LOGPOINT

MSSP Automation & Integration

www.logpoint.com

TABLE OF CONTENT

OVERVIEW

It is no surprise in the current market, there are many pressures on Managed Security Service Providers (MSSPs) these topics have been top of mind for some time as the cyber arms race perpetuates.

1. **Increasing cyber threats:** As the number and sophistication of cyber threats continue to rise, MSSPs are under pressure to provide effective and comprehensive security solutions to their clients. MSSPs must keep up with the latest threats and technologies to offer the best possible protection to their clients.
2. **Cost-effectiveness:** Organizations are looking for cost-effective security solutions that can provide maximum protection for their sensitive data and systems. MSSPs are under pressure to provide affordable security services without compromising on the quality of protection.
3. **Compliance requirements:** Many organizations must comply with various regulations and standards, such as NIS2, GDPR, HIPAA, and PCI-DSS. MSSPs are under pressure to provide solutions that comply with these regulations and standards, as well as to help their clients stay compliant.
4. **Talent shortage:** There is a shortage of skilled cybersecurity professionals in the market, making it difficult for MSSPs to find and retain top talent. MSSPs are under pressure to build strong teams and develop innovative solutions to address this challenge.
5. **Customer expectations:** As cybersecurity threats become more complex, clients are expecting MSSPs to provide more advanced and sophisticated solutions. MSSPs are under pressure to constantly innovate and improve their services to meet these expectations.

While not a new challenge, managing the increasing complexity of cybersecurity threats has become more difficult with a traditional siloed tool and service stacking approaches. Instead, an ECO-System tooling approach to security is becoming more favorable. The underlying challenge is having to do more with less, and in response, Logpoint conducted a survey to understand how MSSPs are adapting to this need and digitally transforming their services via integration, automation, and Orchestration which all play a key part in this conundrum.

Thus, current challenges faced by customers in effectively handling these evolving demands, require the MSSP market to reshape itself. Many organizations are still reliant on traditional silo management technologies, but there is growing pressure to adopt a more advanced approach that can effectively protect against sophisticated attacks that exploit any gaps in security measures.

- **Skills & Knowledge**
- **Time & Resources**
- **Implementation Strategy**
- **Implemented Technology**

The effectiveness of any larger business is heavily dependent on the speed at which the rich tapestry of necessary tasks is handled. These will undoubtedly span departments, rely on both manual and automated processes, and are dependent on both the accuracy and the speed at which this data can be interchanged. Operational efficiency is thus dependent on the process flows for all these nuanced streams of activity. The key takeaway is that there are numerous communication channels, each with varying characteristics being diverse, situationally contextual, and time sensitive.

- **65% Say SOC operations** may be losing time due to inefficient procedures
- **57% Say that the gap** between Mean time to detect to mean to response is below goals
- **35% Say they do not** have the best process or tools for building detection patterns for emerging threats

A SCENARIO

1. **We have a head of operations, who is hard-working, focused, and diligent and knows how to keep things running.**
2. **We also have a head of back-office operations. Who is equally hard-working, and detail oriented.**

Based on past orders, (2.) works on a cyclic basis knowing the quantity and frequency that ingredients should arrive for (1.) which will be stocked, handled appropriately, and ultimately processed to make their resulting product.

For simplicity, these are the only two business units that we are considering from an interaction point of view. Let's say a buyer makes payment and takes their product as soon as it's ready in the desired quantity available.

So far, perfectly logical, but systems are rarely this simple. Now do a mind experiment and play out a year of operation; let's throw in some hypothetical scenarios to mess everything up;

- **Production stops when a problem occurs with ingredients stock level depletion**
- **At the production company (1.) does not speak to (2.).**
- **(1.) stops receiving a regular set of ingredients in perfect ratio**
- **(2.) makes some ingredient substitutions**

Now imagine every complicated scenario that either gets thrown at them from external activities, internal failures, compounded problems and unlikely but plausible situations.

So, have they both been sufficiently challenged and given enough reasons to say "enough is enough"?

