

Overview

Key Findings

- Managed security information and event management (SIEM) is widely adopted by organizations with security that is midlevel in terms of maturity. These organizations are looking to own, deploy and utilize their security tool investments, instead of utilizing shared service provider tools.
- Security teams have a wide range of complex responsibilities. Outsourcing certain elements of security delivery eases the workload of the security teams and provides resources that can be focused on operational requirements.
- Buyers who have invested in SIEM technology use managed SIEM services to derive more value. They can use managed SIEM services to get assistance with decisions around strategy, architecture, maintenance, development or support. This leads to better security operations results.
- Managed SIEM providers offer varying service levels and are able to cater to most buyers' needs.

Recommendations

Security and risk management (SRM) leaders looking for assistance in running and operating a SIEM tool should:

- Evaluate the different service models offered by providers that deliver managed SIEM services, selecting the one that is strategically aligned to the needs of their security team. Such needs may include providing off-hours staffing, augmenting internal skill sets or reducing maintenance overhead.
- Select providers based on partner programs that your SIEM vendor operates. The buyer's SIEM vendor will have a list of dedicated partners that are qualified to support — and specialize in — their SIEM technology.
- Plan engagement with providers by aligning the service capabilities with the objectives and roadmap of security teams in order to drive maximum technology return. Assess whether the vendor can deliver adjacent features such as SIEM use case creation, threat intelligence collation, automation and behavioral analytics.

Market Definition

Managed security information and event management services provide remote management or monitoring of a client-owned SIEM solution. Services include management (for example, ensuring availability and performance), creation of a wide range of SIEM use cases and configuration of APIs, log parsers and reporting content. Other services include detection content writing and tuning (whether this is 24/7 or hybrid), off-hours security monitoring and alerting, and lightweight investigation of security issues.

Market Description

Managed SIEM services are delivered remotely, but provide a dedicated instance of a security information and event management technology on a per-customer basis. Service providers often support multiple SIEM technologies and deployment models. Managed SIEM services offer midmaturity users the opportunity to combine the management and oversight of their detection technology stack (even highly complex examples) with a service that offers only maintenance, monitoring and investigation capabilities. SIEM is delivered using a flexible delivery model that can work in conjunction with a customer's security operations center (SOC), providing off-hours support or 24/7 capabilities.

There are a number of different service capabilities that can be offered as part of a managed SIEM service. The key core capabilities delivered are:

- The initial deployment of a large number of SIEM use cases and the ongoing development of use cases that align with your specific organization. These use cases should cover a broad range of log sources and types of threat, and also help with compliance mandates.
- The installation and configuration of the SIEM tool, associated data source onboarding and configuration of SIEM user interface (UI) in line with client requirements.
- Configuration of the application programming interface (API).
- Configuration of the log parsers.
- Remote performance, availability and capacity monitoring for the SIEM.
- Defined responsibility for keeping the SIEM current (for example, hot fixes, functional updates and minor or major version upgrades).
- Creation of detection content which includes writing and tuning.
- Designing and building detection and reporting content for the SIEM.
- Configuration of SIEM UI in line with client requirements.

Some of the key optional capabilities delivered are:

- Configuration of SIEM applications for SIEMs that have an application marketplace.
- Assistance with migration from legacy SIEM providers.
- Real-time threat monitoring — either 24/7, 8/7, 8/5 or after normal business hours and weekends. Vendors may offer containment and remediation support — usually as add-on services.
- Lightweight investigation of security issues from misconfiguration of engineering to security alert diagnostics.
- Training of personnel in SIEM capability.

Some managed SIEM providers offer services on top of selling and supporting their own SIEM technology, while many other providers support multiple commercial SIEM solutions. Managed SIEM services are generally procured either with the SIEM tool already installed, or less frequently, with the expectation that the provider will recommend a SIEM that will meet the customer's requirements.

