DOCUMENTOS SiC
Nº 28
SEPTIEMBRE 2019

Inteligencia, tecnología y talento al servicio de una ciberseguridad anticipativa

MNEMO

Servicios orientados a la madurez digital

CTI: El valor de la ciberinteligencia de amenazas

Mnemo Intelligent SOC

Defensa adaptativa y conectada

Raúl Sánchez
Director General de Mnemo

Mnemo, inteligencia al servicio de la ciberseguridad gestionada

Desde sus comienzos, hace 15 años, Mnemo ha construido una sólida oferta de soluciones y servicios de ciberseguridad basada en su comprensión de las amenazas y de las necesidades del mercado. Su éxito se basa en la inteligencia combinada con una gran experiencia, una visión innovadora y el mejor talento, una concepción que la ha convertido en uno de los referentes actuales de la ciberseguridad, especialmente en el sector financiero y en los regulados por la legislación de protección de infraestructuras críticas y la NIS.

Evolución, adaptación e inteligencia son tres características que bien definen la trayectoria de Mnemo. Su historia se remonta a 2001, aunque fue cuatro años más tarde cuando la multinacional española decidió intensificar su inversión en ciberseguridad para posicionarse en el mercado con una oferta de soluciones y servicios de ciberseguridad dirigidos a corporaciones y basados en la investigación del origen de las amenazas, su seguimiento evolutivo y el despliegue de recursos tecnológicos para minimizar el impacto de su materialización.

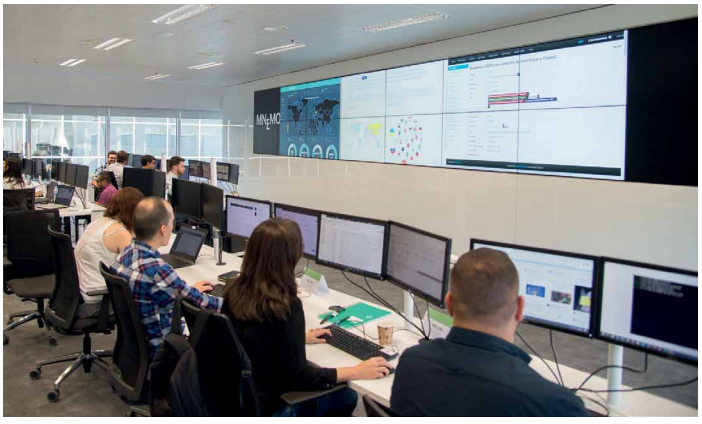
A día de hoy, y como parte de este objetivo, Mnemo defiende un planteamiento único en la provisión de servicios de ciberseguridad gestionada, línea de oferta en la que consolida los aspectos clásicos de esta actividad con el desarrollo y uso de herramientas innovadoras orientadas al tratamiento de grandes datos de valor mediante técnicas de IA.

La herramienta nuclear de la línea MSSP de la compañía es **Mnemo Intelligent SOC**, una red de SOC-CERT en los que trabajan expertos en los distintos frentes de la gestión de la ciberseguridad. La función CERT de Mnemo está homologada por el FIRST, lo que la permite intercambiar información, experiencia, herramientas y técnicas sobre vulnerabilidades y ataques con más de 400 equipos miembro de 90 países, y actualizar permanentemente su conocimiento, especializándose en la lucha contra el fraude electrónico en el sector financiero y en la protección de Infraestructuras Críticas (sector industria), frentes en los que posee las correspondientes certificaciones, y en los que la firma hace foco en su actividad como proveedor de servicios de ciberseguridad gestionada.

Ciberinteligencia en el corazón del negocio

El ecosistema de soluciones y servicios de ciberseguridad de Mnemo está pensado para comportarse como un organismo vivo: adaptándose, evolucionando y tomando decisiones (en los frentes temporales que escapan a la intervención humana directa) para poder hacer frente a ataques y prevenir amenazas.

El corazón de este organismo es una cartera de soluciones propias de Inteligencia Preventiva, que se van refinando continuamente con los productos de inteligencia de amenazas y el conocimiento de la gestión de vulnerabilidades avanzadas. Estas herramientas van más allá de la integración de listas negras procedentes de terceros o de generación propia, para incluir también análisis de grafos para identificar amenazas ocultas y quiénes o qué están detrás de los ataques percibidos, un hecho que trasciende de la mera notificación de incidentes a los equipos para que ellos creen reglas de protección, con la generación y diseminación automática de defensas relacionadas con las amenazas identificadas.



