DOCUMENTOS SiC
Nº 18
SEPTIEMBRE 2015

BT Security – CySOC

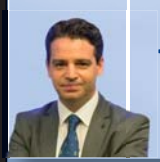
Ciberseguridad end-to-end de última generación adaptable a cada negocio

BT Servicios de Seguridad Gestionada de BT

intel Security Intel Security: tecnología para marcar la diferencia en MSSP

ENTREVISTAS

Jacinto Cavestany
Consejero Delegado de BT España



José Pereiro
Director de BT Security para España y Portugal

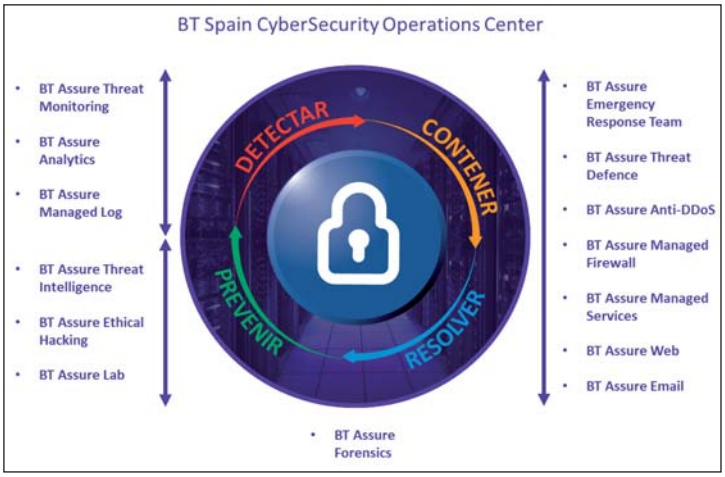
Javier Perea
Vicepresidente de Ventas de Intel Security

Carlos Muñoz
Director Técnico de Intel Security España

BT Security – Servicios CySOC

Ciberseguridad gestionada de ciclo completo

BT cuenta con 70 años de experiencia gestionando la seguridad interna del grupo BT (tanto a nivel físico como lógico), ayudando a las organizaciones en todo el mundo y en todos los sectores a gestionar la complejidad de la seguridad y a mitigar los riesgos de amenazas, tanto actuales como futuras.



¿Por qué se necesita un Centro de Operaciones de Seguridad?

El número de ataques cibernéticos que sufren las empresas no para de aumentar año tras año. Este hecho, combinado con el incremento de la complejidad de los mismos, supone un gran reto para los departamentos de IT y Comunicaciones.

Existen infinidad de riesgos, entre los que se encuentran la fuga de información sensible de los sistemas de información, ataques de denegación de servicio distribuido, *malware* dirigido, intrusiones desde Internet… entre otros muchos. Estos riesgos pueden suponer un serio impacto en nuestros negocios, como el lucro cesante derivado de la indisponibilidad de los sistemas de información, sanciones por parte de reguladores, daño a la imagen de la marca comercial… Sin embargo, identificar, implantar y gestionar las contramedidas necesarias para minimizar estos riesgos no es tarea fácil.

La seguridad IT es un área compleja y especializada, existen infinidad de tecnologías y controles técnicos en el mercado pero si no se dispone de las herramientas y los profesionales de seguridad necesarios para gestionarlas no aportan una protección real. Además hay que tener en cuenta que la amenaza es global, un ataque puede provenir de cualquier lugar del mundo y por esta razón es necesario disponer de servicios de ciberinteligencia con cobertura mundial que nos permitan anticiparnos a dichas amenazas.

Características del CyberSecurity Operations Center de BT España

• El Centro de Operaciones de Ciberseguridad de BT en Madrid (CySOC), forma parte de la red de 14 SOCs Globales de BT que trabajan de forma coordinada para proteger a nuestros clientes y nuestras redes.

• El CySOC de Madrid trabaja ininterrumpidamente 24 horas al día los 365 días del año y está preparado para proteger, tanto a las empresas españolas que operan en territorio nacional como a aquellas que, además, disponen de delegaciones o filiales en otras partes del mundo.

• Equipo de profesionales de seguridad, miembros de la práctica global de seguridad de BT, bilingües (castellano e inglés), certificados y con amplia experiencia en la gestión de multitud de tecnologías y servicios.

