Nov 1, 2017 | Andrew Hoyt

Warning signs that your MSSP isn't the right fit

("It's not you, it's me. OK, I lied, it's actually you.")

There are two sides to every relationship. When they go bad it's easy to blame yourself. But I'm here to tell you, dear reader, that you don't need to (and shouldn't) accept mediocrity. There are many managed security service providers (MSSPs) out there -- some of which do a few things really well, and some that well... don't. If you're trapped in a failing (or failed) relationship with your MSSP you're not alone.

Here are some warning signs to look out for that indicate it's probably time to start considering some other options.

Warning #1: The MSSP can't use the new product(s) you just bought

You fought hard for budget and you've spun up the new [insert cool technology product] in your environment. You even splurged on hiring and training staff to set it up, maintain it and look at the logs/alerts it generates. Why? Because that data is important to you. Except, you were hoping your new MSSP would be able to take that work off your hands so you can redeploy those resources.

That's why you were so surprised when your MSSP told you that not only do they not support your new product, they've got their own flavor of the product you just bought and they're going to have to put in your environment for the service to work. So much for deploying those resources elsewhere. You're also going to need to find a way to correlate that data with the stuff coming from your MSSP, so you'll probably just dump everything into a SIEM and treat the MSSP as another alert feed.

That's not how it was supposed to be (and it really doesn't have to). The right partner should use your existing technology. They shouldn't just integrate with the "meat and potatoes" technologies in your infrastructure (think firewalls, IDS/IPS). They should also use the shiny new technologies you've invested in to find modern threats (think endpoint detection and response (EDR)).

If you see this warning sign here are a few questions to keep in your back pocket:

- **What do you need to do to deploy the MSSP's service?**
  Correct answer: Minimal software, no hardware, simple configuration changes.

- **What, if any, additional products do you have to buy or replace to get value out of the service?**
  Correct answer: None.

- **What products do they support?**
  Correct answer: Hopefully everything you already have.
  Realistic answer: The majority of what you have, especially the technologies you're already monitoring yourself and other important components are on the roadmap. This should include network and endpoint technologies!

Warning #2: The onboarding process never ends

You made it through the procurement process and got a signature on the contract. You thought you'd be off to the races. But your MSSP dumped a bomb on you in the first call...and your stomach dropped a bit. There were hundreds of pages of documentation, dozens of phone calls and meetings and project plans that stretched out into forever. It's month's later and you're still onboarding while the promised value still lies somewhere over the (infinite) horizon.

Your standards can and should be higher. The right partner should provide an onboarding experience that's point-and-click easy -- closer to your smartphone than a call to your Cable TV provider's customer support line. Once data is flowing to your provider, you should be receiving value. In short, onboarding should take days (or even hours), and value should come in less than a week.

If you feel like you're entering the onboarding danger zone ask these questions:

- **How long will it take to onboard all in-scope technologies for the service?**
  Correct answer: A week, max.

- **Is there documentation for the onboarding process? Can I see it?**
  Correct answer: Yes... and yes.

And...a bonus question.

- **Can I onboard a device (or three) as a proof-of-concept before I sign up for the service?**
  Correct answer: We'd love that
  Likely answer: Ummmm... [awkward silence]

Warning #3: You're getting lots of alerts...but few answers

You're onboarded! You're getting ready to sit back and let your MSSP work for you. And then it happens. Your morning email digest shows up... and it's full of alerts. 50 of them to be specific. What happened? Which ones are most important? Has there been a breach or are they just suspicious? Are any of the alerts related to each other? Or are they independent events that should be treated as separate incidents? How were they detected? Is this the beginning, middle, or end of an attack? Why does your MSSP hate you so much that they hand you these tiresome riddles every... single... day?

Each alert should be a means to an end. Rather than accepting a pile of questions, find a partner that will give you answers. What happened? When? How? What's the risk? What should you do next? These are the answers you're paying for, not "hey, here's some alerts." More important, what is the data telling you over time? Your MSSP should be able to help identify trends and make strategic recommendations that reduce overall risk in your environment.

In retrospect, these are the questions you would have asked during the sales process:

- **Can I see a demo of your portal including the technical data and investigative reports I'll receive?**
  Correct answer: Glad you asked. Here are the answers we'll give you.

- **How will I know when there's an incident that matters? How do your analysts investigate them?**
  Correct answer: Click. Look here. You can see exactly what our analysts are doing and why they're doing it
  Likely answer: Blah, blah, blah, alert stream, blah, certifications, blah, intelligence, blah, SLA.

