NextDefense

Servicios NextDefense de Telefónica Tech

¿Qué es lo próximo en Servicios de Ciberseguridad?

ElevenPaths

Part of TELEFÓNICA TECH

1 | Nuevo lanzamiento: NextDefense

Telefónica Tech se complace en anunciar el lanzamiento de NextDefense, su nueva marca de servicios gestionados avanzados.

NextDefense de Telefónica Tech reúne nuestros servicios de seguridad de última generación con el objetivo de ayudar a las grandes y medianas empresas a adoptar un sistema de seguridad eficaz a través de una defensa totalmente gestionada en la nube, el *endpoint* y la red. Los servicios NextDefense amplían tus operaciones de seguridad a través de **nuestros expertos de élite**, respaldados por inteligencia de amenazas propia, la mejor tecnología y procedimientos estandarizados impulsados por la automatización.

NextDefense proporciona las capacidades básicas para apoyar una práctica de seguridad integral basada en el marco del NIST, e incluye servicios de Detección y Respuesta, Gestión de Vulnerabilidades basadas en Riesgo e Inteligencia de Amenazas.

2 | Contexto: La ciberseguridad hoy en día

Cada año se gastan miles de millones de euros en tecnología de seguridad. La investigación predice que el gasto mundial en seguridad alcanzará los 174.700 millones de dólares en 2024 (una CAGR del 8,1% durante 2020-2024). Sin embargo, las organizaciones siguen fracasando y siendo víctimas de ciberataques, como demuestran los últimos informes y tendencias:

En 2020, el volumen de registros de compromisos se disparó un 141% (37.000 millones), la mayor cifra desde 2005. El *ransomware* se duplicó literalmente en 2020 y representó el 27% de los incidentes de *malware* registrados (Gartner). La coyuntura pandémica fue aprovechada por los actores amenaza (al COVID-19 se le atribuye un aumento del 238% de los ciberataques en FinTech en 2020) y se espera que empeore en 2021.Está claro que algo no está funcionando bien en el sector. Se ha buscado una píldora mágica que garantice la salud, una única tecnología mágica que pueda evitar todos los ataques. Como ocurre con muchas enfermedades graves, detener algunos tipos de ataques podría llevarse a cabo de forma completa con alguna medida específica. Pero garantizar que nuestras organizaciones se mantengan sanas frente a los riesgos cibernéticos requiere un esfuerzo mucho más exhaustivo, sistemático y constante.

El NIST ha creado un marco muy completo que explica cómo debe estructurarse un programa de este tipo basado en los siguientes pilares:

IDENTIFICAR

- Gestión de Activos
- Gobernanza del Entorno Empresarial
- Evaluación de Riesgos
- Estrategia de Gestión de Riesgos

PROTEGER

- Control de Acesso
- Concienciación & Capacitación
- Protección de Datos
- Información sobre Protección & Procedimientos
- Mantenimiento
- Tecnologías de Protección

DETECTAR

- Irregularidades & Eventos
- Vigilancia Constante en Seguridad
- Procesos de Detección

RESPONDER

- Plan de Respuestas
- Comunicaciones
- Análisis
- Mitigación
- Mejoras

RECUPERAR

- Plan de Recuperación
- Mejoras
- Comunicaciones

Sin embargo, su aplicación no es fácil. Incluso las grandes multinacionales de los sectores regulados que tienen experiencia relevante en la gestión de riesgos y en la creación de capacidades internas de ciberseguridad, están luchando con la complejidad y los costes que conlleva. Por lo tanto, el panorama para las organizaciones más pequeñas es aún más preocupante si cabe.

Las organizaciones confían ahora más que nunca en los proveedores de Servicios de Seguridad Gestionada (MSS), buscando externalizar los esfuerzos de SecOps a través de modelos operativos híbridos, así como soluciones completas de asesoramiento y llave en mano para construir su programa de seguridad desde la base. De hecho, se estima que el mercado de MSS alcanzará los 41.000 millones de dólares en 2022, con un crecimiento anual compuesto del 16,6%.

3 | De MSS a MDR y más allá

Teniendo en cuenta los retos anteriores, es natural por tanto que los Servicios de Seguridad Gestionada estén pasando de la mera gestión de la tecnología de seguridad a soluciones integrales que pretenden abarcar todo el problema.

