EVALUATION CHECKLIST:

Red Flags That an MSSP Is Overselling Its MDR Services

As the Managed Detection and Response (MDR) market grows, buyers must be careful when considering a detection and response solution from a Managed Security Service Provider (MSSP). Ask the right questions to ensure an MSSP isn't trying to dress up existing offerings without making the necessary investments.

Use the list below when evaluating MDR offerings:

□ What is your team's expertise across the following disciplines?

- Security research
- Advanced detection methodologies
- Threat hunting
- Security analysis
- Incident response
- Forensics
- Security operations
- Security engineering
- Data science
- IT operations

TIP: To really do due diligence, ask to interview specific individuals on the security team. Learn about what they do every day and their areas of expertise.

□ How do you ensure you always have enough analysts and incident responders in your SOC? How do you maintain a pipeline of recruits?

□ What is your process for detection, investigation, and response?

□ What technologies are core to your MDR offering? How do you train your SOC to ensure proficiency?

□ Can you automatically orchestrate data and suppress events to limit investigation of false positives?

□ Are you able to provide metrics showing continuous improvements in analysis time?

□ Can you detect XYZ activity?

  □ For each scenario you present, ask which artifacts will be collected to enable detection and what aspects of the attack will be detected.

□ What is the false positive rate on some of your detectors? Not the false positive rate customers report, rather the false positive rate the provider's internal SOC reports from its own detection technology. (The key here is that internal false positives are okay. You want your MDR provider examining a lot of different activity, even if it doesn't convert to a threat.)

□ What are three new types of threatening behavior you can now identify due to improvements you've made in the last 3 months? (The key here is you don't want the MSSP driving their detection with threat intelligence and you want a provider who is continually improving their detection.)

□ What types of threats are you unable to detect?

□ What is your customer reported false positive rate? False negative rate?

□ What is your average time to detection? Response?

□ Have you ever had a customer get breached? Walk through how that event happened and what your response was. Can a conversation with that customer be arranged?

□ Who do customers typically interact with when they have questions on detections, response best practices, implementation of the MDR service, etc.?

□ Explain your detection and response roadmap. What new techniques and technologies will you incorporate into your offering?

□ How do customers hold you accountable? (You do not want an MDR provider focused on traditional SLAs. They should be focused on breadth and timeliness of detection and response)

⚠ Remember: the majority of MSSPs are not offering true MDR capabilities at this time—even when they advertise that they do. It would take major investments and recruitment of an entirely new staff to realign to certain market niches. Choose your partner wisely. If you wouldn't hire someone with the experience they list, why would you hire them as your MSSP?

red canary

See the difference for yourself. Schedule a demo today.

855.977.0686 | redcanary.com/demo