- **How do you measure the value you provide?**
  Correct answer: Look at this dashboard. You can see how things are trending and the impact of our recommendations.
  Likely answer: Alerts detected each month.

Warning #4: You're finding evil days (or weeks) before your MSSP does

You found something bad (for the fourth time) days before your MSSP ever told you anything. There could be lots of reasons: they can't see it, they can't detect it, their processes are weak... or maybe their analysts just don't know much about you and your environment. Reducing the time from detection to response is a key metric for measuring risk mitigation in your environment. Context around what the threat is, how it got there, and what it's doing (or will do) are all critical when responding to attacks. Your MSSP should have the ability to pull alerts from your technologies, apply threat intelligence, and correlate activity across the network, endpoints and your SIEM before they send the activity to an analyst. This ensures they'll be able to tell the whole story.

A good provider will tell you things about your environment -- including your own tools and investments -- that you didn't already know. In some cases they'll tell you things that aren't even related to a security incident. But you'll still care about them. They might reveal asset misuse or a misconfiguration issue. Either way, fresh eyes should consistently find fresh issues that matter to you.

Your MSSP analysts should have close to (if not the same) visibility into your network that you do. That means shared tools and endpoint visibility. Your MSSP will also have a versatile detection engine to make sure they can catch increasingly sophisticated attacks. If you're being notified late (or never), or getting very little context, it's time to find alternatives.

The answers to these questions will tell you if your team will be better at detecting threats than your MSSP:

- **Can you implement these basic detection use cases that are important to me?**
  Correct answer: Of course, and here's how we'd do it.

- **Can I see examples of incident notifications?**
  Correct answer: Yes, they include all the context you need to respond to the incident.

- **What data do your MSSP analysts see when they triage an alert?**
  Correct answer: They have host visibility (think EDR) and can connect directly to your security technologies to investigate activity.

Warning #5: You're hiring more people to manage your MSSP

You're starting to dig into the service and you're getting that nervous feeling. The service looks great, but it's complicated. And you already know you're not going to be able to use this thing without help. Never fear! That's when your MSSP introduces you to their professional services team! They'd be more than happy to sell you expensive people who can help make the thing you bought actually work (services for a service!).

Or how about this? You still have a tier-1 analyst team that uses the alerts from the MSSP the same way they'd use alerts from any other product. They get ingested into your SIEM and your team looks at them along with all of the other alerts the MSSP isn't capable of generating since they can't support some of the technologies you have. Either way, you're stuck doing it yourself... and creating even more work for you and your team. Yes, this actually happens. We know people (you know who you are) in this exact situation.

Of course, the goal of any managed solution is to augment your existing capability so you and your team (if you have one) can spend less time fighting fires and more time working on strategic initiatives. When you have to add more firefighters to the team, it's probably because your MSSP is adding to the fire and not helping put it out. A good provider will reduce the time and money you spend on security operations tasks, not increase it.

Here's how to tell if you're at risk for being on the wrong end of this equation:

- **Include the people on your team who will be working with the service in the tech demo and let them ask questions.**
  Do they feel comfortable using the service to do their jobs? Are they comfortable with the outputs of the service?

- **Sit down with the vendor and map out the workflow between you and your team.**
  How will your team use the service on a daily basis? Is the MSSP adding more steps to your process, or removing them? Does your workflow overlap, or is the MSSP just throwing more alerts over the fence and expecting you to fend for yourself?

- **Go back to your detection uses cases.**
  Did you bring a few that are important to you? If the MSSP can't implement them then you're stuck hiring people and purchasing technology that can.

Remember, your MSSP should help you get more value out of the technologies you've already invested in and augment your security team. Above all else, your MSSP should give you answers (not just alerts) so you can improve your security posture in a measurable way. This can only happen if the service is easy to setup, easy to use, and versatile enough to align with your team's workflow and goals, not the other way around.

As you evaluate your options, don't be afraid to include your team in the conversation. After all, they're the ones that'll have to work with the MSSP on a daily basis. Are they excited with what they see? If so, you know it's because it'll make their lives easier, not harder. There's no better litmus test than that.

--

Visit the EXE blog for more articles like this at https://expel.io/blog

About Expel
Expel provides transparent managed security. It's the antidote for companies trapped in failed relationships with their managed security service provider (MSSP) and those looking to avoid the frustration of working with one in the first place. To learn more, check us out at www.expel.io.