BUYER'S GUIDE

7 Key Questions for Evaluating Potential Managed Security Service Provider (MSSPs)

With hundreds of MSSPs to choose from, how do you know which one is a good fit for your organization? Not all MSSPs are the same, so it's important to be thorough when you're evaluating potential providers.

This list of questions can help you systematically assess MSSP partners so you select the right one for your organization.

How will you customize your approach to my environment?

- Do you have a rulebook that is customized to my unique environment, processes and rules?
- Do you create use cases, rules and content to benefit my specific technologies and environment?
- Do you run tabletop exercises to test use cases to make sure your team is ready to detect, respond and contain?
- Can your dashboards and reports be customized to the needs of different users in my organization?

What is your onboarding process?

- Do you identify gaps in my current security processes and determine where we need to maximize visibility in order to predict potential risk?
- Do you rely on our organization to have a specific technology to integrate with yours, or do I need to replace my current technology stack?
- Do you have a formalized onboarding process that includes a deep discussion about risk, goals, industry and asset inventory? How often is this process repeated and updated?
- Do you incorporate advanced tools like log management, security information and event management (SIEM), use case analytics, behavior analysis, business context and pattern discovery to detect and prioritize threats?
- Do you provide easy-to-use dashboards, log search, dynamic drill downs and reports to support our security posture?

How do you leverage threat intelligence?

- Do you utilize global threat intelligence for correlation and threat discovery from multiple sources?
- How often do you update the sensors with the latest threat intelligence?
- Do you provide multiple sources of threat intelligence that are correlated to an actionable step?
- Do you have full visibility of security events and the ability to analyze and investigate each event? How do you correlate and prioritize data?
- Do you have more than one source of threat intelligence?

How do you sift through potential threats and select actionable alerts to send us?

- What type of notification will I receive when there is an alert? What criteria needs to be met in order for you to recommend we act on a threat?
- How long does it take you to respond after an actionable threat is detected?
- Does the security operations center (SOC) team proactively investigate suspicious events without overly relying on system-generated alerts?
- What type of case management and incident tools do you use?
- Do you create customized alerts to reduce false positives based on my business requirements?

What is your incident response time?

- What is your process when I have an event that I believe needs to be investigated?
- What is your average time between incident and response?
- Does your SOC team have an incident response and forensic team to respond to active malware or known breaches?
- Do you regularly consult with clients on new threats, alert trends and how to benefit from their security posture?

Do you deliver 24x7x365 managed security services?

- When are your security analysts available?
- How do you ensure threats are addressed in real-time, 24x7?
- How do your security analysts proactively hunt for threats that we may not be aware of?
- Is your SOC in operation 24x7x365?
- Can your security analysts support custom coverage days and times such as 7 p.m. to 7a.m., weekends only or other models?

How will you protect my endpoints?

- Can your technology monitor both endpoints and internet of things (IoT) devices in my environment?
- How long will it take to identify and register all my endpoints and get them up and running?
- Do you provide detection, response, protection and prevention? known breaches?
- Do you regularly consult with clients on new threats, alert trends and how to benefit from their security posture?

nuspire