MEGAPLANIT

WHITE PAPER

The Definitive Guide to SOCaaS

Reduce Costs & Improve Security Outcomes with a Modern Alternative to Managed SIEM

Trusted Security & Compliance Partners

WWW.MEGAPLANIT.COM

Table Of Contents

MEGAPLANIT

Address: 8700 E Vista Bonita Dr, Scottsdale, AZ 85255, USA
Call: 1-800-891-1634
Email: info@megaplanit.com
Visit: www.megaplanit.com

Executive Summary

As cyber threats become increasingly common and sophisticated, organizations are struggling to maintain a sufficient level of security and compliance. Many are turning to managed security service providers to monitor and secure their digital assets and data.

However, most organizations struggle to identify the ideal cybersecurity partners, solutions, and services for their needs. This process is made even more difficult by the industry's prevalence of confusing jargon, conflicting advice, and misleading service descriptions.

Although the term has been badly misused, SOCaaS is a genuinely new model for delivering managed security monitoring services. It can help organizations of all sizes and across all industries reduce costs and improve security outcomes.

This white paper will cover everything security leaders need to know about SOCaaS and help them determine whether it could be an appropriate solution to their organization's security and compliance needs

Key Learning Points:

1. SOCaaS is a managed security monitoring service that encompasses a variety of traditional SOC functions, including log management, intrusion detection, file integrity monitoring, and security incident investigation.

2. Although similar, SOCaaS is not the same as Managed SIEM. The value proposition is similar, but the method of delivery is very different. SOCaaS uses cloud hosting and software agents to avoid the need for secure remote network access.

3. Outsourcing security monitoring offers a host of benefits to organizations, including greatly reduced costs, faster response times, and enhanced security outcomes.

4. While SOCaaS can be delivered as a stand-alone service, but it is often used in combination with other managed security services to fulfill the specific security and compliance needs of the customer organization.

SOCaaS: More Than a Buzzword

Cybersecurity has never been a simple topic. With so many unique threats and such complex network environments to secure, organizations of all types and sizes are struggling to keep up.

Add to this the difficulty of staying compliant with complex and evolving industry compliance frameworks, and it's no surprise that so many security teams are overwhelmed. Despite a 141% rise in cybersecurity budgets between 2010 – 2018, an incredible 73% of security teams are understaffed and overworked.

Put simply, despite an exponential rise in the availability and quality of security technologies and services, most organizations still struggle to achieve "enough" security to meet basic risk-management and compliance needs.

And as the need for cybersecurity has grown and the industry has expanded, organizations have been faced with a further challenge: **Confusion.**

Cybersecurity is complex, and industry jargon, buzzwords, and conflicting advice have made it incredibly difficult for non-security specialists to distinguish between the solutions and services on offer. To make matters worse, vendors routinely use the same terms to describe completely different levels of service.

At best this leads to confusion. At worst, it leads organizations to make the wrong decisions about where to invest their limited security resources.

A Solution To An Overwhelming Situation

One big way that organizations can minimize costs while boosting their capabilities is by outsourcing certain cybersecurity functions to an expert provider, called a Managed Security Service Provider (**MSSP**).

MSSPs offer a wide range of services, from managed security technologies to full detection and response capabilities. And among the most recently added services for many MSSPs is something called SOCaaS. Unfortunately, due to widespread misuse and conflicting definitions, the term SOCaaS — which was only recently coined — is already at risk of being labeled nothing more than a buzzword.

But SOCaaS is not a buzzword. It's a new way of delivering well-established managed security services with lower upfront costs and reduced complexity. In this white paper, we'll provide a definitive explanation of what exactly SOCaaS is, how it's delivered, and the types of organizations it is appropriate for.

After reading this paper, you'll understand:

What SOCaaS is, what services it does (and doesn't) include, and how it's delivered.

Why SOCaaS is often confused with Managed SIEM, and how the two services differ.

How outsourcing monitoring can help organizations boost their security and save costs.

Where SOCaaS fits into the wider landscape of managed security services.

Why MegaplanIT is the ideal SOCaaS provider and MSSP partner for your organization.

*Source: Varonis,:The Future of Cybersecurity Budgeting | Ponemon - Staffing the IT Security Function in the Age of Automation

What is SOCaaS?

