Threat Intelligence

Convierte la exposición digital en inteligencia accionable.

La amenaza empieza fuera

La superficie de ataque digital de una organización ya no se limita a sus sistemas internos. Hoy, los riesgos se originan en entornos externos: credenciales filtradas, suplantaciones de identidad, menciones sensibles en foros clandestinos o la dark web. Estos elementos, si no se detectan a tiempo, pueden convertirse en puertas de entrada para ciberataques dirigidos.

La inteligencia de amenazas permite a las organizaciones anticiparse, actuar con rapidez y proteger sus activos más críticos antes de que el daño ocurra. Detectar lo que otros no ven es clave para mantenerse un paso por delante.

Lo que se filtra hoy, puede explotarse mañana

Cada día se publican millones de datos en fuentes abiertas y clandestinas. Lo que hoy parece una filtración menor, mañana puede ser la puerta de entrada a un ataque dirigido. Las cifras que presentamos no solo reflejan una tendencia creciente, sino también la urgencia de actuar con herramientas que permitan anticiparse, priorizar y responder con eficacia.

3.200m
de credenciales fueron expuestas en 2024, un 33% más que en 2023.

65%
de los ciberdelincuentes usan datos filtrados en la dark web para planear sus ataques.

70%
de las empresas han sido víctimas de suplantación de marca en campañas de phishing o fraude digital.

49%
de las empresas sufrieron intentos de fraude financiero donde un directivo fue suplantado.

2,5x
más probable de tener un ciberataque, cuando las credenciales empresariales están en la dark web.

Nuestra visión sobre un servicio de *Threat Intelligence* eficaz

Creemos que la inteligencia de amenazas debe ser un motor estratégico, no solo una fuente de información. Un servicio eficaz debe integrarse en la toma de decisiones, adaptarse al contexto del cliente y evolucionar con sus necesidades. Por eso, consideramos que los siguientes principios garantizan valor real y sostenido.

Orientado a la acción

La inteligencia debe traducirse en decisiones concretas. No basta con saber qué ocurre: hay que saber qué hacer con esa información.

Contextualizado al negocio

Cada organización tiene un perfil de riesgo distinto. La inteligencia debe adaptarse a su sector, activos críticos y prioridades estratégicas.

Multifuente y enriquecida

Debe combinar fuentes abiertas, comerciales, técnicas y clandestinas para ofrecer una visión completa y precisa del entorno de amenazas.

Integrable y automatizable

La inteligencia debe incorporarse fácilmente en las herramientas de seguridad existentes para mejorar la detección y respuesta.

Escalable y continua

El servicio debe evolucionar con el cliente, adaptándose a nuevos riesgos, tecnologías y necesidades operativas.

Con impacto estratégico

La inteligencia debe apoyar decisiones de inversión, priorización de riesgos y comunicación con stakeholders clave.

Nuestros servicios

KPMG ofrece un servicio integral de Threat Intelligence que permite conocer y reducir la exposición externa en la Clear, Deep y Dark Web. Entregamos información contextualizada y accionable para anticiparse a los atacantes y proteger los activos más críticos.

Vigilancia Digital

Servicio que monitoriza continuamente la presencia digital de la organización en fuentes abiertas y clandestinas con el fin de detectar de forma temprana cualquier abuso, filtración o mención sensible que pueda derivar en un incidente de seguridad.

- Monitorización de credenciales expuestas en repositorios públicos y dark web.
- Vigilancia de registros de dominios sospechosos y suplantaciones de marca.
- Supervisión de redes sociales, foros y marketplaces.
- Identificación de fugas de información confidencial.
- Generación de alertas accionables y recomendaciones de mitigación.

Threat Modeling

Diseñamos una visión táctica de cómo podría ser atacada la organización, anticipando escenarios de riesgo y fortaleciendo la postura defensiva.

- Identificación de actores relevantes y sus técnicas habituales (TTPs).
- Evaluación de activos críticos y vectores de ataque más probables.
- Desarrollo de escenarios de amenaza realistas basados en inteligencia externa.
- Informe estratégico con riesgos priorizados y medidas de mitigación.
- Alineación con marcos como MITRE ATT&CK y TIBER-EU.

Huella Digital VIP

Evaluación puntual del nivel de exposición digital de ejecutivos y personal clave, identificando riesgos específicos que afectan a figuras estratégicas, facilitando acciones preventivas.

- Análisis de datos personales y corporativos expuestos en fuentes abiertas y cerradas.
- Detección de perfiles falsos, dominios similares y campañas de engaño.
- Evaluación de amenazas dirigidas contra VIPs en foros clandestinos.
- Informe personalizado con recomendaciones para reducir la exposición.
- Trato confidencial y seguro de lo identificado.

Threat Intelligence en Pruebas de Penetración

Aportamos inteligencia experta a ejercicios de Red Teaming y pentesting, alineando los escenarios con amenazas reales y actuales. Este servicio potencia la efectividad de las pruebas y asegura su relevancia.

- Diseño de escenarios basados en actores y campañas activas.
- Provisión de inteligencia para guiar el ejercicio.
- Cumplimiento de marcos como TIBER-EU como proveedor independiente.
- Apoyo durante la ejecución con hallazgos en tiempo real.
- Análisis post-ejercicio con contextualización de resultados y recomendaciones.

Beneficios potenciales

- Reducción del impacto operativo, legal y reputacional.
- Protección proactiva de la reputación corporativa y ejecutivos
- Mejora de la capacidad de anticipación y respuesta
- Refuerzo de pruebas de seguridad con inteligencia real

¿Por qué KPMG?

Presencia global

Contamos con más de 265.000 profesionales multidisciplinares en 143 países, siendo 9.300 expertos en ciberseguridad y 45.000 basados en riesgos.

Diferencial

Combinamos una amplia experiencia, con profundos conocimientos del negocio y sector, con profesionales que les apasiona ayudar a proteger y fomentar la confianza entre las partes interesadas.

Comprometida

Las relaciones con nuestros clientes se basan en la confianza mutua y el compromiso a largo plazo para proporcionar estrategias eficaces y eficientes.

Contactos

Sergi Gil
Partner
MDR Lead
T: +34 636 189 222
E: sergigil@kpmg.es

Paúl Martínez
Senior Manager
MDR BD Lead
T: +34 699 410 959
E: paulricardomartinez@kpmg.es

José Sosa
Senior Manager
MDR Tech Lead
T: +34 636 739 221
E: josemiguelsosa@kpmg.es

Sergio Galán
Senior Manager
Threat Intel, Hunting & IR Tech Lead
T: +34 606 286 219
E: sgalan1@kpmg.es

kpmg.es