Survey Report: What MSSPs Really Want

Research

Sponsored by Logpoint

Executive Summary

As cybersecurity continues to increase in complexity and cost, Managed Security Services Providers (MSSP) perform a critical role for businesses who find the task daunting and want help in handling either all or part of their cybersecurity program.

MSSPs are as varied as the businesses they serve. Some offer a standard portfolio of managed firewall, managed SIEM, and compliance services while others provide a broader portfolio including threat hunting and a full complement of managed detection and response (MDR) services.

For this survey report, TP Research spoke in-depth with MSSPs in Europe and the U.S. to understand what drives their managed services business; how they operate and leverage their cybersecurity platforms, and the product/solution capabilities they value most.

We outline several business challenges that influence how MSSPs build and operate their cybersecurity services. Most importantly, we ignore the hype and give you the inside scoop on the kind of cybersecurity tools and capabilities that MSSPs really need to sustain and grow their business.

As cybersecurity continues to increase in complexity, Managed Security Services Providers (MSSP) fulfill a critical role for businesses who want help in handling either all or part of their cybersecurity program. Regardless of size, organizations need to protect their business assets, data, and processes from internal and external security threats, a breach of any kind can have catastrophic consequences on reputation.

At a basic level, the requirements for a regulatory compliant and solid cybersecurity infrastructure are already complex. Moreover, as cybercriminals change their tactics to avoid detection and increase their chances of perceived success, cybersecurity solutions must advance to keep pace with evolving attack methods.

This environment is a daunting task to handle solo. Businesses cite difficulty in acquiring and retaining skilled personnel, specific IT-skill gaps, and the ever-spiraling costs of cybersecurity operations and maintenance as some of the reasons they are turning to managed services. In 2020, MSSP Alert estimated the U.S. MSSP market at US$31.6 billion and expected it to grow by 12% to 15% through 2025.

MSSPs are as varied as the businesses they serve. Some offer a standard portfolio of managed firewall, managed SIEM, and compliance services while others provide a broader spectrum including threat hunting and a full complement of managed

detection and response (MDR) services. Some MSSP services are wholly in the cloud, while others manage on-prem and hybrid infrastructures.

For this survey report, TP Research spoke in-depth with MSSPs in Europe and the U.S. to understand what drives their managed services business; how they operate and leverage their cybersecurity platforms, and the product/solution capabilities they value most. We also asked about future prospects and the additional capabilities they are considering driving profitability and growth. For example, how important are behavior analytics (UEBA), automation, and orchestration (SOAR) to their managed services offering?

The insights and perspectives we present in the following pages come straight from MSSPs around the world who are helping organizations of all stripes and sizes to prevent, detect, and respond to evolving cyber threats.

MSSPs fulfill a critical cybersecurity role

An MSSP can offer a range of services to business clients, or they may specialize in a core area. The breadth of their offering is often determined by the industry or sector they target, the average size of the organizations they serve (number of employees), the regulatory climate, and most importantly – their client's budget. For example, some MSSP clients may want to offload just their cybersecurity compliance operations because they lack the specific knowledge and expertise to do it properly, while other clients want fully managed IDR, EDR and NDR services.

MSSP service offerings may include:

- Managed Firewall
- Managed SIEM
- Next-Generation Antivirus Protection
- Endpoint Detection and Response (EDR)
- Network Detection and Response (NDR)
- Inbox Detection and Response (IDR)
- Insider Threat Detection and Response
- Vulnerability Scanning and Patch Management
- Threat Hunting

MSSPs also offer consulting services, applying the know-how and expertise they have garnered from their diverse clientele to advise organizations regarding market options and to help them pick the best solutions.

MSSP service offerings may include:

- Penetration Testing
- Breach Readiness Assessment
- Risk Assessments and Gap Analysis
- Policy Development and Risk Management
- Solution Scoping
- Solution/Tool Research and Requisition
- Solution Implementation and Configuration
- Compliance Reporting and Auditing
- Training

MSSPs face daunting business challenges

Pricing

Offering the right service package at a price that businesses are willing to pay is the key to acquiring and retaining managed services clientele. The ability to lower costs and make them predictable is one of the main drivers for businesses to outsource security operations to an MSSP.

