DEFENSE.COM™

A buyer's guide to:

Managed Security Information and Event Management (SIEM)

Discover what you need to ask a Managed SIEM service provider before ingesting your logs.

Introduction

When you're thinking about investing into SIEM, handing over the reins to a seasoned Security Operations Centre (SOC) can really pay off, especially when you consider the costs and manpower involved in doing it all in-house. But finding the perfect fit for your business and ensuring you get the best value from a Managed SIEM service requires careful consideration.

In this guide, we've compiled essential resources to assist you in navigating the decision-making process. From understanding crucial considerations to asking vendors the right questions to gauge their suitability, we've got you covered. Plus, we'll provide a handy summary of the onboarding process so you're ready for a smooth transition. Let's dive in, helping you make the right choice.

> *Look for a provider whose SOC analysts can serve as an extension of your security team, allowing you to focus on your core business.*

Why do you need a Managed SIEM Service Provider?

Exploring a Managed SIEM service could stem from various motives within your organisation. Pinpointing the underlying reasons will not only assist in setting practical expectations but also in choosing the ideal Managed SIEM provider and crafting a security monitoring and response strategy tailored to your unique needs. Here's some common drivers for seeking a Managed SIEM service:

1. **Addressing a lack of in-house expertise:**
If you lack the skills to manage and monitor a SIEM platform 24/7, a Managed SIEM service offers access to experienced security professionals who can promptly analyse and respond to security events, enhancing your internal team's capabilities.

2. **Optimising costs:**
Building and maintaining an in-house Security Operations Centre (SOC) with dedicated staff, infrastructure, and resources can be expensive, especially if you are a small or medium-sized business. Outsourcing to a Managed SIEM provider allows you to benefit from enterprise-grade security capabilities at a fraction of the cost.

3. **Scalability:**
As your organisation's IT infrastructure and security requirements evolve, a Managed SIEM service can quickly scale to accommodate changes, ensuring that the appropriate level of security monitoring and analysis is always in place for your growing or fluctuating needs.

4. **Compliance and regulatory requirements:**
Your industry may have strict regulations requiring extensive logging, monitoring, and reporting of security events, or adherence to standards like ISO 27001 or PCI DSS. A Managed SIEM service can automate log collection, correlation and reporting for compliance.

5. **Struggling to keep up with emerging threats:**
Internal teams can be overwhelmed by the volume of threat intelligence and the effort needed to apply it to specific assets and attack surfaces, Managed SIEM providers access the latest threat feeds and security updates, enabling effective detection and response to new cyber threats.

6. **24/7 monitoring and incident response:**
A Managed SIEM service provides 24/7 monitoring and incident response capabilities, ensuring security events are addressed promptly, even outside of business hours when your team is unavailable.

What do you expect from the Managed SIEM Service Provider?

As an IT leader, you must choose the right Managed SIEM provider to suit your organisation's needs. Given the constant evolution of cyber threats, it's important to choose a vendor capable of providing threat detection, investigation, and response capabilities through their skilled SOC analysts. Here's some examples of common requirements and questions you can ask a vendor to see if they'll be a good fit for you:

24/7 service

For reliable security monitoring and incident response, partner with a Managed SIEM provider that offers 24/7 SOC operations. Their round-the-clock coverage enables prompt detection and response to cyber attacks, minimising lateral movement and business impact. In your evaluation process, assess the provider's staffing and availability. Verify they have adequate SOC personnel and technology in place to maintain consistent monitoring and incident response across all shifts, including nights, weekends, and holidays.

Key questions to ask:

- How do you allocate internal resources to ensure continuous and scalable security monitoring and incident response?
- How do you ensure that information is effectively handed over and shared between different shifts within the SOC?
- Can you share examples of how your 24/7 SOC operations have effectively supported customers through high-severity incidents?

Detecting complex threats

A Managed SIEM provider's SOC team needs to have the capability to detect indicators of compromise and potential attacks within your environment. This entails analysing external threat intelligence and comparing it against your organisation's systems and data, enabling you to stay ahead of threats before they can cause harm. Achieving this necessitates experienced SOC analysts who possess a deep understanding of attack lifecycles and can effectively triage alerts.

Key questions to ask:

- Can you describe your processes for incorporating external threat intelligence into your threat detection capabilities?
- How do you ensure that your team is always up to date on the latest attack techniques?
- Can you provide examples of advanced or sophisticated cyber threats that your SOC analysts were able to successfully detect and mitigate?

