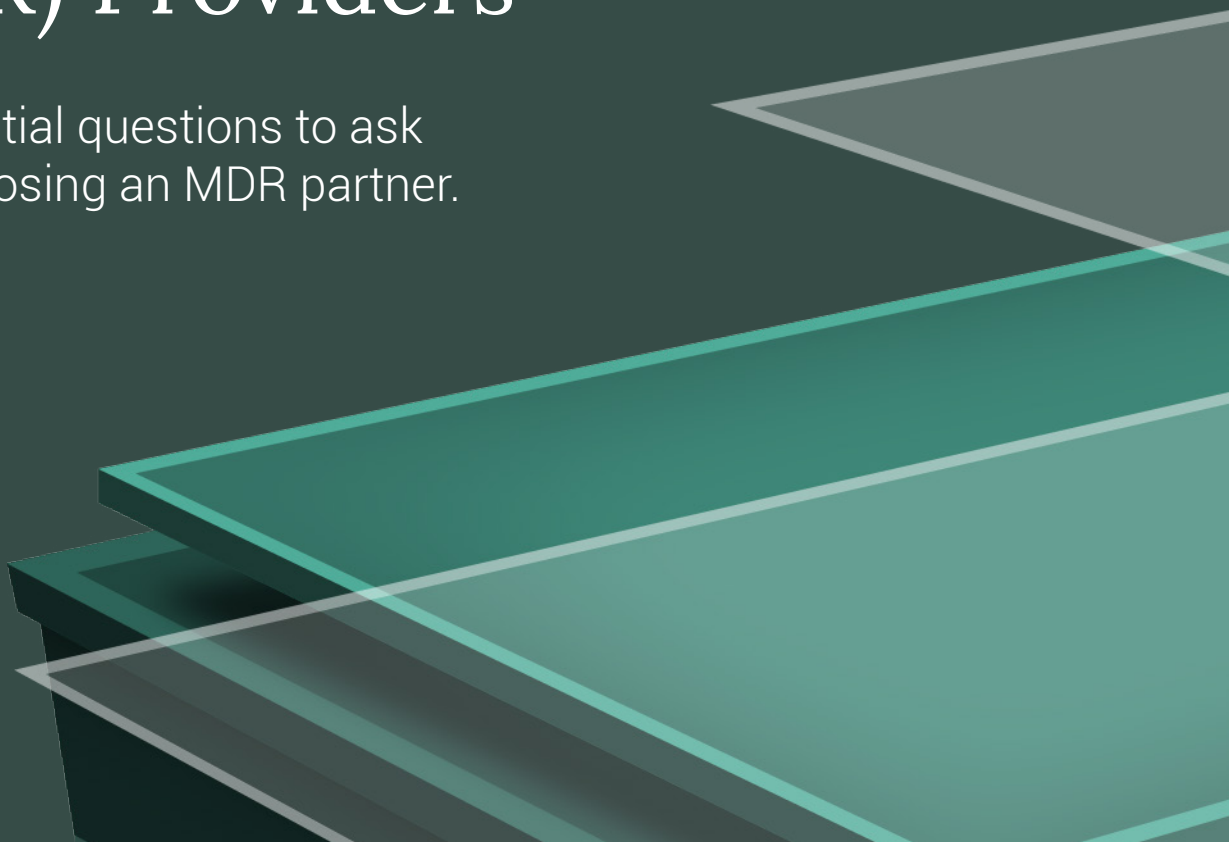
ankura
InterXeptor

EBOOK

How to Evaluate Managed Detection and Response (MDR) Providers

Ten essential questions to ask when choosing an MDR partner.



