Telefónica Tech

Revolucionando las operaciones de seguridad: Ciberinteligencia y el nuevo enfoque CTEM

FROST & SULLIVAN

Índice

01 La creciente superficie de ataque: La expansión del riesgo por la complejidad de IT y las vulnerabilidades de terceros

02 **El cambio de paradigma en ciberseguridad:** La gestión continua de la exposición a amenazas (CTEM)

03 **CTEM:** La clave para detectar y proteger activos críticos

04 Priorización inteligente en la era del exceso de información

05 **Ciberinteligencia:** el catalizador de la gestión continua de la exposición a amenazas

06 Potenciando la seguridad efectiva con ciberinteligencia aplicada a los programas CTEM

07 Protección integral con el enfoque CTEM de Telefónica Tech

01

La creciente superficie de ataque: La expansión del riesgo por la complejidad de IT y las vulnerabilidades de terceros

Las iniciativas de transformación digital, como la migración a la nube, el trabajo remoto y la adopción del Internet of Things (IoT), han ampliado significativamente las superficies de ataque de las organizaciones. A medida que aumenta la complejidad de los entornos TI, las organizaciones luchan por mantener sus operaciones de seguridad en línea con su huella digital.

Desafíos principales de ciberseguridad para las organizaciones en todo el mundo

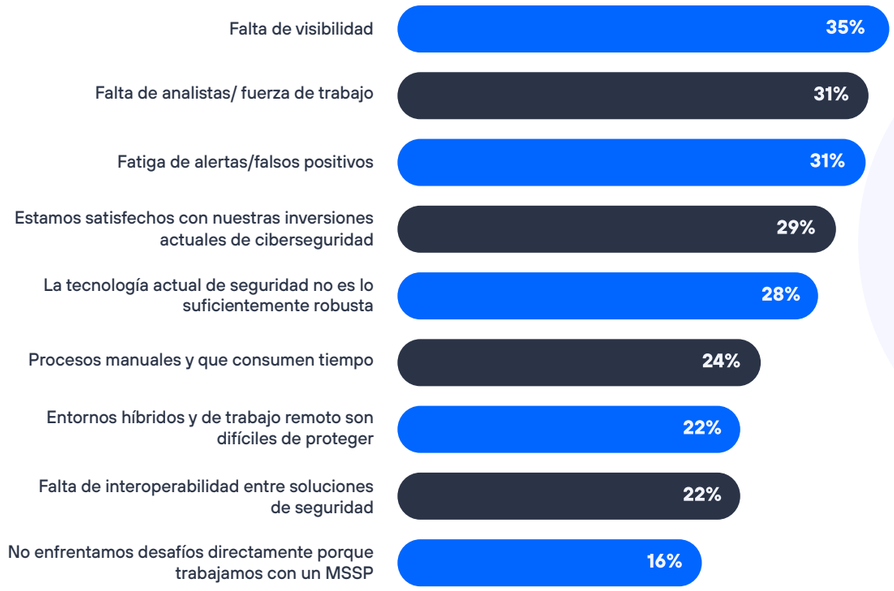


Figura 1. Fuente: *Voice of the Enterprise Security Customer de* ***Frost & Sullivan.***

El principal desafío de ciberseguridad para las organizaciones en todo el mundo es precisamente la falta de visibilidad según el estudio Voice of the Enterprise Security Customer de Frost & Sullivan. El creciente volumen de activos digitales conduce a más vectores de ataque, vulnerabilidades potenciales y, a su vez, al despliegue de más herramientas de seguridad. Esta avalancha de información abruma a las organizaciones, lo que provoca una **sobrecarga de alertas, falsos positivos y dificultades para priorizar las vulnerabilidades.** Cuando los analistas de seguridad carecen del contexto crítico necesario para evaluar los riesgos con precisión, la eficacia y la velocidad de respuesta ante incidentes de seguridad disminuyen.

Como resultado, **la frecuencia de ataques exitosos continúa en aumento.** Según los datos de la encuesta global Voice of the *Enterprise Security Customer* de Frost & Sullivan, las organizaciones sufren cada año un promedio de 26 ciberataques exitosos (es decir, ataques que generan consecuencias negativas de distintos tipos).