Skills and expertise

Your Managed SIEM provider needs to have a highly skilled SOC team capable of effectively managing security data across your environment, configuring, and maintaining the SIEM solution for comprehensive, tailored threat detection and response. The analysts should possess a well-rounded skillset in security monitoring, threat intelligence, and communication, thoroughly trained and certified in the latest security practices and trends.

Key questions to ask:

- Can you share details on the experience levels and qualifications of your SOC analysts?
- What certifications and ongoing training does your team receive to maintain their skills and knowledge?
- How do you ensure your analysts stay up to date with the latest security best practices, threat landscapes, and industry trends?
- Can you provide examples of how your team has effectively configured and optimised SIEM solutions for organisations with similar needs and requirements?
- What processes do you have in place to minimise alert fatigue and ensure efficient triage and analysis of security events?

Threat identification and communication

When the SOC team detects a potential threat, standard practice is often to prioritise it based on severity. For critical (P1) threats, they promptly notify via phone call with detailed analysis and remediation steps. For lower priority (P2) threats, the SOC team will investigate thoroughly but may not call you immediately. Instead, they will provide clear guidance on appropriate actions and next steps via a shared platform or by email.

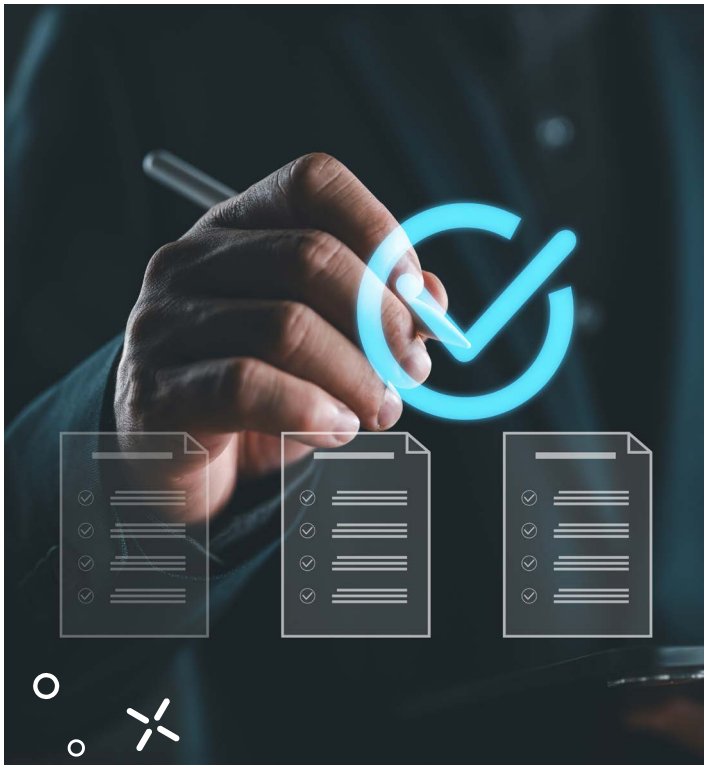
It's important to note that while this outlines a common approach, communication protocols and threat prioritisation methods can vary among Managed SIEM providers.

Key questions to ask:

- Can you outline your threat prioritisation and severity classification methods?
- What are your notification protocols and timelines for different threat severity levels?
- What mechanisms are in place for us to provide feedback or request additional information during ongoing investigations?
- Can you describe your process for sharing detailed analysis and recommendations after an incident has been contained?

Ultimately, the Managed SIEM service needs to give you the benefits of enterprise-grade security monitoring and response, without requiring you to build and maintain the infrastructure and specialised security expertise in-house. Look for a provider whose SOC analysts can serve as an extension of your security team, allowing you to focus on your core business while their analysts handle the complexities of modern threat detection and response.

Key evaluation criteria for selecting a Managed SIEM provider



You need to thoroughly assess potential vendors across several key areas to ensure the chosen solution meets your organisation's unique needs and can grow with you. By examining the factors below, you can make an informed decision that strengthens your cyber security posture while providing good value for money.

Let's look into these key considerations to help you select the Managed SIEM provider that's the best fit for your organisation:

Log collection and platform integrations

Assess how well the Managed SIEM provider's platform collects and integrates log and event data across your IT environment by identifying all relevant data sources (servers, network devices, applications, etc.) and determine if the provider supports them natively or through integration. Evaluate their data collection methods (syslog, APIs, agents, etc.) and ensure they align with your requirements. Test their data normalisation, enrichment, and correlation capabilities across different data sources. Then, review their data ingestion rates, storage capacity, and retention policies to ensure they meet your needs. The effectiveness of the SIEM solution hinges on its ability to seamlessly collect, parse, and normalise data from disparate security tools, network devices, applications, and other business data sources you have already deployed.

