McAfee Enterprise Security Manager.

Resumen

La inteligencia sobre amenazas integrada de McAfee permite ingerir, digerir y administrar la información y así detectar las amenazas con más precisión, eliminar el esfuerzo manual e impedir que los agresores dañen su empresa. Con una mayor visibilidad y conocimiento de la actividad maliciosa en todo el ecosistema de seguridad, estará más preparado para identificar y anticiparse a los ataques selectivos actuales y prevenirlos en el futuro.

Más información

Para obtener más información sobre los componentes de la plataforma integrada de información sobre amenazas de McAfee, visite:

- McAfee Global Threat Intelligence
- McAfee Threat Intelligence Exchange
- McAfee Advanced Threat Defense
- McAfee Enterprise Security Manager
- How to Use a TAXII Feed with McAfee Enterprise Security Manager (Cómo utilizar datos TAXII con McAfee Enterprise Security Manager)

1. https://www.sans.org/reading-room/whitepapers/analyst/who-039-s-cyberthreat-intelligence-how-35767
2. https://www.forrester.com/The+State+Of+The+Cyberthreat+Intelligence+Market/fulltext/-/E-RES123011
3. https://www.gartner.com/doc/2941522/technology-overview-threat-intelligence-platforms
4. http://www.mcafee.com/es/resources/reports/rp-when-minutes-count.pdf
5. https://www.rsaconference.com/writable/presentations/file_upload/cxo-t08r-threat-intelligence-is-like-three-day-potty-training.pdf

McAfee
Together is power.

Avenida de Bruselas nº 22
Edificio Sauce
28108 Alcobendas, Madrid, España
+34 91 347 85 00
www.mcafee.com/es

62161_1015
OCTUBRE DE 2015