• Gestión del Servicio conforme a ITIL y buenas prácticas internacionalmente reconocidas y posibilidad de la integración con las herramientas de gestión del servicio del cliente.

• Posibilidad de disponer de profesionales en las instalaciones del cliente, así como de informes y cuadros de mando personalizados.

• Seguridad Física de las Instalaciones: separación física, control de acceso de doble factor, cristales anti-espionaje y sala de control, entre otras.

• Conectividad con el cliente a través de la Red Privada de BT que en la actualidad cubre la totalidad de las provincias españolas y dispone más de 151.000 conexiones. Esto garantiza la seguridad de las comunicaciones y permite dar SLAs de extremo a extremo. A nivel internacional cubre más de 170 países y territorios.

• Herramientas de Seguridad propias: BT está permanentemente invirtiendo en investigación de seguridad a través de BT Research y fruto de ello han nacido herramientas propias para su uso en la red de SOCs, como BT Assure Analytics. ●

Catálogo de servicios

- **BT Assure Threat Monitoring**: monitorización en tiempo real de ataques a los sistemas de información y comunicaciones del cliente.
- **BT Assure Analytics**: monitorización analítica de grandes volúmenes de datos de seguridad.
- **BT Assure Managed Log**: Servicio de custodia y análisis de los registros de los sistemas de información.
- **BT Assure Emergency Response Team**: equipo de respuesta ante incidentes de seguridad con cobertura nacional y global.
- **BT Assure Threat Defence**: servicio de protección en línea contra ataques APTs y *malware* dirigido.
- **BT Assure Assure Anti-DDoS**. Servicio de mitigación desde la red core de BT contra ataques de denegación de servicio distribuidos.
- **BT Assure Managed Firewall**. Gestión de seguridad, auditoría y cumplimiento de los cortafuegos de cliente.
- **BT Assure Managed Services**. Servicio de gestión de tecnologías de seguridad WAF, IPS, DLP y Endpoint.
- **BT Assure Web**. Servicio de protección en nube para la navegación de usuarios frente a *malware* y control de contenidos.
- **BT Assure Email**. Servicio de protección en nube del correo electrónico frente a spam, *malware*, control de contenidos y de imágenes.
- **BT Assure Forensics**: Servicios forenses para el análisis de incidentes y obtención de evidencias.
- **BT Assure Threat Intelligence**: servicio global de vigilancia electrónica de amenazas externas y fugas de información sensible.
- **BT Assure Ethical Hacking**: Servicios de auditorías técnicas de caja negra y blanca para sistemas y aplicaciones.
- **BT Assure Lab**. Laboratorio de seguridad para la investigación de *malware*, pruebas de nuevos sistemas de seguridad y realización de ingeniería inversa.

Jacinto Cavestany

Consejero Delegado de BT

– Como bien reza su lema "Security that matters", la seguridad importa. Pero, ¿hasta qué punto se ha convertido en un eje clave en la estrategia de BT?

– La seguridad es más que una mera cuestión técnica, también lo es humana. Por eso las organizaciones, para estar efectivamente seguras, necesitan combinar soluciones que pueden parecer sencillas como la colaboración, las alianzas y la capacidad, con la tecnología más compleja.

BT cuenta con una gran base de clientes en todo el mundo a los que presta soluciones de seguridad desde hace tiempo. Ahora, con el foco y soporte de nuestra organización de ventas, estamos llevando la práctica de la seguridad al siguiente nivel, que consiste en abordar un escenario en constante cambio en el que la seguridad sea una condición incorporada en cada una de nuestras ofertas.

– **Uno de los principales argumentos que esgrimen en su innovadora apuesta "Cloud of clouds" es la mejora que la nube proporciona en términos de seguridad. ¿Cómo se integran los servicios de ciberseguridad en esa visión global y holística que BT tiene de dicho ecosistema?**

– La estrategia de seguridad de BT en la nube se vertebra en tres ejes: la seguridad en el cloud, a través del cloud y desde el cloud. Este último es especialmente diferencial, siendo nuestra intención ayudar a los clientes a gestionar la complejidad de la nube posicionándonos a BT como un Cloud Security "Broker". Nuestra visión es la de ayudar a nuestros clientes a trasladarse a la nube con confianza y de manera satisfactoria y, al mismo tiempo, minimizando la complejidad, los riesgos y los costes.