Alerts can be either forwarded to the provider's security analytics platform in the SOC, or the provider can maintain connections (through a secure channel) to the customer's SIEM tool to check for alerts.

Services of this type are suited to organizations that do not have the appropriate amount of resources to manage and monitor the SIEM tool (especially when it comes to 24/7 coverage). Managed SIEM services allow them to keep more control over their SIEM technology and their data, the use cases it supports, and escalation processes and operations.

Market Direction

The managed SIEM market has a long history — sometimes being advertised as “managed SOC” or “SOC as a service.” More recently with the introduction of services such as managed detection and response (MDR) and managed endpoint detection and response (EDR), a more defined level of service has emerged specifically for SIEM. This is coupled with the growing availability and attractiveness of SIEM-as-a-service versions of platforms (sometimes referred to as “SIEM-aaS”). Managed SIEM has a compelling adoption rate and increasing customer demand. SIEM technologies are becoming more accessible and more mid-security-maturity buyers are entering the market having accelerated their security needs and maturity by adopting cloud-based IT. Gartner expects the market to grow over the next 24 months as an increase in custom application development and SaaS adoption demands the flexibility of a SIEM tool for monitoring purposes.

Managed SIEM services are available from providers that partner with a multitude of SIEM providers. Each vendor is likely to partner with at least two SIEM providers, as these vendors also need to reassure clients that they have expertise with the SIEM technology that they offer services around. Buyers will have already worked through their due care and due diligence while building an RFP to select a SIEM technology, and there will be further assessments that need to be made when choosing a managed SIEM provider. [How to Deploy a SIEM Solution Successfully](#) provides recommendations and guidance on how to build the program and implement it.

Managed SIEM vendors will increasingly be required to demonstrate their expertise in industry verticals and their ability to design and build rule content. They will need to show that they can detect potential threats, and configure systems to respond. Aligning the organization's security use cases is necessary for success, whether the organization sits in the financial sector, manufacturing, healthcare or another industry. There are common use cases for each vertical (such as Active Directory password spraying attacks). This generic content is the basis of most of today's offerings. Future offerings will involve vertical-specific content, which may make up part of the subscription cost for the service offered.

Market Analysis

There has been a surge in cloud-based security tooling and multiple service offerings for clients — including services such as MDR (see [Market Guide for Managed Detection and Response Services](#)). SIEM is evolving to be primarily delivered from the cloud as well. This has enabled buyers to purchase SIEM with other cloud offerings. It has also enabled advancements in SIEM vendor offerings — to include adjacent security capabilities, such as security orchestration, automation and response (SOAR), user entity and behavior analytics (UEBA), threat intelligence platforms (TIPs) and case management. These are all traditionally threat, detection, investigation and response (TDIR) use cases.

Before embarking on a managed SIEM journey, the buyer should understand if managed SIEM is the correct option for the organization. SRM leaders should work with peers from different departments to clarify why the purchase is required — not just for the product, but for these styles of services as well. There should be a strong focus on the use cases that are aligned to outcomes that are critical to the organization. Without these requirements, the purchase may fail.

