HOW TO CHOOSE A MANAGED SIEM SERVICE PROVIDER IN 10 STEPS

REDLEGG

TABLE OF CONTENTS

HOW TO CHOOSE A MANAGED SIEM SERVICE PROVIDER IN 10 STEPS

Cyber crime costs the worldwide economy $450 billion annually with 81% of the victims failing to detect the breaches themselves. Due to the high number of attacks, security managers are under pressure with CEOs in the United States as they consider cybersecurity their top business priority.

One successful cyber attack could have critical impact on an organization’s reputation. In addition, the average cost of a data breach is $3.86 million, according to a study by Ponemon Institute.
To avoid breaches, organizations have to keep up with the advancing information security world and be proactive to discover and deal with threats.

However, many organizations have major flaws in their security operations. While many of them have their own Security Information and Event Management (SIEM) systems, their internal team is slow in responding to threats and resolving problems. Instead of being proactive, they are reactive, meaning that the security team would only discover a threat after it is too late, so they are unable to prevent it.

IT team performance is often not optimized, and they are unable to focus on company objectives due to routine tasks taking most of their time. Due to their high workload, they can’t concentrate on innovation. As organizations that store sensitive information have to comply with strict rules, many of them are also backtracking on advancing their cybersecurity measures to meet compliance requirements.

LOOKING TO A SIEM SERVICE

To solve these issues, organizations can hire cybersecurity service providers to help with their team's workload and to optimize the security of their companies. But from all the SIEM providers, how do you know which is the best fit for your company?

First, you have to decide whether to outsource all of your SIEM operations to a Managed Security Service (MSS) provider or use a co-managed SIEM service. We'll show you how to choose a co-managed service provider as this SIEM service type will give you better control and flexibility while maximizing your SIEM's value and enhancing security monitoring capabilities.

So, what factors should you consider when choosing a co-managed SIEM partner? Let's walk through ten simple steps.

-1-

TAKE YOUR GOALS INTO ACCOUNT AND PLAN FOR THE LONG-TERM.

The first and most important step in choosing a co-managed SIEM service provider is to plan ahead and determine your goals. Do you want to hire a co-managed service provider to maintain your company's security for five years or longer? Or is this just a temporary solution while you are planning to switch to self-managed SIEM?

It is crucial to build a feasible, long-term security operations plan based on your goals. Make strategies also for scaling your SIEM operations and determine whether the co-managed SIEM provider can fulfill those scalability goals. Also, look for a SIEM service provider who has multiple scalability options for your IT operations expansion, and don't forget to take the fees of such upgrades into account.

-2-
REVIEW THE STRENGTHS OF THE SIEM SERVICE PROVIDER

Analyzing the strengths and weaknesses of a service is always essential. And – as you are handing over a large part of your security operations to a third-party firm – this step is even more crucial in the case of SIEM management and monitoring providers.

To see how one service provider stands out of the crowd, you need to know the "crowd." You may want to compare the SIEM service provider to other cybersecurity firms: Does your co-managed partner have world-class technology? Does the firm have an impeccable reputation in the information security community and industry? How does their staff compare to the provider's competitors? Did the company achieve something significant in the past (e.g., prevented or mitigated a large-scale security breach)? Does the SIEM service provider utilize an analysis platform?

After you have collected the co-managed SIEM provider's strengths, don't forget to analyze its weaknesses too. While every organization has weak points, a critical flaw should be a dealbreaker in case of security service providers.