Since the start of the COVID-19 pandemic, cybercrime has increased 600%[1], and the average weekly attacks per organization worldwide reached a peak this year of 1.2K attacks, a 32% increase year-over-year.[2]

[1]Cyber Security Statistics: The Ultimate List Of Stats, Data, & Trends For 2022
[2]Check Point Research Report, 2022

Table of Contents

Introduction 3

Why and When Should You Consider an MDR Partner? 5

Ten Essential Questions to Ask When Evaluating MDR Services 7

1) How much of the attack surface can you cover? And how do you plan to protect each part of our organization? 9

2) How do you collect, store, and process security event data? 11

3) How do you build threat detection models to analyze data and reduce risk? 13

4) How do you incorporate external threat intelligence to enhance your ability to detect and respond to threats in my environment quickly? 15

5) What does the deployment process look like? Will I need to replace my existing detection tools? 17

6) How do you integrate into my operations? 19

7) If we do experience a serious incident, how will you pivot to response mode and engage with our legal counsel, insurance carrier, and other stakeholders? 21

8) How do you recruit and train cybersecurity specialists? 23

9) What is your pricing model and how can I determine the balance of scalability and cost? 25

10) How will you adapt your service to support my company as it expands and encounters new risks? 27

Next Steps 29

Introduction

As the cybersecurity landscape evolves, organizations are struggling to keep pace with the changing threat landscape and skills required to combat these threats. This is particularly relevant for growing companies that may not have the in-house expertise or resources to implement and manage a comprehensive security program.

MDR partners provide around-the-clock monitoring and threat detection, as well as incident response services, to help organizations reduce their risk and improve their overall security posture. Using a Managed Detection and Response (MDR) partner is a cost-effective tool for new and growing security teams and organizations that don't have the internal resources to support a full security team.

Why and When Should You Consider an MDR Partner?

You Need a Cost-Effective Solution to Improve Your Security

For most mid-sized organizations, it is not realistic to attempt to manage every aspect of your security program with in-house resources. More and more organizations are recognizing that outsourcing 24/7 threat monitoring is an effective way to create peace-of-mind that your network is always protected while also allowing your internal team to focus on high-impact security initiatives and business priorities. An MDR provider can help **take the burden off your already overstretched security team** and extend their capabilities without breaking the bank. Also, partnering with an MDR provider can help you address cyber threats in a **proactive** rather than reactive manner.

Your Company is Struggling to Keep Pace with the Ever-Changing Threat Landscape

Having both **around-the-clock monitoring and threat detection service**s and **incident response service**s in your security team's toolbelt can help you better **defend against today's – and tomorrow's – threats**. As your business grows and threats evolve, you cannot afford to get locked into security technology or service models that can't adapt to meet your changing needs. The right MDR provider will make sure you are always armed with the best tools and the skilled talent to protect your business.

Hiring, Retaining, and Training Cybersecurity Talent is a Struggle

By 2025, there will be 3.5 million cybersecurity jobs open globally, representing a 350% increase over eight years.[3] This shortage, combined with the increasing complexity and sophistication of cyber threats, has made it difficult for organizations to find and retain qualified security staff – and it will continue to be a challenge. If you struggle to hire, retain, and develop cybersecurity specialists, an MDR provider can help.

[3]Cybersecurity Jobs Report, Cybersecurity Ventures

Warning: Not All MDR Partners Are Created Equal

The right MDR partner can provide your organization with the peace of mind that comes from knowing that you have a team of experienced security experts on your side. It's important, however, to choose a provider that best meets the specific needs of your organization.

Here are ten questions you should ask when considering an MDR partner

1. How much of the attack surface can you cover? And how do you plan to protect each part of our organization?
2. How do you collect, store, and process security event data?
3. How do you build threat detection models to analyze data and reduce risk?
4. How do you incorporate external threat intelligence to enhance your ability to detect and respond to threats in my environment quickly?
5. What does the deployment process look like? Will I need to replace my existing detection tools?
6. How do you integrate into my operations?
7. If we experience a serious incident, how will you pivot into response mode, engage with legal counsel, my insurance carrier and other stakeholders?
8. How do you recruit and train cybersecurity specialists?
9. What is your pricing model and how can I determine the balance of scalability and cost?
10. How will you adapt your service to support my company as it expands and encounters new risks?