This allows you to understand if all the relevant log data can be consolidated into a centralised platform, providing a unified view and correlation of events from across your infrastructure. Without proper data ingestion and third-party integrations, the SIEM will have limited visibility, reducing its monitoring and analysis effectiveness.

User experience and reporting

A managed SIEM is only as effective as your ability to derive value from it. Evaluate the usability of the provider's interface, customisable dashboard, and range of predefined/custom reporting options. Detailed search queries across historical data for compliance monitoring and aiding investigations is a core tenet of most SIEM platforms, and vendors will usually provide at least 90 days of immediate log searching with up to 1 year in archive. By understanding the provider's options for long-term data storage, you ensure that the data retention and retrieval processes align with your organisations policies and regulatory obligations.

Compliance and regulatory support

If you operate in a highly regulated industry, ensure the SIEM provider demonstrates proven expertise supporting mandates like PCI DSS, ISO 27001 and more. You'll want to look for a provider that has use cases tailored to the specific mandate your industry needs to adhere to. They should be able to demonstrate a deep understanding of the technical controls and audit requirements specified in each requirement. For example, PCI DSS compliance requires monitoring for secure system configurations, file integrity, two-factor authentication use, and more.

Scalability and performance

You need to ensure that the platform can handle your organisation's current data volumes and event rates without experiencing performance degradation.

As your business grows and generates more security data, the SIEM solution should be able to scale to accommodate increasing data ingestion and analysis requirements. Ask about the providers infrastructure scalability measures, such as their ability to add more compute resources, storage capacity, and processing capabilities to support higher data volumes and event rates.

Provider reputation and client satisfaction

When evaluating Managed SIEM providers, consider their reputation and client satisfaction. Review online feedback, request client references, and inquire about their client satisfaction metrics like Net Promoter Score (NPS) or Customer Satisfaction (CSAT). This due diligence helps gauge the provider's service quality and client relationship management.

Service level agreements (SLAs) and support

Closely scrutinise the SLAs and support offerings when outsourcing to a Managed SIEM service provider. SLAs outline uptime guarantees, incident response time, and support channels, while the customer support model, including dedicated account managers and security analysts' expertise, determines the promptness of communication and incident response. You'll also want to assess their change management, software updates and patch management processes to ensure the SIEM platform remains current with security updates while minimising operational disruptions. By vetting these aspects, you can ensure your preferred provider maintains a high level of security and operational efficiency for your organisation.

Pricing and cost considerations

When evaluating a Managed SIEM service provider, you need to carefully analyse the pricing model and associated costs. Different providers may employ varying pricing strategies, such as charging per event, per GB of data ingested, per data source, or per user. Thoroughly evaluate the provider's pricing model and ensure that it aligns with your organisation's budget and projected growth. As your business expands and generates more security data, the costs associated with the SIEM solution should scale accordingly and remain within your financial constraints.

How can we prepare for a Managed SIEM service?

Once you've chosen your preferred Managed SIEM provider you can start preparing for onboarding or at least be aware of what to expect. Here's what you need to know:

1 Pre-Implementation planning

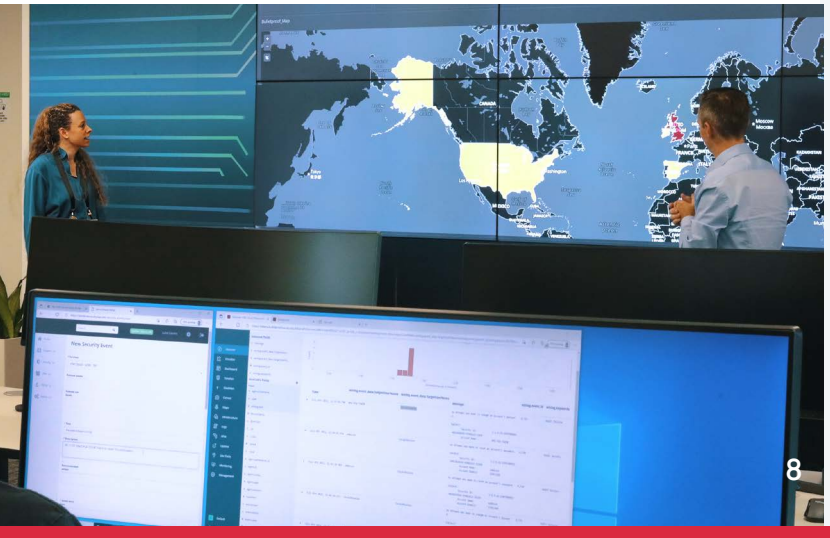
Before beginning the deployment of a Managed SIEM solution, you need to lay the groundwork. Taking these preparatory steps will ensure a smooth implementation tailored to your organisation's specific needs.

