NextDefense

DETECCIÓN Y RESPUESTA

Detección y Respuesta Gestionada

Extiende las operaciones de seguridad para defender tu negocio de los ciberriesgos.

Seamos sinceros, la mayoría de las organizaciones no tienen la capacidad de responder a las sofisticadas amenazas actuales, lo que deriva en dolorosos procesos de negocio, grandes pagos de *ransomware*, gastos legales, pérdidas reputacionales, etc.

La detección y respuesta efectiva requiere una tecnología de detección de primera clase, mejorada por los expertos de SecOps centrados en la optimización de las herramientas, así como equipos de *Threat Hunting* que permitan evaluaciones proactivas de las amenazas y la rápida contención de los ataques.

El servicio de Detección y Respuesta Gestionada de Telefónica Tech ayuda a las organizaciones modernas a ampliar sus operaciones de detección y respuesta, permitiéndoles descargar los esfuerzos de monitorización de alertas 24x7, *Threat Hunting* proactivo y respuesta a incidentes, con el *stack* tecnológico de Telefónica Tech.

A quién va dirigido este servicio

Organizaciones de tamaño medio que requieren una capacidad de detección y respuesta moderna y eficaz, pero que desean **reducir la carga de los costos** de la contratación de **personal** y la compra de **tecnología**.

Grandes organizaciones con una capacidad ya establecida de SecOps pero que buscan externalizar **el gran volumen de trabajo y monitorización 24x7 para centrar sus equipos de seguridad** en actividades estratégicas de mayor valor.

Empresas que buscan **desarrollar su propia capacidad interna a largo plazo** y optan por crecer y aprender de un *partner* de confianza de MDR.

Nuestra propuesta de valor

El servicio de Detección y Respuesta Gestionada de Telefónica Tech tiene como objetivo soportar y ayudar a los equipos de seguridad y acelerar el despliegue de una capacidad de detección y respuesta totalmente funcional, eliminando la molestia de elegir, comprar, operar y mantener un conjunto de herramientas de seguridad.

Este servicio te permitirá:

- **Adoptar la mejor tecnología de Detección y Respuesta en *Endpoints* (EDR por sus siglas en inglés).**
- **Aumentar tu propia capacidad de seguridad y la experiencia del equipo.**
- **Obtener una capacidad de respuesta efectiva a la brecha.**

Para lograrlo, Telefónica ha unido sus fuerzas con el **líder mundial en seguridad de *endpoints*** para proporcionarte **una solución completa llave en mano**, integrando en una sola oferta tanto la tecnología EDR como las operaciones de seguridad para permitir una rápida detección y respuesta a las amenazas.

Entrega y despliegue/instalación

Nuestro equipo se encarga de la entrega y configuración del EDR, proporcionando una estrecha orientación y apoyo durante todo el proceso de configuración.

Threat Hunting proactivo

Nuestros *Threat Hunters* de élite aprovechan la información más reciente de los últimos TTPs y los más recientes IoCs para llevar a cabo búsquedas proactivas de amenazas continuas que han pasado desapercibidas por los controles de seguridad.

Monitorización y respuesta 24x7

Incluyendo la selección y validación de alertas de amenaza, y la contención y escalada remota de cualquier violación confirmada.
Nuestros clientes se benefician de nuestro SLA de 4 horas de escalado para incidentes críticos confirmados que requieren la activación del cliente.

Forense digital y respuesta a incidentes

Este servicio incluye un *retainer* de DFIR sin costo adicional, que proporciona asistencia experta para el análisis forense y la asistencia rápida para gestión *end-to-end* de incidentes complejos y crisis.

Retainer de DFIR incluido en el servicio

Además de la detección y la contención de amenazas, el servicio también incluye un ***retainer* de DFIR (*Digital Forensics and Incident Response*) sin costo adicional.** Esta capacidad DFIR complementa y amplía el servicio de Detección y Respuesta Gestionada, proporcionando una red de seguridad y permitiendo a tu equipo CSIRT obtener una rápida asistencia de nuestro equipo DFIR para ayudarte a responder y recuperarte de una cibercrisis.