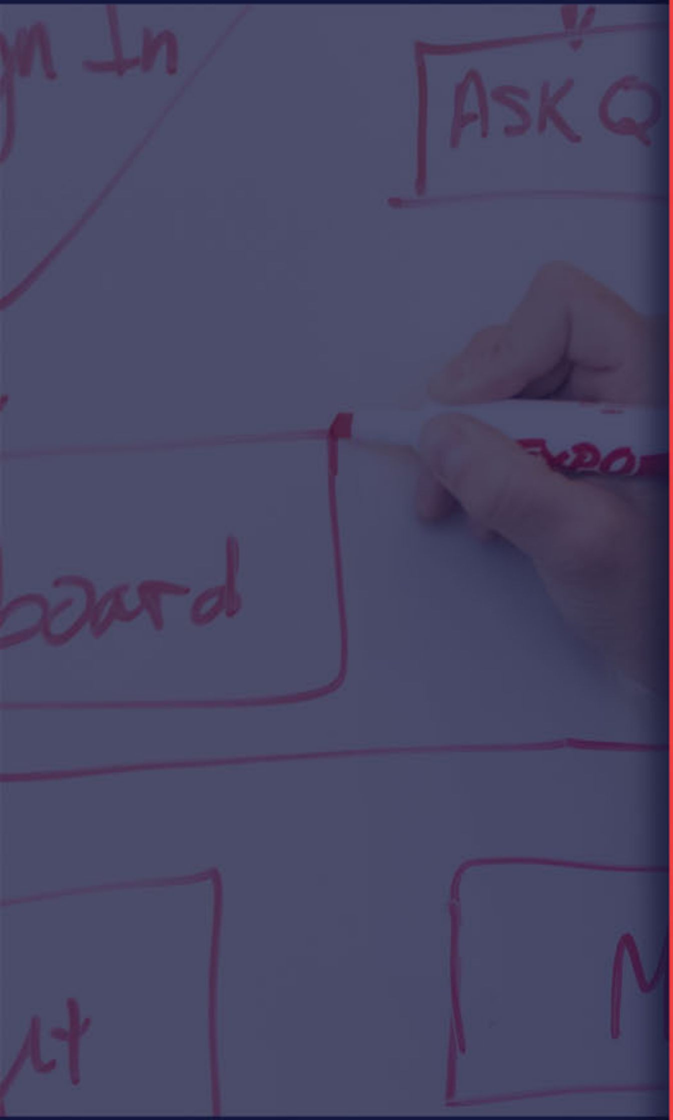
While a SIEM service provider's website or reputation may have you thinking such a service would cost you more than your budget allows, reaching out for a quote may help you weigh your budget and the strengths of a provider. It'll also help you prioritize what you value in a service provider the most, giving you better perspective.

-3- EVALUATE THE SERVICE PROVIDER'S SUPPORT

Cooperation between you and your service provider is crucial. Without it, your SIEM operations will have flaws, and attackers will have a better chance of breaching your network.

To maintain flawless collaboration between you and the service provider and to keep you in the loop, the co-managed partner should offer 24/7 support that is available every day of the year. Say a big NO to any SIEM provider who does not provide a 24/7 x 365 days support. Your business data is at stake, and you want your co-managed partner to promptly respond to your calls and emails, especially in the case of a threat that needs to be prevented or mitigated.

Other than these hard-and-fast guidelines, another important support feature is often customer service. Does the company have an approachable sales team and approachable leadership? Can the service provider communicate clearly and plainly about your environment and discovered gaps in your security?



-4-
CHECK OUT THE CONTENT PACKAGE AND ITS BUILDER

Every SIEM service is different with providers offering various packages and features. Unfortunately, some of the SSPs call their services "SIEM," but they offer only basic security features (e.g., antivirus, firewalls) that will leave your firm's network prone to cyber attacks. Therefore, you need to analyze the content package of the service provider and check if its features provide complete visibility into your business's information technology environment.