When MSSPs use cybersecurity platforms with capacity-based licensing schemes that charge by volume (per message, per gigabyte, per event, or events per second, etc.), costs may become unpredictable and potentially unaffordable. As client businesses grow and more data logs are generated by more users and more cybersecurity systems, it's hard to know where MSSP costs will end up. If MSSPs simply pass growing capacity costs on to the client, they risk losing the client! This is true for basic managed SIEM services (and other services based on SIEM) and is doubly true for services based on SOAR and UEBA platforms that process even bigger volumes of data. The ability to productize and price cybersecurity services is an ongoing challenge.

Customer Relationships

MSSPs often cater to a diverse clientele. There are those wanting basic services, those wanting premium packages, and those wanting expertise to handle a specific task. Basic managed services, mostly automated, do not require a lot of customer engagement. In fact, many clients just want to know that they are cyber-protected and don't feel the need to read weekly or monthly reports. While these clients are in a sense "low maintenance," MSSPs notice that passive clients who do not review status reports and rarely contact the MSSP have a higher tendency to churn. Frequently, the cost of onboarding, configuring and tweaking the churned client is never regained.

On the other hand, active clients who receive regular reports and have frequent contact with the MSSP through an established communication channel (email, portal, etc.) tend to renew service contracts and are more likely to buy additional services. However, the ability to engage requires MSSP personnel, and those resources are always in short supply.

Never Enough Skilled Analysts

MSSPs need to be as effective and efficient as possible and at the same time meet customer expectations without over, or under, staffing. Skilled security analysts are hard to recruit and even harder to retain, and they are constantly being asked to do more with a shrinking analyst-to-customer ratio. Ironically, technology advances that are supposed to increase efficiency and productivity can sometimes make the analyst's job harder. For example, once automation is implemented, customers naturally expect to get even better SLAs. They expect actions by the EDR, SIEM, antivirus, etc. to be triggered in real-time and for the MSSP to handle the incident in real-time. This can place an additional burden on analysts as they work to keep pace with client expectations.

One MSSP in North America described it like this, "As technology advances are introduced, customers expect MSSP features and services to go up, and for prices to go down or at least stay the same." Everyone agrees that automation and orchestration of security services will enable MSSPs to achieve economies of scale and become more efficient. The debate that remains, is how to do it. Should MSSPs use technologies like SOAR to replace analysts and fully automate? Or should they use SOAR technology to augment analyst expertise and make it much easier for them to handle event data from hundreds of different customers?

Flexibility

MSSPs serve a wide variety of organizations in terms of size, sector and outsourcing needs, therefore, they have to be flexible in terms of service packaging and deployment options.

Solutions for every client

Some clients want the MSSP to handle their entire cybersecurity program without their involvement. They aren't interested in rules or playbooks, they just want to be informed of how well the service is protecting their organization and preventing cyber breaches. MSSPs need to be able to show value and keep it simple for these clients.

Other clients want the MSSP to advise, scope, set up and configure their SOC, write the rules and playbooks, and then enable the client to access and operate it. These clients want MSSPs to be an extension of the in-house security team, to be on-call for incident handling as needed, and perhaps to shoulder advanced tasks like threat hunting.

Many clients want to outsource a specific function that their in-house security team does not have the expertise or the capacity to handle. Regulatory compliance is a popular function to offload because it allows organizations to free up security staff, and rest assured that they are doing it correctly. Clients who hire MSSPs to be responsible for a specific security function, often end up buying additional managed services. It's a great foot in the door, even though it may not be a primary or even secondary focus of the MSSP.

Cloud versus On-Premises

MSSPs must also be flexible when it comes to deployment capabilities. While it is "forward-thinking" and highly efficient for MSSPs to operate exclusively in the cloud, many organizations either want or are required to keep their security event data on-premises. All the MSSPs we interviewed offer their services with SIEM/firewall/SOAR deployment on-premises (or in a private cloud) with MSSP management in the cloud. MSSPs told us they could no longer partner with SIEM vendors who migrated the company's entire offering to the cloud. The MSSP was left in the lurch, knowing that there would be very little if any enhancement to on-prem SIEM platforms, and facing the decision to continue maintenance or switch them out.

The need to keep private and sensitive customer data on-premises also complicates matters for MSSPs who want to leverage SOAR and UEBA capabilities to gain operational efficiencies and more accurate security outcomes.

Determining which tools/solutions will best advance MSSP business goals

Investment versus value

When deciding which cybersecurity platforms and tools to buy, MSSPs are serious about due diligence to make sure they do not end up in a corner with the wrong vendor – meaning a vendor that meets their needs in the short run, but not the long run. As noted earlier, MSSPs can end up in a corner when the vendor roadmap takes an unexpected turn, and the product will no longer provide the functionality or stability required by the MSSP.

