DOCUMENTOS SiC
Nº 27
JUNIO 2019

Soluciones avanzadas de ciberseguridad para grandes empresas

CYTOMIC

- Cytomic, la nueva unidad de negocio de Panda para corporaciones
- Tecnologías y servicios: Validación, EDR, Threat Hunting y Soporte Técnico
- Orion, la solución contra el cibercrimen

María Campos
Vicepresidenta de
CYTOMIC Business Unit

Cytomic, exclusividad y valor añadido para grandes corporaciones

Cytomic es la Unidad de negocio de Panda Security que se orienta a la cobertura de las necesidades y demandas específicas del segmento Enterprise. Está avalada por la evolución de la estrategia de una compañía con cerca de tres décadas de historia, en la que las empresas representan más del 80% de su facturación gracias al trabajo llevado a cabo, especialmente, durante los últimos cinco años. Puede presumir, por tanto, de contar con la tecnología, la experiencia y los profesionales adecuados para aportar un valor diferencial en este segmento estratégico del mercado.

Cytomic es, al mismo tiempo, el origen y la culminación de una trayectoria y una gran apuesta empresarial por la especialización en soluciones y servicios de ciberseguridad para las grandes empresas.

El carácter especial que adquiere una gran compañía por su dimensión, por su complejidad estructural y por la sensibilidad de los activos que posee y gestiona, demanda unas necesidades específicas de protección en el mundo digital, donde los ciberataques son cada vez más sofisticados. En los últimos años, por ejemplo, las infecciones por *malware* se han reducido, dando paso a ciberataques en los que los delincuentes no se valen de un software malicioso para conseguir su objetivo, sino que aprovechan herramientas que forman parte de la gestión diaria de los responsables de TI –como aplicaciones o software legítimo– como armas de doble filo para conseguir sus objetivos. Los ataques conocidos como *malwareless*, de hecho, suponen actualmente un coste medio global de 3,8 millones de dólares, poniendo de relieve la necesidad de ofrecer una respuesta sólida a este tipo de ataques.

A tal fin, las grandes organizaciones demandan la capacidad de descubrir amenazas en su propio entorno con búsquedas más especializadas y que requieren otro conjunto de técnicas de analítica de datos y de investigación, acordes con su nivel de madurez en la gestión de la ciberseguridad. Ante este reto, Cytomic nace ligada a las necesidades y demandas particulares del mercado, y está avalada por la evolución de la estrategia de negocio de Panda Security, en la que las empresas representan más del 80% de su facturación gracias al trabajo llevado a cabo, especialmente, durante los últimos cinco años.

La nueva Unidad de negocio es la culminación de una trayectoria focalizada en las grandes cuentas privadas y públicas; pero, también, es el origen de un nuevo rumbo estratégico cuyo negocio cuenta con la tecnología, la experiencia y los profesionales adecuados para aportar calidad y eficiencia en este segmento del mercado.

Valor diferencial

Uno de las grandes bazas por la que Cytomic reclama un lugar destacado en el mercado es su aproximación basada en el binomio tecnología-servicio. Tanto en España como a escala internacional, las organizaciones necesitan adoptar un enfoque proactivo y avanzado, con soluciones crecientemente personalizadas y adaptadas a sus necesidades en la protección de activos. Cytomic, aunque nace en el seno de un fabricante, no se queda solo en el producto, sino que va más

Sede de Cytomic en Madrid.

EL MODELO 'CIBERATÓMICO' DE CYTOMIC

El nombre de Cytomic representa el concepto de modelo "ciberatómico", que refleja su forma de entender la ciberseguridad. Este modelo, más allá de quedarse en el átomo como punto de partida, iría un paso más y se centraría en analizar cómo se unen entre ellos para poder crear un orden superior, ya que sólo a través de estas complejas relaciones se puede entender el proceso de formación de la materia.

