Managed Detection and Response

Transforma tu defensa a una proactiva, inteligente y efectiva.

La urgencia de anticiparse a las amenazas

La ciberseguridad moderna exige mucho más que tecnología. En un entorno marcado por la sofisticación de los ataques, la presión regulatoria y la escasez de talento especializado, las organizaciones necesitan una capacidad de defensa activa, continua y experta.

Lo que está en juego

Las organizaciones se enfrentan a un escenario de riesgo digital cada vez más complejo, donde los ataques no solo son más frecuentes, sino también más difíciles de detectar y contener:

81,6%
de las organizaciones sufrieron al menos un ciberataque exitoso en el último año. La frecuencia de incidentes sigue siendo elevada y muchas empresas no logran detectarlo a tiempo.

267
días es el tiempo medio que tarda una organización en completar el ciclo de respuesta a un incidente. La lentitud en la detección y contención expone a las organizaciones a daños prolongados.

66%
de las organizaciones reportan carencias críticas en habilidades de ciberseguridad. La falta de talento especializado limita la capacidad de respuesta y aumenta la dependencia de servicios externos.

47%
de las empresas consideran que los avances en IA potencian las capacidades de los atacantes. El uso GenAI está facilitando campañas de phishing, fraude y manipulación digital a gran escala.

54%
de las grandes entidades identifican la cadena de suministro como su principal riesgo de ciberseguridad. La falta de visibilidad sobre terceros multiplica el impacto de los ataques.

Nuestra visión sobre un servicio MDR eficaz

Ante un entorno de amenazas cada vez más sofisticado, un servicio de Managed Detection and Response (MDR) debe ir más allá de la simple supervisión técnica. Las organizaciones necesitan una solución que combine capacidades avanzadas con visión estratégica, que actúe de forma proactiva y que se integre con sus operaciones sin fricciones. Un servicio MDR eficaz debe ofrecer:

Monitorización continua 24x7
Monitorización permanente de los activos críticos de la organización, con capacidad para identificar eventos relevantes en tiempo real y activar mecanismos de respuesta sin interrupciones.

Detección avanzada de amenazas
Uso de telemetría enriquecida, correlación de eventos y análisis contextual para identificar patrones de ataque, incluso aquellos que evaden controles tradicionales.

Respuesta inmediata ante incidentes
Capacidad de contener, escalar y gestionar incidentes de forma ágil y coordinada, minimizando el impacto operativo y facilitando la recuperación.

Threat Intelligence integrada
Acceso a inteligencia de amenazas actualizada, contextualizada y accionable, que permite anticiparse a campañas, actores y técnicas emergentes.

Threat Hunting proactivo
Actividades de búsqueda activa de amenazas en el entorno del cliente, incluso en ausencia de alertas, para detectar actividad maliciosa latente y reducir el tiempo de permanencia del atacante.

Enfoque estratégico de vulnerabilidades
Identificación, priorización y seguimiento de vulnerabilidades relevantes, alineadas con el contexto de negocio y el nivel de exposición real de la organización.

Cobertura agnóstica y escalable
Capacidad de operar sobre cualquier tecnología, arquitectura o sector, sin necesidad de sustituir herramientas existentes ni limitar el alcance del servicio.

Visibilidad centralizada y accionable
Un único punto de control que permite visualizar el estado de seguridad, entender el contexto de los eventos y tomar decisiones informadas de forma rápida.

Nuestros servicios

Ofrecemos detección, investigación y respuesta continua frente a amenazas, adaptándonos a cualquier entorno tecnológico. Nuestro servicio MDR combina tecnología avanzada, inteligencia de amenazas y experiencia operativa. Está estructurado en tres bloques clave para proteger tu negocio de forma proactiva.

Threat Detection and Response

Detectamos y contenemos amenazas antes de que generen impacto, combinando tecnología avanzada, analistas expertos e inteligencia de amenazas. Nuestro enfoque permite actuar de forma ágil y eficaz, incluso ante ataques que evaden los controles tradicionales, asegurando una defensa activa y continua.

- **Monitorización y respuesta gestionada 24x7**: Supervisión permanente de los activos críticos, con activación inmediata de mecanismos de contención y soporte experto en la gestión de incidentes.
- **Eficiencia de casos de uso**: Validación y optimización de los casos de uso configurados en las plataformas de seguridad, asegurando que las detecciones sean relevantes y efectivas.
- **Análisis dinámico de malware**: Evaluación en tiempo real de archivos sospechosos mediante sandboxing y técnicas de ingeniería inversa para identificar comportamientos maliciosos.
- **Threat Hunting bajo demanda**: Búsqueda activa de amenazas latentes mediante hipótesis alineadas con el contexto del negocio, utilizando telemetría avanzada y análisis de comportamiento.

Security Platform Administration

Gestionamos e integramos las plataformas de seguridad para maximizar su eficacia operativa y adaptarlas a necesidades específicas. Nuestro enfoque agnóstico y flexible permite operar en entornos cloud, on-prem o híbridos, asegurando una operación fluida, escalable y alineada con los objetivos del negocio.

- **Administración de consolas**: Gestión operativa de SIEM, SOAR, EDR, XDR, NDR y otras plataformas, incluyendo su mantenimiento, actualización y optimización.
- **Integración de fuentes de datos**: Conexión de múltiples sistemas mediante APIs, normalización de datos y enriquecimiento de eventos para mejorar la visibilidad y la detección.
- **Despliegue de agentes**: Instalación y configuración de agentes de seguridad en endpoints, servidores y dispositivos de red, asegurando cobertura completa y continua.
- **Configuración de cuadros de mando**: Diseño de dashboards personalizados para equipos técnicos y ejecutivos, facilitando la toma de decisiones con indicadores clave y alertas priorizadas.

Threat Modelling

Diseñamos estrategias de detección adaptadas al contexto del cliente, anticipándonos a las amenazas mediante inteligencia contextual y análisis de comportamiento. Este bloque permite entender cómo operan los atacantes, priorizar riesgos y fortalecer la postura defensiva con reglas de detección efectivas y personalizadas.

- **Investigación de Threat Intel y elaboración de informes**: Análisis de campañas, actores y técnicas emergentes, con generación de informes accionables para guiar la defensa.
- **Librería de casos de uso**: Desarrollo y mantenimiento de un catálogo de detecciones adaptado al entorno del cliente, alineado con marcos como MITRE ATT&CK.
- **Diseño y despliegue de reglas de detección**: Creación de reglas proactivas y bajo demanda, integradas en las plataformas de seguridad para identificar patrones de ataque específicos.
- **Informe de modelado de amenazas**: Evaluación de la exposición de la organización frente a distintos vectores de ataque, priorizando riesgos y proponiendo medidas de mitigación.

¿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