Una red solo puede ser buena en la medida en que sea segura y una red compleja como la nube híbrida es más susceptible de recibir amenazas que la mayoría. La necesidad de disponer de conectividad segura a través de internet a los recursos en la nube se ha convertido en un aspecto crítico.

Partimos del convencimiento de que la seguridad no es una opción, sino que es un elemento necesario para el normal desempeño de cualquier solución empresarial. Entendemos que la seguridad es una parte transversal de la oferta global de BT y que por lo tanto es un elemento esencial en todas y cada una de las ofertas que la compañía realiza.

– **Como rasgo diferenciador, ustedes apuestan por un agnosticismo tecnológico. ¿Qué reflejo tiene esta estrategia en sus clientes y en sus partners?**

– La posición de BT en el mercado es única porque somos un proveedor *end-to-end* que ofrecemos soluciones de seguridad completas y a todos los niveles. Esto nos permite poder trabajar con múltiples *partners* y proveedores de servicio, y en la medida en que nuestra estrategia gira en torno a las arquitecturas en lugar de las tecnologías, podemos trabajar con cualquier tecnología que utilicen nuestros clientes.

Dicho esto, ser tecnológicamente agnóstico no significa que trabajemos con cualquier fabricante, significa que disponemos de varios *partners* para proveer la mejor alternativa técnica a los clientes, pero dentro de un grupo seleccionado por estar alineados con los valores y visión de BT.

– **En su orientación a los mercados españoles, ¿qué supone el SOC de Madrid en su apuesta por la prestación de servicios gestionados?**

– El de Madrid es uno de los 14 SOCs que BT tiene desplegados por todo el mundo. Evidentemente disponer de un SOC en Madrid supone un valor añadido para los clientes que operan en España, que son tanto empresas nacionales como multinacionales y organizaciones del sector público. Pero también éstos se benefician de formar parte de la red internacional, capaz de monitorizar amenazas en tiempo real y con independencia de donde aparezcan. El SOC de Madrid tiene, además, capacidad NOC que le permite la monitorización y gestión simultánea de las redes de los clientes, aumentando considerablemente la capacidad de detección y mitigación de las amenazas.

Por otra parte, los servicios del SOC no serán únicamente los de monitorización de ciberamenazas y explotación de plataformas tecnológicas, sino que en línea con nuestra visión integral de la seguridad, se gestionarán también servicios de seguridad en la nube y de análisis de seguridad para identificar en tiempo real los patrones de amenazas y actuar con rapidez y en cada caso.

Javier Perea

Vicepresidente de Ventas de Intel Security

– Intel Security propone una Nueva Generación de Arquitectura de Seguridad. ¿Qué problema viene a resolver este nuevo enfoque?

– La Nueva Generación de Arquitectura de Seguridad es la respuesta de Intel al actual reto de aprovechar las enormes ventajas que la digitalización y la conectividad aportan a las organizaciones, y hacerlo de una forma segura, simplificando la complejidad y reduciendo los costes que esto conlleva.

La trepidante evolución tecnológica de los últimos años ha generado a su vez nuevos y cambiantes escenarios tecnológicos con problemas de seguridad no conocidos, o no resueltos correctamente, que han venido siendo sistemáticamente aprovechados por organizaciones de cibercriminales en su propio beneficio.

Esto ha obligado a las organizaciones a reaccionar rápidamente ante las nuevas amenazas según iban surgiendo, aplicando los remedios que había disponibles en cada momento, tomando decisiones tácticas, -muchas veces de urgencia-, en la adopción de tecnología de seguridad, en un modelo acción-reacción que ha desembocado en un sistema de seguridad con multitud de contramedidas específicas, que es necesario mantener, que requieren una interoperabilidad manual y que no son capaces de proteger de los nuevos y sofisticados ataques dirigidos. En resumen, en la mayoría de los casos, el resultado ha sido un sistema de seguridad, –o mejor dicho de inseguridad–, insostenible por costoso, complejo e ineficiente.