El valor diferencial obtenido de los sistemas de inteligencia de Mnemo Arkadia es la integración con el servicio de Defensa Adaptativa, el cual permite el establecimiento de defensas de forma automática ante las vulnerabilidades, amenazas e incidentes detectados desde el SOC-CERT, ofreciendo siempre la mejor solución para cada escenario.

Mnemo tiene un planteamiento diferencial como MSSP, al complementar el uso de tecnologías de terceros para áreas tradicionales de servicio con herramientas IA de diseño propio.

La cultura de innovación de Mnemo se ha traducido, asimismo, en el diseño y desarrollo de una plataforma global de inteligencia, denominada **NERV**, con la que cubre las carencias de las plataformas tradicionales, que no resuelven el ciclo completo de inteligencia. Esta plataforma

tiene funcionalidades de vigilancia digital y da soporte a otra de las actividades más importantes de la compañía: la ciberinvestigación, para la lucha contra el fraude y otros tipos de delicuencia económica y/o vinculada.
Junto a ello, la filosofía de Mnemo también incide en mejorar la resiliencia de los negocios de sus clientes a través de la integración y la búsqueda de sinergias con tecnologías complementarias, recurriendo a soluciones de otras grandes compañías, como IBM, Fortinet, Kaspersky, McAfee, Qualys, SealPath... entre otras muchas, con las que ha establecido alianzas tecnológicas para dar un servicio lo más completo posible al cliente.

La importancia del factor humano

Pero ninguna de las medidas anteriores es eficaz sin un elemento clave: el factor humano. El equipo profesional de Mnemo está formado por cerca de 700 personas, constituyendo un grupo muy sólido técnicamente y con 15 años de experiencia en el mercado, que incorpora, desde su inicio, mucho talento para innovar. Más de la mitad de la plantilla está dedicada al área de ciberseguridad, tanto en I+D, como en la prestación de servicios de prevención, detección y respuesta ante amenazas.

MNEMO INTELLIGENT SOC

Nuestra visión de la Ciberseguridad

1. ADAPTATIVA
Emular un sistema inmunitario eficaz que sea capaz de adaptarse para poder reconocer y hacer frente a la amenaza.

2. EVOLUTIVA
Evolucionar con madurez para hacer frente al mayor reto que plantea hoy cualquier amenaza: Su constante evolución.

3. INTELIGENTE
Aplicar métodos basados en Inteligencia para apoyar la toma de decisiones de manera preventiva, y reactiva una vez ocurra un incidente.

4. ESTRATÉGICA
Conocer en qué nivel de riesgo se encuentra una organización y qué medidas se deben tomar es un proceso
clave que debería poder llevarse a cabo de forma sencilla.

La multinacional española cuenta con una red de SOC-CERT, denominada Mnemo Intelligent SOC, donde reside la base de su estrategia y la fortaleza para prestar servicios globales, centralizados y conectados.

Proyección internacional

Mnemo también destaca por su fuerte proyección internacional. Muestra de ello es que, actualmente, cuenta con oficinas en España, México y Colombia, y está presente en 11 países de Latinoamérica con proyectos activos. Una estrategia de negocio que va a intensificar, al objeto de aumentar su presencia en el mercado de MSSPs en zonas donde aún no posee infraestructuras físicas.
El plan de la multinacional pasa por fortalecer el papel de España dentro de su estructura global con un cambio organizativo que ya ha conllevado el traslado de su sede y del SOC-CERT de Madrid a unas nuevas instalaciones en la capital, y el fortalecimiento de su presencia en otras comunidades autónomas.

Red de SOC-CERT

Como centro neurálgico para la prestación de sus servicios de ciberseguridad gestionada, Mnemo cuenta con una red de SOC-CERT, que la compañía ha denominado **Mnemo Intelligent SOC**. Está formada por tres centros, que cubren actualmente la demanda en ambas partes del Atlántico, ubicándose dos de ellos en Latinoamérica (México y Colombia), y uno en España (Madrid).
Mnemo Intelligent SOC es la base de la estrategia de negocio, que no es otra que ofrecer servicios globales, centralizados y conectados con todos los entornos. Éste último es un aspecto clave para garantizar lo que este prestador entiende por Seguridad Conectada: una arquitectura de defensa integrada, a través de la red de SOCs, fundamentada en una metodología propia, Arkadia, donde cada uno de sus componentes, servicios y tecnologías, están retroalimentando al resto, beneficiándose de la comunicación multidireccional y actuando como un solo 'organismo', independientemente de donde se produzca una alerta o incidente.
Para dar confianza a la demanda de las capacidades de cumplimiento de las diferentes requisitorias de calidad de sus servicios en los distintos escenarios de mercado, Mnemo cuenta con todas las certificaciones nacionales e internacionales de referencia en el sector.