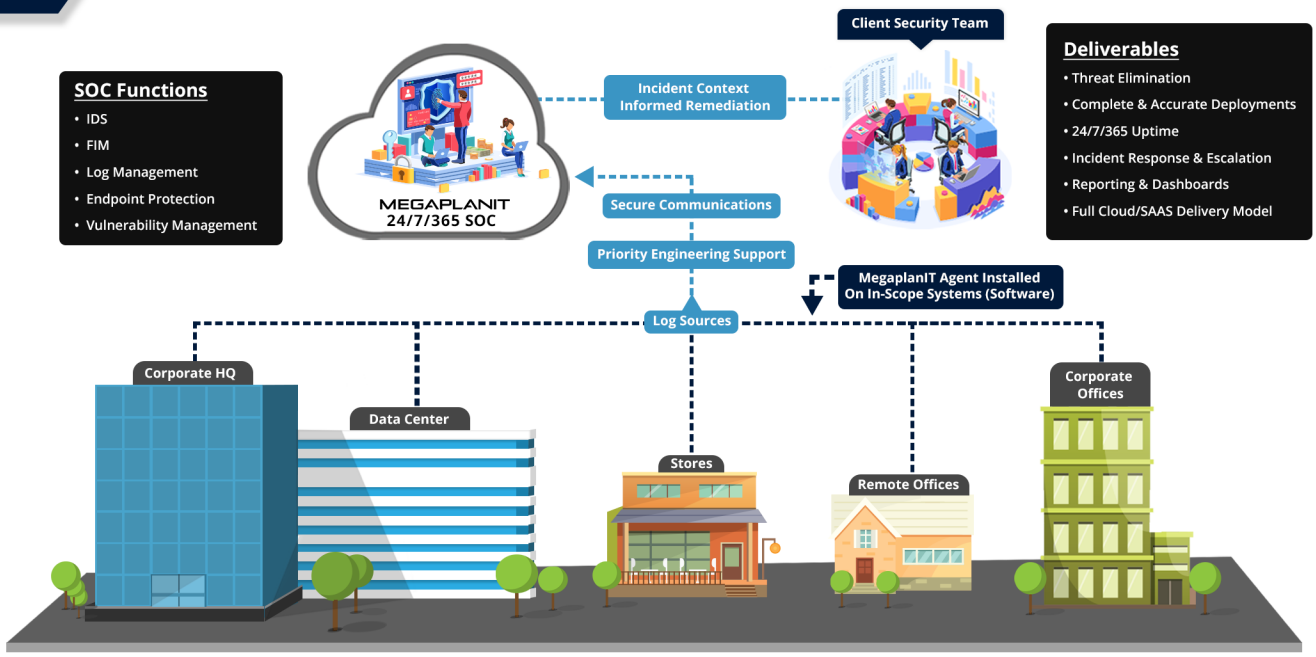
SOCaaS stands for Security Operations Center-as-a-Service. It's a managed security monitoring service that provides organizations with the benefits of a fully-equipped and staffed SOC — without the need to build that resource in-house.

Since building a fully-equipped SOC in-house is both cost-prohibitive and logistically impossible for many organizations (more on this later) SOCaaS is a means for them to achieve an otherwise-impossible level of security against cyber threats.

SOCaaS fulfills a similar purpose to its more commonly recognized cousin, the Managed SIEM. In fact, the value proposition of these two services is so similar that many MSSPs have simply re-branded their Managed SIEM service as SOCaaS. This has caused confusion about what exactly SOCaaS is, and has led many to question whether the term is simply a buzzword.

Despite the term's misuse, SOCaaS is a distinct and clearly definable managed security service, with some key differences to a Managed SIEM. We'll cover these differences in the next section.

SOCaaS



Who is SOCaaS Right For?

SOCaaS can be appropriate for a wide range of organizations. At one end of the spectrum, it is a good fit for small organizations that lack security resources and need to fulfill more comprehensive security and compliance requirements than they can manage in-house. At the other end, SOCaaS can also be an excellent option for larger organizations that are faced with deciding between spending millions on building an in-house SOC or outsourcing some of their security needs.