1 How much of the attack surface can you cover? And how do you plan to protect each part of our organization?

Being able to detect and respond to cyber threats before they cause damage is directly correlated to how much your organization's attack surface is covered. The **attack surface** of your organization can include:

- **Endpoints:** All devices on your network, including laptops, physical servers, and virtual machines.
- **Web traffic:** All traffic going to and from your organization's public-facing website(s).
- **Email traffic:** All inbound and outbound email messages.
- **Network traffic:** All traffic passing through your organization's network.
- **User activity:** All activity by users on your network.
- **Cloud platform activity:** Telemetry gathered from public and private cloud infrastructure including SaaS applications.

Not all MDR partners are the same when it comes to their ability to cover the attack surface. Some providers may only focus on a specific area of security, such as email security or network security, while others provide more comprehensive coverage.

	COVERAGE	FORENSIC CAPTURE
ENDPOINTS	East/West (internal, lateral)	Endpoint telemetry
NETWORK	North/South (ingress/egress)	Packet capture and traffic metadata
CLOUD	IaaS and Sass environments	Cloud provider logs and real-time telemetry
LOGS	Contextual awareness	Multi-month archival
INSIDER THREATS	Behavioral	NetFlow, endpoint, DNS, logs

2 How do you collect, store, and process security event data?

To keep your company secure, ask the managed detection and response (MDR) provider how they will **collect, securely store, and quickly process** massive volumes of event data from a variety of sources – so you can understand how the provider will **identify, detect and respond to threats, and provide insights** to help your organization improve its security posture. MDR providers should have a data collection platform able to ingest data from a variety of sources, including endpoints, web traffic, email traffic, network traffic, user activity, and DNS activity. The most important sources of security event data include the following:

- **Network Monitoring:** A variety of tools are used to **monitor network traffic in real time**. Telemetry sources include routers, switches, and other devices that route traffic through your network, as well as dedicated security tools such as firewalls and intrusion detection systems. By monitoring traffic, the MDR provider can detect precursor attack activity, such as network reconnaissance or abnormal attempts to access sensitive data.
- **Log Management:** This is the process of **collecting and storing logs** from devices on your network, normalizing and enriching those logs and conducting real-time analysis and correlation to support high-value threat detection use cases unique to your organization.
- **Endpoint Detection and Response:** Endpoint detection and response (EDR) tools collect and **continuously analyze data** from laptops, smartphones, and other devices on your network.
- **Cloud Telemetry:** Most organizations rely on some number of cloud-based platforms and applications such as Microsoft Office 365, Workday, Salesforce, and many other SaaS solutions. **Incorporating critical user and session details** such as authentication attempts, destination IP addresses, and file downloads is critical to maintaining broad visibility and enabling comprehensive threat detection monitoring.

Full spectrum coverage (see the graphic in the response to question #1) creates a constant stream of forensic data and telemetry from an expansive threat surface. Alert fatigue is real. Without continuous tuning by experienced security engineers, many "advanced" threat detection tools will generate hundreds of false positive alerts every day, making it impossible for an in-house monitoring team to keep up. At best, the team wastes considerable time resolving alerts that shouldn't have been triggered to begin with. Often, the response to this untenable situation is to either disable certain alerting altogether or simply allow alerts to pile up, leaving a backlog of thousands of unresolved alerts that will never be cleared. An MDR provider should have a defined process to continuously fine-tune detection rules and prioritize alerts to enable analysts to focus their time and attention on real threats rather than chasing ghosts.

When evaluating potential MDR providers be sure to ask exactly how they ingest and process data from their customer base.

> **What processes and technologies are in place?**
> **How are they continually improving their capabilities?**
> **What metrics monitor operational effectiveness?**

Plenty of MSSPs and IT solution providers can deploy and manage security technology (including firewall, IPS/IDS, dual-factor authentication solutions, endpoint protection, and so on) – but modern cybersecurity that can tackle evolving threats is less about operating security technology and more about aggregating and orchestrating vast sums of data and calibrating a dizzying array of specialized tools.