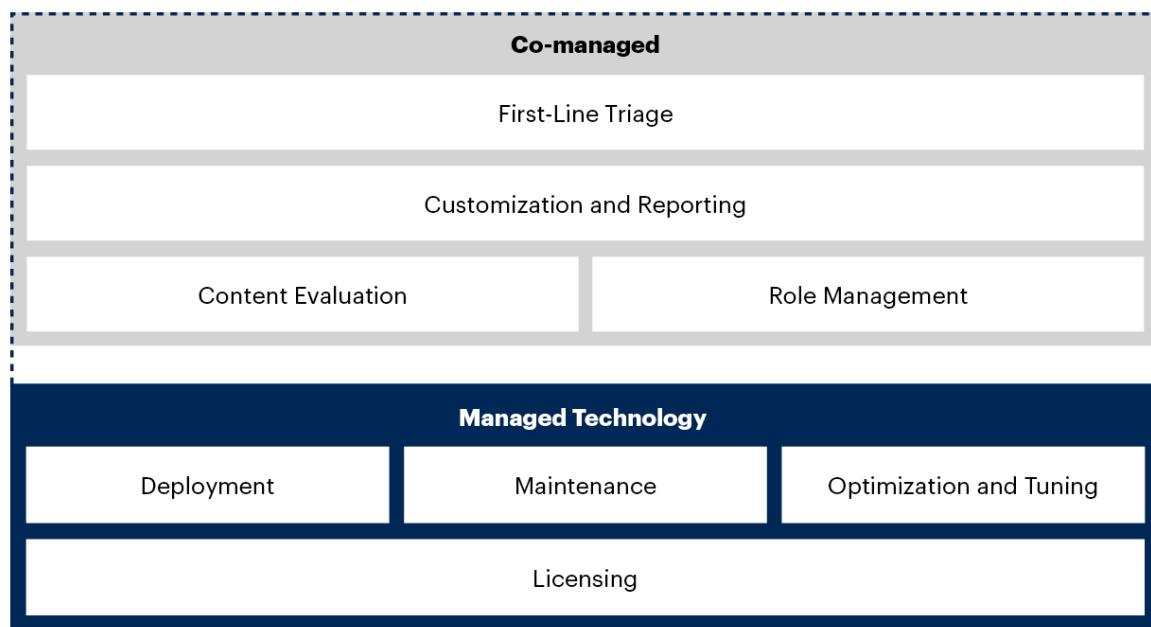
A key value proposition with managed SIEM vendors is the architectural design and implementation services that are offered to the buyer. Clients historically have had issues with strategic and tactical architectural decisions that are not focused solely on SIEM, but rather, are focused on any security tool that has already been purchased. Managed SIEM vendors have experience with service delivery in different markets — for example MDR and managed security services (MSS). For more information, see [Market Guide for Managed Security Services](#) and [Market Guide for Managed Detection and Response Services](#).

Managed SIEM is, however, more nuanced and many MSS don't specifically offer managed SIEM services — opting for more consultative or implementation focused offerings instead. This means that suppliers have encountered many common mistakes and are familiar with areas that have been overlooked by a buyer attempting to design and build security tools and infrastructure. Buyers who employ a managed SIEM vendor to assist in architecture decisions are able to get the most out of the purchase of a SIEM tool.

Managed SIEM services are delivered remotely, and manage the client-owned security information and event management technology. Service providers can often support multiple SIEM technologies and deployment models, which means vendors can have partnerships with SIEM vendors with experience of the service delivery. Service providers can offer midmaturity users the opportunity to combine the management and oversight of their detection technology stack — even highly complex examples in security use case design, content creation, delivery and continuous content revision. Managed SIEM services can be delivered using a flexible delivery model (see Figure 1) that can work in conjunction with a customer's SOC as off-hours support, or deliver 24/7 capabilities with maintenance, monitoring and investigation capabilities. Managed SIEM also helps with maintenance — keeping the SIEM technology current with hotfixes, functional updates, minor or major version upgrades and appliance refresh in end-of-life (EOL) hardware.

Figure 1: Managed SIEM Segments

Managed Security, Information and Event Management Segments



Source: Gartner
756810_C

Gartner

Managed SIEM buyers may also be looking for vendors that can offer further professional services to design the SIEM infrastructure and integrations — providing project planning and implementation. Vendors can assist the buyer's security team with training on different elements of the SIEM, and even assist with items that are not always the top priority (for example, around the configuration of the SIEM user interface [UI]). This service offering is detrimental to the success of a buyer's SIEM program. Poorly deployed SIEM configurations will impact performance when the SIEM is being spun up, when it is operational, and when improving detection or maintaining current detection logic.