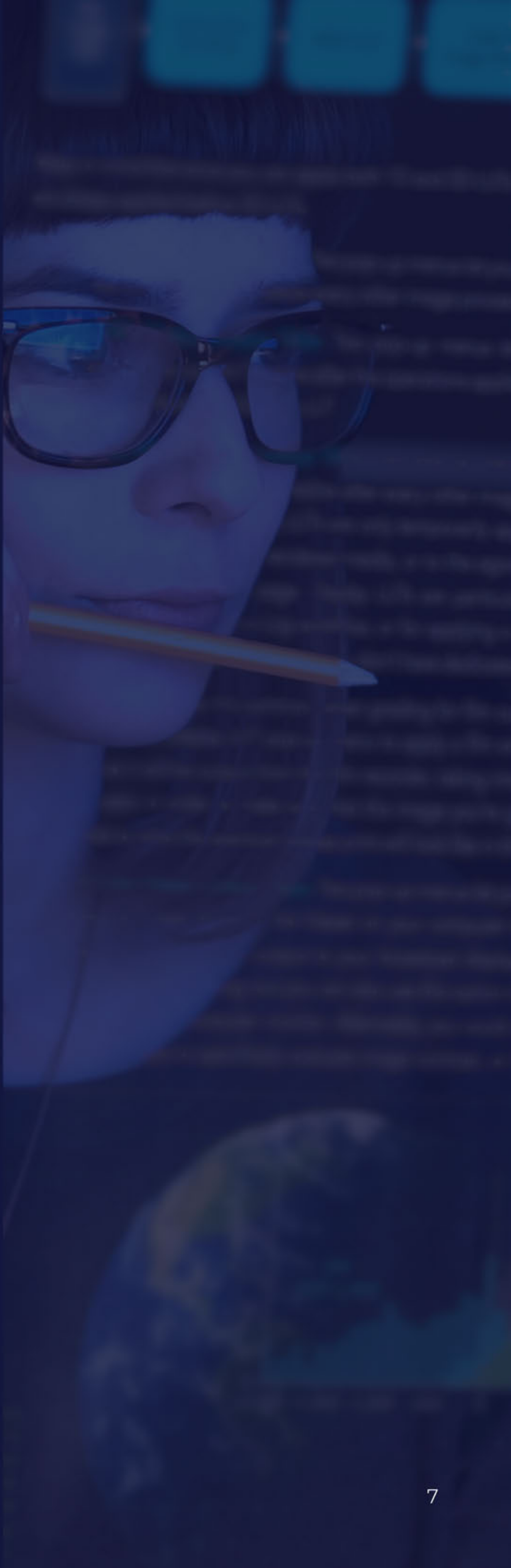
As mentioned in a previous step, you should also vet the service provider who offers the content package.

-5-
CALCULATE THE CONTRACT'S HIDDEN COSTS

While the co-managed partner can quote you a price for its SIEM services, you will most likely have hidden, unrealized costs associated with the service. One of the hidden fees is the purchase of hardware as most SIEM deployments start with this step. An upgrade requires more storage, thus, more hardware purchases. Furthermore, as soon as your machine data grows, so will your expenses associated with processing and indexing that data as most service providers charge fees by data volume.

And finally, one of the most important – and often overlooked – hidden costs is time. As the old quote goes: "Time is money." Signing contracts, deploying your SIEM, as well as training your IT team can all take quite some time. Along with time, you should round up all the hidden costs of a SIEM service and make some rough predictions to avoid any unpleasant surprises.

Also when looking at your SIEM service contract, whether it's a one-year or three-year agreement, don't be afraid to ask these questions up front if your provider doesn't bring this up in your scoping meeting.



-6-
CONSIDER COMPLEMENTARY SERVICES

Many of the co-managed SIEM providers offer extra services, such as integrated threat intelligence to accelerate the detection of new threats (and the remediation process, if needed). While you may not necessarily need such services for a well-functioning co-managed SIEM service, you should at least consider whether you have the budget and whether it is worth it for you to use any extra services the security provider offers.

-7-
GAUGE THE PROVIDER’S METHODOLOGIES

You should carefully check both the methods the co-managed partner uses for threat discovery and analysis as well as determining the costs of the service. Most vendors use a total cost methodology that includes the labor costs of operating the SIEM such as training, deployment and implementation support, turnover, and recruiting as well as fully-loaded labor rates.

-8-
ASSESS THE VALUE OF THE SERVICE PROVIDER'S TRAINING

One of the advantages of using a co-managed SIEM service is training. As your IT team and the co-managed partner work together to operate your SIEM, the provider's team shares its expertise with your employees, helping them optimize their own, and your security system's, performance.

Before hiring a service provider, you should check what type of training they offer and the experience of the provider's team. Finally, add these together to evaluate the value of the security provider's training.