IMPACTS

The point here is, that a cyclic process, that could change over time, that also has other surrounding activities dependent on some of its activity or information, is not a sustainable solution;

If a process is not designed to be adaptable and flexible to changes that occur, it could become outdated or inefficient, causing disruptions to the activities that depend on it such as:

- Decisions made on assumptions rather than fact
- No time critical decisions taken due to lack of exposure to challenge
- No view on negative trends to avert problems before they become critical
- Fragmented process chain causing operational losses
- Unaware of surrounding changes in process that have impact on procedure
- Undue pressure and missed expectations on each of the silo processes

Unfortunately, many organizations operate with a siloed logic in their infrastructure management, where tools do not communicate directly with each other. Swivel chair operations and human interaction are used to address this challenge, which heavily relies on documented processes and experience, making it difficult to enforce or regulate consistency in data interchange.

Like in many experiences in life there is a tendency to neglect spending time and thought to failure scenarios as the focus is always centred on successful activities. This lends thought to a famous philosophical question

"if a tree falls in a forest and no one is around to hear it, does it make a sound?" often used to discuss the nature of reality and perception, but also raises the pertinent question of “When a process is failing is some oversight in our approach to planning and decision-making to detect this?”, where we tend to overlook the possibility of failure and its potential consequences. By neglecting to consider failure scenarios, we may be setting ourselves up for disappointment or even disaster, as we are not adequately prepared to deal with unexpected outcomes.

It is important to remember that failure is a natural part of the learning process, and it is through failure that we can gain valuable insights and improve our decision-making skills. By taking the time to consider failure scenarios and plan for them, we can mitigate risks and increase the likelihood of success. In this way, we can approach our activities and endeavours with a more balanced and realistic perspective, acknowledging the possibility of failure while still striving for success. Acknowledging this rationale leads to a new ethos whereby proactive feedback mechanisms exist to introduce an evolving process rather than a static pattern.

OUTCOME

The simple logic in addressing this predicament is to:

- Create a conversational culture to tackle problems on a 1:1 basis combining knowledge and experience at the right time to solve one or many small issues to avoid impact.
- Create a collation, validation, analysis, and correction structure for full visibility of information.

This simple logic challenge is not dissimilar to how organisations operate their management tools for their IT architecture and security by way of automation and orchestration.

- **Automation** refers to the use of technology to automate repetitive and routine tasks. This involves the use of software and hardware systems to perform tasks that would otherwise require human intervention. Automation is typically used to increase efficiency, reduce errors, and improve reliability in a system.
- **Orchestration**, on the other hand, refers to the coordination and management of multiple automated systems and processes to achieve a desired outcome.

Orchestration involves the use of a centralized system or platform to manage and automate complex workflows that involve multiple systems, applications, and data sources. It typically involves the use of APIs (application programming interfaces) and other integration tools to connect different systems and enable communication and data exchange between them.

In summary, automation is focused on automating individual tasks or processes, while orchestration is focused on managing and automating complex workflows that involve multiple systems and processes. While automation is useful for improving efficiency and reducing errors in individual tasks, orchestration is essential for managing and optimizing large and complex systems that involve multiple automated components.

WHAT AUTOMATION TO ASPIRE TO?

Management tools and their vendors are increasingly providing more capability from market pressure which yielded documented APIs. In the IT world many things are cyclic as technologies advance and deepen their capabilities, we've seen flips between:

- **Centralisation/decentralisation**
- **Terminal/end user compute**

What we are now seeing is the largest arc of these. In the early years of networking IT specialists would hack together solutions from having

- **Knowledge of a challenge or insight into a way of optimising an activity**
- **Interest in collating data from many dissimilar platforms for better insight**
- **Understanding of the component parts at a very deep inner workings level**

Today provides some nuance to this similar solution approach:

- **Infrastructure scale is bigger**
- **Volume of information is on upward trend**
- **Supply chains and associated project engagement add complexity.**

However, it is important to note that this trend toward API-driven solutions is not necessarily an innovative approach. IT specialists have been piecing together solutions for years by collating data from disparate platforms, optimizing activities, and understanding the inner workings of different components. What is new is the scale and complexity of the infrastructure and the volume of information that is being processed.

Overall, the increasing use of APIs and the trend towards more API-driven solutions reflect the IT industry's ongoing evolution towards greater interoperability, efficiency, and automation. As the volume of data and complexity of IT infrastructure continue to grow, it is likely that this trend will continue to gain momentum in the years to come.