SOC de Madrid, el foco de la innovación

El SOC-CERT de Mnemo ubicado en España, que acaba de estrenar nueva sede en Madrid, es el núcleo del conocimiento en modo mejora continua de procesos sectoriales (sector financiero e industrial) y de ciberseguridad aplicada a la alerta temprana, descubrimiento de ataques desconocidos, gestión de vulnerabilidades y defensa evolutiva.
En la actualidad, cuenta con una plantilla de 40 especialistas (en su mayoría ingenieros), entre los que se encuentran expertos en TIC, protección TIC, Análisis Forense, auditoría y Red Team. Algunos de estos especialistas prestan su servicio en el Laboratorio, donde se ejerce el liderazgo en innovación de la compañía y donde se refinan y crean las soluciones orientadas al servicio que, posteriormente, se despliegan en los otros centros. ●

Raúl Sánchez
Director General de Mnemo

Mnemo es una compañía que nació con un foco distinto al actual y que ha vivido un intenso viaje de transformación, especialmente durante los últimos años, en los que ha redoblado y focalizado sus esfuerzos en ciberseguridad. Hoy, su objetivo es seguir ampliando su presencia en el mercado a través de la I+D+i, el apoyo al talento y un catálogo de servicios donde la inteligencia se postula como base de la prevención. Su Director General, Raúl Sánchez, desgrana en esta entrevista la apuesta de la multinacional española por la ciberseguridad y sus próximos pasos.

"Orquestamos las mejores herramientas de terceros y desarrollamos aquellas necesarias para gestionar frentes no cubiertos por el mercado"

– El mercado de proveedores de MSSPs está en auge. ¿Qué distingue a Mnemo del resto de prestadores?

– Una de las fortalezas de la compañía se encuentra en su trayectoria. Llevamos más de 10 años invirtiendo en ciberseguridad. A día de hoy, tenemos un buen posicionamiento en sectores como el financiero, industria y asociaciones que nos proveen un valor diferencial respecto a MSSPs tradicionales o de más reciente creación. Además, tenemos un gran *expertise* en el área de inteligencia, que viene dado por nuestra relación originaria con las Fuerzas y Cuerpos de Seguridad de diferentes estados. Gracias a esta experiencia, proveemos servicios de inteligencia preventiva diferenciales basados, especialmente, en inteligencia de amenazas y de vulnerabilidades. De hecho, la capa de *threat intelligence,* que denominamos CTI y que ofrecemos como parte de nuestros servicios, es uno de nuestros principales valores.

– ¿En qué mercados opera Mnemo y qué lugar ocupa el de España en sus operaciones?

– Nuestro mercado natural es el español, aunque hace más de una década que decidimos invertir en términos de ciberseguridad en Latinoamérica. En la actualidad, Mnemo tiene presencia en Colombia y México, pero también cuenta con operaciones en otros 11 países de la región. Respecto al mercado español, operamos en Madrid y Andalucía, y queremos ampliar nuestro posicionamiento a otras comunidades autónomas.

– ¿Cuál es la estrategia de la compañía?

– Además de desarrollar los mercados actuales, nuestra ambición es ampliar la dimensión de la compañía y aumentar nuestra presencia tanto a nivel nacional como en otras geografías donde poseemos proyectos pero aún no tenemos una infraestructura física. Hemos identificado cuatro ejes de actuación: reforzar la apuesta por la inversión en I+D, captar talento, ampliar cuota de mercado e innovar..., todo materializado en servicios transparentes para los clientes, muy medidos en la capa estratégica de seguimiento en base a SLAs, KPIs... Queremos huir de la imagen tradicional de los proveedores e integradores de ciberseguridad que 'simplemente'

cogen un producto de un gran fabricante y lo implementan. Mnemo es un proveedor de servicios de ciberseguridad que apuesta por la integración y conectividad de grandes herramientas que hay en el mercado y, si no existen, innovamos creándolas.