El auge de la inteligencia artificial agrava aún más esta situación, **permitiendo a los cibercriminales lanzar ataques cada vez más sofisticados y dañinos,** lo que se traduce en una **presión constante para reducir el tiempo medio de detección (MTTD) y el tiempo medio de respuesta (MTTR) a las amenazas.** Mientras las brechas de datos están adquiriendo una mayor gravedad; el coste promedio de una brecha es de €4,49 millones en 2024 *(IBM Cost of a Data Breach Report 2024).* Además, el Instituto Nacional de Ciberseguridad (INCIBE) señala que en 2023 se gestionaron más de 83.000 incidentes de ciberseguridad en España, un incremento del 24% respecto al año anterior. Sin embargo, no todo está perdido. Existe una vía para revolucionar las operaciones de seguridad con inteligencia y continuar ayudando a las organizaciones a mejorar su postura de seguridad de manera efectiva.

El punto de partida es reconocer que los autores de los ataques han evolucionado para explotar debilidades en activos digitales fuera de las redes tradicionales, como el shadow IT (dominios o APIs no monitorizados), errores de configuración en la nube y vulnerabilidades en la cadena de suministro.

Resultados de Incidentes de Seguridad - Top 10 Global

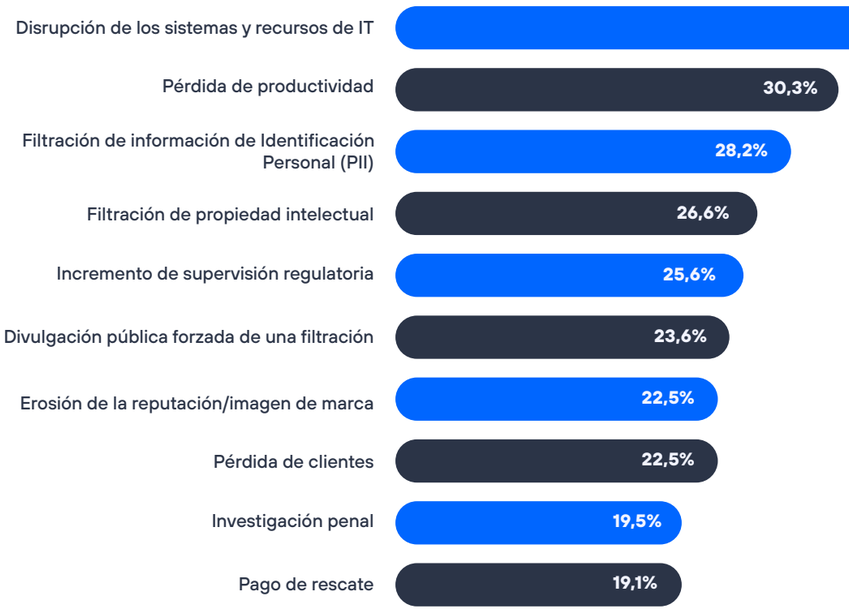


Figura 2. Fuente: *Encuesta Voice of the Enterprise Security Customer* de Frost & Sullivan

Las medidas de seguridad tradicionales, de carácter reactivo, pierden efectividad a medida que los ataques se vuelven más frecuentes y complejos. Las organizaciones que no protegen su huella digital externa se enfrentan a consecuencias graves, entre las que se incluyen interrupciones operativas, merma de ingresos, pérdida de clientes y daños duraderos a su reputación e imagen de marca (Figura 2).

En el Informe sobre el Estado de la Seguridad 2024 H1 publicado por Telefónica Tech, se identifican las principales brechas de seguridad ocurridas en el primer semestre de 2024, incluidas las que **afectaron a empresas en sectores importantes como el energético, bancario, asegurador y de retail,** entre muchos otros, subrayando las graves consecuencias de las filtraciones de datos y los ataques de *phishing,* especialmente su impacto en la confianza del cliente y la reputación digital.

En uno de los casos analizados, una entidad financiera, víctima de una campaña de *phishing* a gran escala, los atacantes lograron engañar a los destinatarios mediante correos electrónicos fraudulentos, lo que derivó en una revelación de credenciales sensibles. **Estas credenciales otorgaron a los atacantes acceso no autorizado a una base de datos de terceros que contenía información personalmente identificable y confidencial,** como nombres, direcciones, cuentas bancarias y números de seguridad social de aproximadamente 30 millones de clientes y empleados en España, Chile y Uruguay.