– **Este es un reto conocido y al que se enfrentan muchas organizaciones, ¿Qué tiene realmente de novedad esta propuesta sobre lo que la industria ofrece hoy?**

– La Nueva Generación de Arquitectura de Seguridad se basa en la creación y adopción de un nuevo estándar, abierto, no propietario, que permita a los distintos controles de seguridad, ya sean de sistemas ya de redes, ubicados in situ o en la nube, comunicarse entre sí en todo momento siendo capaces de analizar comportamientos contextualizados, transformando los datos aportados por cada uno de los controles en información y esta información en inteligencia accionable, tomando decisiones de forma inmediata basadas en los indicadores de compromiso (IoC) establecidos previamente para una determinada organización.

Este nuevo enfoque consta, por una parte del nuevo canal de comunicación llamado Data Exchange Layer (DxL), que permite la interoperabilidad de los distintos silos tecnológicos en los que vienen trabajando las distintas contramedidas. Junto con DxL, Intel ha desarrollado Threat Information Exchange (TIE), que permite a la organización el uso de IoC utilizando la información aportada por cada uno de los controles de seguridad a través de DxL. Esto permite a cada contramedida impedir la ejecución de un objeto en base a su reputación, adicionalmente a la capacidad natural de cada una de las contramedidas.

En resumen, esta Nueva Generación de Arquitectura de Seguridad posibilita que las distintas contramedidas trabajen conjuntamente entre sí, eleva el nivel de protección de la organización y habilita la defensa combinada y coordinada frente a los nuevos y sofisticados ataques dirigidos, reduciendo a su vez los costes de operación de los sistemas de seguridad de las organizaciones.

– **¿En qué medida esta Nueva Generación de Arquitectura de Seguridad puede facilitar el gobierno de ciberprotección tanto a los MSSPs como a sus clientes?**

– La mayoría de las organizaciones se enfrenta a la necesidad de trasformar su sistema de seguridad para proteger sus activos de información en un entorno de hostilidad creciente, sin que la complejidad o el coste que esto conlleva se lo impidan. En esta trasformación, los MSSPs tienen un papel esencial, ya que proporcionan soluciones *end-to-end* en las que la integración de las distintas contramedidas de seguridad y la eficiencia en la operación son fundamentales para poder cumplir SLAs de alta calidad dentro de unos costes razonables.

Desde Intel Security llevamos muchos años colaborando con BT en la definición de arquitecturas que proporcionan el nivel de seguridad necesario a sus clientes, a la vez que permiten la evolución de las mismas de forma rápida y eficiente, dentro de un *partnership* tecnológico a largo plazo.

José Pereiro

Director de BT Security para España y Portugal

Como máximo responsable del área de ciberseguridad de BT en nuestro país, José Pereiro desvela la innovadora estrategia de la compañía en la prestación de servicios gestionados a partir de su red de 14 SOCs y cómo su firma apuesta por un modelo de negocio que requiere profesionales muy cualificados y una reglamentación del mercado.

"Los clientes necesitan que entendamos su negocio y en BT nuestros profesionales también están especializados en cada uno de ellos"

– ¿Qué estrategia está llevando a cabo BT en la comercialización de servicios gestionados de seguridad?

– La estrategia surge de la necesidad de proteger a nuestra propia compañía, dada nuestra naturaleza como empresa de servicios IT en red con presencia en más de 170 países y con más de 50 centros de datos.

El objetivo es proteger a nuestros clientes de una forma *end-to-end*, es decir, desde la consultoría inicial, pasando por la integración de las tecnologías, hasta la posterior gestión. Y que esta protección no incluya solo la seguridad, sino también servicios de computación, de *data center*, de *big data*, de comunicaciones…

Asimismo, nuestro modelo de trabajo es de servicio: incluimos en un contrato todo (hardware, software, personas, infraestructuras, comunicaciones…), sin que por ello se menoscabe la flexibilidad y el trato directo. De hecho, cuanto más complejo y más grande sea el proyecto, más posibilidades hay de que se aprecie nuestro valor.

– BT basa esta fortaleza en su red de 14 SOCs, ¿cuáles son los principales servicios que ofrecen?

– En primer lugar, hay que señalar que todos nuestros SOCs cuentan con equipos profesionales bilingües para responder a las necesidades domésticas y globales de nuestros clientes.