– ¿Qué papel juega el SOC-CERT de Madrid en la red de SOC-CERT Mnemo?

– Contamos con tres SOC-CERT adscritos al organismo First que cuentan, desde 2014, con certificaciones en fraude electrónico y protección de infraestructuras críticas. Creo que fuimos visionarios en este sentido porque, a día de hoy, son los dos grandes nichos de futuro y forman parte de los retos a los que se enfrenta la ciberseguridad. Actualmente, estos tres centros están totalmente coordinados, operando 24/7 *follow the sun* con las mismas herramientas y procedimientos, y complementándose en las distintas geografías. En particular, el SOC-CERT de Madrid ejerce el liderazgo en innovación. Aquí es donde está el I+D y donde se crean las nuevas soluciones que luego se integran en los otros Centros y que formarán parte de nuestro catálogo.

– ¿Qué servicios gestionados de su compañía destacaría?

– Intentamos alejarnos de lo que se podría considerar el estándar actual en la industria, como es la monitorización y la gestión de incidentes a través de un SIEM. Mnemo va un paso más allá para ofrecer, además, una capa de inteligencia preventiva. En este sentido, hemos invertido mucho en soluciones de inteligencia de amenazas y de vulnerabilidades, donde destaca la capa de gestión *end-to-end* del ciclo completo de la vulnerabilidad. Además, ofrecemos unos servicios muy acotados en torno a la monitorización y gestión de todo el catálogo TIC de las compañías, para intentar eliminar el Shadow IT, que es uno de los principales riesgos de las empresas.

Mnemo presta servicios diferenciales de inteligencia preventiva. Para ello, contamos con un gran equipo de analistas expertos en control de fraude electrónico y en protección de infraestructuras críticas y con tres SOC-CERT adscritos al First

– ¿En qué sectores de la demanda tiene mayor presencia Mnemo?

– La demanda es totalmente transversal y multisectorial, desde cadenas hoteleras hasta empresas de logística, industriales, salud, etc. No obstante, a día de hoy, las principales referencias las tenemos en entidades financieras y en operadores de infraestructuras críticas, los dos 'verticales' que estamos explotando.

– Mnemo también cuenta con un equipo de desarrollo de productos orientados al servicio. ¿Seguirá apostando por esta línea?

– Sí. Uno de nuestros objetivos estratégicos es mantener nuestra inversión actual en I+D+i. Para nosotros es básico. Somos agnósticos en cuanto a tecnología. Confiamos en los mejores fabricantes para dar servicio a nuestros clientes pero, también, intentamos cubrir los *gaps* que tienen sus tecnologías generando 'piezas' de valor que ellos pueden tardar más en lanzar al mercado. A esto se le une el desarrollo de soluciones específicas, entre las que destacan nuestras tres grandes plataformas: la de inteligencia de amenazas, la de vulnerabilidades, y la propia de inteligencia, llamada NERV, que es la que nos da el soporte para los servicios de vigilancia digital y de ciberinvestigaciones.

– Y, ¿cuál es su política de alianzas con los fabricantes?

– Con los fabricantes hemos definido un portafolio bastante amplio para que se cubran todas las necesidades que una entidad pueda llegar a tener en la materia. Pero, para Mnemo lo importante es la definición del servicio en sí, con independencia de la tecnología que se vaya a utilizar. La razón es que si surge un cambio de paradigma tecnológico, o un nuevo *player*, seamos capaces de cambiar la 'pieza' tecnológica, incrustar la nueva y poder seguir dando el mismo nivel de servicio.

– Por último, ¿qué medidas está tomando Mnemo frente al déficit de profesionales en ciberseguridad?

