RAPID7

EVALUATION BRIEF

How to Choose a Managed Detection and Response Provider

Smart moves: you're making them. How do we know? For one, you're investigating ways to close the gaps in your threat detection and incident response. Which makes sense, given that assembling the talent and tech to thoroughly thwart attackers requires more than most organizations can commit to. Even smarter, you're checking out Managed Detection and Response (MDR) Services, an increasingly popular solution which combines expertise and tools to provide monitoring and alerting, as well as remote incident investigation and response that can help you detect and remediate threats.

You're two for two. To help you make Smart Move #3 – choosing the MDR provider perfect for your organization – we put together this list of things to think about while searching for an MDR partner. Happy hunting!

Service Basics

- Is 24/7 support available?
- Does the solution bring expertise as well as technology?

Deployment

- Are any infrastructure changes needed?
- Will I need any new hardware to be deployed?
- Is dedicated deployment support available?

Expertise

- Does the service employ their incident response expertise for threat detection?
- What is the average number of years of experience on the breach detection team?
- What is the average number of years of experience on the incident response team?
- Does the vendor have experience responding to large enterprise breaches?
- Does the vendor have experience responding to targeted threat actors?

Communication

- What is the SLA for reporting a threat within your environment?
- What information is provided in the threat report?
- Is information provided that is digestible by both executive and technical customer contacts?
- What is the frequency of periodic updates?
- What information is provided in periodic updates?

Service Tailoring

- How does the vendor customize the offering to your business?
- Does the vendor learn about the criticality of your users?
- Does the vendor learn about the criticality of your assets?
- Does the vendor learn about the criticality of your data?
- What type of tailored notification options are available from the vendor?

Threat Detection

- Does the solution propose to detect known and unknown threats by applying several threat detection methodologies? Which ones?
- Will the solution detect:
- Anomalous user behavior by identifying deviations from the normal behavior of your users? How?
- Attacker tools? How?
- Attacker activities? How?
- Does the provider use threat intelligence? How?
- Can the solution detect threats across multiple platforms? How?
- Are they about to detect threats in cloud services? How?
- Are threats validated before you are notified?
- Does the solution propose to notify you about attacker campaigns against your industry? Request an example.

Proactive Threats

- How will you be notified about threats to your technology platforms? Request an example.
- Does the solution come with a threat intelligence research function? Ask for details.
- Does the solution include endpoint technology for higher fidelity validation?
- What's the feedback loop to reduce potential false positives?
- Are incident response services a part of the offering?

Incident Response

- Will you receive detailed investigation reports?
- Does it include business-focused remediation recommendations and mitigation techniques?

Remediation and Mitigation

- Will you receive support in implementing remediation recommendations and mitigation techniques?
- Does the vendor provide a dedicated point of contact for this service?

So, You've Got Questions. Rapid7 Has Answers.

While searching for the Managed Detection and Response provider right for your organization, keep Rapid7 in mind (Smart Move #4). With Managed Detection, our security experts act as an extension of your security team, providing 24/7 protection and response in your environment, and giving your organization everything it needs to stay safe, without the need to bulk up on teams and tools. You'll get:

- People who understand the difference between user behavior and attacker behavior (and have the time to focus on hunting and processing threat intelligence)
- Technology that understands your environment and can be automated to detect and respond
- A plan and a team with the experience required to solve your toughest security problems

Let's talk MDR. Learn more and get in touch:

https://www.rapid7.com/services/detection-and-response-services/managed-detection-and-response-services/