Out-of-the-box integrations and flexible feature sets are very important to MSSPs because it saves them the time and effort of developing those capabilities in-house and implementing them for each client. This is especially true for MSSPs who bundle components together at a single price point and need the integrations to work smoothly. Out-of-the-box integrations also make it easier to sell MSSP services by allowing clients to "bring their own technologies" such as firewalls, EDR tools, etc. and easily integrate them with the MSSP's SIEM.

When the MSSP also uses a SOAR platform, clients can leverage best-practice workflows and playbooks that are built into the SOAR to trigger incident response actions on those same BYO technologies. According to the real-life experience of MSSPs, the best OOTB features are those that allow flexible configurations and easy customizations per client. MSSPs don't want to be limited by an interface that provides a one-size-fits-all menu of clickable boxes and buttons.

MSSPs who possess in-house expertise often develop their own or augment existing tools because vendor tools don't have everything they need. In contrast, in-house tools provide the precise capability they want, and MSSPs feel in control of the outcome. For example, rather than invest in a SOAR platform and all the setup, rule configuration and playbook tweaking it involves, many MSSPs take it upon themselves to automate only specific processes or to build custom use cases and advanced correlations together with their clients.

Reality versus hype

MSSPs work with hundreds of vendors who knock on their door every week to try to sell them the latest technologies and systems. It takes a lot of due diligence to get past the hype and to understand the actual capabilities of new platforms like SOAR and XDR. For example, everyone agrees that automation speeds up processes and takes a load off analysts, however, automating incident detection and response processes in a single company is quite different from automating MSSP processes for hundreds of companies.

MSSPs told us they are using SOAR-driven data consolidation, enrichment, and normalization, but not necessarily the automated response. The best response for a 50-person company may not be the best response for a 5,000-person company. Furthermore, MSSPs need to obtain customer agreement to reset a password, activate an account, lock the switch or isolate a user's system automatically. Most rely on the judgement of their skilled analyst and are not quite ready for full end-to-end automation.

Will clients buy it?

Advanced technologies and innovative cybersecurity products create opportunities for new managed services. However, MSSPs are cautious about adopting new technologies and products that may change the vendor licensing scheme and raise costs. MSSPs need to be confident clients want to buy the new capability before they take that step. As a rule, MSSPs seek solutions that can drive business growth without necessarily increasing licensing costs.

What MSSPs really want

Flexible platforms

MSSPs can't afford to be tied into one vendor. They seek platforms and tools that promote operational savings and efficiency by being easily integrated, easily swapped out and replaced if needed, and able to be deployed on premise or in the cloud or a bit of both.

> "With Logpoint SIEM we are able to offer eight delivery models for the SIEM engine in our MSSP service. We can deploy on customer hardware, premises, datacenter, cloud, or on our own MSSP hardware, data center, private cloud."
>
> Leading Nordic MSSP

As the collector and repository of all security event data, SIEM forms the foundation or "backend" of many managed security services. In addition to SIEM, a typical MSSP SOC manages IDR, MDR, NDR, vulnerability scanning, threat intelligence and threat hunting services. Many MSSPs sell these services in single or tiered packages!

Other tools such as central management, customer dashboards and portals, EDR, SOAR, and UEBA are then integrated with the SOC setup. These tools can be located in the cloud or on-prem – whatever best suits the client.

Some MSSPs judge flexible platforms by their ability to get under the hood, understand how the platform works and augment its functionality with home-grown development. This is especially relevant when capabilities that the MSSP needs are not built into the platform. This kind of flexibility requires a tight partnership from which both MSSP and vendor can benefit.

> "Logpoint SIEM is the most flexible tool in our security solution stack. We build everything around it."
>
> Major North American MSSP

Tools that augment and make security easier

MSSPs don't want tools that promise to "replace" security analysts. Analysts bring many skills to the table. One MSSP analyst told us the way he relates to an incoming incident on any given day depends not only on forensic data from the security platforms, but also on what he heard on the news that morning, something he saw two days ago on a different customer's SIEM, and his gut feeling triggered by years of experience. You can't replace that kind of expertise, but you can make the analyst's job much easier with the right kind of tools.