Así es como Cytomic trata de abordar la ciberseguridad ya que, en lugar de centrar sus esfuerzos en detener el *malware*, centra sus enfuerzos en intentar descifrar las relaciones entre los diferentes eventos que componen un proceso de ataque, en investigar los comportamientos que tienen en común, en unir eventos aparentemente aislados, y en desgranar y definir todos los enlaces que se dan entre máquinas, personas, programas y comportamientos y que desencadenan un evento de ciberseguridad cierto.

allá ofreciendo servicios adicionales de ciberseguridad marcados por una fuerte especialización.
La oferta de la Unidad integra soluciones Endpoint Protection Platform (EPP) y Endpoint Detection and Response (EDR); pero, sin duda, una de las claves de la potencia de su *offering* se manifiesta en los servicios avanzados para grandes compañías, facilitando la personalización de la oferta según las necesidades. Esos servicios encuentran sus principales pilares, por un lado, en el Threat Hunting, con un equipo de expertos en ciberseguridad dedicado y, por otro, en una plataforma propia especialmente diseñada para cubrir las demandas de la gran empresa, que se ha denominado Orion, "el cazador".
Los servicios de clasificación temprana de aplicaciones es otro de los pilares sobre los que se sustenta la oferta de Cytomic, con los que sus clientes pueden reducir drásticamente su superficie de ataque. Junto a ellos, completan el portafolio los servicios de validación de amenazas, investigación y los nuevos niveles de soporte técnico adecuados a los requerimientos del segmento Enterprise.
Cabe destacar, además, que la plataforma de Cytomic está preparada para su despliegue en nube (híbridas, privadas) y *on-premise*. En este sentido, es interesante incidir en su origen europeo, dispone de certificaciones específicas adaptadas a las necesidades de cumplimiento y asegura a los clientes que el dato reside en Europa.

Un equipo altamente cualificado

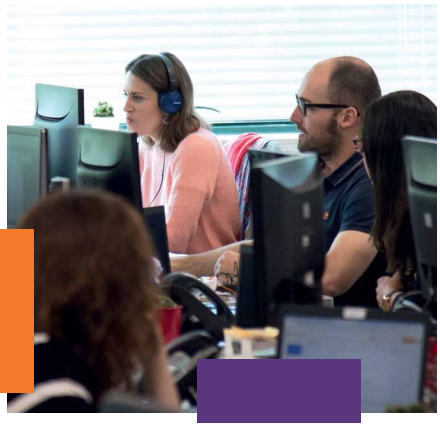
Para sustentar el abanico de servicios, Cytomic cuenta con un equipo de más de 20 personas pertenecientes exclusivamente a la Unidad de gran cuenta. A este equipo se suman los 200 expertos en I+D compartidos con Panda Security, además de asimilar los recursos necesarios del laboratorio para poder atender a las exigentes demandas del mercado.

La Unidad para grandes empresas tendrá capilaridad en los países en los que ya está presente la compañía matriz, con 16 subsidiarias en distintos mercados como Estados Unidos, Latinoamérica y Europa, además de contar con más de 180 puntos de servicios y distribución repartidos por todo el mundo.

A medio plazo, se espera reforzar la plantilla con nuevas contrataciones, incorporando nuevas áreas para atender de forma más rápida y personalizada a este segmento –especialmente en el plano de la consultoría técnica– con equipos dedicados a los servicios de Threat Hunting e investigación de amenazas.

MSSPs y grandes integradores

Cytomic también estará rodeado de Partners especializados al objeto de atender los requerimientos de sus clientes de una manera más personalizada y especializada. Cuenta ya con un canal de 20 socios con grandes capacidades de SOC, servicios CSIRT y de respuesta a incidentes, entre los que se encuentran compañías muy importantes en el mercado tecnológico.
Al mismo tiempo, teniendo en cuenta la falta de recursos especializados en el mercado, la propuesta de Cytomic resulta particularmente atractiva para aquellos proveedores MSSPs y MDRs que quieran ampliar su oferta de servicios de detección y respuesta temprana a incidentes de ciberseguridad de los puntos finales.



