Resumen de la Solución

Haciendo que la Inteligencia de Amenazas Sea Operacional

Detrás de casi cada alerta de seguridad legítima que recibe su TI, hay un adversario utilizando diversas técnicas de ataque para penetrar en su infraestructura y poner en peligro sus activos de datos o sistemas vitales. Los ataques dirigidos de múltiples fases de hoy, constan de una serie de pasos que componen la cadena del ciber-ataque: reconocimiento, análisis de vulnerabilidades, explotación y, finalmente, ex-filtración de datos corporativos valiosos.

Los analistas de seguridad están conscientes de estas técnicas y dependen de la inteligencia de amenazas para captar conocimiento sobre métodos de ataque y motivaciones. Pueden detectar e interrumpir amenazas avanzadas, aplicar corrección adecuada, y estar mejor preparados la próxima vez que suene la alarma de seguridad. Pero con demasiada frecuencia, les falta de visibilidad hacia determinados sistemas o están inundados con demasiados datos y muy poca inteligencia. Según el estudio del Instituto SANS, *¿Quién Usa la Inteligencia de Ciber-amenazas y Cómo?*, "… sólo el 11,9% de los entrevistados han obtenido la capacidad de agregar información de amenazas desde prácticamente cualquier fuente, y sólo el 8,8% tienen una visión completa que pueden combinar eventos con los locales[1]".

En un reciente informe, Forrester señala que el 77% de los tomadores de decisiones de seguridad de empresas norteamericanas y europeas, informaron que mejorar las capacidades de inteligencia de amenazas es prioritario[2]. La inteligencia de ciberamenazas promete dar aviso anticipado a los profesionales de seguridad cuando los ciberdelincuentes atacan su región, industria o incluso empresas concretas, de manera que tengan tiempo para tomar medidas de seguridad, pero la seguridad de TI todavía enfrenta grandes desafíos:

- Cómo recolectar inteligencia de amenazas desde fuentes externas e internas.
- Cómo correlacionar los datos y priorizar los riesgos.
- Cómo distribuir la inteligencia a lo largo de controles de seguridad de múltiples proveedores en toda la empresa.
- Cómo obtener mayor visibilidad en el escenario de TI para permitir una acción adecuada y rápida.

Las empresas modernas necesitan una arquitectura abierta e integrada que facilite la adopción de inteligencia de amenazas y les permita aprovechar sus beneficios, desde la recolección básica de amenazas para análisis forenses, hasta su uso para enriquecer los análisis SIEM. En otras palabras, los usuarios necesitan poner a funcionar la inteligencia de amenazas a través de procesos automatizados que permitan analizarla, digerirla y gestionarla.

intel Security

Las Nuevas Amenazas Requieren un Nuevo Abordaje Hacia la Inteligencia de Amenazas

En la medida en que los ataques crecen en complejidad, precisión y volumen, el abordaje de inteligencia de amenazas del ayer ya no es adecuado. Investigar los ataques dirigidos no es una tarea fácil. El comportamiento dinámico de los atacantes, la mayor variedad y disponibilidad de las fuentes de inteligencia de amenazas locales y globales, y la diversidad de los formatos de datos de inteligencia sobre amenazas pueden hacer que la agregación y la digestión de la inteligencia de amenazas en las herramientas del centro de operaciones de seguridad (SOC) sea más desafiante que nunca.

Un entorno de múltiples proveedores, que es típico de la mayoría de las empresas, se suma a la dificultad de compartir datos de eventos y promover visibilidad de eventos a lo largo de toda la organización. Como Gartner señala en su informe, Visión General de Tecnología para Plataformas de Inteligencia de Amenazas, "La incapacidad de una organización de compartir TI es una ventaja para los perpetradores de los ciber-ataques. Compartir TI es un multiplicador de fuerza y se está convirtiendo en un elemento clave para mantenerse al paso del creciente número de perpetradores de amenazas y de los ataques que utilizan[3].