Una vez sustraídos, los datos fueron publicados en la dark web por un precio de venta de 2 millones de dólares. Las repercusiones no se limitaron a las pérdidas económicas, ya que la filtración incrementó significativamente los riesgos de robo de identidad y fraude para las personas afectadas.

A pesar de los esfuerzos de respuesta de la entidad financiera, el incidente generó serias dudas sobre la idoneidad de las medidas de seguridad existentes y las prácticas de gestión de terceros. **Esto provocó una erosión de la confianza del cliente y un daño notable a la reputación de la organización.**

Este tipo de ataques pone de manifiesto la necesidad urgente de implementar estrategias de seguridad proactivas basadas en ciberinteligencia que incluyan entre sus objetivos:

- Reducir los riesgos relacionados con el shadow IT, configuraciones incorrectas en la nube y exposición de datos sensibles.
- Proteger la reputación de marca.
- Minimizar el impacto de incidentes como fugas de datos, suplantación de identidad o vulnerabilidades explotables.

4,49 millones €

es el coste promedio de una brecha en 2024.

Fuente: IBM Cost of a Data Breach Report 2024

+24% de incidentes

a gestionar respecto el año 2023.

Fuente: Instituto Nacional de Ciberseguridad (INCIBE)

02

El cambio de paradigma en ciberseguridad: La gestión continua de la exposición a amenazas (CTEM)

El término ***Continuous Threat Exposure Management*** (CTEM, que se traduce al español como gestión continua de exposición a amenazas) refleja una evolución de las prácticas tradicionales de ciberseguridad, moviéndose de enfoques reactivos a modelos proactivos y dinámicos. CTEM permite a las organizaciones **identificar, evaluar y mitigar continuamente las ciberamenazas** en evolución, fortaleciendo su resiliencia y capacidad de respuesta frente a ataques. Este enfoque combina tecnologías avanzadas, como la inteligencia artificial y la automatización, con procesos iterativos que priorizan los riesgos más críticos en tiempo real, lo que permite a las organizaciones mantener una monitorización constante y adaptarse rápidamente a nuevas amenazas. Es especialmente relevante para sectores como finanzas, salud, telecomunicaciones y energía, donde las interrupciones o fallos de seguridad pueden tener consecuencias graves.

CTEM busca proporcionar una visión clara y actualizada de las vulnerabilidades de seguridad, considerando tanto activos digitales internos como externos, con el objetivo de mantener una postura de ciberseguridad sólida y adaptable frente a amenazas en constante evolución. En este sentido, CTEM se basa en un proceso cíclico compuesto por varias fases interrelacionadas, que se retroalimentan a medida que el programa avanza, como se puede ver el gráfico.

Programa CTEM

CTEM no es una herramienta. Es un proceso.

Un programa de cinco pasos:

- Ciclos repetitivos simultáneos
- Exposiciones parcheables y no parcheables
- Validación de prioridades
- Movilizar primero, remediar después

Proceso cíclico y adaptable para reducir la exposición a las amenazas en este mundo en constante cambio

1 **DEFINICIÓN:** Como primer paso, las organizaciones deben **definir sus superficies de ataque y evaluar la importancia de cada activo.** Este proceso, que debería ser continuo, establece un marco para las evaluaciones de exposición, priorizando el impacto en el negocio sobre la gravedad de la amenaza. También asegura la alineación con los objetivos organizativos al aclarar qué, por qué y cómo se evaluarán los activos, fomentando la colaboración entre departamentos.

2 **DESCUBRIMIENTO:** Tras la definición del alcance, el siguiente paso es identificar los activos, vulnerabilidades y amenazas presentes en la organización. Para ello, se emplean herramientas y métodos como el descubrimiento de superficie de ataque *(attack surface discovery)*, evaluaciones de vulnerabilidad y pruebas de penetración. Estas actividades permiten mapear y entender los vectores de ataque más relevantes. Adicionalmente, el modelado de amenazas juega un papel clave al proporcionar una representación estructurada de los posibles escenarios de ataque y sus consecuencias. **Este enfoque asegura un entendimiento detallado del entorno digital y sus riesgos asociados.**