Cytomic ofrece en este frente servicios de base muy cualificados para que el socio pueda construir más valor por encima de ellos. Permite, por ejemplo, expandir el portafolio hacia un servicio de tipo Managed Detection and Response (MDR), que gestione la seguridad en el *endpoint*. Algo que ha sido difícil hasta ahora, ya que los proveedores no contaban con herramientas accesibles, escalables, completas y suficientemente automatizadas. También, aquellos socios que quieran contar con recursos de Threat Hunting para ofrecerlo a un tercero, pueden hacerlo a través del servicio que Cytomic proporciona con la plataforma Orion.

Alcance internacional

El lanzamiento de Cytomic no viene solo acompañado de la capacidad tecnológica y la experiencia acumulada durante los casi 30 años de vida de la compañía matriz. A ello, se suman las certificaciones y la cobertura geográfica necesarias para abordar proyectos internacionales de gran envergadura. Y es que, como nueva Unidad de negocio, Cytomic es también global y tiene capilaridad en los países en los que ya se registra la presencia de Panda Security, con 16 subsidiarias en distintos mercados como Estados Unidos, Latinoamérica y Europa, además de contar con más de 180 puntos de servicios y distribución repartidos por todo el mundo. ●

María Campos

Vicepresidenta de Cytomic Business Unit

Durante los últimos años, Panda Security ha ido conformando un catálogo especializado de servicios y soluciones de ciberseguridad para grandes empresas que le ha llevado a asumir un nuevo reto estratégico. Su apuesta se ha traducido en la creación de una Unidad de negocio con nombre propio, Cytomic, cuya dirección corre a cargo de María Campos, quien se unió a la compañía para liderar el segmento de grandes cuentas a nivel global.

"Cytomic pone en el mercado productos especializados orientados al servicio y exclusivamente dirigidos a la gran empresa"

– ¿Por qué Panda Security ha decidido crear Cytomic como Unidad independiente?

– A día de hoy, el 82% de nuestras ventas proviene de B2B y el 18% de B2C.Y durante los últimos cinco años, Panda Security ha modificado su estrategia ofreciendo tecnología avanzada para grandes empresas. De hecho, fue pionera en el movimiento a la nube y del modelo SaaS en ciberseguridad. Obviamente, las claves del mercado corporativo no se corresponden con las de los segmentos pyme y residencial, y esta es la razón por la que hemos creado la Unidad independiente, Cytomic, que nos permite especializar en las grandes empresas nuestra experiencia en ciberseguridad.

– ¿Cómo va a operar Cytomic en la estructura de Panda Security?

– Como Unidad independiente, cuenta con equipos independientes en consultoría, comercial, preventa, producto y marketing. Pero también asimila recursos de Panda Security para aprovechar la experiencia y dilatada historia de I+D de la compañía y aportar los servicios avanzados, proactivos y personalizables que demandan las organizaciones que tienen ya un alto grado de madurez en gestión de la ciberseguridad.

– ¿Cuál es el alcance de los servicios y soluciones que ofrecerá Cytomic?

– Quiero dejar claro que no se reparte el portafolio de Panda Security, sino que, en la nueva Unidad, todo se especializa. Los servicios que van a marcar la diferencia se enmarcan fundamentalmente en Threat Hunting, Clasificación y Soporte. Por ejemplo, si una gran empresa necesita una oferta de Threat Hunting avanzada, con acceso a una plataforma propia y que pueda disponer de especialistas a través de proveedores específicos de MDR o de *Partners* con servicios especializados, Cytomic se la proporcionará. Lo mismo ocurre con nuestros servicios

de clasificación temprana de aplicaciones y de soporte, donde brindamos tiempos de respuesta y SLAs a medida. Asimismo, los clientes de la nueva Unidad podrán contar con una instancia diferenciada en Azure.

– ¿Cuál es el mensaje diferenciador que trasladará desde Cytomic para reclamar su hueco en el mercado de la seguridad TIC frente a otros actores?