Pero compartir exclusivamente inteligencia de amenazas no necesariamente generará acciones correctivas y prevención sostenibles. Los analistas de seguridad pueden verse rápidamente abrumados con demasiada información. La mayoría de los equipos de seguridad están involucrados en el extenuante proceso manual (ver Figura 1) de analizar millones de eventos de seguridad y archivos sospechosos en un esfuerzo por unir las piezas de una montaña de datos e intentar reconstruir el ataque dirigido. A final de cuentas, esto menoscaba la minuciosidad y la velocidad del proceso de respuesta. Con una comprensión deficiente de las amenazas, los equipos de seguridad están luchando para contener los ataques de manera oportuna. Según un estudio reciente de Intel Security: *Cuando los Minutos Cuentan, 2014*, menos del 25% de los encuestados dijeron que podían detectar un ataque en menos de 4 minutos[4].

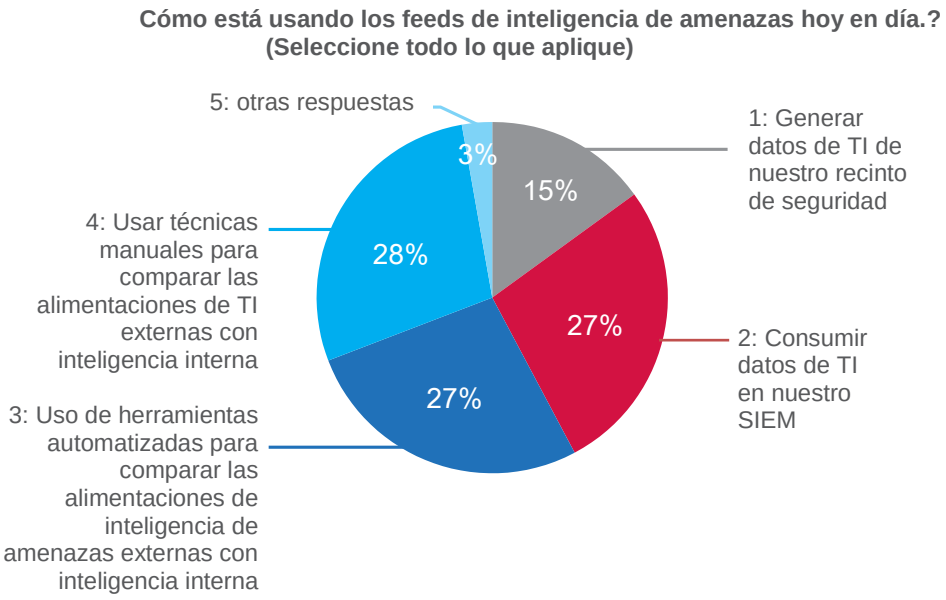

Figura 1. Según una encuesta de Intel Security en BlackHat 2015, un gran grupo de usuarios todavía emplea técnicas manuales para comparar las alimentaciones de inteligencia de amenazas externas con inteligencia de amenazas internas

"Para nuestra infraestructura de seguridad, necesitábamos mucho más que un proveedor de tecnología. Fue absolutamente esencial haber construido una relación con un partner que pudiera ayudarnos a gestionar nuestro conjunto diverso de los requisitos del cliente y una situación de amenazas en continua evolución. McAfee ofrece esa sociedad, y la inteligencia de seguridad permanente que recibimos de las soluciones de McAfee es crucial para que nos ayude a mantener nuestras operaciones de negocios a la vanguardia".

– Anurana Saluja
CISO y Vicepresidente de Information Security Sutherland Global Services

Haga que la Inteligencia de Amenazas Sea Operativa

La detección y corrección de amenazas conducida por inteligencia requiere algo más que importar manualmente direcciones IP de los adversarios, que se publican en un sitio Web abierto hacia una tabla de lista de vigilancia SIEM una vez a la semana. En lugar de eso, requiere consumo y correlación de inteligencia de amenazas en tiempo real de todas las facetas de un ataque, incluyendo métodos y campañas globales, de modo que las empresas puedan anticiparse incluso a las amenazas más discretas y más rápidamente adaptables. Los SOCs empresariales necesitan una manera de "hacer operativa la inteligencia de amenazas" para obtener un panorama completo de los ataques que afectan a sus entornos. Necesitan una manera de clasificar

la enorme cantidad de datos para analizar, correlacionar y priorizar inteligencia de amenazas, y determinar lo que es relevante para su industria, su geografía y su compañía. Y necesitan ser capaces de obtener conocimientos sobre ataques únicos que pueden estar sucediendo en el presente, así como conocimiento sobre tendencias con base en los datos históricos de eventos de seguridad. Como señala Forrester, el hacer operativa la inteligencia de amenazas es crítico, ya que el 75% de los ataques se propagan desde una víctima hacia la siguiente en menos de 24 horas. Las empresas necesitan cerrar la brecha entre "velocidad para compartir y velocidad de ataque"[5].