Las organizaciones están cambiando su enfoque y exigiendo a sus proveedores de MSS que eleven su papel y se conviertan en un socio estratégico que pueda empoderar a sus CISOs y ayudar a proporcionar resultados empresariales tangibles.

Y como elemento central de esos resultados empresariales, está la Detección y Respuesta, la verdadera columna vertebral de las operaciones de seguridad modernas. La Detección y Respuesta Gestionadas (MDR), a diferencia de las capacidades tradicionales de MSS para la gestión de la tecnología de seguridad, centran sus esfuerzos en ampliar los controles de seguridad a través de expertos cualificados que buscan y eliminan las amenazas que pasan desapercibidas.

La Detección y Respuesta no es tarea fácil, y se prevé que muchas organizaciones compartan esfuerzos con socios especializados:

"2025, el 50% de las organizaciones utilizarán los servicios de MDR para funciones de vigilancia, detección y respuesta a las amenazas que ofrezcan capacidades de contención."
Gartner

Los proveedores de servicios MDR mejoran los programas de seguridad de una organización, al tiempo que disminuyen en gran medida los costes de adquisición para adoptar esta capacidad. En comparación, el despliegue de una detección y respuesta madura es casi inalcanzable para las medianas empresas, teniendo en cuenta las barreras de entrada para configurar esta práctica y los costes continuos para mantener el talento y la tecnología.

Como regla general, una capacidad media para una organización de tamaño medio requeriría al menos 900 mil euros en personal, y más de 300 mil euros en licencias e infraestructura. Algo inasequible para la mayoría de las empresas de este segmento.

Es un reto incluso para las organizaciones más grandes con los bolsillos más abultados: la escasez de talento a nivel mundial (se prevé que habrá 3,5 millones de puestos de trabajo sin cubrir en todo el mundo en 2021) hace que sea realmente difícil conseguir y retener el talento. Por otra parte, la complejidad de la evolución de la tecnología de seguridad crece constantemente a medida que se transforman los nuevos modelos de negocio (por ejemplo, BYOD, trabajo remoto, SaaS, aplicaciones sin servidor, etc.) y los perímetros de la empresa siguen su curso (dispositivos no gestionados, nubes privadas/públicas, OT e IoT, móviles, etc.).

Por el contrario, los principales proveedores de MDR pueden ofrecer una visibilidad global de las amenazas en todos los sectores y zonas geográficas y, a diferencia de la mayoría de las organizaciones, pueden permitirse unos costes fijos elevados gracias a las economías de escala. Las grandes bases de clientes les permiten soportar elevados costes de personal (contratación, formación, rotación, retención de expertos de nivel 3, etc.). Además, estos actores han realizado grandes inversiones en estandarización, automatización y análisis que les permiten reducir los costes del nivel 1 para las operaciones más ruidosas y de bajo valor. El alcance global de los principales proveedores les permite establecer relaciones estratégicas con los principales proveedores de tecnología, obteniendo así ventajas competitivas como precios basados en el volumen y programas de soporte *premium*.

Volviendo a nuestro marco NIST y a nuestra misión de apoyar programas de seguridad completos, reconocemos que los MDR por sí solos no son suficientes. Una capacidad de detección y respuesta moderna es crucial, pero una práctica de seguridad eficaz fracasará si no prestamos la misma atención a todas las demás áreas de operaciones de seguridad y al propio programa de seguridad en su conjunto.

Para habilitar también las funciones "Identificar" y "Proteger", es fundamental aprovechar también una capacidad de Gestión de Vulnerabilidades basadas en Riesgo (VRM). Tenemos que saber **qué proteger, de qué**

amenazas tenemos que protegerlas y cuál es nuestro nivel de exposición ante ellas.