The critical point here is that SOCaaS isn't chosen in place of other managed services. It fulfills a specific set of security requirements that are valuable to many organizations, and which combine well with a variety of other managed security services depending on the customer organization's needs.

Remember: MegaplanIT provides a wide range of managed security services that cover the full Prevent, Detect, Respond spectrum.

How is SOCaaS Delivered?

One of the most important things to understand about SOCaaS — which sets it aside from many other managed security services — is that it does not require inbound access to the customer organization's servers or systems. Instead, as the name suggests, SOCaaS takes a cloud-hosted, Software-as-a-Service (SaaS) approach to security monitoring.

The SOCaaS vendor providers customer organizations with a software agent, which is installed on all in-scope terminals. Whether an in-scope system is considered in-scope is usually determined by compliance frameworks like PCI-DSS, HIPAA, and NIST. SOCaaS is charged on a per system basis.

Once the SOCaaS agent is installed on a systems, security monitoring data is sent securely to a cloud server, and retrieved securely from there by the SOCaaS vendor. Again, no inbound access is required — SOCaaS uses a pure SaaS delivery model, enabling rapid deployment and avoiding the cost of additional hardware and maintenance.

Key Benefits

• **Reduce Cyber Risk:** SOCaaS helps organizations manage cyber risk by drastically reducing the likelihood of security and/or data breaches occurring.

• **Defend against the latest cyber threats:** Expert MSSPs equip their SOCs with real-time threat intelligence, enabling them to correlate suspicious network activity with the very latest cyber threats.

• **World-class incident response and recovery:** Dedicated MSSPs can identify and respond to cyber threats in minutes, instead of days or weeks, drastically reducing the risk of asset damage or theft. MSSPs also use file integrity monitoring to determine whether an attack has caused any real damage, greatly aiding recovery efforts.

• **Cutting-edge talent and technology:** MSSP's retain professional SOC analysts who are accustomed to working in many different environments and have broad security experience and expertise. They also equip them with the very latest security technologies.

• **24/7/365 security:** SOCaaS guarantees organizations always-on protection for their in-scope systems. This is something most organizations can't achieve in-house.

• **Fulfill and maintain compliance:** Easily fulfill some of the more difficult requirements of common compliance frameworks like PCI-DSS, HIPAA, and NIST.

• **Reduce costs:** The costs of SOCaaS are far lower than those associated with building and maintaining an in-house SOC, making it much more attainable for most organizations.

Choosing Managed Security Services

The important thing to realize about MSS is that it's not a tiered system that starts with simple monitoring services and ends with MDR. While it's understandable to consider Managed Response the "gold standard" of MSS, in reality, MDR is unsuitable for many organizations for a variety of reasons — most notably, because most organizations don't want to give the level of access needed for MDR to an external vendor, nor are they comfortable with an MDR vendor taking action or making changes within their environment without their review and approval.

Instead, choosing an MSS — and, for that matter, an MSSP — is more like selecting from an à la carte menu. It's about determining the specific security needs of the organization and choosing the appropriate combination of managed services to meet those needs.

What's Included in SOCaaS?

SOCaaS combines a number of crucial SOC monitoring and threat analysis functions that many organizations are unable to conduct effectively in-house. The principal functions of SOCaaS include:

Intrusion Detection
Full monitoring of incoming, outgoing, and internal network traffic for potentially malicious activity using the latest network monitoring and intrusion detection (IDS) technologies.

File integrity monitoring
Tracking of all file modifications made by users or digital services. This is often the only way to determine whether a cyberattack has caused any damage. It's also a core requirement under most industry compliance frameworks.

Log management
Continual monitoring, validation, secure storage, archiving, and retention of critical system logs. This is essential for compliance and security purposes but is often extremely labor-intensive when performed in-house.

Security incident investigation
Identifying, investigating, and assessing security incidents. This routinely takes days or weeks to be done in-house, but can be completed in minutes with the involvement of an expert MSSP. With SOCaaS, remediation and recovery actions are determined by the MSSP and completed by in-house security personnel.

Incident contextualization and threat intelligence
Rapid confirmation and categorization of security incidents by experienced security analysts and confirmed using the latest real-time threat intelligence. This process ensures the fastest possible identification and resolution of security incidents, even when they involve the latest cyber threats.