Aproveche la Arquitectura Integrada de Intel Security

Intel Security proporciona una plataforma de colaboración unificada con todos los componentes necesarios para hacer operativa la inteligencia de amenazas, incluyendo alimentaciones de inteligencia de amenazas globales, creación de inteligencia local, intercambio en tiempo real de información de amenazas en toda la infraestructura de TI, información de seguridad y gestión de eventos, y entrega de protección adaptable y automatizada.

Requisitos de Inteligencia de Amenazas	McAfee® Threat Intelligence Exchange	McAfee Advanced Threat Defense	McAfee Enterprise Security Manager	McAfee Global Threat Intelligence
Recopila inteligencia de amenazas de fuentes externas	STIX, McAfee Global Threat Intelligence (McAfee GTi) Import, y VirusTotal	McAfee GTI Import, TAXII/STIX	McAfee GTI, TAXII/STIX Import y feeds de amenazas HTTP mediante el gestor de ciberamenazas McAfee Enterprise Security Manager	Inteligencia de amenazas proveniente de múltiples partners de la Cyber Threat Alliance y fuentes públicas. McAfee GTI extrae inteligencia de amenazas de millones de sensores desplegados por los clientes en productos de Intel Security como endpoint, web, correo, sistemas de prevención de intrusiones en red (IPS) y dispositivos de firewall
Recolecta inteligencia de amenazas interna	Recolecta muestras de McAfee VirusScan®, McAfee Application Control, McAfee Web Gateway, McAfee Advanced Threat Defense, McAfee Enterprise Security Manager y de productos de proveedores terceros que envían información por McAfee Data Exchange Layer	Consume los archivos de muestra para detonación desde McAfee Threat Intelligence Exchange o mediante la red	Vía STIX/TAXII y McAfee Data Exchange Layer	
Produce inteligencia de amenazas local	Registra los incidentes de archivos sospechosos y crea una base de datos local que registra el primer contacto y la trayectoria de las amenazas mediante McAfee Data Exchange Layer	Disecciona y condena a malware, genera inteligencia de amenazas locales, y distribuye a lo largo de McAfee Data Exchange Layer o como una API formateada como STIX	Crea listas de vigilancia, informes y vistas de inteligencia de amenazas con base en los eventos correlacionados	
Distribuye inteligencia de amenazas a lo largo de controles de seguridad	Mediante McAfee Data Exchange Layer	Vía McAfee Data Exchange Layer y API de producto	Vía McAfee Data Exchange Layer, API de producto e integración de script	McAfee GTI está integrado con diversos productos de Intel Security, tales como McAfee Web Gateway, McAfee Enterprise Security Manager, y soluciones de endpoint de McAfee
Ofrece visibilidad hacia inteligencia de amenazas recolectada	Vía paneles de McAfee Threat Intelligence Exchange	Vía informes	Vía paneles, vistas e informes proporcionados en paquetes de contenido o generados por el cliente	Vía McAfee Threat Center y trimestralmente McAfee Threats Report

Tabla 1. Plataforma integrada de inteligencia de amenazas de Intel Security

Consumir, Analizar y Propagar

McAfee Global Threat Intelligence

Un buen lugar para comenzar la construcción de su plataforma integrada de inteligencia de amenazas es McAfee Global Threat Intelligence (McAfee GTI), un servicio de reputación completo, en tiempo real y basado en la nube, que está plenamente integrado con los productos de Intel Security y les permite bloquear mejor las ciber-amenazas a lo largo de todos los vectores - archivos, web, mensajes y red- de manera rápida. McAfee GTI proporciona puntuaciones de reputación para miles de millones de archivos, URLs, dominios y direcciones IP con base en datos de amenazas recopilados de múltiples fuentes: millones de sensores globales monitoreados y analizados por McAfee Labs, feeds de amenazas de partners de investigación y a través de la Cyber Threat Alliance, e inteligencia inter-vector de la web, correo electrónico y datos de amenazas de red. Respaldado por su alta calidad y feeds de amenazas relevantes, McAfee GTI proporciona asesoría de riesgos precisa, que fomenta una política de toma de decisiones informadas y activa los controles para bloquear, limpiar o permitir, según sea necesario.