3 **PRIORIZACIÓN:** Una vez identificado el panorama de activos y amenazas, es esencial clasificar las vulnerabilidades en función de su impacto y la probabilidad de explotación. La priorización ayuda a enfocar los esfuerzos de los analistas de ciberseguridad en los problemas más críticos, maximizando así la eficiencia operativa. Este enfoque permite optimizar la gestión de incidentes y reducir los riesgos asociados a vulnerabilidades de alto impacto. Al priorizar adecuadamente, **se garantiza que los recursos se asignen de manera estratégica, contribuyendo a una protección más eficaz de los activos clave de la organización.**

4 **VALIDACIÓN:** Esta fase implica realizar pruebas controladas para descubrir y validar brechas de seguridad antes de que puedan ser explotadas por atacantes. **La validación confirma si los riesgos son reales, evalúa la efectividad de las técnicas de mitigación y garantiza que la respuesta sea rápida y efectiva.** Se emplean métodos manuales y automáticos, como ejercicios de red teaming, pruebas de penetración y simulaciones de ataques, asegurando que las medidas de ciberseguridad sean eficaces y permitan mejoras continuas para reforzar la seguridad. Así, según entrevistas de Frost & Sullivan, un responsable de seguridad declara de media declaró que el proceso manual para probar una aplicación web era de aproximadamente dos semanas en su organización. Gracias a la implementación de evaluaciones de vulnerabilidad y pruebas de penetración automatizadas, en conjunto con escaneo activo de aplicaciones, el tiempo de análisis de aplicaciones web se redujo significativamente y liberó al responsable para trabajar en otros proyectos.

5 **MOVILIZACIÓN:** En esta fase, se despliegan los recursos necesarios para mitigar las amenazas y vulnerabilidades identificadas. Esto incluye la implementación de nuevos controles de seguridad, la mejora de los existentes o la adaptación de procesos comerciales para reducir la exposición. La movilización es un esfuerzo constante, ya que las nuevas amenazas y los cambios en el panorama digital exigen actualizaciones constantes al proceso CTEM. **Esto garantiza que la organización se mantenga proactiva en la gestión de riesgos.** Este incremento de la eficiencia tiene como consecuencia un uso más eficiente del presupuesto de seguridad: de acuerdo a entrevistas realizadas por Frost & Sullivan, las organizaciones que implementan un programa CTEM reducen en promedio un 30% sus costes de *pentesting* gracias al escaneo activo y la automatización.

03

CTEM: La clave para detectar y proteger activos críticos

Las fases de definicion y descubrimiento en un programa CTEM son fundamentales, ya que establecen claramente los objetivos y el alcance del programa, además de identificar los activos críticos que requieren protección.

Sin embargo, estas fases suelen representar un desafío importante para las organizaciones. Para muchas de ellas, resulta complicado identificar eficazmente los activos digitales en entornos híbridos y multi-nube, especialmente cuando estos incluyen dispositivos IoT, OT y sistemas de terceros. Esta dificultad se agrava aún más cuando las organizaciones dependen de métodos obsoletos, como el uso de hojas de cálculo de Excel.