En cuanto a nuestro catálogo, ofrecemos servicios destacados como el Assure Threat Intelligence, con el que damos ciberinteligencia global en varias modalidades (desde la genérica, hasta la personalizada por sector o incluso por cliente), o el Assure Threat Monitoring, para la detección de amenazas en tiempo real.

Por supuesto, también proporcionamos servicios de gestión de cualquier tipo de tecnología de seguridad (desde *firewall*, hasta otros más avanzados), además de servicios adicionales que damos desde nuestra propia red *core*, como la protección frente a ataques de denegación de servicio. Precisamente este servicio que prestamos desde nuestro SOC es una buena muestra de una de las líneas estratégicas de la compañía: "The cloud of clouds". Se trata de una iniciativa que tiene el objetivo de convertir a BT en un *hub* de servicios en la nube, de forma que los clientes puedan acceder a través de nuestra red a servicios con independencia de que sean suyos, de un tercero o de BT.

Hay que señalar que en la parte de seguridad, podemos dar los servicios en casa del cliente, de un modo gestionado o en *cloud*.

– ¿Qué ventajas ofrece la modalidad *cloud*?

– Hay servicios que se hacen mejor desde la nube, como el de ciberinteligencia o el anti-DDoS, incluso la navegación o el correo seguros. En BT ofrecemos ya algunos como Assure Web, Assure Email o Assure Threat Monitoring. Las ventajas del *cloud* son muchas, especialmente económicas, pero también supone una buena oportunidad para el CISO, que normalmente está supeditado al departamento de IT, y que con la

"Nuestro objetivo es proteger a los clientes de una forma end-to-end, es decir, desde la consultoría inicial, pasando por la integración de las tecnologías, hasta la posterior gestión".

nube tendría una mayor independencia y, de esa forma, podría enfocarse en definir políticas y supervisar.

– ¿Qué servicios de BT se pueden considerar únicos en este mercado donde cada vez hay más jugadores?

– En primer lugar, Saturn, que ha sido desarrollado por BT Research, es una herramienta de análisis visual para la información del *big data*. Gracias a él, un analista de seguridad puede trabajar en tiempo real sobre un incidente, dado que traduce una ingente cantidad de datos de una forma muy visual (gráficos, geolocalización…).

En segundo lugar, Assure Cyber es un entorno muy complejo donde el objetivo ha sido crear un ecosistema de seguridad completo. Este gran sistema se basa en la integración de todas las fuentes de datos, hasta obtener el tráfico de red por completo, observarlo en tiempo real y detectar anomalías. Toda la información va a un lago de datos en el que ponemos una serie de módulos para detectar ataques, disponer de consolas para los analistas de seguridad y tener cuadros de mando ejecutivos en tiempo real. Los proyectos con Assure Cyber son muy grandes y ya lo hemos implementado en varias multinacionales. Es la visión final de la seguridad.

– Hablando de clientes, ¿a qué tipo se dirigen los servicios de BT? ¿Existe una tendencia a la sectorización?

En BT estamos enfocados en la mediana y gran empresa con la excepción de Reino Unido donde también cubrimos el mercado residencial y la pequeña empresa. Tenemos clientes de todos los sectores (bancario, militar, de distribución…) y cada uno tiene una serie de requerimientos. Por ello, la sectorización forma parte de la estrategia. Los clientes necesitan que entendamos su negocio. Las tecnologías no son las mismas para un entorno industrial SCADA que para la banca. Por ello, nuestros profesionales también están especializados en cada uno de ellos y requerimos certificaciones específicas. La mayor parte de los servicios ya los tenemos sectorizados y estamos enviando a 40 empresas españolas un informe concreto de su sector, aportando, eso sí, la visión global de BT.

– Ustedes apuestan por un agnosticismo tecnológico. ¿Cuál es su política de *partners*?

Somos agnósticos pero no promiscuos. Somos agnósticos en el sentido de que queremos dar la mejor solución a nuestros clientes, pero no vamos a trabajar con cualquiera. Elegimos a *partners* que sigan los mismos principios de BT respecto a la seguridad, que tengan presencia global y que sean capaces de proveernos tecnología, pero también servicios, modalidades de MSSPs… Por descontado, la confianza es fundamental. Apostamos por relaciones a largo plazo y acuerdos estratégicos y globales.

