SELECTING A MANAGED SECURITY SERVICES PROVIDER

A What-to-Look-for Worksheet:

By contracting for managed security services, your organization gets access to security expertise and resources that it probably doesn't have — and can't easily or cost effectively acquire. Companies that specialize in IT security maintain highly experienced teams of experts. They stay on top of emerging threats, employ IT security best practices, and invest in leading-edge cyber defense tools and mitigation strategies.

But how do you choose the best managed security services provider for your organization?

The services offered are important, but there's much more to consider when evaluating these companies. Use the following questions as "thought starters" to determine what you need from a managed security service provider — and how to get it.

COMPANY BACKGROUND:

How long has your organization provided managed security services?

How do managed security services fit into your overall company portfolio and strategic focus?

Do you maintain a dedicated Security Operations Center (SOC)?

Are 100% of your IT security team and resources in the United States?

How does your company ensure that its own infrastructure is secure?

Does your company undergo regular audits for compliance with various regulations, government mandates and/or industry standards? If so, which ones?

Please provide three references.

Have you ever had a customer get breached?

Describe your process for vetting staff that have access to client data.

Do you have Disaster Recovery and Business Continuity Plans?

How long has your back-end technology been in place?

Describe your vulnerability management approach for ensuring the security and integrity of the SOC.

SECURITY OPERATIONS CENTER:

What hours does your SOC operate?

How do you ensure you always have security experts on staff?

How do you train your SOC staff to ensure proficiency and keep them up to date on current and emerging threats and best practices?

What is your team's expertise across the following disciplines: security research, advanced detection methodologies, threat hunting, security analysis, incident response, forensics, security operations, security engineering, data science, and IT operations?

How is communication with the SOC conducted?

TOOLS AND TECHNOLOGIES:

What managed security services do you offer?

Are these services backed by service level agreements?

Can these services be combined to provide a more comprehensive security approach?

Can you provide the services necessary to implement a defense in depth strategy?

Can you help us implement a zero-trust strategy?

Are any of these services customizable?

Are all the various security services offered provided directly by your company or by third-party companies?

If any of the services are offered through third-party companies, what role does your organization play in managing them?

If any of these services are provided by third-party companies or based on their technologies, how do you determine which ones to offer your customers?

Can you assess our current IT security and make recommendations for the appropriate managed security services?

DETECTION + RESPONSE

What options do you provide for detection, investigation, and response?

What technologies are core to these offerings?

Are these offering all supported by/administered through your SOC?

Can you automatically orchestrate data and suppress events to limit investigation of false positives?

Are you able to provide metrics showing continuous improvements in analysis time?

Can you detect XYZ activity?

What types of threats are you unable to detect?

What is your customer reported false positive rate? False negative rate?

What is your average time to detection? Response?

Who do customers typically interact with when they have questions on detections, response best practices, implementation of the EDR, MDR or XDR service, etc.?

Explain your detection and response roadmap. What new techniques and technologies will you incorporate into your services?

How do customers hold you accountable?

LOG RETENTION + COLLECTION

If any of the services entail log retention and collection, do we have access to the logs?

How long are logs available online to be queried?

How are the logs stored? Can they be accessed if the particular security service is no longer required?

If we need to retain logs for an extended period of time, what are the options?

Who is responsible for backing up collected logs?

MONITORING

Will the SOC work with us to prioritize incidents?

How do you monitor threat actors and how do you leverage this information?

How far do you go in evaluating whether or not we have an incident?

Are fully encrypted computing resources and/or communications used?

Can EDR events be monitored and action be taken?

Do you take any actions if malware is identified on EDR protected systems?

What type of blocking response actions can you take, such as deleting a fill or a registry key?

VULNERABILITIES

How is vulnerability data leveraged as part of incident analysis and presentation?

Do we have access to the vulnerability data?

Are dashboards available to help turn raw vulnerability data into a management program?

SERVICE ON-BOARDING

How do you handle on-boarding for the managed security services?

How long does it typically take bring a new customer onboard and start reporting alerts?

How long does it take to realize full benefits of the SOC?

Approximately how long to does it take to add a new device for monitoring?

PRICING

Describe your pricing model, licensing agreements, and maintenance agreements.

Is pricing designed to maximize utilization or is it a charge per device?

Is there a charge to change out or add new technologies / servers?