For example, Logpoint SIEM allows security analysts to take the rule set of one customer and propagate it to all MSSP customers at once. When analysts create a specific detection rule or another kind of value for one customer, they want it to be available for all customers. If they must manage each customer SIEM one by one, it's almost impossible to deploy a use case within a normal SLA timeframe. A tool that allows them to create a rule once and automatically deploy it to all SIEMs is a game-changer for MSSPs.

> "Logpoint SIEM's central management allows us to take the rule set of one customer and deploy it for all customers at once This is exactly the kind of tool we MSSPs are looking for."
>
> Major North American MSSP

Likewise, MSSPs could leverage a single SOAR platform to have a group of security analysts working on event data from all clients at the same time, rather than working in client silos. Not only would this improve the quality of threat intelligence,

but it would also allow a single dashboard and a unified set of rules and playbooks to be leveraged across all MSSP customers. As a bonus, it would take security analysts out of the client silo and make their jobs much more interesting!

Simple ways to show value

In the MSSP business, price is inelastic, and expectations are high. Customers want to pay a low and predictable price to detect and stop every cyber threat that comes their way and to be in full compliance with all cybersecurity regulations. Most customers don't want to know about all the work that goes into cybersecurity. They just want peace of mind from knowing that their MSSP is taking care of it. That makes it very difficult to show the value the MSSP is delivering.

MSSPs say some of their most understanding customers have in-house SOC teams who have decided to outsource some of their more time-consuming and complex tasks. They know the effort that is involved. However, that doesn't alter their desire to pay a low and predictable fee for the service.

MSSPs also cite the need for simple and frequent reports as well as regular (monthly) contact with customers to discuss report statistics which may include:

- How many attacks have been blocked
- How many alerts have been investigated
- How many and what vulnerabilities have been found
- Whether leaked company credentials have been found on dark web forums
- How many phishing attacks were detected/stopped on web and email platforms
- How many employees clicked through a phishing awareness campaign and what level of training each employee has.

While MSSPs may look to vendor platform reporting functions to help them show value, it appears that simple and regular engagement with the customer is the key.

Ability to create new services

MSSPs say that their ability to create new, value-added service packages still is quite limited. This is partially due to the inelastic pricing of MSSP services in the eyes of the customer. One of the main reasons companies seek MSSP services is to lower costs – significantly. To justify a price increase, the value must be compelling.

Cybersecurity vendors claim that new SOAR and UEBA platforms will create opportunities to build new revenue streams. To date, however, SOAR and UEBA systems are sparsely deployed at MSSPs – even though everyone seems to agree that automation and orchestration will be needed to fill the widening gap between what needs to be done and the resources needed to do it. The same holds true for UEBA. Experts agree that detecting anomalous behaviors in real time will make threat hunting much easier and more effective.

> "Currently, the customers who ask us about automated incident response are the exception. They want to know their MSSP can do it, but they aren't ready for it yet."
>
> Central European MSSP

As noted earlier, some MSSPs are using SOAR, but only for data consolidation, enrichment and normalization (which happens behind the scenes), and not for automated incident response (which could be a chargeable service).

SOAR

The MSSPs we spoke to explained that SOAR is not something that works for them out of the box, without any modifications. SOAR requires planning and needs to be discussed with customers because every customer may have a different setup. MSSPs need to weigh whether SOAR capabilities can be covered by their base fee. Even so, having to work with each customer to get the right rules and playbooks in place will make new SOAR services quite visible to customers, who may agree to pay more for such improvements.

SOAR

MSSPs who have tried specific UEBA solutions have had a hard time justifying the additional cost to their customers. UEBA analyzes huge volumes of data and requires significant infrastructure capacity. In many cases, this is precisely the kind of data that many companies are required to keep on-premise, so the cheaper "cloud" alternative may not be an option.

The MSSPs who find a clear path to new service creation using SOAR and UEBA systems will be big winners in this market.

Scale and flexibility are key

When planning their infrastructure, MSSPs need to assure service stability and continuity. If a particular vendor gets acquired, they may have to replace that vendor component of their security stack with a new one. One MSSP has assured such flexibility by building a front-end portal that the customer sees and places all the systems behind it. They can replace any system, without disrupting the customer view or experience. Not everyone has gone to such lengths. Other MSSPs rely on platforms that use open interfaces and standard protocols to easily integrate with other vendor products. For example, many MSSPs we interviewed use Logpoint SIEM as the backend engine of their SOC, and rely on its built-in ability to collect security event data from any device.

