HIRDMAN
uncovering weaknesses using hacker methodology

VENDOR EVALUATION · 2026

Vendor evaluation checklist: 26 questions

For your breach monitoring, domain monitoring, brand protection and perimeter vendor. Ask to see the work on real data: that way every answer can be checked.

☐ Solid answer ☐ Red flag *Tick as you go through the call*

01 Data quality and credibility

☐ ☐ 01 **Do you detect fake and generated leaks — and how exactly?**
Red flag: "we have filters" with no process behind it; a repackaged old set passed off as a new breach.

☐ ☐ 02 **How do you establish freshness and the real date of compromise?**
Red flag: "date added" passed off as "date breached"; findings dismissed as old without checking whether the password still works.

☐ ☐ 03 **Do you work with stealer logs — and how?**
Red flag: public combo lists only; just passwords pulled from the log; after a stealer incident the advice is "change the password".

☐ ☐ 04 **Is your "dark web" public onion sites — or real closed platforms?**
Red flag: a public onion site presented as a closed source; no capacity to pull and process large dumps.

☐ ☐ 05 **Which sources do you monitor — can you name a concrete list?**
Red flag: a vague "many sources" with no list; collection limited to public channels and aggregators.

02 Depth of analysis

☐ ☐ 06 **Do you account for 2FA/MFA bypass risk based on breach data?**
Red flag: the advice stops at a password reset, ignoring that a stolen session bypasses MFA entirely.

☐ ☐ 07 **Do you do reverse checks?**
Red flag: "password no longer works, risk closed"; personal and corporate accounts never linked; privilege behind a login like admin goes unnoticed.

☐ ☐ 08 **What scope of data do you actually process from a breach?**
Red flag: only login, password and URL are stored, everything else normalised away; you get "this email was found" with no context.

☐ ☐ 09 **Breaches as an investigation tool — do you take those cases?**
Red flag: they can only show a list of leaks; forensics and insider work are out of scope.

☐ ☐ 10 **Coverage depth: basic leaks only — or recon through an attacker's eyes?**
Red flag: only the breach database is examined; ports, shadow IT, secrets in code and mobile builds stay out of scope.

03 Signal, noise and delivery

☐ ☐ 11 **How do you cut the noise and confirm findings?**
Red flag: you spend weeks tuning filters; brand search comes down to grep on a keyword.

☐ ☐ 12 **What do we get at the end — a counter dump or a report built around our goals?**
Red flag: a line saying "an email was found" with no priority; an interface overloaded with modules that never reduces risk.

☐ ☐ 13 **Do you take the work on — or does the client handle it?**
Red flag: the "here's an alert, you deal with it" model; a portal that takes weeks to learn.

04 Speed, integrations, price and trust

☐ ☐ 14 **What is the lag between event and finding — and what drives priority?**
Red flag: one batch cycle, weekly or monthly, with no prioritisation; weeks between a finding and any reaction.

☐ ☐ 15 **Do you have an API and integrations — and in what form is data delivered?**
Red flag: report download only; no API, or it sits behind a separate paid module.

☐ ☐ 16 **How do pricing and licensing work?**
Red flag: "price on request", licences by assets, export caps, expensive add-ons.

☐ ☐ 17 **Is there a pilot or POC on real data?**
Red flag: a polished demo on someone else's data; to see anything you fill in questionnaires and wait months for approval.

☐ ☐ 18 **Where is our data processed — is it run through public AI and the cloud?**
Red flag: data run through public AI and cloud; one shared environment for all clients; the vendor itself has had incidents; a model conclusion with no grounds in the record's data; a model decision no person reviews.

05 Brand protection

☐ ☐ 19 **How do you find look-alikes of our brand?**
Red flag: one generation algorithm and a spreadsheet of hundreds of thousands of names; a substring search on the name; certificates and the day's fresh registrations are not watched.

☐ ☐ 20 **What tells you a domain is dangerous?**
Red flag: "looks similar" as the only ground; mail, favicon, screenshot and registration go unchecked; a decision with no visible reason.

☐ ☐ 21 **How many lines does our team end up reviewing?**
Red flag: the whole list "for review"; the client works out priority; a decision has no grounds.

☐ ☐ 22 **How do you show what exactly was checked?**
Red flag: an empty cell reads as "clean"; a failed source looks like "no look-alikes".

06 Cases and takedown

☐ ☐ 23 **What do we get to hand a finding to lawyers and the registrar?**
Red flag: a screenshot in an email; the client gathers evidence alone; no hashes, capture dates or action log.

☐ ☐ 24 **You found a fake mobile app — what do you do next?**

Red flag: just a link to the app store; nobody takes the code apart or knows what was changed and where the data goes; the takedown is left to the client.

07 Perimeter

☐ ☐ 25 **Do you track changes to our own perimeter?**

Red flag: a one-off scan with no history; an inventory the client keeps alone; certificates, SPF/DMARC and open storage are out of scope.

08 Reporting and the regulator

☐ ☐ 26 **Can you show a regulator what work was done, by whom and when?**

Red flag: a report of counters with no action log; history can be rewritten after the fact; a past state of the perimeter cannot be restored.

Want to compare on your own data?

We'll show findings for your domain with no commitment. The core cabinet is available right away: `demo.hirdman.pro`, login `demo`, password `demo`. Pilot: `info@hirdman.pro`