– La diferencia es que por diseño ofrecemos diferentes capas de servicio asociadas al producto. Por otra parte, al ser nuestra compañía de origen europeo, garantizamos a nuestros clientes que el dato reside en Europa.

– ¿Qué estructura tiene el equipo humano de Cytomic?

– Por un lado, contamos con los recursos y la dilatada experiencia del equipo de I+D de Panda Security, donde una parte muy importante de las más de 200 personas que lo componen están enfocadas en el desarrollo del *offering* para la nueva Unidad. Además, en el último año hemos llevado a cabo un proceso de contratación de un equipo especializado de 20 personas para esta área.

– ¿Qué papel juega PandaLabs dentro de la nueva división?

– Dentro del laboratorio de Panda Security es crucial el trabajo que realizan los analistas con los que llevamos a cabo todos los procesos de investigación avanzada y, especialmente, los servicios de Threat Hunting. Esto permitirá a los clientes de Cytomic, por ejemplo, contar con un equipo de *hunters* dedicado a través de un *partner* y recibir un servicio propio suscribiéndose a la nueva plataforma Orion. Esta solución permite estandarizar los procesos de investigación, con lo que también ayuda a las empresas a profesionalizar sus propios equipos de *hunting,* en caso de que los tenga. Una vez más, Cytomic aprovecha la experiencia y el desarrollo tecnológico de Panda Security con los servicios de laboratorio más avanzados.

"Vamos a comercializar nuestros productos a través de alianzas con MSSPs y con firmas que dispongan de servicios avanzados de Threat Hunting, capacidades de SOC y CSIRT y de respuesta a incidentes"

– ¿Cómo van a comercializar sus productos?

– No tenemos una estrategia de apertura masiva de *Partners.* Eso sí, apostamos decididamente por firmar alianzas con MSSPs y con empresas que ofrezcan servicios avanzados de *Threat Hunting*, respuesta a incidentes, capacidades de SOC y servicios CSIRT. Por ahora trabajamos con unas 20 compañías y nuestra idea es que ellas proporcionen la capa de servicio adicional a lo que es el primer nivel que ofrece Cytomic.

– ¿Con qué tipo de clientes cuenta ya Cytomic?

– Ya hay empresas que están utilizando la plataforma avanzada de Threat Hunting, como Telefónica y Eulen, e iremos migrando los clientes que ya tenemos en gran cuenta a la nueva Unidad de negocio. También tenemos clientes como Renfe, la Comunidad de Madrid, CaixaBank, Orange, Gobierno de Navarra, Deloitte y distintos ministerios. El CCN, además, ha apostado por crear una nube híbrida dedicada a Administración Pública con Cytomic con lo que tenemos una alianza muy fuerte para que los clientes del sector público tengan servicios en una instancia diferentes del resto. A ello, se le une la certificación del cumplimiento con el Esquema Nacional de Seguridad (ENS), que también nos ayuda a generar confianza, una característica que en ciberseguridad es muy importante.

– ¿Qué objetivos se han marcado para Cytomic?

– A día de hoy, dentro de las ventas para el mercado corporativo, el segmento de la gran empresa representa en torno al 15% y, en dos años, esperamos que la facturación de Cytomic alcance un 40%. Además, como parte de nuestra apuesta por los servicios de *Threat Hunting* dentro del mercado EDR, nuestra intención es estar entre los tres primeros fabricantes a nivel mundial. Son objetivos ambiciosos pero se trata de la gran apuesta de Cytomic.