3 How do you build threat detection models to analyze data and reduce risk?

Prevention is ideal…but detection is a must. How your MDR partner analyzes data is essential in detecting and responding to threats. If your MDR partner isn't engineering threat detection playbooks that fit your unique risk profile and available telemetry, it can lead to missed threats and potential data breaches. That's why it's important to **ask how an MDR partner plans to analyze your data and what their threat detection engineering function looks like.** This will help ensure that your organization is in a position to adapt to the evolving tactics and techniques of cyber adversaries.

Typical methods for analyzing data include three ways to identify potential threats:

- **Statistical analysis:** This is used to identify anomalous volumetric or temporal patterns in telemetry data that may be indicative of a threat. It can help the MDR provider quickly and accurately detect potential threats.
- **Rule-based analysis:** This method involves creating rules that are based on known indicators of compromise. When these rules are matched, it can indicate a possible threat. Detection rules must be continuously refreshed through real-time threat intelligence feeds and watchlists.
- **Behavioral analysis:** This kind of analysis consists of analyzing the behavior of users on your network and looking for any anomalies that may be indicative of malicious activity.
- **Hypothesis-based threat hunting:** This is a proactive effort built using real-world scenarios that model potential threat actor activity your organization is likely to encounter.

The MDR provider should communicate their findings to you continuously through a reporting function. Reporting should detail any potential threats that were detected and what steps were taken to mitigate them.

4 How do you incorporate external threat intelligence to enhance your ability to detect and respond to threats in my environment quickly?

A key advantage to engaging an external MDR partner is getting the benefit of threat intelligence the provider collects from its global monitoring activities, as well as access to quality threat intelligence feeds. **Your MDR partner should provide you with customized threat intelligence on an ongoing basis so detection and response can happen quickly**. The intelligence they share should be relevant to your organization's exposure to identified threats, as opposed to consisting of a list of general threats to companies overall, which would put the burden on your team to sift through threats – and slow down threat detection and response.

Make sure your MDR provider is able to conduct ongoing monitoring of deep and dark web locations to identify references to past, present, or future attacker campaigns targeting your industry or your specific organization. Maintaining back-stopped personas in key dark web forums and sites is a critical piece in performing this function; make sure your partner is up to the task.

Make sure your MDR provider is able to conduct ongoing monitoring of deep and dark web locations to identify references to past, present, or future attacker campaigns targeting your industry or your specific organization

5 What does the deployment process look like? Will I need to replace my existing detection tools?

A true MDR partner should be able to get your company up and running with basic 24/7 coverage within a day, and provide full coverage of your attack surface by quickly deploying sensors and connectors to ingest telemetry from critical sources. In the first 30-60 days of deployment, your MDR provider should do the following:

- **Kickoff**
- **Rollout Plan and Schedule**
- **Sensor Deployment**
- **Detection Engineering and Tuning**
- **Steady State Monitoring**

Ask your potential MDR partner if they can offer **ongoing vulnerability scanning**, which can help identify any weak spots that could be exploited by a cyber attack. Also, explore whether the potential MDR partner can recommend enhancements or a full overhaul of the cybersecurity tools if the scan reveals that your current tools are not effective in protecting you from cyber attacks.

In all likelihood, you have already made significant investments in security tools that have been effective in keeping your organization safe. Your MDR provider should be able to help you optimize those previous investments and not require you to rip out and replace with another set of required tools. So another key question to **ask is whether your potential MDR provider is technology agnostic** and if you would be stuck with the same tools as your company grows and threats evolve. These changes – including scalability – can be unexpected, so it's important to ask if you will be locked into a set of technologies.