Managed SIEM vendors can assist buyers with alerting and detection services. Many clients who use SIEM struggle with the challenge of responding to the alerts generated by the SIEM. There are many reasons for this — from lack of training, lack of process, volume of alerts, length of working hours and even a lack of resources. Managed SIEM vendors can ease the burden by utilizing their resources to assist their clients in different types of delivery. Managed SIEM vendors can provide staff augmentation for triaging alerts and training. A benefit of the service is to utilize the vendor's resources to assist with hybrid working. For example, organizations can use the vendor's analysts as a tier-1 and tier-2 triage team that identifies where issues should be escalated. Alternatively, organizations can ask the vendor to provide support in the form of an out-of-hours service.

Managed SIEM is a service delivered to clients that are looking to own their SIEM technology, but want to be able to pick and choose the

options required, rather than relying on what the vendor wants to provide.

Different Service Models Offered by Providers

There are multiple ways to consume managed SIEM services. Terminology and marketing can make it confusing for buyers to purchase the service that they require to meet their needs. Managed SIEM delivery can be split into two subcategories. These capabilities can be delivered in isolation or incrementally to enable more customized offerings (see Table 1 and Table 2).

Table 1: Managed Technology-Driven Functions

[Enlarge Table](#)

Delivered Capability	Description
SIEM licensing	The procurement, maintenance and negotiation of SIEM licensing based on customer needs.
Deployment	The installation of the SIEM software, and the configuration of data ingest integrations for response and ticketing.
Maintenance	The monitoring and management of the health of the platform, including patching and technology maintenance.
Optimization and tuning	Iterative assessment processes to evaluate the performance of data sources and licensing resource consumption of configured correlation rules and reconfiguring and implementing fixes to these elements.

Source: Gartner (August 2022)

Table 2: Co-management Functions

[Enlarge Table](#)

Delivered Capability	Description
Content evaluation	User-driven and threat-landscape-driven assessments of the validity, usefulness and relevance of configured correlation rules, alerts and data sources. Implementing new correlation rules based on customer or industry demands.

First-line triage	Delivered out of normal working hours or as a 24/7 service capability to support functions within the buyer's business. Delivering false positive reduction and investigation.
Customization and reporting	The on-demand creation of new reports and dashboards to meet business needs.
Role management	The management of roles on the platform — providing access and role changing needs of the business and to maintain security and policy for compliance.

Source: Gartner (August 2022)

Both the technology management and co-management of the SIEM platform require regular professional services engagement that will improve and enhance the level of service offered by vendors. This team extension allows an organization to achieve improved security outcomes from their SIEM technology investment without needing to employ or train a large team. Buyers must understand which elements of the offering best serve the needs of their security teams.

Dedicated Partners Who Are Qualified to Support and Specialize in Your Chosen SIEM Technology

When the organization has made the decision to go to an external managed SIEM service partner, it can start focusing on selection. Selecting the correct partner for the managed SIEM journey is a decision that should be planned with the goals of the business and the security strategy at the forefront. Selecting a partner requires a large amount of planning in terms of technology, procedures and key requirements. Creating and building an RFP will help the organization with all the requirements that are needed from the vendor. [Quick Answer: The Best Way to Formulate a SIEM RFP](#) will help a buyer with the requirements that are needed to formulate the RFP.

In most scenarios, the organization has chosen the technology, and wants to review the vendors that have experience with the SIEM. Making sure the business selects the correct vendor with the criteria needed to support the SIEM is critical to success. Selecting the right partner requires organizations to take a comprehensive approach:

- Evaluate a managed SIEM partner that uses the technology as part of other service deliverables the vendor might have, including MDR and MSS.
- Question the potential provider as to how long they have been a technology partner and have used the SIEM technology. The provider partnership level (silver, gold, platinum or equivalent) can indicate the level of investment and partnership maturity with a particular SIEM vendor. Ideally the vendor should have a minimum of two years experience with the technology.
- An established managed SIEM provider will have extensive security expertise and experience with the product. Question the vendor on the roadmap of the product and how it integrates with the service they provide. How does the

vendor work with the technology partner and how do they show those lessons in deliverables within the service?