– Intentamos proteger lo que llamamos el *core* de nuestro conocimiento. Para mitigar el impacto que tiene la escasez de talento lo que hacemos es, por un lado, reciclar profesionales de otras líneas, como desarrollo, implantación, consultoría… a ramas de ciberseguridad. Esto nos ha permitido conseguir un crecimiento muy fuerte en los tres últimos ejercicios, más que si hubiéramos tratado de captar talento en el mercado, donde escasea. Además, intentamos activar acuerdos con universidades y centros de formación. Y, como tercera vía, aprovechamos nuestro posicionamiento en el mercado latinoamericano también, para conseguir talento. Aun así, el problema existe, y está teniendo efectos perniciosos en la oferta y la demanda. ●

Talento y tecnología para ofrecer seguridad proactiva y a medida

Mnemo dispone de un catálogo de servicios, a medida y bajo demanda, que incluye desde la monitorización y gestión de amenazas hasta el análisis de malware y APTs o la consultoría evolutiva, para acompañar a sus clientes en el proceso de madurez en la gestión efectiva de la ciberseguridad como factor clave para lograr cotas satisfactorias de resiliencia operativa y de negocio.

Mnemo cuenta con una oferta de servicios de ciberseguridad interconectados que cubren toda la cadena de valor, permitiéndole analizar el caso específico de cada cliente y proporcionar una respuesta personalizada centrada en las necesidades detectadas. Para ello, la compañía basa su modelo de seguridad en cinco bloques: identificar y monitorizar, inteligencia de amenazas, análisis de seguridad, tratamiento y medidas, así como evaluaciones de seguridad.

La oferta incluye desde los servicios más tradicionales hasta los más avanzados, divididos en tres opciones: por un lado, los asociados con la 'Metodología Mnemo Arkadia', aplicada a cada pilar y que incluyen identificación y monitorización de activos, inteligencia de amenazas, de vulnerabilidades, servicios de Red Team, monitorización y gestión de incidentes, defensa adaptativa, ingeniería de seguridad, gobierno de la seguridad… entre otros.

CATÁLOGO DE SERVICIOS DE CIBERSEGURIDAD

En segundo lugar, los denominados 'Security Packs', con un alto valor añadido, utilizando la tecnología de fabricantes punteros en sus respectivas áreas: seguridad perimetral, seguridad de *endpoint*, protección inteligente del dato, concienciación de usuarios, etc.

Y, por último, sus servicios verticales derivados del alto conocimiento y experiencia de la compañía en cada segmento del mercado, un ámbito que incluye servicios de ciberinvestigación, de control y gestión del fraude, de identidades y de accesos, así como análisis tácticos de *logs*, entre otros.

CTI: EL VALOR DE LA CIBERINTELIGENCIA DE AMENAZAS

Las capacidades que Mnemo ofrece desde CTI –Cyber Threat Intelligence–, una de sus áreas de alto valor añadido, tienen por finalidad introducir una capa de inteligencia sobre las operaciones de ciberseguridad para anticiparse a los riesgos y amenazas más frecuentes y los más impredecibles, un trabajo que se basa en contextualizar e interpretar los incidentes y amenazas globales más persistentes, así como la problemática de cada cliente. Para ello, la compañía ha desarrollado una plataforma propia que se nutre de herramientas avanzadas de *big data* y *machine learning*. No obstante, su gran valor es su equipo multidisciplinar de profesionales, provenientes del ámbito de la Inteligencia y con contrastada experiencia internacional en investigaciones complejas sobre el cibercrimen.

Concebido como un servicio bajo demanda y a medida, CTI basa su éxito en dos aspectos muy concretos. Por un lado, el análisis de hipótesis y posibles escenarios que permitan al cliente anticiparse a las amenazas y, por otro, la identificación de actores y relaciones, así como motivaciones personales o profesionales con una visión estratégica.

De esta forma, en esta área se busca ofrecer la excelencia en seguridad proactiva para reducir el impacto de los riesgos y amenazas que más afectan a las empresas. En el contexto, todos los trabajos se orientan a un único fin: "elevar el nivel operativo de protección hacia una seguridad proactiva que repercuta directamente en la mejora de las operaciones globales".

Mejora continua

La propuesta de Mnemo destaca por utilizar herramientas propias, que brindan una capa de protección diferencial y, cuando es necesario, se complementan con tecnología de terceros. En este método de trabajo residen la mejora y renovación constantes de las fórmulas y el modo de servicio al cliente aportando, también, un valor añadido de especialización técnica y sectorial.

Mnemo comenzó hace tres años el proceso de evolución a futuro de los servicios de ciberseguridad, convirtiendo su SOC-CERT en un SIC (Security Intelligence Center). Su proceso continuo de I+D+i tiene como objetivo situar a la compañía a la cabeza de la innovación en tecnología.