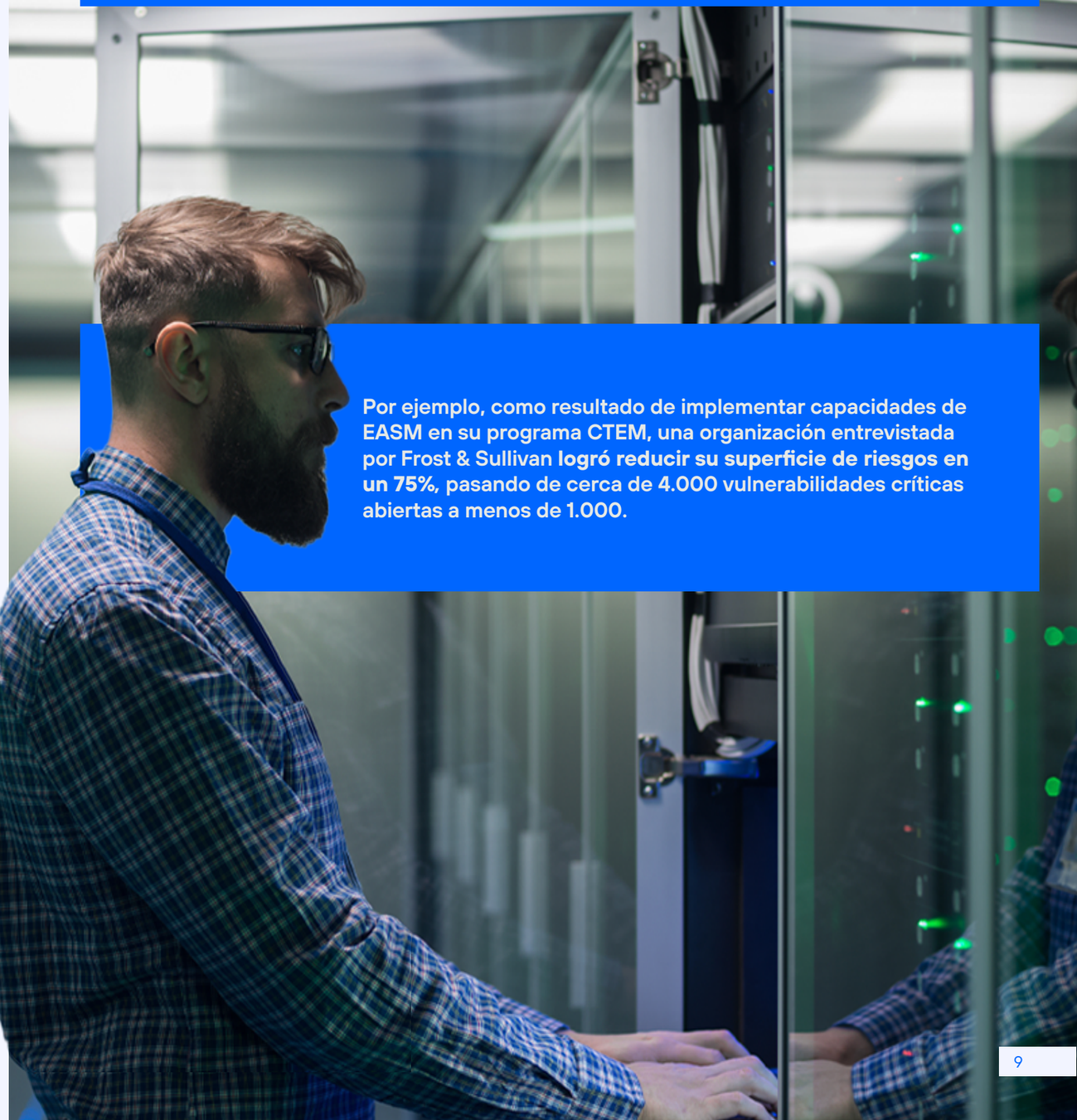
La gestión manual de activos, que implica rastrear sistemas expuestos a la web, etiquetar activos, realizar auditorías y colaborar con los equipos de TI, es un proceso laborioso, propenso a errores e insostenible en los entornos dinámicos actuales. Esta problemática se ve intensificada por la sobrecarga de trabajo derivada de la escasez generalizada de personal especializado en seguridad.

No es de extrañar que el desafío más significativo para las organizaciones sea la falta de visibilidad sobre su entorno digital (Figura 1). Sin una monitorización continua desde perspectivas internas y externas, las organizaciones carecen del contexto necesario para identificar todos sus activos críticos y, en consecuencia, comprender su superficie de ataque y los riesgos asociados. Por otro lado, los activos intangibles, como la propiedad intelectual, los datos de clientes, las estrategias comerciales y la reputación de la marca, son fundamentales para el éxito y la competitividad de una organización.

Estos activos no solo representan un valor significativo en términos económicos, sino que también son esenciales para diferenciarse en el mercado. Esto los convierte en objetivos especialmente atractivos para los ciberatacantes, quienes buscan robar información sensible y valiosa, como secretos comerciales, fórmulas patentadas o bases de datos de clientes. **La pérdida o el compromiso de estos activos intangibles puede generar daños irreparables a la reputación de la empresa, pérdida de confianza por parte de los clientes y, en última instancia, un impacto f inanciero considerable.**

En este contexto, es esencial que un programa de CTEM abarque tanto los activos intangibles como los tradicionales. **Elementos como marcas, perfiles en redes sociales, directivos clave (VIP) y propiedad intelectual deben ser gestionados de forma integral junto con otros activos tradicionales para garantizar una protección completa contra ciberamenazas.**

Apoyándose en capacidades como *External Attack Surface Management* (EASM/ASM), *Digital Risk Protection* (DRP) y *Cyber Threat Intelligence* (CTI), las organizaciones pueden obtener mayor visibilidad e identificar, priorizar y mitigar los riesgos más fácilmente, protegiendo así sus activos críticos y preservando la confianza de sus clientes en un panorama de amenazas cada vez más sofisticado.