- **Identify stakeholders**
  Gather the right people across the organisation to align on goals and provide input.

- **Define environment**
  Document all existing security tools, data sources, and infrastructure to integrate with SIEM.

- **Review policies and requirements**
  Ensure the SIEM implementation accounts for regulatory needs and follows internal processes.

- **Allocate resources**
  Determine the budget, staffing, and resources required for a successful deployment.



2 Implementation

With planning completed, the next phase focuses on the actual implementation of the SIEM solution. This involves kickstarting the project, deploying the SIEM technology across your infrastructure, and integrating it with various data sources.

- **Project kick off**
  Formally initiate the project with the chosen SIEM provider. They will work with you to understand what your network infrastructure, users and systems look like so that they can design your implementation.

- **SIEM deployment**
  You'll then be supported by the provider's technical team with the deployment package including scripts, software, and documentation to get the SIEM up and running. This will include deploying agents or collectors to ingest security logs into the SIEM platform.

- **Baseline environment**
  The SOC team will then work closely with you to understand what normal looks like for your organisation. This is where you need to provide information such as who your users are, what times they are accessing your systems, what kind of tooling you have within your environment and what kind of behaviour they should expect to see. This baselining not only helps the SOC team understand you as an organisation but also helps them tune out any false positives.

3 Ongoing operations

Once implemented, the SIEM solution transitions to a live service for continuous monitoring and management by the SOC team.

- **Live monitoring**
  The SOC team will be constantly monitoring your environment but also tuning on detection rules or alerting so they can identify what is and isn't an abnormal event.

- **Periodic reviews**
  You will regularly review the service quality, make enhancements, and optimise your logging with the provider to ensure the service continues to meet your needs.

- **Reporting and compliance**
  Work with the Managed SIEM provider to set up monthly reports and dashboards to allow you to review logs and integrate the findings into processes. This will help your compliance efforts and allows you to leverage SIEM insights into your future security strategy.

SIEM isn't a one and done thing

Things are going to change within your organisation, your systems, and your processes and that inevitably means you are going to need to adapt on the security side as well.

Here are a few things to keep in mind once your SIEM is live:

- Make the customer success team and the SOC team aware of your point of contact within the business. This is important to ensure critical alerts are escalated quickly and appropriately.

- Have an incident response plan. It doesn't matter if you have the best Managed SIEM solution, if things are coming in and nobody knows what to do when you receive an event or an indicator of compromise, you're not going to deal with that incident very quickly. Make sure the right people are involved and everyone is up to date with training.

- Keep the SOC team informed about any organisational changes that may impact security monitoring. For example, if new employees are hired, particularly those working remotely, their initial login attempts may generate alerts within your SIEM system. By proactively notifying the SOC team about such changes, they can incorporate this information into the existing baseline data, reducing the likelihood of false positive alerts.

Summary

Securing your organisation against cyber threats is an ongoing commitment that requires constant vigilance, advanced security tools, and specialised expertise.

Partnering with a reputable Managed SIEM service provider can be an invaluable way to bolster your security posture while optimising resources and costs. When you leverage the capabilities of a Managed SIEM solution, you can also gain access to:

- A team of highly skilled security analyst
- Cutting-edge threat detection technologies
- Robust incident response processes