Un buen ejemplo es McAfee –ahora Intel Security–, que se ha convertido en uno de nuestros principales *partners*. Teníamos una gran relación con ellos que se reforzó aún más con la adquisición por parte de Intel. Destacan por ser globales y permitirnos suministrar a los clientes un sistema *end-to-end*. Y es que el catálogo de Intel Security es muy completo para atender cualquier necesidad en *firewalling*, DLP, IPS… aunque si algo les diferencia es su consola única capaz de integrar todos sus elementos. Además, están realizando grandes innovaciones en ciberinteligencia y han creado un gran bus de datos al que se pueden suscribir las tecnologías para compartir información como si fuera una red social. El acuerdo que BT tiene con McAfee es a nivel mundial en servicios gestionados, pero hay que mencionar que el equipo de España es particularmente excelente.

– Uno de los principales problemas a los que se enfrentan los proveedores de servicios es la rotación en sus plantillas, ¿cómo afrontan esta realidad?

Las personas son un componente crítico para BT. Contamos con un equipo joven –que no junior– que tiene objetivos de certificación, de desarrollo profesional, etc. Nuestros índices de rotación son bastante bajos. Esto se consigue aportando seguridad laboral a los empleados, con programas de formación muy estrictos o con la posibilidad de colaborar en foros internacionales.

El equipo de BT, eso sí, está compuesto por profesionales entrenados para la seguridad. No reutilizamos profesionales del mundo de las IT o de las comunicaciones, pues entendemos que es una forma de pensar absolutamente diferente.

– En la actualidad se está planteando la regulación de los proveedores de servicios gestionados de ciberseguridad privada, ¿la considera necesaria?

Es fundamental que haya una regulación que marque una línea base que tengan que cumplir todos. Creo que hay mucho intrusismo en el sector. Es novedoso y llamativo y quieren entrar empresas que no son de seguridad. Esta regulación debe establecer unos mínimos en seguridad física, seguridad del personal, capacidades de seguridad, acreditaciones y ciberinteligencia. Es necesario que se profesionalice, que se demuestre con acreditaciones y que además se establezca una colaboración con la administración pública, compartiendo inteligencia en los dos sentidos. Creo que es necesario para que el intrusismo ni desacredite ni precarice el sector de la ciberseguridad. ●

Carlos Muñoz

Director Técnico de Intel Security España

– ¿Qué productos y soluciones ponen a disposición de proveedores de servicios gestionados? ¿Cuáles son las tecnologías más demandadas?

– En Intel Security contamos con múltiples soluciones de seguridad que están orientadas a MSSPs, tanto en el ámbito del licenciamiento como en el de la administración de entornos *multitenant*.

Las soluciones de Intel Security están diseñadas para ser implementadas en entornos distribuidos, como ejemplo pudiera ser la posibilidad de implementar múltiples dispositivos ATD, múltiples consolas EPO o *brokers* TIE que sean capaces de reportar eventos de seguridad a un entorno SIEM centralizado con posibilidades de gestión multicliente.

– La imparable demanda de servicios avanzados y/o a medida augura un potente recorrido a los proveedores de herramientas y soluciones para detección de amenazas sofisticadas, ciberinteligencia… ¿Qué singulariza la oferta de Intel Security frente a otras opciones?

– A esta pregunta le podríamos dar respuesta con tres términos: rendimiento, 'customización' de máquinas e integración con el puesto. Unas de las principales ventajas en el ámbito del *malware* avanzado o Zero Day es que nuestras soluciones de End Point permiten integrarse de forma nativa con nuestras soluciones de análisis de *malware* avanzado basado en métodos de detección, tipo Sandbox, como es el caso de nuestra solución de ATD, y gracias a la estrategia de Security Connected los IoC que genera dicha solución ATD (*Advance Threat Defense*) pueden ser consumidos por contramedidas de red de Intel Security e incluso por contramedidas de terceros. Hay que resaltar la escalabilidad de la que hace gala la solución de Sandboxing de Intel Security, dado que podemos movernos en entornos de decenas de miles de puestos y múltiples contramedidas de seguridad de red sin afectar a la saturación de la red, latencias y permitiendo de forma inmediata reaccionar ante a una amenaza.