MSSPs have developed home-grown applications, dashboards, portals, etc. to overcome vendor limitations and to get the functionality they need. While these solutions have served them well, they also present a challenge because adding features also adds complexity in terms of the management and scalability of the solution. As a result, it becomes difficult to add new features. Unlike vendors, who develop cybersecurity platforms and solutions for 'the enterprise," MSSPs need platforms and solutions that will allow them to manage hundreds and perhaps thousands of enterprises at the same time, and from a central and unified management tool.

> "When we look at new security features or capabilities like SOAR, we want to know how to make it scalable and handle it globally for hundreds of clients– not just for one client."
>
> North American MSSP

Close vendor partnerships

Even MSSPs who have developed home-grown solutions would prefer to use a vendor solution that is highly scalable, backed by support and regular updates, and offers a roadmap of advanced features. In real life, the perfect platform or tool is a work in progress. All the MSSPs we interviewed said they value the close working relationship they have with their vendors and the ability to influence vendor roadmaps in terms of feature requests and timelines, and also to assure that capabilities like scalable management are built in at the design phase. MSSPs

also believe that vendors can benefit from the home-grown solutions they have developed. A closer relationship would allow them to share and leverage what they have rather than replace it.

MSSPs are also keen on maintaining the stability of basic platforms like SIEM, firewall, IDR, etc., that form the foundation of their business. Solution vendors naturally want to be forward looking so they place a good deal of focus on new markets and emerging technologies that combine many different cybersecurity technologies in one platform. In the meantime, MSSP services rely on existing SIEM installations that must be maintained, improved and kept stable. Being involved in vendor roadmap and feature request discussions is one of the ways MSSPs can maintain the stability and performance of systems that are critical to their managed services business. Strong partnerships allow the MSSP to recommend a particular SIEM vendor or next-generation firewall in full knowledge and confidence of where the vendor is headed in the future.

> "We don't just use vendor tools. We build things around them to help our analysts. We want to understand inner workings and push enhancement requests to the developers. That's why tight partnership is so important to us."
>
> MSSP in Northern Europe

Key Takeaways - Flexibility in all aspects of the MSSP busines

Cybersecurity vendors take note – this is what MSSPs really want in their managed cybersecurity services stack:

MSSPs don't want tools that promise to "replace" security analysts. Analysts bring many skills to the table.

Flexible deployment and delivery options:

MSSPs want the ability to bundle multiple cybersecurity functions into a single service package that can be deployed on-premises, in the cloud, or in hybrid infrastructure. They want their security stack to integrate smoothly with itself and with a wide array of customer technologies so they can onboard, configure, and start delivering value to customers quickly.

Flexible architectures that supports business growth:

To be competitive, MSSPs want to bundle multiple services into a single package with a simple (and low) price tag. This gets harder to do as new technologies

emerge. MSSPs will prioritize vendors who are able to converge new technologies such as SOAR and UEBA with existing SIEM platforms and make it easy to deliver a wide array of cybersecurity services under a converged and predictable licensing structure.

Agile management of vendor and client relationships:

MSSPs know from experience that even the best out-of-the-box features require configuration and tweaking to make them work for customers. Also, many MSSPs want to build on the vendor platform with in-house development. Having a close working relationship with solution vendors is essential to understanding the inner workings of their cybersecurity platform and being able to influence roadmap decisions to assure the continuity of affordable services and efficient operations.

Flexible implementation of SOAR:

Even though many MSSPs are not yet using SOAR, they know that automation and orchestration will be necessary to remain competitive and grow their business. MSSPs are looking for SOAR vendors who will simplify the process by offering flexible licensing options and hands-on training to teach MSSP analysts how to design playbooks and implement use cases to speed response and shorten SLAs.

Flexible reporting that shows value:

MSSPs must show value for their managed services. Customers want to know that security incidents are being detected, managed and responded to quickly, and that they comply with regulations. To demonstrate this value, MSSPs will look for a simple reporting dashboard that customers easily understand and that that can me managed centrally by the MSSP for hundreds and even thousands of clients.

Research

About TP Research

We empower our clients with actionable, incisive research to make even the toughest decisions a little easier. Collaboration is at the heart of our model and our mission is simply to deliver expert insight that has tangible value for your company.

/logpoint

About Logpoint

Headquartered in Copenhagen, Denmark, with offices across Europe, the USA, and Asia, Logpoint is the creator of a reliable, innovative cybersecurity operations platform.