Por ejemplo, como resultado de implementar capacidades de EASM en su programa CTEM, una organización entrevistada por Frost & Sullivan logró reducir su superficie de riesgos en un 75%, pasando de cerca de 4.000 vulnerabilidades críticas abiertas a menos de 1.000.

04

Priorización inteligente en la era del exceso de información

Ante la sobrecarga de información, las organizaciones se enfrentan a serias dificultades para priorizar alertas, amenazas y vulnerabilidades.

El exceso de ruido, los falsos positivos frecuentes y los volúmenes abrumadores de datos dificultan que los equipos de seguridad identifiquen qué amenazas son reales (ver Figura 1). **Muchos responsables de seguridad recurren a numerosas fuentes abiertas para investigar brechas y amenazas de *ransomware*. Sin embargo, la falta de contexto y oportunidades para integrar esta información complica el proceso, generando retrasos en la toma de decisiones.**

Además, el acceso limitado a foros de la *dark web* suele impedir una evaluación completa de las amenazas y filtraciones de datos, lo que obliga a los equipos a invertir semanas de trabajo y múltiples analistas para completar investigaciones. La situación se complica aún más cuando los responsables de seguridad deben priorizar vulnerabilidades en una amplia variedad de activos, pero carecen de la validación adecuada. Esto puede conducir a una asignación ineficiente de recursos y respuestas atrasadas.

Es en este punto donde un programa de CTEM, y en particular en las fases de descubrimiento y priorización, cobra relevancia. **Incluir servicios de *digital risk protection* (DRP) es fundamental en la fase de descubrimiento y priorización de un programa de CTEM.** Estos servicios proporcionan visibilidad sobre las amenazas digitales a las que se enfrentan las organizaciones.

Mediante la monitorización constante de activos tangibles e intangibles, como redes sociales, dominios y otros activos expuestos, DRP identifica amenazas y riesgos potenciales que podrían ser explotados por actores maliciosos. Analizando datos sobre amenazas emergentes y tendencias, DRP permite a las organizaciones priorizar sus esfuerzos de mitigación, centrando la atención en los riesgos más críticos que podrían impactar sus operaciones.

Esto se traduce en una respuesta más ágil ante incidentes y asegura que las medidas de seguridad se alineen con las amenazas más relevantes.

Por tanto, un servicio de DRP optimiza la efectividad del programa de CTEM en dos puntos clave: visibilidad y priorización de amenazas.

05

Ciberinteligencia: el catalizador de la gestión continua de la exposición a amenazas

En el panorama actual de ciberamenazas en constante evolución, las organizaciones necesitan adaptar un enfoque proactivo para gestionar su exposición. La aplicación de un programa CTEM emerge como una estrategia fundamental y la ciberinteligencia se revela como su principal catalizador. La creciente sofisticación de los ataques exige una ciberinteligencia de última generación que proporcione contexto crítico y procesable. Como, por ejemplo, el nivel de explotabilidad de los activos; la actividad de cibercriminales tanto a nivel general como focalizada en industrias específicas; y conocimiento sobre herramientas, tácticas, y tecnología usada por los actores maliciosos. Esta información permite a las organizaciones priorizar sus activos, vulnerabilidades y esfuerzos de seguridad en función del riesgo real.