- Most modern SIEMs have orchestration and automation capabilities (see [Market Guide for Security Orchestration, Automation and Response Solutions](#) and [SOAR Will Not Make You Better at Running SIEM](#)).
- Ask for examples of other managed SIEM deployments that they have completed and support. Ask how the deployments are planned and what is the average length of the deployment. Additionally, the ongoing improvement of the SIEM is critical as most SIEMs have minimum deployment life cycles measured in the three-to-five-year time frame.
- Managed SIEM vendors will have professional security professionals who can provide expertise in deployment and, importantly, optimization of the technology. Investigate how the provider can assist with any log retention planning, log collection management, and asset identification.
- Probe the vendor on how they plan to integrate with your organization's existing technology. Managed SIEM can demonstrate value in the way that it allows the SIEM to integrate with the organization's technology and the subsequent security outcomes when there is potential malicious activity. The vendor should have experience in onboarding different technologies and illustrate the value that the integration will provide in the generation of security alerts.
- Managed SIEM vendors have trained staff across multiple disciplines. The buyer's organization will need to review qualifications, number of staff and level of staffing. The buyer will require the vendor to have managed SIEM staff and security analysts with the correct levels of seniority. They will need to have security engineering staff with disciplines in API creation and maintenance, parser creation and maintenance, and content creation related to the technology of the buying organization.
- Buying organizations should review the managed SIEM level of support from the vendor's security analysts. Subject to the delivery model that the buyer selects, the support could be in hours or off-hours. The buyer must understand what deliverables the supplier will provide.
- Another beneficial element to managed SIEM is training and maintaining a strong partner alliance. In simplistic terms, the vendor should act as an extension to your security team and provide training related to the SIEM technology and analyzing alerts to build queries in the SIEM. Organizations should aim to understand the engagement protocol and the additional benefits that a partner program with managed SIEM can bring.

Align Service Capabilities With the Objectives of Your Security Teams

An organization's SOC should be operating in line with the cybersecurity strategy, which aligns with the organization's business strategy in understanding and

addressing cyber risk. Every security team will have goals and objectives. There is also a strong focus on the technology operated within the team.

When conducting research on managed SIEM, there must be an internal exercise to establish the goals of introducing managed SIEM to the security team and what is required. What is the project scope and why is the security team looking to partner with a managed SIEM provider? Creating a list of requirements will greatly assist in aligning the priorities and thought process of the team. While discussions in the security team will align security priorities, there is an option to improve the process of gathering requirements by engaging with other areas of the business (such as infrastructure, networks, application, HR and finance). Understanding where different areas of the business see risk, and how the security team builds the requirements into managed SIEM, will greatly improve the decision making in selection of the vendor.

Identifying gaps in the SOC can be an awkward discussion to have internally if the focus is purely on gaps, but conducting these meetings will show where the organization has gaps worth addressing. Concurrently, it will highlight your organization's strengths, and services should help you improve on existing capabilities as well. Therefore, identify the security use cases the organization is trying to cover for managed SIEM. SRM leaders should look for answers to the following questions:

- What is the vertical that the organization resides in and the threats we are susceptible to?
- Why are we moving to managed SIEM?
- Is the organization using managed SIEM for 24/7 incident coverage or is it using a hybrid model?
- How will incident escalations work? Will the SOC need to create security playbooks or other SOAR use cases for the desired outcomes?
- How can the vendor assist with any compliance or local law regulations — assuring the organization has thought about coverage with PCI DSS, HIPAA and other regulations?
- Does the organization require managed SIEM to address gaps in its security landscape?
- Is vendor assistance required for security expertise in alert analysis or security engineering?
- Will using a managed SIEM vendor assist with scalability and expertise in different facets of the technology, cloud, application and other areas?
- How will introducing managed SIEM reduce or optimize the team's workload? Will the SOC have to create a responsible, accountable, consulted, informed (RACI) matrix of responsibilities?
- How will the organization's SOC work with the vendor's managed SIEM services with regards to DevSecOps? Who will work on developing APIs and building security into our workflows?

