BUYER'S GUIDE

5 Key Questions for Evaluating Cybersecurity Consulting Services

MSSPs (managed security service providers) not only use technology to protect your organization, but also often provide consulting services. The best offerings focus on pairing your team with a dedicated executive-level security expert, such as a virtual CISO (also called vCISO or executive advisory services).

However, how do you evaluate whether an MSSP offers this type of service and determine if it's 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 an MSSP's vCISO solution, so you select the right one for your organization.

How will you support my organization?

- Will a dedicated security expert, such as virtual CISO, be assigned to assist my team? When are they available?
- What is the expert's background in security? How many years have they been working in the field? Do they have experience supporting companies like mine?
- How will they familiarize themselves with my environment and security challenges?
- Do you have a team of trained security specialists who will also support my team in critical areas? Can you bring in specialists to diagnose issues when needed?
- What is your client retention rate?

How will you customize your approach to my environment?

- Will you review our security architecture and identify areas for improvement?
- Will you review our applications, including SaaS applications, for security holes?
- Will you create a security roadmap and develop programs specific to my environment?
- How will you create security policies and standards? How will they be enforced?
- Do you have a runbook that is customized to my unique environment, processes and rules?
- Do you offer third-party risk assessment?
- Do you offer audit and compliance support? What specific standards and frameworks do you support and have experience with?
- Will you support our security engineering activities?
- Can you support technology stack optimization and reduce any areas of overlap?

What is your onboarding process?

- 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?
- Will you identify gaps in my current security processes and determine where we need to maximize visibility 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?

What is your incident response time?

- What is your escalation process when I have an event that needs investigation?
- What is the average time between incident and response?
- Does your SOC have an incident response team that responds in real time 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?
- Can your security analysts support custom coverage days and times such as 7 p.m. to 7 a.m., weekends only or other models?