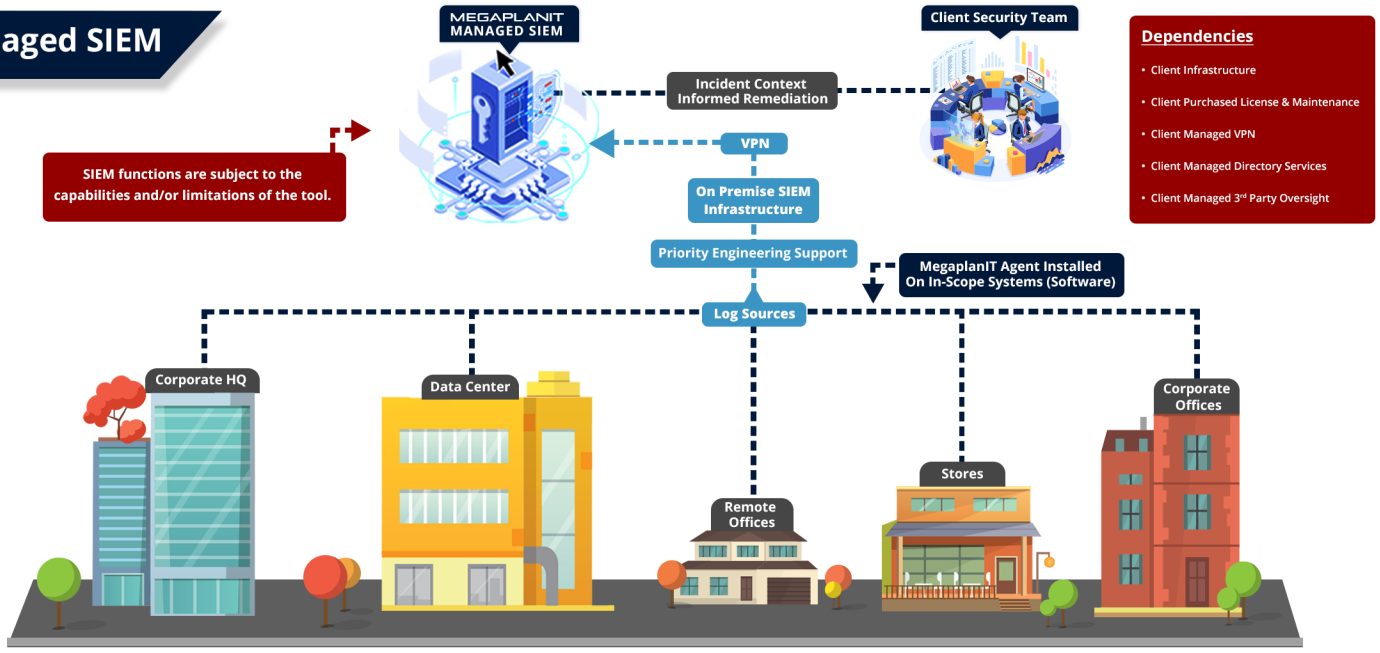
24/7/365 coverage
SOCaaS ensures organizations are protected at all times from cyber threats by the latest cutting-edge security technologies, manned by highly skilled and experienced security practitioners.

SOCaaS vs. Managed SIEM

If SOCaaS has so many benefits, why isn't its uptake more widespread? As we alluded earlier, perhaps the biggest hurdle to increased uptake of SOCaaS has been the term's misuse. Ultimately, as with most security buzzwords, SOCaaS has been used so widely — and with such varied meaning — that it has become almost meaningless to many potential customers.

In particular, a number of cybersecurity information sources and vendors have repeatedly used the term SOCaaS when they were really talking about Managed SIEM. That's problematic because, as we're about to see, there are some key reasons why an organization might prefer SOCaaS over the more traditional Managed SIEM.

Managed SIEM



The Key Difference: Inbound Access

As noted earlier in this paper, the initial value propositions of SOCaaS and Managed SIEM are essentially the same. Individual MSSPs may draw small distinctions between what's provided with each service, but even then the differences are typically very minor. What is different, however, is the manner in which each service is provided.

