expel

12 revealing questions
any MSSP or MDR should be able to answer

Ask predictable questions and you get — that's right — predictable answers. Try these 12 atypical prompts to gain insights from your MSSP or MDR vendor.

1 — **Have you adapted your service to your customers' environment and can you grow with us?**

One size doesn't fit all. A good MSSP or MDR provider fine-tunes responses and services. And remember, you're probably growing and your provider needs to grow with you. Ask for a real-world example.

2 — **How long did onboarding take for your last 10 customers?**

Did it wrap up in a week or drag on for months? Say no to hypothetical numbers. Get real and referenceable data on average onboarding times for actual customers. And be sure to ask if service during onboarding will cost you.

3 — **Can you use our existing security technology, or do we have to implement something new?**

Your provider shouldn't dictate your technology choice. They should build on what you have and operationalize it to fill their data pipeline.

4 — **Does your detection and response strategy differ among on-prem technology, cloud infrastructure, and cloud applications?**

Beware of pat/canned answers. Make sure your provider "speaks cloud" and approaches security differently in the cloud vs. on-prem.

5 — **How will we work together during a security incident?**

Hair on fire? Let's hope not. Seek transparent, rapid, multi-person communication during incidents. And make sure you know who does what and when.

6 — **What have you learned from a customer that improved your service?**

Yep, this one's a softball. Run away if your security service fumbles the answer and isn't learning and adapting its threat response.

7 — **How much visibility will we have into your decision making?**

Trust, yet verify. Get full visibility into triage, investigation, and reporting and response decisions.

8 — **When things start to break, how quickly do you find and fix the problem?**

Your provider should detect when a device becomes unreachable or unstable – and immediately give you a heads-up. Then do you remediate or do they?

9 — **Have you successfully engaged with an active red team assignment?**

What if you bring in a sophisticated red team partner but your service provider can't see mock adversaries? Make sure any potential partner has identified and reported on a red team engagement and asked what they learned after they did.

10 — **How do we reach your team with a non-urgent question or concern?**

Anonymous support portals or dodgy ticketing systems won't cut it. You need direct access to individuals from your provider's security team.

11 — **What's your price and how is it calculated?**

Beware of rambling answers. Crisp, easy-to-understand prices bode well for establishing trust.

12 — **If selected, can you provide a free 30-day proof of concept?**

Get a feel for your new provider – and allow them to meet expectations – by hopping on their service on an interim basis.

Ready to see what it's like to work with Expel? Take a look at **this** - no email required.

www.expel.com