Además, la compañía ofrece servicios específicos para verticales de cada sector, siendo uno de los referentes el financiero. La multinacional española ha realizado una significativa apuesta por esta línea de negocio, donde cuenta con una larga trayectoria y capacidades experimentadas en la prevención y lucha contra el fraude, que le permiten ofrecer soluciones específicas para su problemática diaria. Se trata de una de sus líneas estratégicas más destacadas con grandes proyectos de alcance internacional en entidades españolas de referencia. Esta particularidad hace de Mnemo un socio especialmente versado en esta problemática de los negocios bancarios.

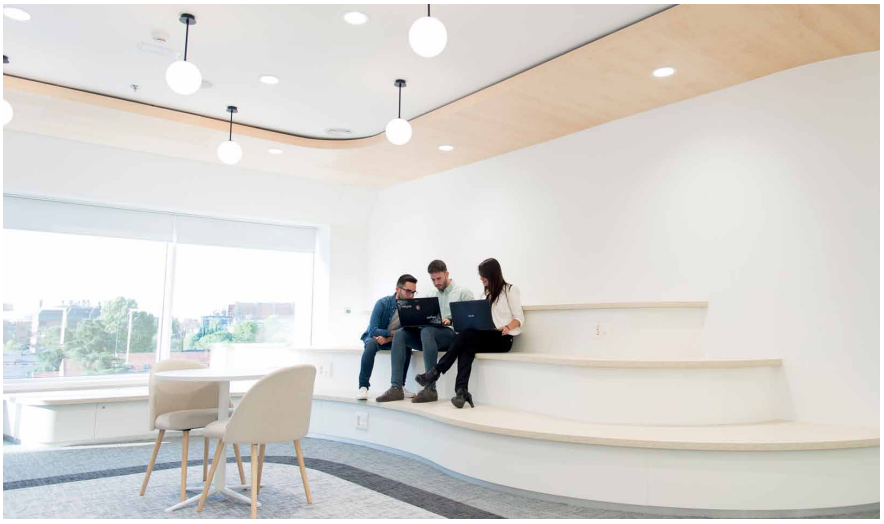
MNEMO LABS: ANÁLISIS AVANZADO DE MALWARE Y SERVICIOS FORENSES

Los laboratorios de seguridad son la apuesta de Mnemo para la adquisición de evidencias en tiempo real, la búsqueda y análisis de software malicioso, de tráfico y servicios forenses, liderados por ingenieros experimentados. Las investigaciones de seguridad se llevan a cabo en tres frentes: investigación en patrones y ataques sobre dispositivos o arquitecturas, sobre plataformas y dispositivos, así como la generación de capacidades tácticas y ofensivas para evaluación de fortalezas.

Para estos servicios, la multinacional española ha desarrollado con tecnología propia una plataforma avanzada de inspección de malware. A partir de la experiencia de sus ingenieros y el departamento especializado en reversing e investigación de patrones de ataque, la compañía ha creado una metodología y motores de inspección inteligentes, disponibles *off-line* para pruebas controladas de sus clientes.

Mnemo Labs consiste en dos líneas principales de servicio:

- Análisis de Tráfico multi-protocolo y Análisis de Malware y APT con soporte en binarios y/o objetos lógicos.
- Análisis Forense Digital avanzado, multi-plataforma y multi-dispositivo.



SERVICIOS DE AUDITORÍA EVOLUTIVA: SEGURIDAD EN CONSTANTE CRECIMIENTO

Mnemo basa sus servicios de Auditoría Evolutiva sobre el concepto de Gestión Estratégica de Vulnerabilidades, que proporciona una imagen real y continua del estado de la seguridad de una organización. Permite conocer el nivel de protección del cliente para establecer las medidas de seguridad correctas de forma preventiva y de acuerdo a una valoración completa de riesgo (Mnemo Risk).