– No es pequeño el reto de dirigir y coordinar Cytomic a nivel mundial…

– Me uní hace casi un año a Panda Security para desarrollarla en el segmento de gran empresa. Durante estos meses, además de crear un equipo propio, hemos desarrollado un *offering* adecuado. Y el lanzamiento de Cytomic, aparte de a España, afecta a nuestros mercados prioritarios en Latinoamérica y Europa –como Reino Unido e Italia–, además del de EE.UU. Es un privilegio poder aportar mi experiencia y esfuerzo. ●

Soluciones y servicios especializados de Clasificación, EDR, Threat Hunting y Soporte Técnico

Cytomic, como una Unidad de negocio especializada en grandes cuentas, proporciona un amplio abanico de servicios de última generación y a medida de un mercado cuyo nivel de madurez en ciberseguridad es más alto y exigente.Y lo hace con un ADN propio para abordar la protección de las grandes empresas de manera más personalizada y proactiva ante las amenazas más críticas que ponen en riesgo sus activos, como son los ataques dirigidos.

En este sentido, la filosofía de Cytomic se basa en el hecho fundamental de que la ciberseguridad no es solo un producto, además es un proceso donde la anticipación y la producción de inteligencia son claves para hacer frente a las ciberamenazas avanzadas. Sus soluciones, por tanto, integran múltiples capas de tecnologías y servicios de protección basados en técnicas de detección, respuesta y remediación, búsqueda proactiva de amenazas, análisis de comportamiento, investigación y un enfoque de clasificación tempana.

Los servicios que marcan la diferencia en la propuesta de Cytomic son:

• **Cytomic EDR (Endpoint Detection and Response).** El objetivo principal de los atacantes siguen siendo los puestos de trabajo, donde encuentran la información más sensible y pueden abusar de credenciales, lo que les permite ir pivotando internamente de un sistema a otro. Para evitarlo, las capacidades EDR de Cytomic van más allá de las medidas EPP (Endpoint Protection Platform) que los clientes ya tienen activas, enfocándose en analizar, entender y visualizar el flujo de información que se produce tanto dentro de una organización como hacia fuera, y viceversa. Cytomic registra, correlaciona y clasifica el comportamiento de los *endpoints*, las aplicaciones y los usuarios para detectar actividades sospechosas, bloquear comportamientos anómalos y actividades maliciosas, y proporciona soluciones orientadas a la restauración de los sistemas afectados.

• **Threat Hunting.** Los clientes de Cytomic pueden contar también con un equipo de *hunters* dedicado, a través de la suscripción a la plataforma Orion, que permite estandarizar los procesos de investigación y ofrece al cliente un servicio propio sobre sus datos, ayudando a las empresas a profesionalizar sus equipos. Las tecnologías de EDR de Cytomic brindan la telemetría necesaria para que los analistas puedan llevar a cabo los procesos de búsqueda proactiva a través de las redes para detectar y aislar amenazas avanzadas capaces de evadir las soluciones de seguridad existentes. Las empresas pueden contar con este servicio tanto a nivel interno como a través de un Partner.

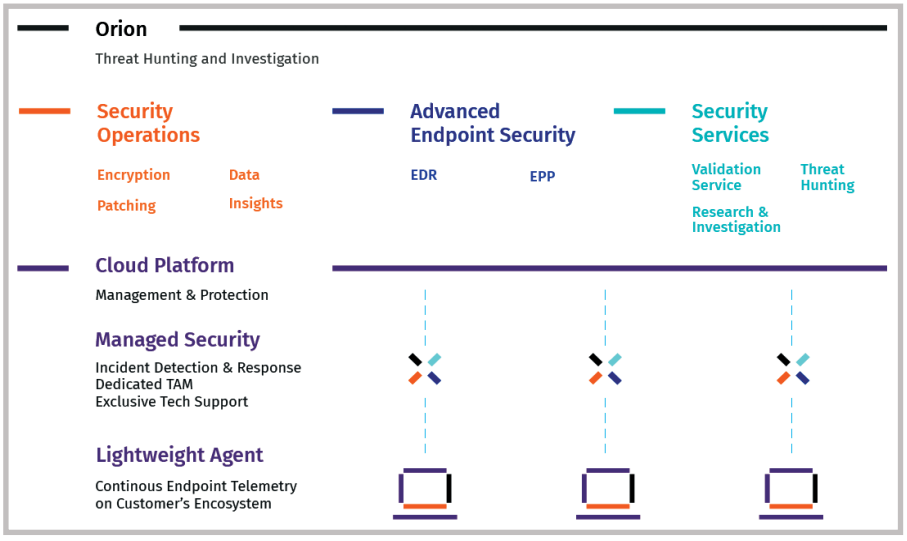
• **Clasificación temprana de aplicaciones.** La clasificación de todas las aplicaciones mediante el servicio de validación permite reducir drásticamente la superficie de ataque. Una clasificación temprana da la posibilidad, además, de reducir al máximo el tiempo de resolución o clasificación de aquellos ficheros desconocidos que hayan podido ser bloqueados, con lo que el impacto en la usabilidad o conveniencia para el usuario es mínimo.