6 How do you integrate into my operations?

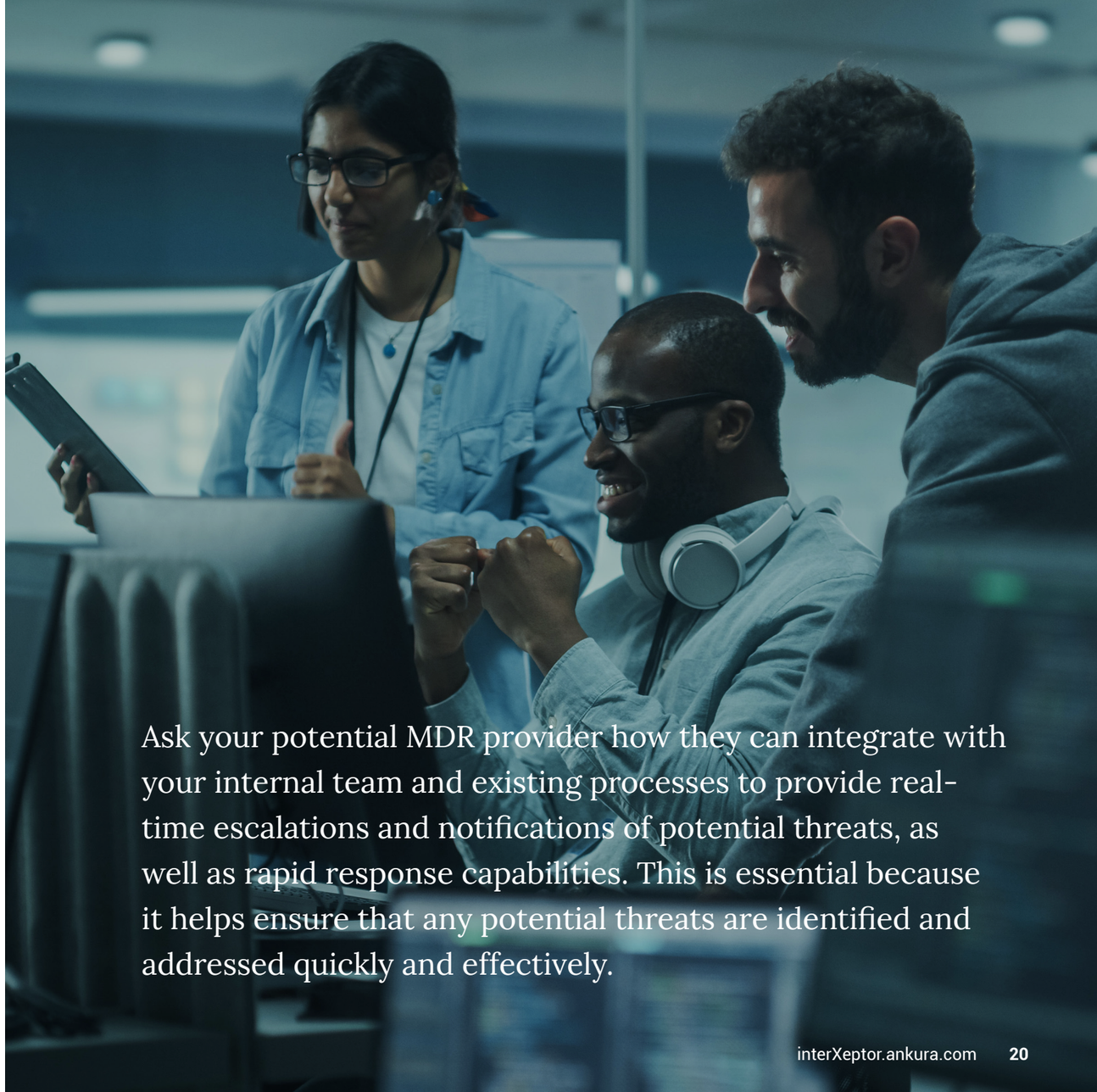
To protect you from cyber attacks, an MDR partner should integrate with your **security operations** to provide a comprehensive and collaborative security solution. Maintaining an active, ongoing dialogue between your internal security team and your partner's security operations center (SOC) is arguably the most important aspect of an effective MDR relationship.