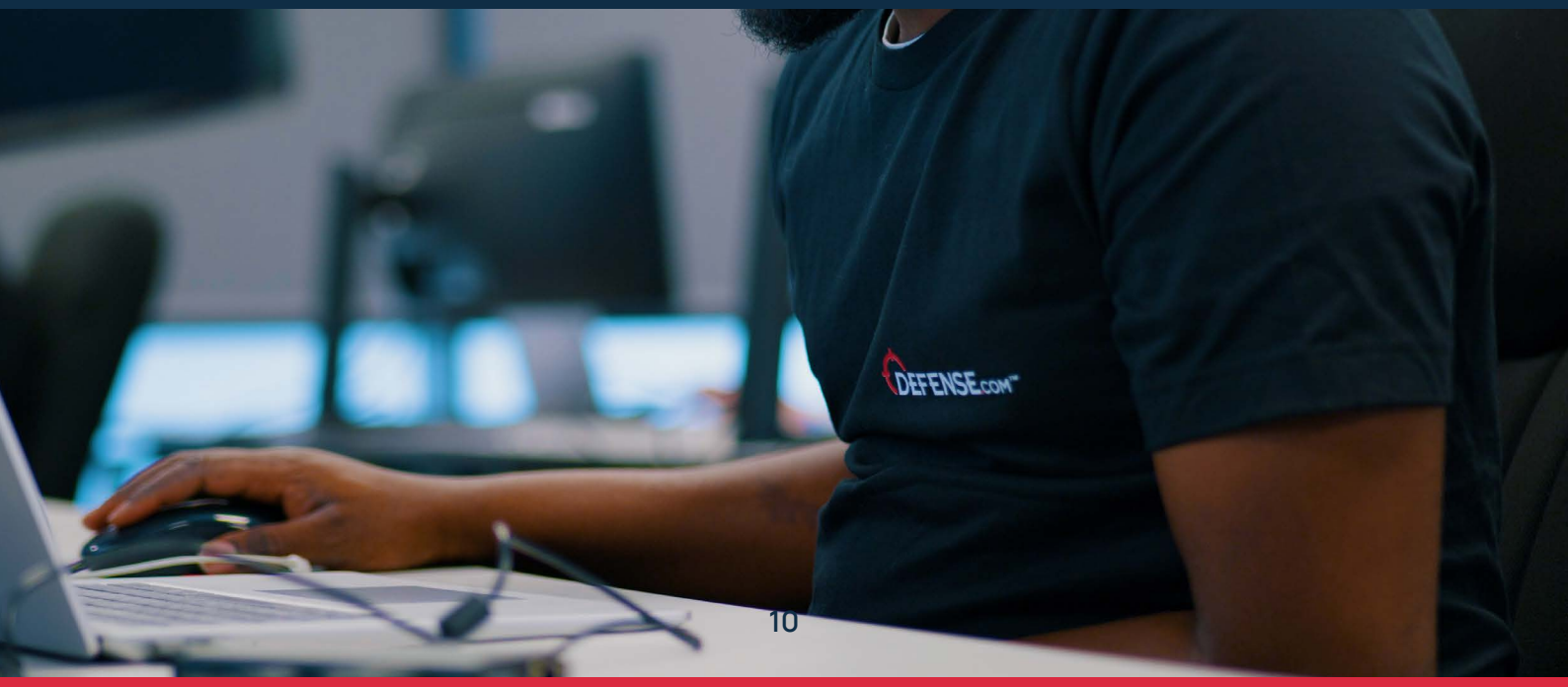
This combination empowers your organisation to:

- Stay ahead of threats
- Rapidly identify and mitigate potential breaches
- Maintain compliance with industry regulations and standards

Ultimately the decision to embrace a Managed SIEM service is a strategic investment based on your organisation's capabilities and priorities.

By entrusting your security operations to a team of dedicated professionals, you can redirect valuable internal resources towards core business objectives while maintaining peace of mind knowing your systems and data are protect by industry-leading security measures.

> *When considering the right provider, remember that a Managed SIEM service is not a one-size-fits-all solution. You need to foster a collaborative partnership with your chosen provider and maintain open communication channels. This allows you to tailor the service to align with your evolving business needs, ensuring maximum value and return on your investment.*
>
> **Daniel Sampson,**
> **Head of Customer Operations,**
> **Defense.com**



Case study

Housing provider chooses Defense.com to provide a Managed SIEM/SOC service.

A housing provider successfully streamlined their security operations with automatic alert prioritisation and outsourced SOC analysts.

Here's what you can learn from their experience:

Read the full client success story

Context is key: A constant stream of security alerts without context or priority can cause real threats to be missed. You can avoid this by tuning your SIEM deployment so that only genuine security incidents are raised to your attention.

Scalability matters: As your business evolves, so should your security solutions. When considering your threat detection options, choosing a solution that can scale with the growth of your business will help ensure you don't have to switch vendors, and potentially lose your attack surface visibility during the transition.

Peace of mind: You need to know your business is protected 24/7 and not just during working hours. An outsourced SOC solution provides the peace of mind that security alerts are identified round-the-clock.

Added value across the board: An outsourced security solution can offer additional benefits to standard log monitoring. Selecting a vendor that offers other security tools can help you bolster other areas of your defences and make better use of your resources.

About Defense.com

Defense.com offers a Managed SIEM service delivered by a team of UK-based expert SOC analysts.

- **Deploy anywhere**
  Collect security logs from any source, including endpoints, applications and cloud systems.
- **Uncover threats**
  Never miss a security risk with experienced SOC analysts monitoring your network 24/7.
- **Prevent breaches**
  Quickly respond to threats with clear, step-by-step remediation advice.
- **Stay compliant**
  Meet the requirements of PCI DSS, ISO 27001 and more with proactive SIEM log monitoring.

Learn more

+44 (0)1438 500 209 contact@defense.com www.defense.com