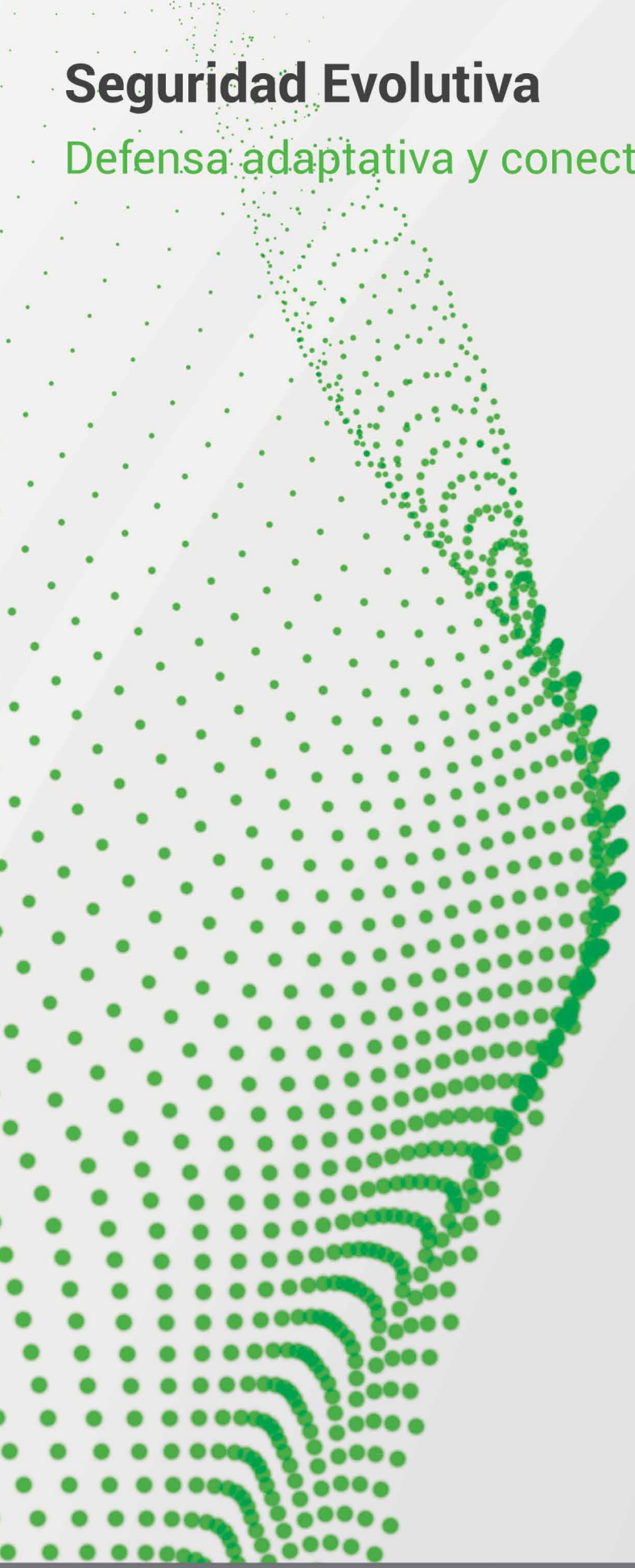
– **Análisis de Vulnerabilidades interno**, con el que se evalúa de forma permanente la integridad de la infraestructura interna para descubrir infraestructura oculta. Con él se dispone de un informe de exposición a amenazas no invasivo, un análisis continuo para identificar dispositivos activos o pasivos no autorizados e información sobre actividades anómalas en la infraestructura.

– **Análisis de Vulnerabilidades externo**, que se encarga de realizar de manera continua un escaneo de los activos externos del cliente. Mnemo ha desarrollado una plataforma completa para las auditorías continuas de seguridad y el análisis periódico de los activos externos, obteniendo un informe con todas las vulnerabilidades detectadas y la criticidad de las mismas.

– **Gestión estratégica de Vulnerabilidades**. Se establece un proceso continuo de detección y resolución de vulnerabilidades, en ciclos iterativos separados que se retroalimentan de forma permanente. El objetivo es dotar al SOC-CERT de un procedimiento eficaz que al mismo tiempo permita alimentar la Base de Conocimiento de la organización, así como definir planes de acción que aseguren el cierre correcto de la resolución de cada vulnerabilidad.

Seguridad Evolutiva

Defensa adaptativa y conectada



GESTIÓN ESTRATÉGICA DE VULNERABILIDADES

DEFENSA ADAPTATIVA

CSIRT FINANCIERO

INTELIGENCIA DE AMENAZAS

MONITORIZACIÓN Y GESTIÓN DE INCIDENTES

RED TEAM

PROTECCIÓN INTELIGENTE DEL DATO

MNEMO LABS

España | México | Colombia

www.mnemo.com info@mnemo.com

MNEMO