MDR providers typically integrate into an organization's operations in a few ways, including, but not limited to, the following:

- **Dedicated instant message channels:** Maintaining an "always-on" instant messaging channel in Slack or Microsoft Teams can be an excellent way to stay connected to your MDR partner.
- **Incident response "rules of engagement" and defined escalation triggers:** Make sure your MDR provider is appropriately empowered to take immediate action in response to a serious threat detected after hours. The ability to immediately quarantine an infected machine or ban a malicious process from executing can make the difference between a near-miss and a full-blown data breach.
- **Emergency communication planning:** You should have an agreed upon method for communicating securely in the event that your network suffers a disruption. Updated call trees and escalation paths should be maintained at all times.
- **Incident response services:** Incident response is the process of identification, containment, eradication, and recovery from a security incident. This can help an organization quickly and effectively respond to any potential threats. Make sure your MDR partner can demonstrate strong capabilities and deep experience responding to real-world incidents and advanced threats.

Ask your potential MDR provider how they investigate, respond, and remediate threats quickly to prevent damage from being done. **If a threat is not investigated and resolved quickly, it can lead to data breaches and other serious damages. That's why it's crucial to also ask an MDR provider how they manage an active incident response process.** Knowing this will help ensure that your organization is prepared to respond and suppress an attack.

These services can help you reduce the impact of a cyber attack and minimize the downtime associated with it. **It's essential to partner with an MDR provider that has the capabilities and resources to provide the right response for your organization's needs.**

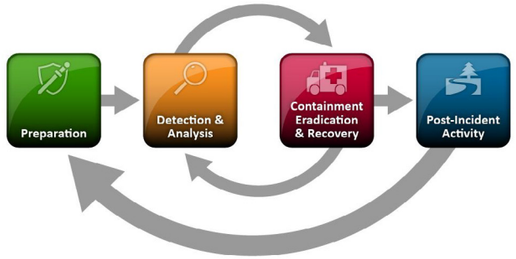


7 If we do experience a serious incident, how will you pivot to response mode and engage with our legal counsel, insurance carrier, and other stakeholders?

Ask your potential MDR partner if their analysts have **live-fire experience and industry-leading techniques** to quickly evaluate and mitigate security incidents. It's important that they have expertise in crisis handling and response while leveraging endpoint detection, user behavior, and threat analytics to quickly contain and eradicate threats.

Inquire about what incident response frameworks your potential MDR provider uses. For example, do they utilize the NIST workflow, as shown below?

National Institute of Standards and Technology (NIST) Incident Response Steps



Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

In addition, make sure to discuss with the potential MDR provider whether the MDR team that would be working with you has a range of deep and broad experience and expertise. The analysts from this team should be trained in incident response (IR) and have the ability to resolve nearly every incident. In the event that an analyst is not able to resolve an incident, the MDR provider should have a defined process to escalate the matter to a senior team member or specialist with the expertise to conduct an investigation.

You should **also ask the potential MDR provider if they're already approved by your insurance company to deliver incident response services under your existing policy.** Moreover, you should inquire whether they have processes for engaging with an organization's legal counsel, insurance carrier, and other stakeholders – and what those processes are – to ensure that this can happen quickly in the event of an incident.

8 How do you recruit and train cybersecurity specialists?

It's crucial to ask a potential MDR partner how they recruit and train their analysts and other staff so you're confident they have the necessary skills and knowledge to protect your organization from cyber attacks. Explore with them how they integrate a number of specialized skill sets including advanced threat detection engineering, incident investigation, and compromise containment and recovery. **Do their specialists have a deep understanding of the cyber threat landscape and how threat actors are evolving their strategies and leveraging different attack vectors** to undermine security systems?

Not only that, but you should ask if these specialists have the knowledge necessary to leverage best-in-class technologies to cover your threat surfaces and efficiently identify and respond to sophisticated threats. Also, inquire whether your potential MDR provider has a program that establishes a talent pipeline to maintain access to cybersecurity professionals despite the global shortage.

It's also critical to ask an MDR partner about their ability to provide 24/7 monitoring coverage. The overall size of the team is one thing, but adequate staffing during off-hours, weekends, and holidays is also critical.