McAfee Enterprise Security Manager

McAfee Enterprise Security Manager (SIEM) lleva la ingestión de inteligencia y análisis de amenazas hacia el próximo nivel, proporcionando un hub de consolidación, análisis y acción para cada tipo de inteligencia de amenazas. Esta vista de 360 grados permite una visibilidad completa y la conciencia situacional para acelerar la detección y la respuesta para ataques dirigidos. Su avanzado sistema de gestión de datos se ha diseñado específicamente para almacenar y asimilar altos volúmenes de datos contextuales en tiempo real.

McAfee Enterprise Security Manager recolecta datos de actividad y eventos de todos sus sistemas, bases de datos, redes y aplicaciones. También las importa alimentaciones de amenazas globales y consume inteligencia de amenazas en formatos y transportes estándares, como Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Indicator Information (TAXII) y Cybox, típicamente publicados por comunidad o grupos de industria como el Financial Services Information Sharing and Analysis Center (FS-ISAC). A través de análisis avanzados, traduce la información recopilada en inteligencia de seguridad comprensible y accionable. Y lo más importante, proporciona visibilidad más profunda de las amenazas emergentes a través de vistas en tiempo real y acceso a información de seguridad histórica. Esto le permite investigar regresando en el tiempo para entender la prevalencia y los patrones de un ataque, y también para crear listas de vigilancia automatizadas para detectar la ocurrencia o re-ocurrencia de eventos en el futuro. Al enriquecer la sensibilidad de su sistema a eventos conocidos por ser maliciosos, puede aumentar su capacidad para detectar actividades sospechosas y patrones de actividad en distintas fases de la cadena de ataque y posteriormente priorizar la respuesta.

¿Qué es la Cyber Threat Alliance?

La **Cyber Threat Alliance** es un grupo de profesionales de seguridad de las organizaciones que trabajan juntas para compartir información sobre amenazas, y ayudar a mejorar las defensas contra los adversarios a lo largo de las organizaciones miembros y sus clientes. Intel Security es uno de los miembros fundadores, que ha dedicado sus recursos para determinar las formas más eficaces de compartir datos sobre amenazas, fomentar la colaboración entre los miembros y progresar en la lucha contra los ciber delincuentes sofisticados.

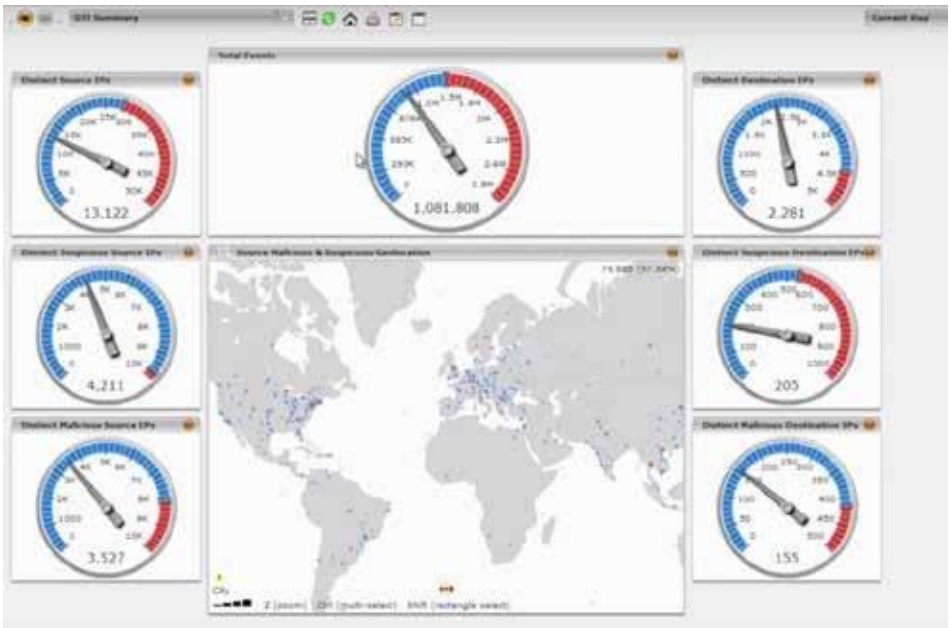

Figura 2. Vista de McAfee GTI.