– ¿Cómo se garantiza dicha escalabilidad?

– Esta escalabilidad la garantiza la implementación de un protocolo estándar denominado DXL (*Data Exchange Layer*) cuyo objeto es aportar un *framework* de comunicaciones entre elementos de Intel Security, como permitir a su vez la integración de otras soluciones de seguridad de otros fabricantes, cuyo objeto es usar este protocolo como un estándar abierto de seguridad. Gracias a la integración de nuestra solución SIEM dentro del protocolo DXL, es posible utilizar IoC (Indicadores de Compromiso) generados por la solución Sandboxing de Intel (ATD), como información de base para realizar investigación o análisis forense e identificar no solo los dispositivos afectados sino cuál es el paciente zero desde el que se produjo la propagación del *malware* avanzado.

Otra de las diferenciaciones de nuestra solución ATD de Sandboxing es que la ejecución del *malware* se realiza desde máquinas COE de la organización, permitiendo un análisis más preciso del impacto de dicho *malware* en la infraestructura de la compañía. Nuestra propuesta de ATD es, además, una de las soluciones con mayor rendimiento de análisis del mercado gracias a que dispone de mecanismos de análisis poco pesados a nivel de proceso previos al análisis *sandbox* puro.

– La IoT sigue creciendo. ¿Qué tipo de tecnología para operación y gestión de seguridad va a ir requiriendo y cómo observa Intel Security su estandarización?

– La seguridad es esencial para la expansión y consolidación del IoT –este fue uno de los principales motivos por los que Intel adquirió McAfee–, y en el que desde Intel seguimos trabajando muy activamente estableciendo y promoviendo estándares que favorezcan la conexión y la gestión inteligente del flujo de información entre dispositivos, sin importar su forma, sistema operativo o el proveedor de servicios. En este aspecto, entre otras iniciativas, Intel ha creado junto con Siemens, Honeywell, Samsumg e IBM, entre otros, el *Open Interconnect Consortium (OIC)* para el *Internet of Things,* lo que creemos que es un paso en la dirección adecuada; pero nos esperan muchos más.

Intel Security:

Como una de las principales compañías del mundo dedicada a la tecnología de la seguridad, **Intel Security** (**McAfee**) cuenta con soluciones de última generación para todo tipo de clientes. Uno de estos colectivos en el formado por los proveedores de servicios gestionados de ciberseguridad, para los que cuenta con una completa oferta. La innovación que impregna a sus productos ha llevado a BT a suscribir un acuerdo a nivel global para trabajar con la tecnología de este fabricante como parte de los servicios que proporciona a sus clientes en todo el mundo.

Un buen ejemplo de esta innovación que Intel Security proporciona a la operadora de origen británico se puede observar en tres productos con los que BT busca marcar diferencias: **McAfee Advanced Threat Defense**, **McAfee Threat Intelligence Exchange** y **McAfee Enterprise Security Manager**.

Freno a las amenazas avanzadas

McAfee Advanced Threat Defense tiene como principal misión ayudar a las organizaciones a detectar los ataques selectivos avanzados, ya sea en forma de *malware* sigiloso o de amenazas de tipo *zero-day*. La solución combina firmas antivirus que no requieren intervención, datos de reputación y emulación en tiempo real con análisis de código estático en profundidad y análisis dinámicos en entornos aislados.

Esta modalidad de análisis (*sandboxing*) se caracteriza por realizar evaluaciones más detalladas y por ofrecer información sobre la clasificación del *malware*. Además, McAfee Advanced Threat Defense emplea un potente sistema de descompresión para romper la protección a través de técnicas de evasión, lo que permite un análisis y una clasificación más precisos.

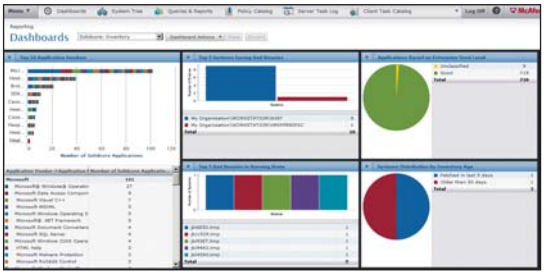
A esto hay que añadir que su despliegue centralizado hace posible que varios dispositivos de red de McAfee compartan el mismo dispositivo de análisis de *malware*, lo que reduce la cantidad necesaria de equipos de protección frente a las amenazas avanzadas, simplificando de este modo la administración, al tiempo que se amplía la seguridad de la red de forma rentable.