Nuestro *retainer* de DFIR incluye:

- **Acceso a la unidad de élite del DFIR, disponible 24x7** para proporcionar experiencia y respuesta rápida, así como capacidades forenses bajo demanda.
- Diseño de **plan de respuesta a incidentes** durante el *Kick-off* inicial. Este protocolo describe los procedimientos y puntos de contacto relevantes, y estandariza las acciones de respuesta en base a cada caso de uso.
- En el caso de una ciber-crisis, nuestro cliente puede activar rápidamente **nuestra capacidad DFIR**. El servicio le concederá un *incident handler* dedicado a proporcionar apoyo integral a sus equipos durante todo el ciclo de vida del incidente, incluyendo la investigación completa, recogida de evidencias, las primeras recomendaciones de contención, la asistencia para construir una estrategia eficaz de erradicación y recuperación.
- El *retainer* de DFIR incluye un **acuerdo de nivel de servicio estándar** (SLA por sus siglas en inglés) para el tiempo de respuesta inicial, tiempo de informe inicial, y tiempo para asistencia *in situ*. También, nuestros clientes pueden adquirir SLA de asistencia *premium* para una respuesta aún más rápida.
- Además de obtener el *retainer* de DFIR sin costo alguno, los clientes de nuestro servicio de Detección y Respuesta Gestionada también se benefician de un **importante descuento en el precio de las jornadas de DFIR**.

Beneficios de Detección y Respuesta Gestionada

Reduce significativamente el riesgo de un ataque cibernético.

Controla el gasto en Detección y Respuesta Gestionada de tus operaciones de seguridad y gestión de incidentes.

Aumenta la madurez de tu negocio en ciberseguridad.

La mejor tecnología EDR de Telefónica, un proveedor líder

- *Threat Hunting* proactivo basado en la inteligencia de amenazas de Telefónica Tech.
- Capacidad bajo demanda de DFIR para apoyar el análisis forense y la respuesta a un incidente de seguridad.
- Equipos de *Customer Success Team* y de *hotline* 24x7 de DFIR disponibles.
- Informes semanales de servicio y seguimientos trimestrales.
- Portal del cliente con un *dashboard* en tiempo real y gestión de casos.
- Integración completa con la plataforma de Telefónica Tech, incluyendo SOAR y TIP.

Nuestros equipos y nuestros logros

Nuestros equipos

- +1.800 empleados de SecOps.
- +1.500 certificaciones de seguridad.
- +200 analistas de élite en la *Threat Hunting*.

Logros

- 159 adversarios monitorizados.
- 565K campañas detectadas en 2020.
- Más de 32,7 millones de IoCs generados en los últimos 12 meses.
- <1 h promedio para detección y contención de *ransomware*.
- +100 h de intervenciones DFIR *in situ* en 2020.

Nuestro modelo comercial

Es un servicio completo llave en mano, es decir, una suscripción anual que tiene todo lo necesario para estar protegido. Consigue un iSOC de primera clase, respaldado por la tecnología líder de EDR, sin poner en peligro tus finanzas y protegiéndote al mismo tiempo de los *ransomware* y de todo tipo de ataques.

Ediciones disponibles

El precio del servicio depende del número de los *endpoints* protegidos y de la edición seleccionada:

	PRO edition	ENTERPRISE edition
El despliegue de la tecnología *endpoint*	NG-AV	NG-AV+EDR
Health monitoring y mantenimiento de la tecnología	✓	✓
Monitorización, análisis y reporte de amenazas 24x7	✓	✓
Threat Hunting proactivo	X	✓
Soporte y asistencia 8x5 para incidencias	✓	✓
DFIR - Asistencia 24x7 para incidentes complejos	✓	✓

Nota: El *retainer* incluye SLAs definidos, precios especiales de jornada y la elaboración de un plan de respuesta.

elevenpaths.com