COMTACT
Cloud. Security. Delivered.

5 Essential Questions To Ask When Choosing a SOC Provider

IBM's CEO Ginni Rometty has said: "Cybercrime, by definition, is the greatest threat to every profession, every industry, every company in the world".

Fuelled by the digital transformation of our lives, it's a threat that has grown exponentially in the 21st century. And in the wake of the pandemic, the stakes are even higher: the FBI has reported a 300% increase in cybercrime as homeworking increases the vulnerability of organisational networks.

It's no surprise, then, that many organisations are choosing to outsource their Security Operations Centres (SOCs) to specialist providers who can manage the sophisticated technology platforms required to mitigate this threat.

But, in this complex field, how do you go about selecting a SOC provider? Bypassing the jargon and getting straight to the issues, here we look at five essential questions to ask.

1 Why are an increasing number of businesses turning to SOC-as-a-Service?

To help you evaluate better which SOC provider to choose, it's useful to understand exactly why an increasing number of businesses are turning to SOC-as-a-Service. By looking at the many potential reasons for outsourcing cybersecurity, it's easier to assess which SOC provider can best meet your needs.

Of course, there are a variety of important drivers for the growing number of organisations opting to choose a SOC as an outsourced service. These include:

- The exponential pace of digital and cloud transformation across all industry sectors
- Increasingly sophisticated cyber assaults across diverse attack surfaces
- Massive growth in data volume and complexity generated by organisations of all sizes
- Lack of qualified in-house resources to manage cyber threats and respond quickly
- Lack of visibility across business networks
- Increased pressure to improve efficiency and manage cybersecurity costs
- Growing requirements to demonstrate cybersecurity compliance from clients
- Increases in remote working leading to a growing range of network "weak points"
- Future proofing for rapidly changing commercial and technological environments.

Detailing your specific needs within the context of common issues helps to define a clear set of requirements in which to analyse SOC provider offerings.

2 How do you future-proof your technology choice?

Future-proofing your technology choice involves understanding how a technology platform can benefit your long-term cybersecurity needs. The Security Incident and Event Management (SIEM) platform is at the heart of a SOC, so it's crucial to have a clear set of criteria through which to evaluate this technology.

To provide a framework for this analysis, consider the following four perspectives:

- **Platform architecture**
- **Threat detection**
- **AI and machine learning**
- **Threat response**

Platform architecture

Traditional appliance SIEMs are increasingly unable to manage the growing pace and complexity of today's security challenges. Many organisations are, therefore, turning to cloud-native SIEM solutions which are more scalable, cost-effective and offer better performance.

Cloud based SIEMs have an inherent technology advantage due to their architecture, collecting data across a comprehensive range of users, devices and applications while scaling performance to respond to peak and non-peak activity. Find out how the provider's platform architecture can respond to your needs.

AI and machine learning

Artificial intelligence (AI) and machine learning (ML) are an integral part of the most advanced cybersecurity technology platforms. Check for the capability of AI-powered solutions to analyse millions of events autonomously and learn from previous patterns of behaviour so as to predict new threats.

Threat response

Detecting threats is only useful if an effective and timely response is then triggered. Check what kinds of automated threat responses are available on the technology platform, how they can be customised to your particular needs, and how they are flagged in real-time for the attention of incident-response teams.

3 How do you get the most out of your technology?

Technology platforms on their own do not mitigate cybersecurity threats; it is the ability of the SOC provider to leverage the technology which enables a platform to operate successfully.

To get the most out of your technology, it's important, therefore, to assess the provider's ability to leverage it across four key aspects:

- **Threat hunting**
- **Threat identification**
- **Incident response**
- **Compliance management**

Threat hunting

Effective cybersecurity is as much about anticipating potential future threats (and planning for them) as it is dealing with actual events as they occur.

The fast-changing nature of this field means proactive threat hunting is a crucial part of any effective SOC solution. To be best placed to do this, your SOC provider should be dedicated to mapping the unique topology of your network and its potential weak points.

They should present a clear methodology of how they will hunt for threats which could bypass standard detection protocols. As part of your service provider analysis, find out how they connect with threat-intelligence networks (both via AI and human interaction) and how this informs their approach to your cybersecurity.

Threat identification

Look for a SOC provider who takes a comprehensive approach to risk assessment and threat profiling for your particular organisation. Once this is established, find out how the provider will customise its technology platform to identify risks specific to your activities and sector.

They should provide a security baseline to measure improvement and future success, as well as visibility across all connected systems, identifying high-risk devices.

Incident response

Cybersecurity breaches can happen at any time, so it's critical that your SOC provider has a 24/7 incident-response team that is ready to investigate suspicious activity at a moment's notice. Find out how incidents are triaged and tracked within any automated system; note also how escalation procedures are triggered when a cybersecurity threat requires human analysis and response.

Compliance management

Cybersecurity compliance is an essential part of any due diligence undertaken by your existing and potential clients. Look for a provider that takes a proactive approach to your compliance issues; this should involve a detailed understanding of the regulatory environments in which you work and a pre-emptive model for identifying and implementing required changes. Check they are compliant with ISO27001, PCI-DSS and Cyber Essentials.

4 How do you identify the right people for the job?

As with any complex technology solution, it's crucial to work with people you can trust who will go the extra mile.

To identify the right people for the job, ask yourself how focused the provider is on your particular needs. Will they customise their offering to your specific operations? Will they integrate seamlessly with your in-house specialists? And are they clearly looking for a long-term partnership?

Check the credentials of the specific team that will be designated to manage your account. Assess their level of expertise and years of experience in security analysis and engineering, data science and analysis, threat hunting and incidence response.

Look for transparent financial reporting and verifiable customer testimonials. Check also for the provider's cybersecurity credentials, including 3rd-party audits, certification, use of encryption and operating across multiple sites (to mitigate operational threats).

5 How can you pay flexibly and spend less?

Clearly, you'll want to find the most competitive and flexible price for the quality of service you require from your provider.

To that end, it's worth considering the pricing model a potential service provider offers. A provider who uses scalable cloud-native technology platforms will often provide a consumption-based pay-monthly pricing model, which means you don't pay a fixed monthly fee for capacity that may go unused. Costs can then grow sensibly with your business.

If you're switching to a cloud-based solution you should expect to see a significant reduction in the price you pay.

The takeaway

Choosing a SOC provider is a business-critical issue which can seem a dauntingly complex task requiring high levels of technological understanding.

However, the right provider will help to clarify all the important choices and explain the options relevant to your particular organisation.

With that in mind, asking these five questions is the best way to ensure you find a SOC provider best tailored to your needs at the right price.

Ready to take your cybersecurity to the next level?

Comtact are the UK's leading SOC provider for mid-market through our unrivalled Cyber Defence Centre.

Get in touch to arrange a free consultation.

enquiries@comtact.co.uk | 03452 757575 | www.comtact.co.uk

COMTACT
Cloud. Security. Delivered.