EXTENDED DETECTION & RESPONSE

Managed Detection & Response

¿CÓMO TE AYUDAMOS DESDE TELEFÓNICA TECH?

Nuestra Detección y Respuesta Gestionada (MDR) ayuda a las organizaciones modernas a estar protegidas y responder frente a amenazas avanzadas

Actualmente, la mayoría de las **organizaciones no disponen de suficiente capacidad para responder a las ciberamenazas avanzadas,** derivando en complejos procesos de negocio, aumento de costes, pérdida de operatividad, implicaciones legales o pérdidas reputacionales, entre otros factores.

La detección y respuesta efectiva requiere una **tecnología de seguridad de primera clase,** mejorada por los expertos de SecOps, centrada en la optimización de herramientas y apoyada en el conocimiento experto de equipos de *threat hunting*, permitiendo evaluaciones proactivas de las amenazas y una rápida contención de los ataques.

Nuestro servicio tiene como misión proteger a las empresas 24/7, aumentando su propia capacidad de seguridad y generando un mayor grado de madurez y resiliencia.

¿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 costes de 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 valor.

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

NUESTRA PROPUESTA DE VALOR

Nuestro servicio

Telefónica Tech tiene como objetivo soportar, ayudar a los equipos de seguridad y acelerar el despliegue de una capacidad avanzada y madura en detección y respuesta, eliminando los complejos procesos de compra, operación y mantenimiento de un conjunto de herramientas de seguridad las 24 horas.

Disponemos de las mejores tecnologías líderes del mercado, expertos en seguridad y procesos automatizados para garantizar una protección completa.

¿Qué te permite?

Este servicio te permitirá:

- Adoptar la mejor tecnología de **Detección y Respuesta en Endpoints (EDR) gestionada por equipos de analistas que han estado en una gran cantidad de incidentes.**
- Aumentar tu propia capacidad de **seguridad, tiempo medio de respuesta y anticipación frente a amenazas.**
- Obtener una capacidad de **respuesta efectiva,** rápida y completa a ciber brechas incluyendo capacidades DFIR (opcional).

Beneficios del servicio

Entrega, despliegue, configuración y soporte

Nuestro equipo se encargará de la entrega y configuración de la tecnología EDR, proporcionando una orientación personalizada y apoyo durante todo el proceso de implantación.

Monitorización y respuesta 24x7

Incluyendo el triaje, análisis, contextualización y validación de alertas de amenaza. El servicio incluye la contención remota y escalado de cualquier infracción de seguridad confirmada enriquecido con nuestra plataforma de inteligencia.

Threat Hunting proactivo

Nuestros *threat hunters* de élite aprovechan la inteligencia de amenazas más reciente para llevar a cabo búsquedas proactivas de amenazas basados en TTPs que han pasado desapercibidas y han logrado evadir los sistemas de seguridad.

Capacidad de respuesta ampliada

Detección y bloqueo de amenazas críticas en fase inicial, mitigaciones automáticas y capacidad DFIR (opcional) para una respuesta global.

Valor diferencial de Telefónica Tech

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

Reduce significativamente el riesgo de un ataque cibernético aumentando tu madurez de negocio.

Visualización de métricas y *ticketing* con nuestro equipo de analistas SOC a través de nuestro Portal de Clientes.

EQUIPO Y LOGROS

Nuestros equipos

- **+1.800** expertos en SecOps.
- **+1.500** certificaciones de seguridad.
- **+25** expertos en ***threat hunting.***

Logros

- Más de **300.000 dispositivos** monitorizados.
- **4.000 incidentes críticos** gestionados de media anualmente.
- Más de **160 atacantes monitorizados** y **565.000 campañas maliciosas** gestionadas anualmente.

MODELO COMERCIAL

MDR es un **servicio completo,** que consta de varias modalidades adaptadas a las principales necesidades de las organizaciones, con diferentes capacidades y opciones de protección de seguridad. El modelo comercial del servicio ofrece un precio cerrado mensual (evitando costes inesperados) según la modalidad elegida y en el número de *endpoints* a proteger.

Opcionalmente, el servicio se puede complementar con los servicios DFIR, mediante jornadas flexibles, para una respuesta completa.

PARTNERS RELACIONADOS

CROWDSTRIKE paloalto NETWORKS Microsoft WatchGuard

SERVICIOS RELACIONADOS

Digital Forensics & Incident Response

Solución de respuesta ante ciberincidentes y cibercrisis para minimizar daños y acelerar la recuperación operativa.

SIEM Management

Monitorización y correlación de eventos de seguridad con gestión de alertas 24x7, proporcionando una base sólida en la detección de amenazas de seguridad.

Cloud WiFi/SD-LAN

Optimiza el servicio con la conectividad integrada en tu sede, creando una solución SD-Branch regulada por las mismas políticas en toda la red y controlada desde un único dashboard

Contáctanos para empezar la transformación digital de tu organización.