Muy pocas empresas ofrecen algo similar. Existen soluciones que tienen funcionalidades de reputación de ficheros pero, al final, hay casos en los que no pueden determinarlo y dejan en manos del usuario la responsabilidad de determinar y confirmar un ataque de *malware*, ya que siguen indicando que algo es sospechoso. En el caso de Cytomic, todos los ataques de *malware* se confirman y no se deja esa responsabilidad en manos del usuario.

En lo referente al soporte, los clientes de Cytomic pueden contratar compromisos de nivel de respuesta (SLAs) adecuados a la calidad del servicio que requiere el cliente, identificando y definiendo sus necesidades, a la vez que controla las expectativas de dicho servicio.

Seguridad en la nube

En el entorno *cloud*, la plataforma de Cytomic está preparada para ser desplegada tanto en la nube pública, donde esta Unidad tiene toda la inteligencia colectiva, como en las propias instalaciones del cliente.



La filosofía de Cytomic se basa en un hecho fundamental: que la ciberseguridad no es solo un producto, además es un proceso. Sus soluciones, por tanto, integran múltiples capas de tecnologías y servicios avanzados de protección.

Cytomic también posee una nube híbrida dedicada a Administración Pública y certificada por el Centro Criptológico Nacional (CCN). De esta forma, las instituciones del sector público pueden disponer de servicios diferenciados del resto de clientes.

Asimismo, como valor diferencial, los clientes de Cytomic contarán con una instancia diferenciada en Microsoft Azure. Esta posibilidad refuerza la confianza en que sus datos no estarán compartidos con los de otros clientes de Azure. Esta segmentación, mediante una instancia separada, supone mejorar la valoración de riesgo para el cliente al trabajar con Cytomic. ●

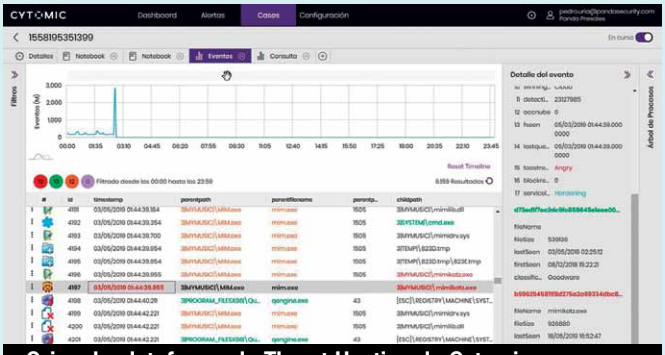
Orion, la solución de Cytomic para luchar contra el cibercrimen especializado en la gran empresa

PandaLabs es el centro neurálgico de la compañía, y el área en la que se coordinan las actividades de investigación de amenazas y de desarrollo de técnicas de ciberdefensa. Una labor que se desempeña gracias a la experiencia, dedicación y habilidad de un equipo de expertos en distintas áreas de la seguridad digital: técnicos en *malware* y en detección de ataques sin código malicioso, analistas, especialistas en seguridad perimetral, en forensía y en tratamiento de datos e IA.

Con motivo de la creación de la unidad Cytomic, en PandaLabs se ha ido creando una línea de especialización de diseño de soluciones orientada exclusivamente a los mercados corporativos.