Inteligencia como valor

Por su parte, McAfee Threat Intelligence Exchange suministra en tiempo real información acerca de amenazas, de reputación

tecnología para marcar la diferencia en la prestación de servicios

y de vulnerabilidades, de cara a proporcionar una protección resiliente e inmunidad ante las infecciones. Esta prevención se caracteriza por ser adaptable gracias a que comparte los datos de seguridad relevantes entre *endpoints*, *gateways* y otros productos de seguridad. Y es que el hecho de compartir estos datos facilita el intercambio de información colectiva y la posibilidad de reaccionar ante ella como una unidad



En su objetivo de optimizar dicha prevención de amenazas y reducir el tiempo que transcurre entre la detección y la contención, McAfee Threat Intelligence Exchange permite a los administradores personalizar la información integral sobre amenazas procedente de varias fuentes de datos y utiliza la capa de intercambio de datos de McAfee, un tejido de comunicación bidireccional que proporciona información de seguridad y una seguridad adaptable gracias a la simple integración de los productos.

Otra característica destacada de McAfee Threat Intelligence Exchange pasa por la protección de los *endpoints* utilizando McAfee VirusScan.

Respuesta en tiempo real

Finalmente, como base de la familia de soluciones de administración de información y eventos de seguridad (SIEM) de la compañía, McAfee Enterprise Security Manager ofrece información útil y conocimiento de la situación en tiempo real con la rapidez y el alcance que necesitan las organizaciones de seguridad para identificar, comprender y responder a las amenazas ocultas.

Para lograrlo, conecta la información sobre amenazas –en constante cambio– con una visión de los riesgos, la importancia de los activos y el estado de la seguridad en toda la empresa. Este contexto dinámico se combina con el motor de correlación inteligente, puntúa los riesgos y prioriza las amenazas. Además, se integra con McAfee Global Threat Intelligence (GTI) y McAfee ePolicy Orchestrator (McAfee ePO) para ayudar a detectar, correlacionar y corregir dichas amenazas en toda la infraestructura de IT.

Asimismo, dado que los requisitos de las diferentes normativas evolucionan, McAfee Enterprise Security Manager facilita la gestión de su cumplimiento con paneles preconfigurados, pistas de auditoría completas e informes para la DSS del PCI, HIPAA, NERC-CIP, FISMA, GLBA, SOX, etc. ●

BT Assure Analytics - BT Saturn, inteligencia analítica en tiempo real

BT Assure Analytics, también llamado **Saturn**, es una de las soluciones más innovadoras empleadas en los centros de operaciones de seguridad. Es un servicio desarrollado por expertos de BT en sus laboratorios de investigación en Adastral Park. Proporciona una interfaz visual inteligente y en tiempo real para el análisis de datos, filtrado y clasificación de la información, de cara a que los analistas de seguridad de BT puedan estudiar todo tipo de amenazas y ataques en el mismo momento en el que estos se producen. Se muestran los aspectos geográficos, temporales, cuantitativos y cualitativos de los datos, y los eventos pueden ser agrupados y modelizados para obtener patrones más sutiles de actividad utilizando para ello técnicas de Inteligencia Artificial. Es válido para analizar cualquier tipo de evento o anomalía, no sólo de Ciberseguridad, sino también de Seguridad Física.

BT Security.

La seguridad consiste en estar un paso por delante.

Luchar contra el cibercrimen es una batalla constante, las tecnologías IT y sus desafíos evolucionan continuamente. El riesgo no se puede eliminar completamente, pero con BT podrá gestionarlo con antelación y evitar ataques. BT, siempre preparados y en alerta para proteger su negocio.

INVITACIÓN

Si desea ver nuestras capacidades operativas en tiempo real, le invitamos a visitar nuestro CyberSecurity Operations Center de Madrid. Póngase en contacto con su responsable comercial de BT, o solicite su visita a través del siguiente enlace: www.bt.es/visite-nuestro-cysoc

BT