DARKReading

TOP TIPS

Evaluating Your Managed Extended Detection and Response Provider

Managed Detection and Response (MDR) solutions have become a vital tool for cyber security, but the glut of available offerings can be confusing for enterprise teams to evaluate. These solutions evolved out of 1990s-era managed security service (MSS) options which were limited to attack prevention and perimeter-based firewalls. MXDR now provides a far more holistic approach including data collection and processing, incident response, analysis support and access to experienced security experts.

While more than 200 organizations claim to provide MDR, many haven't moved much beyond the outdated defensive MSS model of the 1990s and do not offer MXDR. For enterprise teams, it's become more important than ever to ensure that the solution they choose can deliver the best outcomes, especially in the wake of increasingly sophisticated cyber-attacks. In such a complex landscape, these tips offer critical guidelines for evaluating your MXDR provider and making sure they are fit for purpose.

1) Prioritize digital forensics and investigation expertises

As preventing cyber threats outright has become increasingly challenging, security teams are emphasizing detection and response. In this context, the provider's investigative experience – especially in terms of digital forensics – is critical. Examine their ability to analyze data from managed infrastructure as well as the evolution of investigative expertise in their history. In particular, the provider should have a track record of not only detecting advanced or elusive threats, but also understanding their root causes through deeper analysis.

2) Look out for alert-based service offerings masquerading as MDR

The sheer number of organizations claiming to provide MDR and now MXDR means a trickier evaluation scenario. Enterprise teams must be wary of alert-based services that masquerade as MDR but outsource their vital incident-response functions to partners. Make sure that your vendor has all the necessary expertise to investigate and deal with threats in-house and avoid costly incident response retainers.

3) Integrated with SIEM and EDR technologies

Your MXDR provider should take on the burden of keeping up with the latest technologies, so you don't have to. The solution should integrate signature-based tools or SIEM (security information and event management) and your preferred endpoint detection and response (EDR) software for the most effective defense.

4) Threat-hunting is part of the package

This is another feature that should be included as a vital tool in your MXDR without any add-on fees. Threat-hunting helps you proactively identify attackers automatically before they infiltrate your environment and cause damage. And it's vital to ensure that the team's threat-hunters have years of experience doing exactly that.

5) Help your team avoid "alert fatigue"

A headache inherent in MSS systems is the volume of alerts that clutter your security team's email inbox and take up their time with false positives. Ideally, your MDR provider avoids these problems by verifying attacker presence and tackling the root of the situation to limit false alarms. And they should also use a smoother communication platform, such as Slack, to ensure that important messages aren't lost in the shuffle.

6) See beyond the endpoint

Extended detection and response (XDR) systems are becoming increasingly valuable for a comprehensive view of your enterprise. A provider incorporating these cutting-edge capabilities – an MXDR -- helps you see beyond endpoint security with full visibility for cloud and application data, network appliances and other log sources. The ability to analyze network traffic using network detection and response (NDR) capabilities provides organizations an additional layer of network-level security and threat prevention capabilities. As such, an MXDR's threat-detection methods overcome the limitations of relying on signatures and indicators of compromise – no longer sufficient for comprehensive security. Moving beyond typical detection, it consolidates multiple products into a unified platform.

7) Catch ransomware attacks

Ransomware encrypts your system and extorts money for its release. Often, these types of malware can bypass traditional defenses and take down your network. Make sure your MXDR is specifically attuned to identifying and remediating these critical risks. Threat actors are not only encrypting data, but are also demanding large ransom amounts and threatening to release customer data publicly. When it's a race against time, you need a team of security experts backed by best-of-breed technology on your side. Your MXDR provider should have the ability to understand how the threat actors gained initial access, how they maintained persistence and how they escalated privileges and moved laterally – then close the gaps so that it doesn't happen again.

8) Around-the-clock monitoring

Your MXDR provider should have the capacity to keep your security system's lights on, no matter the time or season. At the very least, your vendor should be able to monitor your enterprise 24 hours a day and seven days a week – including over holiday periods. This can be a challenge for smaller operations, which are also at greater risk of breaks in service due to intermittent staff shortages or turnover.

9) Adaptation and change

The best MDR providers aren't satisfied with "good enough." Make sure your provider has systems in place to measure success as well as their effectiveness in terms of delivering on targeted outcomes. And ideally, they have a track record when it comes to adapting their practices to emerging business and security needs so you stay protected through change.

10) Reporting

Transparency throughout this process is also key to ongoing success and an effective long-term defense. Your MDR provider should supply your enterprise with regular and accessible reports that track protection progress, access to the platform, detail controls in place and make recommendations on addressing security weaknesses. And these are your tools and your business – so for full transparency, you should have complete access to the platform so you can see what's going on at any given time.