CyVig

Essential Questions for MSSP Interviews

This checklist will help your IT team determine the potential effectiveness of a managed security services provider (MSSP) and its managed detection and response (MDR) solutions:

First, consider your organization's specific IT needs:

How much time does your IT department invest in cybersecurity?

Is your IT team monitoring your entire attack surface 24/7, or are you doing less monitoring and only handling desktop support/response?

How does your IT handle security monitoring and does the team include subject matter experts to proactively secure the environment?

How are you measuring cybersecurity program effectiveness?

What aspects of the security program are you most concerned with?

Be critical about the MSSP's documented processes:

How would the MSSP work with your IT team to develop a proactive strategy?

Why is the MSSP saying your organization can be more security conscious - and which specific elements of your program is the MSSP able to improve?

Which specific security metrics does the MSSP track?

How does the MSSP present and analyze data from your program?

Does your MSSP use intelligence to make recommendations on alerts and tickets?

Ponder the MSSP's people, processes and technologies:

What up-front work does the MSSP conduct to understand and adjust your security program to the unique aspects of your environment?

How does the MSSP demonstrate that its experts won't just plug in and walk away?

How specifically does the MSSP tune your environment?

What informs the MSSP's detection and response process and how would tuning occur without disrupting existing IT processes?

How does the MSSP communicate with your IT team?

Does the MSSP's approach feel supportive of your IT team and well-documented, or not?

How does the MSSP hire? What does the MSSP value in:

- IT experience
- Certification
- Policies and standards
- Customer support

There's no cookie-cutter solution to cybersecurity.

Visit **cyvig.com/about/our-approach** to measure the maturity of your security program based on your team's specific dynamics.