Por ejemplo, mediante el uso de CTI dentro de un programa CTEM, un responsable de seguridad puede identificar y analizar:

- Una **vulnerabilidad de día cero** que está siendo aprovechada activamente por grupos de *ransomware*
- Que dicho grupo **está enfocado en atacar al sector de su organización**
- **Las tácticas y las técnicas particulares** que el grupo de *ransomware* está utilizando
- Detalles de **cómo otras empresas similares resolvieron esta u otras situaciones semejantes**

Gracias a CTI, los responsables de seguridad pueden mitigar estos riesgos mediante la aplicación de parches y la resolución de problemas de configuración, y recibir recomendaciones de soluciones de seguridad específicas. Además, la información proveniente de CTI provee un marco central para la integración y automatización de la seguridad a través de plataformas de *security information and event management* (SIEM), y *security orchestration, automation and response* (SOAR).

De acuerdo con estudios realizados de Frost & Sullivan, el 51% de las organizaciones en todo el mundo ya tienen un proveedor de CTI designado. **El uso de CTI dentro de un programa CTEM, perfecciona todas las fases del proceso, especialmente las de descubrimiento, priorización y movilización.** Según entrevistas de Frost & Sullivan a usuarios de servicios de CTI y DRP, los responsables de seguridad pueden reducir el tiempo de enriquecimiento y análisis de amenazas hasta en un 50% en comparación a organizaciones que no usan esta tecnología.

51% de las organizaciones
ya tienen un proveedor de CTI designado

Fuente: Voice of the Enterprise Security Customer de Frost & Sullivan.

Hasta un 50%
reducción del tiempo de enriquecimiento y análisis de amenazas en organizaciones que usan tecnologías de CTI y DRP

06

Potenciando la seguridad efectiva con ciberinteligencia aplicada a los programas CTEM

Como hemos visto, un programa de CTEM impulsado por ciberinteligencia, que integre ASM, CTI, DRP, *Vulnerability Management* (VM), seguridad ofensiva y servicios de seguridad gestionados ofrece beneficios únicos que refuerzan la postura de seguridad de una organización.

- **Visibilidad integral de la superficie de ataque:** CTEM ayuda a mejorar la visibilidad de la exposición de las empresas y aumenta así la eficiencia de la detección de amenazas. Según entrevistas realizadas por Frost & Sullivan a CISOs y responsables de seguridad de diversas organizaciones, tras la implementación de un programa CTEM, 2 de cada 4 de estas aumentaron entre un 60% y un 90% sus tasas de detección de sitios de phishing con la ayuda de servicios de CTI y DRP, contribuyendo a eliminar contenido malicioso y protegiendo la integridad de su marca. Además, una de las organizaciones entrevistadas reportó un aumento del 80% en el descubrimiento de activos tras desplegar una solución de ASM, lo que les permitió incorporar nuevos activos de manera efectiva y mitigar vulnerabilidades de forma proactiva.

- **Anticipación y respuesta mejoradas mediante ciberinteligencia:** CTEM aumenta significativamente la productividad de las organizaciones mediante la optimización de los procesos de seguridad. La inteligencia en tiempo real y la detección proactiva de riesgos reducen el tiempo necesario para identificar y responder a amenazas: de acuerdo con entrevistas realizadas por Frost & Sullivan a CISOs que han implementado CTI en el último año, más del 90% experimentó una mejora en el tiempo medio de respuesta ante amenazas (MTTR), con incrementos que van desde un 30% a un 165% dependiendo de la organización.

- **Minimización del impacto financiero:** Gracias a la aplicación de un enfoque CTEM se produce una mejor priorización de inversiones en ciberseguridad. Esto permite a las organizaciones centrarse en las áreas que realmente requieren atención, evitando gastos innecesarios en soluciones que no abordan sus riesgos más críticos. Una de las organizaciones entrevistadas por Frost & Sullivan ahorró cerca de 300.000€ en el plazo de un año al utilizar una combinación de CTI y DRP para prevenir fraudes mediante el uso de información sobre tarjetas de crédito comprometidas. Al contar con una visión clara de las amenazas a las que se enfrentan, las empresas pueden optimizar sus recursos, reducir el tiempo de respuesta ante incidentes y, en última instancia, minimizar el impacto financiero de los posibles incidentes que puedan sufrir.

En resumen, un programa de CTEM impulsado por ciberinteligencia, que integre ASM, CTI, DRP, VM, seguridad ofensiva y servicios de seguridad gestionados, no solo optimiza las capacidades de ciberdefensa, sino que también permite una mayor resiliencia ante amenazas, reduciendo riesgos y mejorando la capacidad de respuesta ante eventos de seguridad.