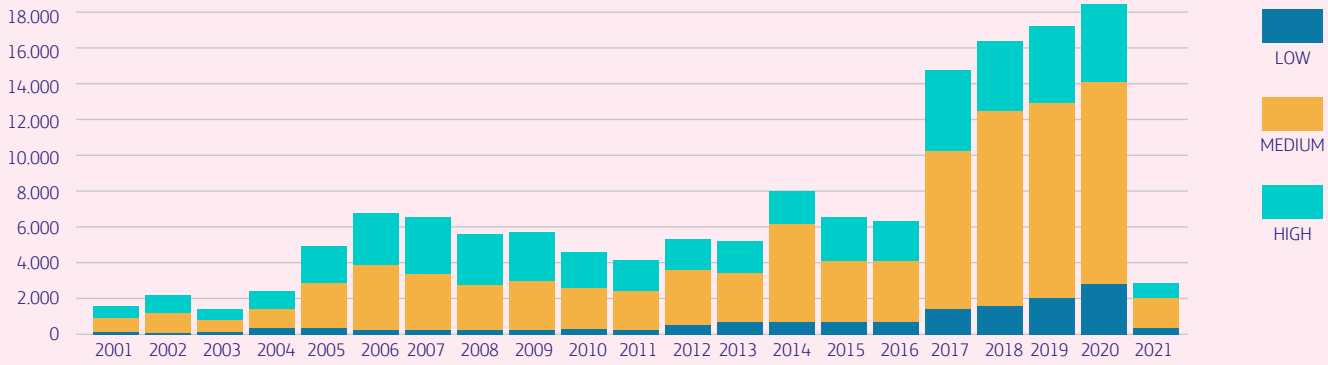
Los cimientos de una práctica de seguridad sólida se establecen en el inventario de activos, las evaluaciones de seguridad y la priorización de la gestión de la vulnerabilidad en función del riesgo empresarial, el contexto organizativo y la información disponible sobre la actividad de las amenazas.

Una gestión eficaz de las vulnerabilidades puede reducir drásticamente la carga de las operaciones de Detección y Respuesta, y en la mayoría de los casos incluso evitar las dolorosas intrusiones y filtraciones de datos. De hecho, según un estudio de Ponemon, **el 60 % de las vulnerabilidades en 2019 afectaban a *software* no parcheado.**

De este modo, el reto para la gestión de vulnerabilidades sigue siendo el aumento de nuevas vulnerabilidades denunciadas (en 2020 se registraron 17.447 vulnerabilidades, marcando el cuarto año consecutivo con una cifra récord), junto con las dificultades tanto para el seguimiento de todos los activos, como para detectar nuevos fallos de seguridad y priorizar la corrección de los más urgentes.

CVSS Severity Distribution Over Time

The visualization is a simple graph which shows the distribution of vulnerabilities by severity over time. The choice of LOW, MEDIUM and HIGH is a based upon the CVSS V2 Base score. For more information on how this data was constructed please see the NVD CVSS page.



Y para empeorar las cosas, no todas las vulnerabilidades pueden ser encontradas por escáneres automáticos. A veces existen fallos más sutiles en aplicaciones específicas o en sistemas completos que sólo pueden ser detectados por los *pentesters* o el Red Team.

Por último, es necesario contar con una capacidad multifuncional que ayude a informar de la función de "identificación", al tiempo que amplía la función de "detección" e impulsa la "respuesta" y la "recuperación". Y aquí es donde entra en juego la **Inteligencia de Amenazas**.

Desde el punto de vista estratégico, la Inteligencia de Amenazas amplía la gestión de riesgos al permitir una mejor comprensión de las intenciones, los motivos y la capacidad de nuestros adversarios.

Y en el aspecto operativo, la Inteligencia de Amenazas se convierte en una extensión de los controles de seguridad para mejorar las capas de protección y detección. Incluso cuando se responde a un incidente, disponer de información sobre el ataque, el actor o la campaña puede simplificar en gran medida la mitigación y la reparación al permitir una adecuada priorización y proporcionar información y orientación sobre el contexto.

Sin embargo, muy pocas organizaciones disponen de capacidades de Inteligencia de Amenazas para prepararse, detectar y responder mejor a los incidentes digitales.

4 | Introducción a nuestro servicio NextDefense

Creemos que la mayoría de las organizaciones se beneficiarán definitivamente de un proveedor de Detección y Respuesta, Gestión de Vulnerabilidades basadas en Riesgo o Inteligencia de Amenazas.

Pero seguramente serán pocas aquellas que se beneficien de un socio completo que pueda ayudar a crear un programa de ciberdefensa más completo.

Un socio que pueda ofrecer todo esto: una solución integrada, adaptarla a tus necesidades particulares, que esté cerca y entienda tu negocio. Un socio que domine la tecnología, tenga un profundo conocimiento del panorama de las amenazas y sepa por experiencia lo que supone proteger un negocio digital. Un socio que pueda innovar y prepararse para todo lo que está cambiando en el mundo actual.