McAfee GTI for McAfee Enterprise Security Manager lleva el poder de las capacidades de investigación de McAfee Labs hacia el monitoreo de seguridad empresarial. Este feed de McAfee GTI constantemente actualizado y enriquecido, mejora la conciencia situacional permitiendo el rápido descubrimiento de los eventos involucrando comunicaciones con IPs sospechosas o maliciosas y permite a los administradores de la seguridad determinar qué hosts de la empresa se han comunicado o actualmente se comunican con actores maliciosos conocidos.

McAfee Threat Intelligence Exchange

El tercer componente que puede añadir conforme desarrolla un ecosistema de inteligencia de amenazas integrado es McAfee Threat Intelligence Exchange, que agrega y comparte inteligencia de reputación de archivos a lo largo de la infraestructura de seguridad. McAfee Threat Intelligence Exchange recibe información de amenazas de McAfee GTI, importaciones de archivos STIX, alimentaciones de amenazas provenientes vía McAfee Enterprise Security Manager, e información proveniente de endpoint, control de aplicaciones, dispositivos móviles, gateway, centros de datos y tecnologías de recinto de seguridad tanto de las soluciones de Intel Security como de otros proveedores. Recolectar datos desde todos los puntos de su infraestructura proporciona información sobre las amenazas que pueden estar presentes únicamente en su entorno, como es común con muchos ataques. A su vez, la reputación del archivo se comparte de forma instantánea en todo el ecosistema hacia todos los productos y soluciones conectados a McAfee Threat Intelligence Exchange vía McAfee Data Exchange Layer. Por ejemplo, si McAfee Threat Intelligence Exchange emite información acerca de un archivo ejecutable malicioso, McAfee Data Loss Prevention recibe esta información a través de McAfee Data Exchange Layer y posteriormente inicia el monitoreo de ese ejecutable para detectar cualquier acceso a archivos delicados.

Los datos de las amenazas compartidos a lo largo de McAfee Data Exchange Layer incluyen reputaciones de archivos, clasificaciones de datos, integridad de aplicaciones y datos de contexto de usuario, que se comparten con y entre productos integrados en el tejido de McAfee Data Exchange Layer. Cualquier producto o solución puede integrarse en McAfee Data Exchange Layer, y posteriormente configurarse para determinar qué información publicar en el sistema y qué información escuchar y suscribirse.

McAfee Threat Intelligence Exchange trabaja estrechamente con la solución avanzada de recinto de seguridad de Intel Security, McAfee Advanced Threat Defense, que alimenta datos de análisis de malware a McAfee Threat Intelligence Exchange. Si se descubre que un archivo es malicioso, McAfee Threat Intelligence saca una actualización de reputación de archivo para actualizar todos los sistemas conectados a lo largo de McAfee Data Exchange Layer. Esto también funciona al revés. Cuando los endpoints habilitados por McAfee Threat Intelligence Exchange encuentran archivos con reputaciones desconocidas, ellos pueden ser enviados a McAfee Advanced Threat Defense para determinar si el objeto es malicioso, eliminando puntos ciegos desde la entrega de carga útil fuera de banda. Estos dos productos funcionan juntos para proporcionar una protección adaptable automatizada contra amenazas emergentes. La información sobre ataques descubiertos se entrega a lo largo de su entorno para ayudar a bloquear la cadena de ciber-ataque antes se haga más daño.

Figura 3. Panel de McAfee Threat Intelligence Exchange.

McAfee Threat Intelligence Exchange habilita la detección y respuesta a amenazas adaptable al hacer operacional la inteligencia a lo largo de sus soluciones de endpoint, gateway, red y centro de datos en tiempo real. Al combinar la información de amenazas globales importada con inteligencia obtenida localmente y compartirla al instante, se permite que las soluciones de seguridad funcionen como una, intercambiando y actuando sobre la inteligencia compartida.

