CHECKLIST

Top 4 Questions MSSPs Need To Ask Before Delivering Managed Detection and Response Services

The shift to services-oriented business models has created opportunities for managed service providers (MSPs) to expand their portfolios by including managed security services, transforming them into managed security service providers (MSSPs).

Aspiring MSSPs should ask these 4 questions before selecting a technology partner for delivering managed detection and response (MDR) services.

Do You Need To Offer Full MDR Services Immediately?

Current MDR solutions have significant differences in both capabilities and costs, but you can start small and grow. For example, a security information and event management (SIEM) platform would typically be the backbone of an MDR service, but SIEM alone may not be competitive. Typically the MDR security operations center (SOC) team would require more sophisticated orchestration and an enhanced layer of telemetry and behavioral analytics that spans endpoints, network, and cloud.

To generate revenue quickly, consider starting with SIEM-as-a-Service (SIEMaaS) or SOC-as-a-Service (SOCaaS) while building toward the full MDR service. Be sure to select a technology partner that can deliver the building blocks you ultimately need with preintegrated components. Also avoid attempting to integrate products from different vendors because it can lead to problems and ongoing frustration.

Does the Technology Match Expectations?

Building a SOC can be difficult and expensive, so it's not surprising that setting up SOCaaS would be even more difficult and more expensive. Unfortunately, technology vendors often pitch products that are unlikely to lead to a successful MDR business:

- Managed endpoint detection and response (EDR) should be a component of an MDR solution, but focusing only on endpoints doesn't offer enough visibility and response.
- Managed extended detection and response (XDR) is new and lacks the third-party integrations, scalability, and operational maturity to handle MDR.
- "Built-for-MSSP" solutions with claims that sound too good to be true often don't live up to the hype. Be extremely cautious.

Does the Vendor Force You To Buy Like an Enterprise?

Many aspiring MSSPs have preexisting relationships with traditional enterprise security vendors, so these partners often are the first consideration when building managed services. Many of these vendors have programs to support their channel in delivering these services, but they often don't appreciate the risks of moving into the managed security services arena. MSSPs need low upfront costs and growth assessments, not contract minimums and other terms that add risk to a fledgling MSSP business.

Is the Vendor Competing With You? (Or Likely To?)

Most technology vendors offer a level of direct cloud-based services, but the rapid pandemic-induced transition to remote work and the crippling chip shortages have led many security hardware technology vendors to add directly delivered security services. Although this move offers more delivery options for traditional reseller channel partners, it also can be a competitive threat to services providers. MSSPs can end up competing with their own technology partner to offer hosted, co-managed, and managed services. Be sure to understand a potential technology partner's vision and roadmap in terms of their own cloud-based solutions.

Start Off Right

Becoming an MSSP comes with new challenges and risks. It's important to ask the right questions to get the right technology and support to successfully deliver MDR services.

www.fortinet.com

September 2, 2021 1:39 AM
1175101-A-0-EN