It is not feasible for an individual or a team within a business to handle all aspects of security, as the complexity of modern technologies is vast. While it is possible to learn about specific aspects of security and gain a deeper understanding through individual post-mortems, this approach is not practical on an industry-wide level. Additionally, most individuals have a specialisation in one or more security technologies and lack some knowledge of technologies

As an MSSP there is a fine line between just maintaining and true management of a platform where security is concerned, which is the difference in providing a valuable service or one that is replaceable.

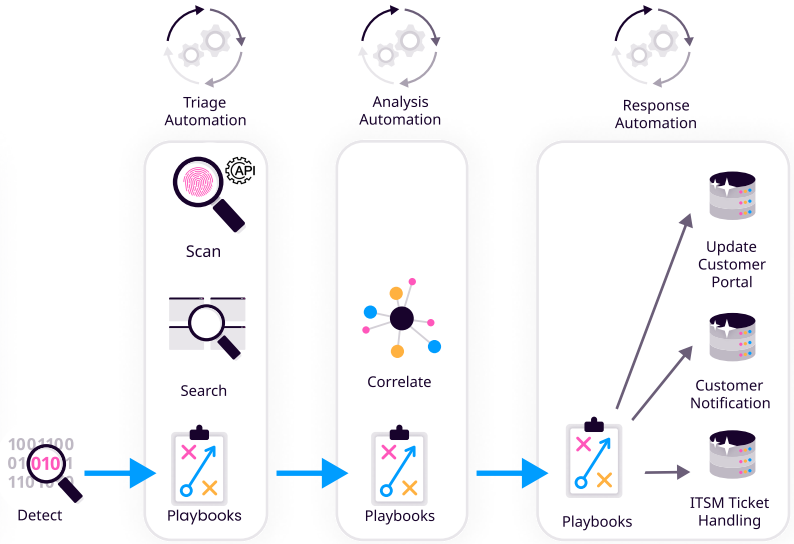
- **Trusting only in the technology inhibits curiosity of the unusual**
- **Service becomes blinkered to issues without the right market-trend tools**
- **Service lack process to evolve and management style limits capacity for adaptation**

By incorporating a DevSecOps style skillset into security system integrations a comprehensive and proactive approach to cybersecurity can be attained. This approach promotes collaboration between security teams and operations teams by utilising DevOps tooling approaches to daily activities, which is fast becoming more essential for identifying and mitigating security risks in a timely and efficient manner.

SIMPLIFY INVESTIGATIONS WITH ORCHESTRATION

PRINCIPLES

- Search for multiple matches on alert event
- Perform extra data recoveries
- Trigger scan activities
- Validate results against other platforms
- Feedback mechanisms to 'source of truth'
- Leave an appropriate audit trail



When looking at the process logic for a 'true security management' a service cannot be static, it must evolve and adapt to the changing threats; this results in three desirable traits in the next generation of managed detection & response SOC services:

1. **Ability to create new orchestration tasks as a day-to-day operational activity**
2. **Shifting priority towards threat hunting over a dependence on alerts to trigger activity**
3. **Dynamic promotion of a qualified threat hunt as service expansion**

In the context of a service provider providing security, these points are especially relevant. As a security service provider, it is important to have the ability to create new orchestration tasks as a day-to-day operational activity, as this enables the organization to stay ahead of emerging threats and respond quickly to new attack vectors.

Similarly, shifting the focus towards proactive threat hunting rather than simply relying on alerts can help service providers deliver more effective and comprehensive security solutions to their clients. By developing the ability to dynamically promote qualified threat hunts as a service expansion, service providers can showcase their expertise and differentiate themselves from competitors in the marketplace.

Overall, these points underscore the need for service providers to adopt a proactive, agile approach to cybersecurity operations, one that enables them to stay ahead of evolving threats and deliver value-added services to their clients. By doing so, service providers can help their clients mitigate risks, safeguard critical assets, and build trust and credibility in their security offerings.

WHAT AUTOMATION TO ASPIRE TO?