Entre los servicios más importantes que se proporcionan a las grandes empresas se encuentra el de Threat Hunting avanzado. La compañía ha formado un equipo de *hunters*, que caza y analiza cualquier comportamiento anómalo. La tificación de comportamientos extraños, tanto de usuarios, como de procesos y máquinas.

En este frente, las estrategias de Threat Hunting, donde la ciberseguridad y la ciencia de datos convergen, adquieren un creciente protagonismo, pues implican no sólo la detección, sino el análisis, formulación de hipótesis y resolución de



Orion, la plataforma de Threat Hunting de Cytomic.

Orion es, por tanto, una plataforma web integrada, avanzada y especializada, que proporciona visibilidad de todos los comportamientos generados en los *endpoints*, siendo capaz de procesar miles de millones de eventos en tiempo real, generar alertas cuando se detecta una anomalía y activar las acciones precisas que se requieren sobre dichas alertas.

A esto une su naturaleza multiorganización y multiusuario con conexión desde cualquier sitio, de forma que una organización con sedes ubicadas en varios países, puede gestionar la densidad de los datos que desee en un lugar determinado. Cuando la consola de exploración encuentra una coincidencia, ésta se traslada a la consola de forensía donde es posible investigar una máquina determinada en un momento concreto para correlacionar las anomalías que se han detectado. La presentación de la información y los datos se produce en un *dashboard* desde el que se gestiona el funcionamiento de todas las alertas e incidentes, y que permite generar informes de manera automática que se pueden enviar al cliente y/o responsable del servicio.

Orion está preparada para su uso tanto por los SOC internos de grandes compañías como también por los MSSPs que requieran ampliar su oferta de detección y respuesta temprana.


Analistas en el laboratorio de Cytomic, ubicado en una de sus sedes en España.

combinación de tecnologías avanzadas y servicios gestionados permite clasificar los procesos activos y saber qué está pasando en el momento que está pasando con visibilidad detallada de la actividad, el control de procesos en ejecución y la reducción de la superficie de ataque.

Orion y la investigación de amenazas avanzadas

Las organizaciones cuentan con diversas soluciones para combatir el *malware* tradicional; pero la evolución de las amenazas hacia ataques sin fichero o a través del uso de *scripts* o código en memoria, hace que el reto se centre en la identificación de una ciberamenaza, incluso, antes de que pueda hacerse realidad, así como la incorporación de las pautas aprendidas al modelo de detección.

El Threat Hunting enfocado al segmento Enterprise se traduce en un servicio más especializado y proactivo para atender las necesidades de protección de grandes empresas. Y en el corazón de dicho servicio se encuentra la nueva plataforma Orion, orientada a la protección del *endpoint* y preparada tanto para que las grandes empresas usuarias puedan utilizarla en sus SOCs internos, como también para que lo hagan los MSSPs que consideren la necesidad de ampliar su oferta de detección y respuesta temprana a través del Threat Hunting.

Desarrollo continuo de talento

El proceso de Threat Hunting y su mejora continua depende en gran medida de la experiencia y el conocimiento de los analistas. Por este motivo, una de las máximas de PandaLabs es la colaboración entre equipos y la incorporación en tales equipos de analistas senior y los nuevos expertos que se suman al laboratorio. Esto permite a los jóvenes ir adquiriendo conocimiento. Un valor diferencial que se lleva a cabo a través de un programa de *kids management*, con el que consigue suplir las carencias de un mercado laboral en el que, sólo en la UE, hay un déficit en expertos de ciberseguridad que supera las 800.000 vacantes. ●

CYTOMIC

De la hipótesis a la caza

Threat Hunting: Zero Trust y Analítica de comportamiento

Nuestros servicios de **Threat Hunting e investigación** estudiarán y clasificarán todos los comportamientos de aplicaciones, máquinas y usuarios para erradicar las ciberamenazas avanzadas en tu entorno corporativo.