DIGITAL FORENSICS & INCIDENT RESPONSE

Digital Forensics & Incident Response

¿CÓMO TE AYUDAMOS DESDE TELEFÓNICA TECH?

El servicio de Análisis Forense Digital y Respuesta a Incidentes ayuda a las organizaciones a responder eficazmente a los ciber-incidentes

El aumento y sofisticación de las ciber-amenazas actuales exige a las organizaciones una respuesta ágil y completa mediante capacidades avanzadas que reducen los impactos en el negocio tras una brecha de seguridad.

Estas amenazas, como los APT o *ransomware*, pueden derivar en altos impactos económicos, reputacionales, operativos o legales exigiendo una respuesta *end-to-end* que ayude a su contención, mitigación y recuperación.

Telefónica Tech mediante tecnologías de élite, equipos especializados y experiencia puede minimizar el impacto de los incidentes en las organizaciones, así como sobre sus procesos, operaciones y servicios críticos.

¿A QUIÉN VA DIRIGIDO ESTE SERVICIO?

Organizaciones de tamaño medio y grande que requieren una capacidad de respuesta rápida, eficaz y completa pero que desean **reducir la carga de costes en contratación de personal y herramientas** para las actividades DFIR.

Organizaciones con una capacidad ya establecida de respuesta ante incidentes que buscan externalizar o ampliar el **volumen de las operaciones de seguridad,** reduciendo costes de forma flexible.

Empresas y organismos públicos que han sufrido un incidente, brecha de seguridad o ciberataque y necesitan apoyo en la respuesta y contención mediante un equipo experto en: análisis *malware* y forense, coordinación de incidentes, inteligencia de amenazas, *threat hunting*, entre otros.

NUESTRA PROPUESTA DE VALOR

Nuestro servicio

La creación de un equipo de respuesta a incidentes capacitado y experimentado es un reto incluso para las organizaciones más maduras. Telefónica Tech incorpora esta capacidad a través del servicio de Análisis Forense Digital y Respuesta ante Incidentes (DFIR).

Nuestro principal objetivo es proporcionar ayuda, soporte y orientación a los equipos de TI y de seguridad en las brechas de seguridad, con capacidades diseñadas para abordar amenazas como: *ransomware*, compromiso de correo electrónico, denegaciones de servicio, fugas de información, atacantes *insiders* o APTs.

¿Qué te permite?

Este servicio te permitirá:

- **Asegurar la coordinación, contención, investigación y mitigación tras un incidente de seguridad** con el apoyo de un equipo experto basado en una metodología sólida.
- Aumentar tu ciberseguridad mediante **capacidades avanzadas de análisis *malware* y forense.**
- Obtener una **respuesta rápida, efectiva y exhaustiva** ante ciber-crisis para reducir tiempos de respuesta y recuperación.

Beneficios del servicio

Apoyo y soporte *end-to-end*

Respuesta completa durante el incidente y posteriormente al mismo, proporcionando una estrecha orientación en las acciones a realizar a nivel técnico y ejecutivo.

Basado en la Inteligencia de amenazas

Adoptamos un enfoque basado en la inteligencia de múltiples fuentes para obtener respuestas efectivas en las investigaciones, validando las alertas de compromiso y sirviendo de base para la búsqueda en profundidad de amenazas.

Gestor de incidentes dedicado

El gestor de incidentes proporciona apoyo integral y coordinación a tus equipos a lo largo de todo el ciclo de vida del incidente, incluyendo triaje inicial, recogida de evidencias y recomendaciones de contención, así como la asistencia para construir una estrategia eficaz de erradicación, recuperación y comunicación.

Equipo de élite

Equipo especializado compuestos por analistas forenses y de *malware, threat hunters*, gestores de incidentes, expertos en redes, analistas de inteligencia de amenazas y especialistas legales disponibles para darte asistencia en las investigaciones.

Valor diferencial de Telefónica Tech

Equipo global con soporte local y disponibilidad 24x7 para una rápida respuesta y contención.

Respuesta personalizada a cada situación, a través de un gestor de incidentes dedicado en modalidad remota o in-situ.

Tiempos de respuesta y descuentos comerciales al pre-comprar jornadas DFIR.

EQUIPO Y LOGROS

Nuestros equipos

- **+30** especialistas globales en **forense** y ***malware.***
- **+25** expertos en ***threat hunting.***
- **+70** analistas de ***inteligencia de amenazas.***

Logros

- +40 **incidentes *ransomware*** gestionados en los últimos 12 meses.
- 30 minutos: **tiempo medio de respuesta inicial** ante una crisis.
- **70.100 de *IoCs* investigados** anualmente y **19 millones de *IoCs*** almacenados en nuestra *TIP.*
- +8.800 **procesos de *threat hunting*** de media al año.

MODELO COMERCIAL

Basado en jornadas, nuestro servicio DFIR se adapta de forma flexible y personalizada a las necesidades de los clientes con asistencia en **remoto** u ***on-site*** y con disponibilidad 8x5 o 24x7 atendiendo cualquier situación.

Nuestra modalidad ***DFIR Retainer*** ofrece a los clientes la seguridad en la respuesta a incidentes con un *partner* de confianza como Telefónica Tech, mediante la **pre-compra anual de jornadas** incluyendo tiempos de respuesta, precios especiales pre-acordados con descuentos por volumen, conversión de jornadas no consumidas por otros servicios y protocolo de comunicación y actuación con los clientes.

PARTNERS RELACIONADOS

CROWDSTRIKE paloalto NETWORKS

SERVICIOS RELACIONADOS

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.

Managed Detection & Response

Monitorización completa de la seguridad de los *endpoints* gracias a la detección, contención y respuesta rápida a brechas de seguridad 24x7 con *Hunting* Proactivo continuo y asistencia experta ante cibercrisis, basado en la mejor tecnología EDR y XDR.

Contáctanos para empezar la transformación digital de tu organización.