Hasta un 165% mejora del tiempo medio de respuesta ante amenazas (MTTR) después de 12 meses de implementar CTI

Fuente: Según entrevistas de Frost & Sullivan

07

Protección integral con el enfoque CTEM de **Telefónica Tech**

En definitiva, los responsables de ciberseguridad hoy en día se enfrentan a múltiples desafíos como hemos visto (fatiga de alertas, aumento de la frecuencia de los ataques y mayor sofisticación, entre otros). Lo que supone que los responsables de ciberseguridad deben apoyarse en socios tecnológicos como managed security service providers (MSSPs) para superar estos problemas. De acuerdo con datos de la encuesta *Voice of the Enterprise Security Customer* de Frost & Sullivan, casi el 70% de las organizaciones han subcontratado parcial o completamente sus operaciones de ciberseguridad a proveedores externos, lo que muestra la importancia de los MSSPs para mejorar la resiliencia de ciberseguridad.

Telefónica Tech es el aliado ideal para implementar un programa efectivo de *Continuous Threat Exposure Management* (CTEM) porque combina tecnologías líderes con la experiencia comprobada de su equipo de analistas en seguridad. Su propuesta integral abarca desde la gestión de la superficie de ataque hasta inteligencia de amenazas, simulaciones de ataques y estrategias ofensivas controladas, todo basado en el marco CTEM.

70%

de las organizaciones han subcontratado sus operaciones de ciberseguridad a proveedores externos.

Fuente: datos de la encuesta Voice of the Enterprise Security Customer de Frost & Sullivan.

Además, el portafolio de servicios de Telefónica cubre todas las fases del proceso, desde la identificación y priorización de riesgos hasta la remediación automatizada, garantizando una postura de seguridad más sólida y la reducción efectiva de exposiciones críticas.

La Plataforma NextDefense de Telefónica centraliza capacidades de CTI, DRP, VM, ASM y simulaciones de ataques, entre otras, permitiendo a las organizaciones pasar de estrategias de seguridad reactivas a proactivas.

Incidentes como los que se han visto en este escrito destacan cómo estas soluciones pueden jugar un papel crítico, tanto en la prevención como en la mitigación. Los responsables de ciberseguridad deben aprovechar las capacidades de CTI y DRP, para identificar campañas de *phishing* en sus primeras etapas, detectando dominios maliciosos y actividades sospechosas en la *dark web* antes de que resulten en daños significativos. De manera similar, herramientas de seguridad como ASM y VM ofrecen monitorización continua de los activos digitales y vulnerabilidades, ayudando a asegurar los sistemas de terceros. Incluso después de una brecha de datos, las soluciones DRP sirven para mitigar aún más los riesgos rastreando, investigando y abordando las credenciales filtradas en la *dark web*.

En general, estas soluciones optimizan la visibilidad de la superficie de ataque y mejoran la anticipación y respuesta ante amenazas. Esto no solo minimiza el impacto financiero en las empresas, sino que, lo más importante, asegura la confianza de los clientes.

Acerca de Telefónica Tech

Telefónica Tech es un integrador de tecnología global, líder en transformación digital. La compañía cuenta con una amplia oferta de servicios y soluciones tecnológicas integradas de Ciberseguridad, Cloud, IoT, Big Data o Inteligencia Artificial. En todas estas verticales, contamos tanto con nuestras propias tecnologías como también con los mejores ecosistemas de partners estratégicos y así nos lo reconocen tanto los analistas de la industria como nuestros clientes. Y todo ello es posible también gracias a nuestros hubs en España, UK, Alemania, Brasil e Hispam llegamos a más de 5,5 millones de clientes en más de 175 países.

Acerca de Frost & Sullivan

Frost & Sullivan, the growth pipeline company, enables clients to accelerate growth and achieve best in-class positions in growth, innovation, and leadership. The company's Growth Pipeline as a Service provides the CEO and the CEO's Growth Team with transformational strategies and best-practice models to drive the generation, evaluation, and implementation of powerful growth initiatives. Frost & Sullivan leverages over 60 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from more than 40 offices on six continents

Si tienes alguna duda y quieres saber más sobre cómo podemos ayudarte, por favor:

→ **CONTÁCTANOS**

Telefónica Tech

FROST & SULLIVAN