Cybersecurity professional Megan McMahon with Brooklyn Cyber Center graduates, Brady Mejia (left) and Rakeem Hope (right).

Supporting the Future of Cybersecurity

Institutions like the Brooklyn Cyber Center aim to address two perennial challenges in the cybersecurity industry: the severe talent shortage in the sector, which has made it difficult for organizations to fill open security positions with qualified staff, and a historic lack of diversity in the information security profession.

9 What is your pricing model and how can I determine the balance of scalability and cost?

It's essential to discuss pricing and scalability with potential MDR providers so you **don't have surprises later in the contract term**. It's crucial to ensure that their pricing model fits within your budget and meets your firm's unique needs.

Examples of specific aspects of the contract that you should ask about are:

- What services are included in the contract?
- What are the term length options, and do you offer flexible terms?
- Will my pricing change if our organization grows? For example, will pricing go up if the number of endpoints increases and/or if we add software as a service (SaaS) applications?
- Is there a cap on the number of consultation hours? If so, how are we charged after we reach the cap?
- Will investigations and escalations be included in the pricing? If not, how are they charged?
- Will we have ongoing access to your experts? Is that included in the pricing, or will there be an additional charge for that?
- Are regular executive briefings to review open issues, relevant threat intelligence, any changes that our organization is experiencing, and significant incidents included in the pricing? If not, how is that handled?

Ask your potential MDR provider about their pricing model so you're confident that it fits within your budget and is scalable as your organization evolves. Inquire as to whether their solutions are based on the size of your organization and your unique needs. **Predictability and proportionality are key attributes to an optimal pricing model**. The cost of the service should reflect the level of effort necessary to deploy and maintain your infrastructure, as well as the inclusion of required tools and technology.

10 How will you adapt your service to support my company as it expands and encounters new risks?

Ask your potential MDR partner if they are flexible and able to adapt to your evolving business, as well as changing risks and potential threats. Explore with them **how they will proactively and continuously assess your security posture and business priorities so that they can be nimble and pivot quickly when needed**. In addition, **your MDR partner should continuously evaluate your coverage, fit, and impact of their service to** ensure optimal value and delivery quality, timeliness, and accuracy. This flexibility should include support for any future migration to cloud infrastructure, such as Microsoft Azure, that may require a completely different set of cloud-native tools to monitor effectively.

Moreover, you should ask your potential MDR partner if they are technology agnostic and if they will work with you to choose tools that support your company and your unique needs – not just when you start working with them, but also in the future, as more changes occur. These changes – including growth factors – can also be unexpected, so it's crucial to ask if you will be locked into a set of technologies or even a specific service model.

Ask your potential MDR partner if they are flexible and able to adapt to your evolving business, as well as changing risks and potential threats.

What are the next steps?

Now that you've asked these 10 questions and evaluated potential MDR providers, you can be confident that you will be partnering with an organization that has the experience and expertise to protect your business from potential cyber threats. Once you've decided which cybersecurity company is the best fit for your company, you will start working closely with your new MDR team so they can get to know your organization in depth, go through the deployment process, and get you up and running with 24/7 protection. As your company grows and evolves, your MDR partner should continually review your attack surface, tools, and vulnerabilities to keep you up-to-date and protect your network.

Take a Look at Ankura InterXeptor™

A successful Managed Detection and Response (MDR) relationship is characterized by expert-led services and commitment of human capital from the start, not just when your security stack runs out of machine smarts. Our Ankura InterXeptor security experts will invest time to understand your business landscape, not just your cyber attack surface – and our door is always open for advice.

We can quickly adapt Ankura InterXeptor to meet new and escalating threats as your company expands. Our experts continuously assess your security posture and business priorities to provide you the precise solution you need today – and the flexible strategy you need for tomorrow. That's the Ankura InterXeptor difference.

Learn more about our MDR solution at **interXeptor.ankura.com.**

For more Ankura InterXeptor information contact:

Andy Mercer
Global Sales Leader, Cybersecurity & Data Privacy
andy.mercer@ankura.com
Direct: +1 (678) 323-9716