Interrumpa la cadena ciber-ataques
Independientemente de si el primer punto de contacto sucede mediante un archivo de malware desconocido, una vez condenado, todo el entorno conectado se actualiza inmediatamente. Cuando un archivo es condenado por McAfee Advanced Threat Defense, McAfee Threat Intelligence Exchange publicará esta condena mediante actualización de reputación, que se difunde mediante McAfee Data Exchange Layer hacia todos los controles de seguridad dentro de su organización. Las gateways habilitadas por McAfee Threat Intelligence Exchange evitan que el archivo entre a su infraestructura. Mediante la acción coordinada de compartir inteligencia de amenazas a lo largo de todos sus controles de seguridad, resulta más fácil interrumpir la cadena de ataques y prevenir daños adicionales sin la necesidad de intervención manual.

Digiera y Aplique: Detecte con Exactitud y Tome Mejores Decisiones

Después de que los datos son consumidos, McAfee Enterprise Security Manager actúa como un punto central de visibilidad, correlacionando los feeds de McAfee GTI, McAfee Threat Intelligence Exchange, e indicadores de riesgo (IoCs) formateados como STIX/TAXII con los datos del evento, detectados en tiempo real o históricamente cuando los nodos de su red se están comunicando con actores maliciosos conocidos o dominios sospechosos.
El panel de gestión de amenazas proporciona a los analistas una visión única y completa de los indicadores recolectados de amenazas, las alimentaciones fuentes, la tasa de aciertos contra los indicadores, y los detalles más relevantes que pueden ser leídos por humanos de indicadores de riesgo (IoCs).

Figura 4. Indicadores de ciber-amenazas de McAfee Enterprise Security Manager, hits de backtrace, y detalles de amenazas IoC.

Al usar el sistema Intel Security SIEM sistema junto con otras herramientas de colaboración en inteligencia de amenazas se reducen los gastos operativos asociados con reglas de configuración de configuración, que generalmente son un engorroso proceso manual. Por ejemplo, los analistas de seguridad pueden revisar directamente la información de amenazas recientemente recibida en un formato legible para humanos, permitiendo una mejor comprensión de las nuevas amenazas detectadas. Lo que es más importante, la inteligencia de amenazas recibida pueden ser automáticamente adoptada por reglas de correlación históricas o en tiempo real, reduciendo así el tiempo para detectar actividad nueva o en curso de adversarios. Los usuarios también pueden seguir el progreso de las amenazas a lo largo de su entorno de TI, así como información contextual en vistas de alarma, lo que permite decisiones más informadas. Toda esta inteligencia recolectada mejora y acelera la detección e investigación de los ataques dirigidos. Debido a que las amenazas irrumpen en la infraestructura de TI de forma rápida y están diseñadas para cambiar a lo largo del tiempo, McAfee Enterprise Security Manager puede actualizar periódicamente toda la inteligencia de amenazas adquirida, eliminando datos viejos menos relevantes. Por ejemplo, servidores de comando y control removidos o sitios Web limpiados con puntuaciones de reputación maliciosa menores, se borran automáticamente para eliminar falsos positivos que puedan distraer la atención de su personal de seguridad e impedirle ir detrás de amenazas reales.

Los siguientes productos de Intel Security brindan soporte a inteligencia de amenazas en formato STIX:

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

Resumen

La inteligencia integrada de Intel Security Threat Intelligence hace que el consumo, digestión y gestión de la inteligencia de amenazas sea operacional, lo que le permite aumentar la precisión de detección de amenazas, eliminar los esfuerzos manuales y evitar que los adversarios dañen a su negocio. Con visibilidad y conocimiento mejorados sobre la actividad maliciosa en todo su ecosistema de seguridad, estará mejor preparado para identificar y prevenir los ataques dirigidos de hoy y evitarlos en el futuro.

Conozca Más

Para obtener más información sobre los bloques de construcción de la plataforma de inteligencia de amenazas integrada de Intel Security, visite:

- **McAfee Global Threat Intelligence**
- **McAfee Threat Intelligence Exchange**
- **McAfee Advanced Threat Defense**
- **McAfee Enterprise Security Manager**
- **Cómo utilizar un Feed 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/us/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. Parte da Intel Security. 2821 Mission College Boulevard Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com