The sophistication and commonality of cyberattacks has become a top concern for businesses across the world. This concern has even trickled down to the SMB space. Clients are expecting an elevated level of protection services (that they’re willing to pay for) to keep their data and digital assets secure. However, many MSPs are having difficulties meeting the more stringent customer requirements and, in return, are looking at Security Operations Center-as-a-Service (SOCaaS) offerings to help them capitalize on the opportunity. This guide is designed to provide some clarity into these issues as you advance your managed security services.

MDR and SOCaaS 101

From a MSP viewpoint, managed detection and response (MDR) services and SOCaaS are so entangled, they are virtually one in the same. SOCaaS is an outsourced security approach that combines technologies—such as extended detection and response (XDR), AI, and machine learning—with processes and a team of security experts. One of the key differentiators to this approach is the human element—specifically, security threat experts and analysts.

Components of a Security Operations Center (SOC)

- **People:** Includes teams of security analysts, threat intelligence experts, and supporting technology administrators. They provide services such as 24/7 monitoring, alert triage, threat hunting, anomaly detection, and incident response.

- **Processes:** Beyond human knowhow, without a process there could be inefficiencies. A SOC tends to have consistent methods by which it conducts its security operations. Some of the processes involved include incident triage, reporting and analysis, post-incident activities, and remediation.

- **Technology:** Traditionally, technologies used in a SOC included intrusion detection/prevention systems, security information and event management systems, data loss prevention (DLP) software, and threat intelligence. Today’s SOCs not only include aforementioned technologies, but now also leverage AI and machine-learning systems.
Impracticality of Building a SOC

For many MSPs, building out a SOC to deliver scalable and profitable MDR services is just not a practical reality. This is true for a myriad of reasons, including:

1. Finding talent and associated costs

MSPs are fully aware of the “skill-shortage” that the IT industry is experiencing, but this talent gap is further worsened when looking specifically at the cybersecurity space.

Let’s assume you can hire a security-focused team as you are building or expanding your cybersecurity practice. The challenge then becomes keeping and training said talent. According to U.S. News and World Report, Information Security Analysts made a median salary of $99,730 in 2019. The best-paid 25 percent made $128,640 that year, while the lowest-paid 25 percent made $75,450. No matter how you slice the numbers, this would be risky a proposition for even mature MSPs.

2. Toolset

While the “people power” is key to any SOC, the technology and toolsets being used are just as important and expensive. Traditionally, key technologies such as Security Information Event Monitoring (SIEM) and Security Operations, Automation, and Response (SOAR) platforms were foundational technologies of a SOC. Besides being complex from an administration perspective, these tools also tend to be prohibitively expensive investments. While outsourced SIEM solutions have helped to lower the cost of this type of technology, the evolving cyberthreat landscape and the sheer amount data being collected from various sources necessitates investments in modern technologies such as AI-driven analytical platforms.

3. Time

Even if the budget and appetite is there to build in-house, it is usually the time-to-market that is the deal-breaker. By the time you hire talent, procure and deploy the technology, you are one million dollars in and a year later. If you are considering building your own SOC the people, processes, and technology for a 24/7 coverage easily surpasses $700,000/year and takes 6+ months to setup. The current cybersecurity climate and customer demand makes executing now the priority versus building for future opportunities.

After reality has set in, most MSPs have made the decision that the best way to extend and elevate their cybersecurity practice is to partner and augment existing resources.

---

1 Information Security Analyst Salary, U.S. News and World Report
2 How SOC-as-a-Service Enhances Security Operations, MSSP Alert
The Value of MDR Services to Your Clients

Faced with rising cybersecurity concerns, organizations of all sizes are maturing their posture beyond basic security. By 2025, according to Gartner 50% of organizations will adopt Managed Detection and Response (MDR) services, up from 5% today.

Besides combating sophisticated and stealthy threats, organizations are looking to adopt MDR services for a variety of reasons and business outcomes, including:

- **Cutting mitigation costs** – Clients who have been affected by a breach know the high costs (time and financial) associated with just a single breach.
- **Evidence of proper security measures** – Increased cyber and data regulatory standards has organizations looking to simplify audit and compliance readiness.
- **Increased visibility and insight across security layers** – Many organizations have various siloed security solutions in place, while MDR services can offer an opportunity for both solution consolidation as well as centralizing and correlating threat data from different security vectors.

Your clients' viewpoint on cybersecurity has shifted. They now recognize the traditional “defensive/reactive” approach only goes so far and a more “offensive/proactive” posture must also be incorporated. This shift in perspective makes conversations about advanced managed security services more beneficial.