Agent Tesla – Download

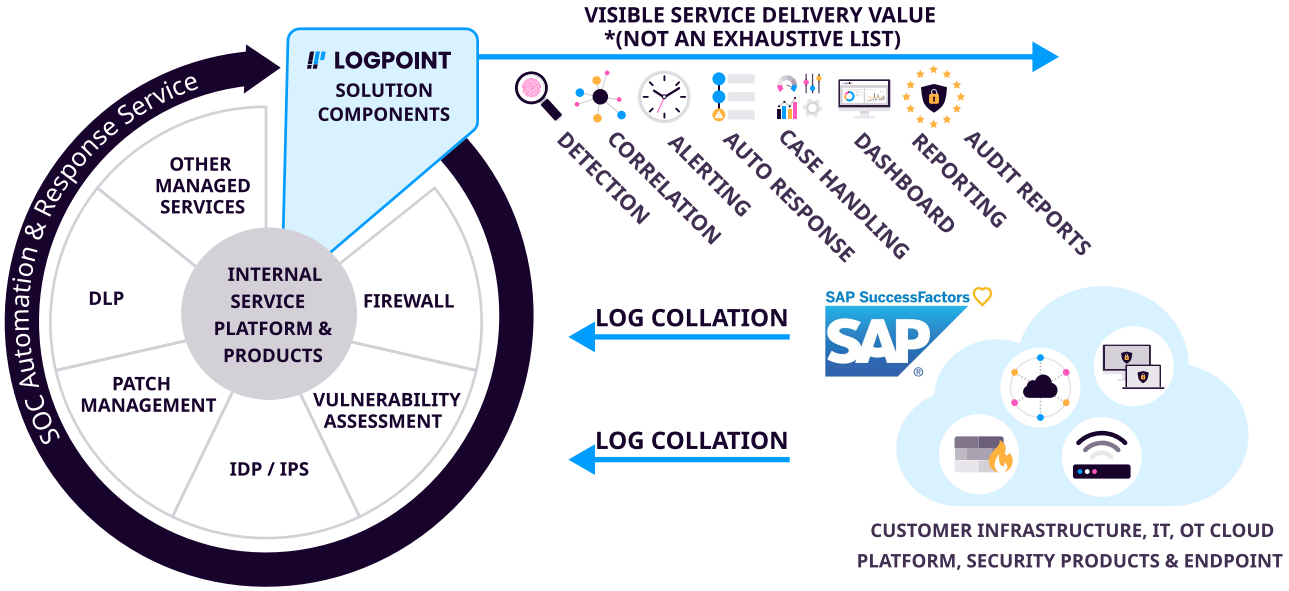
Russia/Ukraine - Download

PLAY – Download

HIVE - Download

REVIEW

In the same way that very simple and regular conversations between (1.) & (2.) could have helped avoid all the previously mentioned situations, creating cross platform communication and central points for analysis can also be straightforward when evaluation of data dependency and process logic is done.



MSSPs have an opportunity to provide skilled and highly valuable services as outsourcing to a third party can provide many benefits to a client, such as access to specialized expertise, operational cost savings, increased efficiency and most importantly lower the risk of brand damage due to breaches.

- **Access to expert resources:** An MSSP typically employs a team of skilled security professionals with expertise in managing and monitoring SIEM and SOAR solutions. By outsourcing to an MSSP, businesses can benefit from the MSSP's expertise, knowledge, and experience.
- **Orchestrated Service Stacking:** Stacking security services with integration's an MSSP offers a comprehensive and layered approach to cybersecurity, reducing the risk of cyberattacks and enhancing overall security posture. By combining multiple services, businesses can benefit from increased visibility, threat detection, and incident response capabilities.
- **Cost-effective solution:** Building an in-house SOC with the necessary technology, tools, and personnel can be expensive. Outsourcing to an MSSP can provide a cost-effective solution that allows businesses to benefit from state-of-the-art technology and expertise without the capital and operational expenses associated with building an in-house SOC.
- **Scalability:** An MSSP can offer a scalable solution that can grow or shrink as business needs change. This allows businesses to quickly adjust to changing security requirements without having to invest in additional infrastructure or personnel.
- **Enhanced threat detection and response:** SIEM and SOAR solutions provide real-time monitoring and threat detection, enabling rapid response to security incidents. By outsourcing to an MSSP, businesses can benefit from the MSSP's advanced threat detection and response capabilities, reducing the risk of security breaches and minimizing the impact of any incidents.