In a traditional **Managed SIEM** service, the MSSP will install, configure, and maintain a physical, externally-managed SIEM server inside the customer organization's network. This server will gather information about network activity from software clients which are installed on all in-scope servers and assets. Why is this important? For two reasons:

1. There are additional costs associated with Managed SIEM services due to the need for hardware installation and maintenance.

2. The MSSP will need to set up secure inbound access to the server in order to manage the SIEM product and access collected monitoring data.

Many organizations are reticent to allow inbound access because it adds ongoing complexity to their network environment and requires additional 3rd party oversight. With SOCaaS, there is no need for inbound access to the customer organization's network, because the service is cloud-based and delivered "as-a-service". A software client is installed on each in-scope asset, which sends monitoring information securely to a dedicated cloud server. The MSSP collects information directly from the cloud server via a secure communication protocol, so no direct access is required to the customer's network.

Understanding Managed Security

To understand how SOCaaS fits into the wider MSS landscape, it's important to consider the three basic functions of cybersecurity:

1. Prevent
2. Detect
3. Respond

Prevention is primarily achieved through security technologies like firewalls and anti-virus solutions, and through ongoing security precautions such as vulnerability and patch management. All of these solutions can be managed in-house or delivered as a managed service, depending on the organization's needs.

Detection relies on security monitoring and analysis — the main functions of a SOC. Security monitoring uses SIEMs and other security technologies but usually requires a human analyst to make a final decision, which is sometimes informed by threat intelligence. Both SOCaaS and Managed SIEM fit into the Detect function, as do individual services like log management, intrusion detection, and file integrity monitoring.

Response is the business end of cybersecurity, where direct action is taken to block, remediate, and/or recover from a security incident. Many managed security services — including SOCaaS — are designed to inform this final stage, but the action is usually taken by internal security personnel. The only exceptions to this are Managed Detection and Response (MDR) services, in which MSSPs take complete responsibility for both Detect and Respond security functions.

Which is Right of My Organization?

SOCaaS and Managed SIEM are two delivery models that have similar goals and benefits. Neither is objectively better or worse than the other — it comes down to the specific needs of the customer organization. If your organization is considering outsourcing security monitoring, and you need help deciding which model is appropriate for your organization, you should discuss your requirements with your MSSP.

With that said, the following is a simple overview of the unique benefits of each solution. Note that both solutions deliver a level of security monitoring that far exceeds what most organizations can achieve in-house.

SOCaaS Benefits:

- Rapid set up
- Lower up-front costs
- Reduced complexity
- Cloud analytics draws upon shared threat models
- Simplified architecture
- Subscription licensing model without multi-year contracts (OpEx friendly)

Managed SIEM Benefits:

- Includes direct management of SIEM solution (which is complex)
- May deliver a higher standard of security and compliance depending on technical capabilities and tuning of the solution
- Threat sharing models can be limited
- Traditional CapEx financing

Why Outsource Security Monitoring

There are three primary reasons why it may be worthwhile for an organization to outsource security monitoring to a SOCaaS vendor.

Cost

Building SOC capabilities in-house can be extremely expensive and labor-intensive. One estimate places the annual cost of building and maintaining a SOC at between $1.42 – $6.25 million, depending on the level of functionality required.

Of course, the exact cost of building a SOC varies significantly depending on the size, complexity, and security needs of an individual organization. Keep in mind, though, that building a true 24/7/365 SOC requires at least six full-time security analysts. Given that security analysts earn somewhere from $72,000 – $123,000 per year (and the costs of employment conservatively add at least 30%) even an entry-level team will cost in excess of $500,000 per year just for staffing.

Most organizations simply do not have the security resources to build even basic SOC capabilities, and certainly can't hope to rival the level of service available from MSSPs.

Lack of In-House Skills

The widely publicized cybersecurity skills gap is not a joke, nor is it exaggerated. For a typical organization, it can be extremely difficult to find and retain security analysts with the skills and experience needed to fulfill crucial SOC functions. Even when they can, candidates often require a considerable amount of training — an investment that could prove misplaced given the security industry's high rate of turnover.

And when SOC personnel inevitably move on, the difficult recruitment process starts again.

And it's not just about cost. In many cases, organizations are simply unable to find qualified candidates to staff their SOC. And given that the latest research suggests that the skills shortage is getting worse over time rather than better, this problem is not likely to go away any time soon.