The Opportunity at Hand for MSPs

MSPs have also had a mind shift on the role managed security services play in their business. In the early days of managed services, cybersecurity was just a “check-box,” and advanced security offerings were “nice-to-haves.” This is no longer the case, cybersecurity is now viewed as a growth engine and area of strategic importance. Both mature and emerging MSPs have prioritized building or expanding their cybersecurity practice. In a study of 380 cybersecurity professionals, 41% of their organizations believe that as much cybersecurity functionality should be outsourced as possible. Partnering with a trusted SOCaaS provider is both a time- and cost-effective approach to meet this business objective and capitalize on customer demand.

Some of the key benefits and business outcomes MSPs are looking to achieve with SOCaaS include:

- **Staff-Augmentation**
  - Focus existing IT resources and personnel on mission-critical initiatives

---

2 Market Guide for Managed Detection and Response Services, Gartner
4 Cybersecurity Outsourcing Trends: Research Findings, MSSP Alerts
» An uncomplicated way to extend their security operation to 24/7
» Security expertise without the associated expense

• Cybersecurity Operational Efficiency
  » Quicker response and containment of client security related incidents
  » Centralize and connect information and reporting across security layers and clients

• Risk Mitigation
  » Business: Enables MSPs to deliver high-value services as OpEx
  » Security: Diversify risk with an “always on” approach

• New Opportunities
  » Extends managed security services’ portfolio to create new MRR (Monthly Recurring Revenue) streams
  » Opens doors to larger accounts with more stringent security requirements

• Peace of Mind and Customer Retention
  » Rest easy knowing a team of skilled experts are constantly monitoring your clients’ environments
  » These services are more sticky than mere security products, and customers would be less likely to switch providers
Partnering with the “Right” SOCaaS Provider

As a service provider, beyond feature set and cost, two of the most important evaluation criteria when considering SOCaaS providers should be:

1. **Is the offering a “co-managed” solution?** In this model, there is collaboration and shared responsibility between the MSP and the provider to secure clients. The pass-thru service should be transparent to the client and viewed as an extension of the MSP’s service delivery team.

2. **Is the offering multi-tenant?** As multiple clients are under your company’s management, cross-customer threat detection and response capabilities are necessary. Without such capabilities, visibility and the ability to respond across multiple customers is limited and operationally inefficient.

**How the Co-Managed Model Works**

Other Considerations

- **Which technologies does the service utilize? Are they included in the price?**

Understanding what technology is involved, for example EDR (endpoint detection and response) vs XDR is important, as some providers will require you to buy your own tools, while others will offer the
full technology stack in addition to the services. Also, EDR only includes endpoint security, which does not include detection and response for email - the #1 threat vector.

• Threat intelligence and researchers

The provider’s knowledge and involvement with ongoing threat research is an important factor in the selection process. A rich set of past and up-to-date threat intelligence enables security professionals to make more informed decisions.

• Is the service just “managed EDR”?

Without diverse data sources and threat intelligence, scope and visibility of an incident is limited.

• Does the service include threat hunting, incident response, and investigation?

Some providers offer a “monitoring-only”-type service. The idea is to prioritize and notify when potential security incidents arise. They typically only advise on what actions might need to be taken.

• Procurement Terms

Consider whether the provider offers pay-as-you-go, usage-based licensing, or whether an upfront commitment is required. Additionally, investigate whether licensing and billing are centralized and automated to alleviate your administrative burden.

Partnering with Trend Micro™

There are many options when it comes to selecting a security vendor or adding a security vendor to an existing technology stack. Trend Micro views the MSP partnership as more than just product and economics. It’s about closing security gaps, open communication, and long-term focus on people and partnerships. We’re an expert in security and an advocate for MSPs so your focus can be on supporting your customers and running your business.

Trend Micro’s solution is truly co-managed so MSPs maintain control over the interactions with their customers. As part of the incident response service, Trend Micro’s 24/7 threat experts can provide customized recommendations or remediation actions if authorized by you.

Additionally, this service provides proactive threat assessments across the MSP’s entire customer base and protects multiple customers at once. Taking it one step further, our threat analysts review similar threats across partners, especially those in the same industry, to provide proactive response.

Peace of mind is important for an MSP who is responsible for the security of many customers. Trend Micro’s SOCaas solution provides the visibility, confidence, and level of sophistication MSPs need to protect their customers.