- How will the organization's SOC work with the vendor's managed SIEM services on content development with regards to new and existing content? What will be the process of identification of threats within current alerts? Will the organization generate new content on new threads with the vendor?

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Market Introduction

A list of representative vendors is provided in Table 3. This is not intended to be a list of all the providers in the managed SIEM market. It is not, nor is it intended to be, a competitive analysis of the providers (see Note 1).

Table 3: Representative Vendors in Managed SIEM

[Enlarge Table](#)

Vendor Name	Representative Product
AT&T	Managed SIEM
Advantio	Managed Detection & Response
BlueVoyant	Platform Management for Azure Sentinel
BT	Security Managed SIEM
CyberCX	Managed SIEM
Capgemini	Invent
GoSecure	Titan Managed SIEM
Herjavec Group (Cyderes)	Managed Services
IBM	Security Qradar SIEM

<u>Integrity360</u>	Managed SIEM
<u>Kroll (Redscan)</u>	Managed SIEM
<u>NCC Group</u>	Managed Security Services
<u>NTT</u>	Managed SIEM Services
<u>Optiv</u>	Co-Managed SIEM and Security Monitoring
<u>Proficio</u>	Managed SIEM
<u>ReliaQuest</u>	Greymatter
<u>SharkStriker</u>	SIEM as a Service
<u>Stratejm</u>	SIEM-as-a-Service
<u>Talion</u>	SIEM Platform Management
<u>Tata Consultancy Services (TCS)</u>	TCS SIEM
<u>Trustwave</u>	Managed SIEM
<u>Unisys</u>	Managed Security Services
<u>Verizon</u>	Managed SIEM

[Vodafone](#)

Managed SIEM

[Wipro](#)

Security Management Center

Source: Gartner (August 2022)

Market Recommendations

When deciding if to use a managed SIEM provider and services, consider the following:

- Is our organization actually mature enough to utilize a SIEM? SIEM platforms are complex. Managed SIEM services are designed to remove some of the burden of operating and maintaining a SIEM platform, while ensuring that the organization maintains some of the required skill sets. Organizations that consider themselves to be low-security-maturity should consider more in-depth, non-technology-oriented detection and response services, such as MDR.
- Does the organization want to remain on-premises or move to the cloud? Many organizations are cautious when moving to the cloud from legacy, on-premises SIEM. Many are nervous about the skills needed to move and whether planning or licenses are required. Managed SIEM providers can provide assistance throughout the entire planning process.
- What are the organization's long-term goals for managing security monitoring? Managed services provide an easy-to-acquire skills graft for organizations. This provides a short-term solution, but security and risk management leaders must consider their long-term strategy. If developing maturity internally is part of that plan, then managed SIEM is a solid stepping stone.
- How long can the organization wait for the capability to be up and running? SIEM is not an out-of-the-box security solution. Managed SIEM providers offer some acceleration to the development and installation of a SIEM platform, however the typical SIEM deployment still takes between three and six months to deliver recognizable value. Buyers should consider their immediate security monitoring requirements and whether managed services or less-complex security solutions such as EDR could meet their needs.
- Are the requirements for monitoring well developed? Service providers offer varying levels of customization. However, without a full understanding of what you require from a SIEM or the associated service, the initial quotation for such a service could spiral. Buyers must set delivery milestones, with actionable requirements; and they must fully understand the cost of overrun.
- What happens when changing technology or service provider? Some managed SIEM engagements add on the delivery of the technology and licensing, and are delivered on third-party infrastructure. Buyers must make themselves aware of, and plan for the eventuality that they may wish to

change provider or technology, ensuring that they can get a copy of their data, and correlation rule and report logic. They should also look to ensure that they have the option to continue utilizing the technology without the services provider.