Y esa es exactamente la misión de NextDefense. Nuestra nueva familia reúne la mejor capacidad operativa y técnica para ofrecer una solución totalmente gestionada que combina servicios de Detección y Respuesta, Gestión de Vulnerabilidades basadas en Riesgo e Inteligencia de Amenazas.

Los servicios de NextDefense pueden ser entregados a través de soluciones completas llave en mano, incluyendo el rápido despliegue de las tecnologías de seguridad de Telefónica que permiten la detección, hunting y respuesta avanzadas. Esta opción es la mejor para organizaciones medianas y grandes con menor nivel de madurez de seguridad e inversión tecnológica desplegada.

Asimismo, nuestro NextDefense ofrece soluciones a medida para organizaciones muy maduras, basadas en la experiencia acumulada por Telefónica durante décadas prestando servicios de seguridad a grandes corporaciones y gobiernos. Las soluciones a medida de NextDefense están dirigidas a organizaciones con programas de seguridad de mayor envergadura e inversiones tecnológicas existentes, que requieren una mayor integración con su pila existente, equipos de SecOps y procesos. Esta oferta incluye altos niveles de personalización, incluyendo acuerdos de nivel de servicio personalizados y un modelo de operaciones híbrido, con un mayor compromiso y comprensión del negocio del cliente.

NextDefense ha sido diseñado para ayudar a construir y apoyar programas completos de seguridad eficaces, permitiendo las cinco funciones de seguridad del NIST. NextDefense cumple este propósito apoyado en sus tres pilares:

Servicios de Detección y Respuesta, para la supervisión continua, *hunting* y la mitigación de las amenazas de seguridad y las vulneraciones. Incluye una solución Detección Y Respuesta llave en mano totalmente gestionada, así como servicios independientes de Análisis Forense Digital y Respuesta a Incidentes (DFIR) y servicios de *Threat Hunting*.

Servicios de Gestión de Vulnerabilidades basada en Riesgo, para obtener el control de sus activos críticos a través de la visibilidad y el análisis continuos para una identificación y corrección más rápida. Incluye funciones de Escaneo de Vulnerabilidades, Emulación de Adversarios y capacidades de Red Team, así como *Benchmarking*, Auditoría y Cumplimiento.

Los servicios de Inteligencia de Amenazas tienen como objetivo ayudarte a comprender tus riesgos digitales, proporcionándote una ventaja estratégica y un conocimiento de la situación para una mejor identificación y anticipación contra las amenazas que tienen como objetivo tus activos digitales. Incluye el servicio de Protección de Riesgos Digitales, así como *Feed* de Inteligencia de Amenazas basadas en el *feed* propio de Telefónica Tech y los productos de inteligencia de nuestros socios.

Más información sobre la familia NextDefense en la página web: **https://elevenpaths.com/es/productos-servicios/next-defense**

Sobre ElevenPaths

ElevenPaths es el equipo de ciberseguridad de Telefónica Tech, que aglutina los negocios digitales con mayor potencial de crecimiento de la compañía.

En un mundo en el que las ciberamenazas son inevitables, como proveedores de servicios de seguridad gestionada inteligente, nos enfocamos en prevenir, detectar, dar respuesta y disminuir los posibles ataques a los que se enfrentan las empresas. Garantizamos la ciberresiliencia de nuestros clientes a través de un soporte 24x7 gestionado desde once i-SOC alrededor del mundo con capacidad operativa global.

Creemos en la idea de desafiar el estado actual de la seguridad, característica que debe estar siempre presente en la tecnología. Nos replanteamos continuamente la relación entre seguridad y las personas con el objetivo de crear productos innovadores capaces de transformar el concepto de seguridad y, de esta manera, logramos ir un paso por delante de nuestros atacantes, cada vez más presentes en nuestra vida digital.

Trabajamos para garantizar un entorno digital más seguro a través de alianzas estratégicas que nos permitan mejorar la seguridad de nuestros clientes, así como a través de colaboraciones con organismos y entidades líderes como la Comisión Europea, Cyber Threat Alliance, Cloud Security Alliance, Cyber Security Alliance, EuroPol, Incibe, OpenSSF, OEA, ISAAC, OCA, FIRST, IoT Security Foundation, Centro de Ciberseguridad Industrial (CCI) y APWG.

Más información

elevenpaths.com | **@ElevenPaths** | **blog.elevenpaths**