Cyber Risk

Even when an in-house SOC exists, organizations rarely have the security resources or skills needed to monitor security information and events in real-time.

This problem is an extension of the well-known "alert fatigue" phenomenon, where security analysts become apathetic to incoming security alerts because the volume is far beyond what they can expect to cope with. According to a 2018 study by Cisco, organizations are only able to investigate 56% of security alerts, with the remaining 44% going unchecked or incorrectly classified.

As a result, it often takes days or even weeks to identify and respond to a cyber threat that could have been dealt with in minutes by a specialist MSSP. Naturally, this delay can have a huge impact on the damage caused by an incident, as well as the resulting costs of remediation and recovery.

*Sources: Expel - How much does it cost to build a 24x7 SOC? | US News - How Much Does an Information Security Analyst Make?
*Sources: ESG & ISSA - The Life and Times of Cybersecurity Professionals 2018 | Cisco - Annual Cybersecurity Report 2018

MegaplanIT: Your Partner for Security & Compliance

As the volume and sophistication of cyber threats rise, many organizations are turning to MSSPs to help them build and maintain a high level of security and compliance. In this paper, we've seen how SOCaaS can help organizations of all sizes boost their security capabilities while minimizing costs and reducing the burden on in-house security resources.

Before you can realize these benefits, however, you must choose an MSSP to partner with.

At MegaplanIT, our SOC analysts and security consultants are fully certified and have decades of experience helping organizations like yours stay safe from cyber threats. Based out of our state-of-the-art SOC in Scottsdale, Arizona, our SOCaaS service is one part of a wider service offering that can meet the specific security and compliance needs of your organization.

Why Partner With MegaplanIT?

We pride ourselves on being the world leaders at delivering tailored security and compliance solutions with outstanding customer service. Here are some of the top reasons why our customers choose to partner with us year after year:

Cutting-Edge, 24/7/365 SOC — MegaplanIT's SOC is equipped with the latest security technologies and fully staffed at all times to deliver always-on protection for your in-scope systems.

Highly Skilled & Experienced Analysts — All our SOC analysts are fully certified and highly experienced at protecting a wide variety of systems and environments.

Compliance Specialists — All our managed services are designed with compliance in mind, and we retain experienced compliance assessors in-house at all times. Got a question about compliance? Our customers are free to ask us about any issues or concerns they have and rely on us to help them solve their toughest compliance challenges.

Full Range of Services — We take pride in being the one partner your organization needs for all its security and compliance requirements. In addition to our comprehensive managed security services, we also provide a full range of compliance, security testing, consulting, and training services.

Adapted to Your Needs — Unlike many of our competitors, our services are flexible and matched to your organization's specific requirements.

Trusted Partners — We build long-term relationships with our customers, and partner with them year after year. We understand their organization and go beyond the contract to help them stay secure and compliant.

100% US-Based — None of our services are outsourced or subcontracted. Everything is delivered directly from our headquarters in Scottsdale, Arizona.

Get Started Today

Choosing an MSSP to partner with is not a decision to be taken lightly. Equally, deciding on a specific combination of services to meet your organization's needs can be difficult. If you have any questions about SOCaaS, managed security services, or anything else to do with security or compliance, we can help.

Visit our website today to arrange a FREE consultation.

AICPA SOC | PCI DSS COMPLIANT | Nevada Gaming Control Board IT Service Provider Gaming License

About MegaplanIT

At MegaplanIT, our expert security consultants and QSAs are fully certified and have decades of experience helping businesses like yours stay safe from cyber threats. We build long-term relationships with our customers and provide holistic services to meet all your security and compliance needs.

Every business has security and compliance challenges. Maybe you've had to repeatedly ask a compliance assessor to complete reports you could share with internal management, or your QSA was switched out halfway through an assessment. Maybe you've been sent a different security consultant every year, or your supplier surprises you with unplanned and unbudgeted extras to complete the project. Whatever the situation, the result is the same—the cost and level of effort required to stay secure and compliant never go down.

Most of all, with MegaplanIT everything is clear and above board. There are no hidden costs or surprises, and you'll never have to track down one of our consultants or assessors. That's our guarantee.