Evaluación de proveedores de protección de marca

Haz las mismas nueve preguntas a cada proveedor. Puntúa cada respuesta de 0 a 3, multiplica por el peso (1 a 3) y compara totales. Después, haz un piloto de dos semanas con tu propia marca.

PROVEEDOR A _____ PROVEEDOR B _____ PROVEEDOR C _____

PREGUNTA	BUENA RESPUESTA	SEÑAL DE ALERTA	PESO	A	B	C
1. ¿Quién presenta los takedowns?	El proveedor los presenta y da seguimiento sin tu intervención en los casos normales	Los presentas tú, o cada takedown necesita tu aprobación	☐	☐	☐	☐
2. ¿Cuántos takedowns incluye por mes y qué pasa si se superan?	Ilimitados o según tu volumen, con precio claro por excedente	Límites mensuales de un dígito; “uso razonable” sin cifras	☐	☐	☐	☐
3. ¿Cuál es la mediana y el percentil 90 del tiempo hasta la advertencia y hasta la eliminación?	Ambas cifras, con cómo se midieron y en qué período	Solo un “promedio” o “en horas” sin datos	☐	☐	☐	☐
4. ¿Qué significa “resuelto”?	Fuera de línea y verificado desde varias ubicaciones, con evidencia	“Reporte enviado” cuenta como resuelto	☐	☐	☐	☐
5. ¿Qué monitorean y con qué frecuencia?	Dominios nuevos, certificados, DNS, páginas, redes y marketplaces, de forma continua	Revisiones semanales o mensuales; pocas fuentes	☐	☐	☐	☐
6. ¿Qué pasos están automatizados y cuáles pasan por un analista?	Un flujo claro que muestre qué se automatiza de punta a punta	Sin respuesta, o solo términos de marketing	☐	☐	☐	☐
7. ¿Qué evidencia capturan y podemos reutilizarla?	Capturas, código de la página, registros DNS y de registro, fechas, exportables	Solo capturas; no exportables	☐	☐	☐	☐
8. ¿Cómo definen y miden los falsos positivos?	Una definición, una tasa medida y quién los revisa	Sin definición; tú revisas todo	☐	☐	☐	☐
9. ¿Podemos hacer un piloto con nuestra marca?	Un piloto de 2 semanas con tu marca, con las mismas amenazas para cada proveedor	Solo una demo preparada	☐	☐	☐	☐

TOTAL (PUNTAJE × PESO) _____

RESULTADOS DEL PILOTO: DETECCIONES REALES, ELIMINACIONES, TIEMPO HASTA ADVERTENCIA Y ELIMINACIÓN _____

¿COMPRAS ALERTAS O AMENAZAS ELIMINADAS?

Decídelo primero. Una herramienta que se queda en la detección deja el trabajo de takedown (búsquedas, reportes, seguimiento) en tu equipo, y ese es la mayor parte del esfuerzo.