- **Compliance with security standards:** Many industries are subject to security standards such as HIPAA, PCI-DSS, or GDPR. Outsourcing to an MSSP that is knowledgeable about these standards can help businesses comply with regulations and avoid costly fines.
- **Focus on core business activities:** Outsourcing SIEM and SOAR SOC functions to an MSSP allows businesses to focus on their core competencies and strategic business activities, rather than worrying about security operations.

OUTSOURCING

Overall, outsourcing SIEM and SOAR SOC functions to an MSSP can provide businesses with cost-effective, scalable, and expert security monitoring and response capabilities, enabling them to focus on their core business activities and avoid the cost and complexity of building an in-house SOC.

However, outsourcing also introduces security risks that need to be carefully managed. One of the primary concerns with outsourcing is that it can create additional security silos, which can lead to a lack of integration and data fragmentation. This can be especially problematic if the outsourced services require access to sensitive data or systems. To mitigate this risk, it is important to establish clear policies and procedures for integrating the third-party's systems and data with the company's internal systems securely.

Another critical component of a strong security posture is conducting a thorough risk assessment before outsourcing any services. This assessment should identify potential risks and vulnerabilities associated with the outsourced services, as well as any regulatory requirements that need to be met. This assessment should be conducted regularly, and any changes to the outsourced services or the security landscape should be promptly evaluated.

SECURITY INFRASTRUCTURE

It is also important to ensure that MSSP's have a strong security posture in place. This can include conducting due diligence on the MSSP's security practices, such as their access controls, data encryption, and incident response protocols.

Additionally, it is likely the MSSP's security performance will be monitored regularly by their clients, as the MSSP can be held accountable for any security incidents that occur as a result of their actions or negligence.

CONCLUSION

In summary, outsourcing to a third-party can be advantageous, but it is essential to have a strong overall security posture spanning the whole B2B relationship that includes risk assessment, due diligence, regular monitoring, and contract provisions that address security and data protection. By taking these steps, clients can reduce the risks associated with outsourcing and ensure that their data and systems remain secure.

MSSPs should work to build strong relationships with clients by understanding their business objectives and aligning security solutions with those goals.

Effective communication is key to retaining customers. MSSPs must keep clients informed about the status of their platform and any security incidents, as well as provide guidance on best practices and emerging threats.

Thankfully there exists an abundance of knowledge and the essential skill sets to Investigate and understand the challenges to find a fitting solution alignment. While this is positive, it also indicates a need for continued innovation and improvement to meet evolving customer needs and emerging threats.

SURVEY RESULTS

- The mean time to detect vs. meantime to respond is mixed, with a mean score of 3 out of 5. This may indicate a risk of slow response times to threats, which could impact the organization's ability to provide effective protection.
- MSSP organizations offers a wide range of services, including managed security monitoring, vulnerability management, threat intelligence, penetration testing, patch management, and more. While this is a positive sign, it also indicates that the organization may be spread too thin, making it difficult to provide high-quality services across all areas.
- Manual alert response indicates that some SOC operations have a low percentage (25%) of automatic runbooks/procedures for alert response. This means that alerts may not be responded to in a timely manner, leading to increased risk for customers.
- Some SOC services may not have API integration with other technologies, potentially limiting their effectiveness and ability to respond to threats.
- When looking at the capability in building detection patterns some respondents rated their capability in building detection patterns for emerging threats as low (1) or average (3). This could lead to delays in detecting and responding to emerging threats.
- Review of technology automation shows that some SOC operations may not be automating responses into key technologies such as EDR, Firewall, and User Management, which could increase the gap on MTTR and risk.
- In Inefficient procedures: reveals that some SOC operations may be losing time due to inefficient procedures, potentially leading to slower response times and increased risk.
- The survey reveals that most MSSP's are looking to create new services over the next 12-24 months, including NDR, EDR, and Managed CSIRT, SOAR NDR, and MDR and SOC for SMB.

ABOUT LOGPOINT

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats.

By combining sophisticated technology and a profound understanding of customer challenges, Logpoint bolsters security teams' capabilities while helping them combat current and future threats.

Logpoint offers SIEM, UEBA, and SOAR technologies in a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more.

Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company.

For more information visit **www.logpoint.com**