Threat Hunting

Descubre lo que los controles no ven

La amenaza no siempre genera alertas

Los atacantes más sofisticados diseñan sus técnicas para evadir los controles tradicionales. Muchas amenazas permanecen ocultas durante semanas o meses, sin ser detectadas por herramientas. El Threat Hunting permite descubrir estos compromisos latentes antes de que generen impacto.

Lo que está pasando

Las siguientes cifras ilustran la magnitud del desafío y por qué es imprescindible contar con servicios de Threat Hunting:

35%
de las amenazas identificadas por equipos de Threat Hunting no aparecen en feeds comerciales ni en herramientas tradicionales.

12%
de las amenazas detectadas por hunters nunca han sido vistas antes en ningún otro entorno.

100%
de las organizaciones analizadas presentan puntos ciegos explotables sin generar alertas.

60%
de los ejercicios de hunting revelan activos desconocidos o mal configurados.

70%
de los casos de ransomware-as-a-service y espionaje económico fueron descubiertos por hunting manual.

Nuestra visión sobre un servicio de Threat Hunting eficaz

Un servicio de Threat Hunting eficaz no se limita a ejecutar búsquedas. Es una disciplina que combina creatividad, intuición y metodología para descubrir lo que las herramientas no ven. En KPMG, creemos que un programa de hunting debe cumplir con estos seis pilares:

Hipótesis bien definidas

Todo ejercicio de hunting debe partir de una premisa clara: ¿qué estamos buscando y por qué? Las hipótesis se construyen a partir de inteligencia de amenazas, conocimiento del entorno y objetivos específicos. Esto permite enfocar los esfuerzos en detectar comportamientos que podrían indicar actividad maliciosa, incluso si no hay alertas previas.

Validación con datos reales

Las hipótesis se contrastan con la telemetría disponible en el entorno del cliente. Se analizan eventos, logs y patrones para confirmar o descartar la presencia de amenazas. Esta validación permite descubrir ataques que han evadido los controles tradicionales, o confirmar que no hay actividad sospechosa dentro de los parámetros definidos.

Capacidad de acción inmediata

Cuando se detecta una amenaza, el hunting debe activar una respuesta rápida. Esto incluye escalar el hallazgo, coordinar la contención con los equipos técnicos, y generar recomendaciones para prevenir que el mismo ataque vuelva a ocurrir. El hunting no termina en el análisis: debe habilitar decisiones operativas.

Cobertura de puntos ciegos

El hunting revela activos desconocidos, sistemas mal configurados o datos expuestos que no estaban bajo control del equipo de seguridad. Estos hallazgos permiten mejorar la visibilidad del entorno y cerrar brechas que podrían ser explotadas por atacantes.

Contribución a la ingeniería de detección

Los resultados del hunting alimentan la mejora continua de las reglas de detección. Cada hallazgo se convierte en una oportunidad para ajustar el SIEM, el XDR o las herramientas de respuesta, fortaleciendo la capacidad de identificar amenazas similares en el futuro sin intervención manual.

Valor incluso sin hallazgos

Confirmar que no hay intrusiones también aporta valor. Permite a los responsables de seguridad comunicar tranquilidad a la dirección, demostrar control del entorno y validar que los mecanismos de protección están funcionando. Un hunting sin hallazgos es una señal de madurez, no de fracaso.

Nuestros servicios

El servicio de Threat Hunting busca proactivamente amenazas sigilosas en el entorno del cliente, incluso en ausencia de alertas. Se basa en hipótesis de ataque, análisis de comportamiento y telemetría avanzada.

Threat Hunting Proactivo

Para detectar amenazas avanzadas que evaden los controles tradicionales, mediante búsquedas continuas en el entorno del cliente sin depender de alertas previas. Se basa en hipótesis de ataque, inteligencia de amenazas y análisis de comportamiento para identificar señales tempranas de compromiso y reducir el riesgo antes de que se materialice.

- Diseño de ejercicios de hunting basados en alertas de amenazas reales y patrones observados en campañas activas, adaptados al contexto del cliente y sus activos críticos.
- Revisión exhaustiva de la telemetría generada por sistemas de detección como SIEM, EDR o XDR, con foco en identificar comportamientos anómalos, secuencias inusuales de eventos o indicadores débiles que podrían pasar desapercibidos para las reglas tradicionales.
- Formulación y validación de hipótesis de ataque mediante el análisis de tácticas de adversarios conocidos, utilizando frameworks como MITRE ATT&CK para guiar la investigación y priorizar los vectores más relevantes.
- Ajuste y enriquecimiento continuo de las reglas de detección para mejorar la cobertura frente a amenazas persistentes avanzadas (APT), incorporando nuevos indicadores, patrones de comportamiento y correlaciones entre eventos.
- Elaboración de informes periódicos con los hallazgos obtenidos, incluyendo evidencias técnicas, análisis de impacto, recomendaciones de mitigación y evolución de las amenazas detectadas en el tiempo.

Threat Hunting Bajo Demanda

Orientado a investigar amenazas específicas, validar sospechas o apoyar auditorías. Permite una respuesta rápida y especializada ante posibles compromisos, aportando visibilidad detallada y recomendaciones accionables.

- Ejecución de ejercicios de hunting dirigidos sobre fuentes específicas de información como logs de red, eventos de endpoints, tráfico DNS o registros de autenticación, priorizando los activos más críticos o sospechosos.
- Validación de hipótesis de compromiso utilizando inteligencia de amenazas actualizada, incluyendo indicadores de compromiso (IOCs), tácticas emergentes de grupos APT y patrones de comportamiento asociados a campañas recientes.
- Apoyo directo a investigaciones internas, revisiones regulatorias o auditorías técnicas, proporcionando evidencia objetiva y trazabilidad de las acciones realizadas durante el proceso de hunting.
- Elaboración de un informe técnico detallado con los hallazgos obtenidos, incluyendo análisis de causa raíz, recomendaciones de contención y remediación, y propuestas de mejora para fortalecer la detección futura.

Beneficios potenciales

- Detección temprana de amenazas que no generan alertas
- Reducción del tiempo de permanencia del atacante
- Mejora de la postura defensiva frente a APTs
- Refuerzo de la capacidad de investigación y respuesta

¿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