-9-
EVALUATE THE PROVIDER’S WORK

Ideally, the SIEM service provider had numerous past clients and is currently working with multiple companies. You have to use the experiences of these organizations to your advantage in order to get a picture of how the provider would handle your co-managed SIEM operations.

Analyze the services the SIEM partner has provided to its clients by requesting case studies (or finding existing ones), look for trusted reviews, and reach out to companies the service provider is currently working with or worked with before and ask about their experiences.

-10- MAKE SURE YOU KNOW YOUR ROLE IN THE SERVICE RELATIONSHIP

The final step in choosing a co-managed SIEM service provider is to ask yourself one question: are you okay with the responsibilities? Unlike managed security services, a co-managed SIEM needs you to have an existing IT team, even if you only have a handful of people, that will work together with the co-managed partner to handle your security operations. Therefore, you need to dedicate time and other precious resources in order to achieve a working security system.

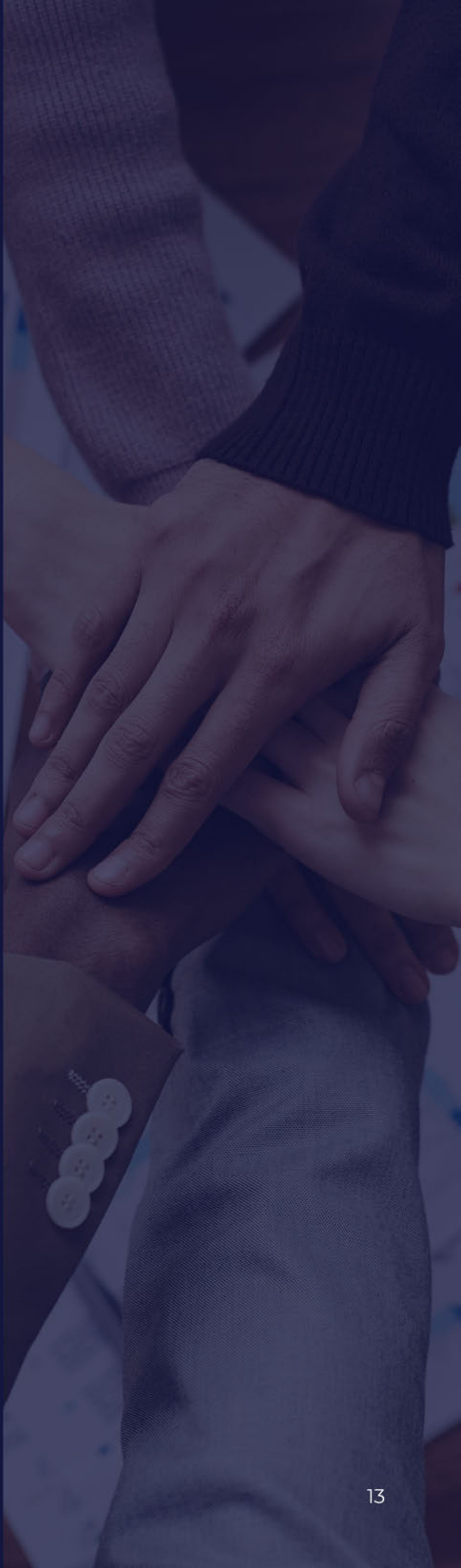
Be honest when answering this question. Some companies don't have the necessary resources or don't want to dedicate them to setting up and maintaining co-managed SIEM. For these firms, hiring a fully managed security services provider may be a better choice.

YOUR ORGANIZATION'S SECURITY IS AT STAKE

Hiring a co-managed partner will free up a significant part of your IT team's workload while providing them the necessary training and enhancing the security of your company. In the meantime, the co-managed option will also give you a fine balance between control and flexibility.

However, you should take your time to assess your options before hiring a service provider. Remember to follow the steps listed here, and it's okay to be "picky" in choosing a co-managed SIEM service provider: Essentially, you're hiring your newest team member.

If you are looking for a co-managed SIEM service provider, then feel free to check out RedLegg's services to start!



CONTACT US

Geneva, IL

877.811.5040

dotell@redlegg.com

redlegg.com

REDLEGG