

Best Practices for Integrating your SOC Team with MDR Services

Table Of Contents

04 Introduction

06 Five areas to consider when planning the integration of your SOC with an MDR service

- Assessing the current state of your SOC
 - Identifying any potential challenges or barriers to integration
 - Defining the goals and objectives of the integration
 - Understand the roles and responsibilities of both teams
 - Developing a roadmap for the integration process
-

12 Seven best practices when implementing the integration of SOC and MDR

- Clear communication
 - Aligning security tools
 - Understanding roles and responsibilities
 - Defining incident escalation processes
 - Holding regular meetings and reviews
 - Clarifying the retention policy
 - Monitoring/measuring progress
-

15 Measuring the success of the integration

- Defining Key Performance Indicators (**KPIs**) to track the effectiveness of the integration
 - Regularly reviewing and analyzing the data to identify areas for improvement
 - Adjusting as needed to optimize the integration
-

16 Conclusion

- Recap of the key points discussed in this white paper
- The importance of continuously reviewing and optimizing the integration of the SOC and MDR
- Future considerations for integrating the SOC and MDR

Forward

A Security Operations Center (SOC) plays a crucial role in an organization's security.

Still, the perfect storm of challenges SOC's face is compromising their effectiveness in combating data breaches and other cyber threats. As we continue to move past the peak of the COVID pandemic and into a new year filled with economic uncertainty, SOC's are trying to stay ahead of the increase in remote work (and, therefore, an increase in vulnerable attack vectors), a severe shortage of cybersecurity professionals and a high team turnover rate fueled by alert fatigue.

Companies are acutely aware of these challenges, and while we know that Managed Detection and Response (MDR) services can help augment the capabilities of a SOC team by providing additional resources and expertise to detect and respond to cyber threats, some organizations are concerned about partnering with an MDR service. This may be due to a lack of trust, cost concerns, worries over complexity or increased vulnerabilities, or the belief that they already have sufficient in-house resources.

According to MarketsAndMarkets' 2022 [Managed Detection and Response \(MDR\) Market Report](#), the global MDR market is expected to grow from an estimated value of USD 2.6 billion in 2022 to USD 5.6 billion by 2027, yet a "lack of trust in third-party applications and a lack of modern IT infrastructure" are predicted to curb overall market growth¹.

In this high-risk environment where customer trust and retention, brand value and the economic success of organizations teeter on the razor's edge of reliable cybersecurity infrastructure, security professionals are under increasing pressure to protect and shield their organizations from the ever-evolving threats of cyberattacks.



This white paper explores how organizations that have decided to enlist the help of a third party to support their security professionals, future-proof their cybersecurity infrastructure and increase the overall security posture of their company can most effectively integrate their SOC team with their chosen MDR service provider.

¹ MarketsAndMarkets. *Managed Detection and Response (MDR) Market Report*. (MarketsAndMarkets, 2022)



Introduction

A SOC is used interchangeably to mean a team and a secure physical location.

A SOC can be considered a control tower for an organization's security. Like an airport control tower that monitors and directs traffic to ensure safety and efficiency, a SOC monitors an organization's networks and systems in real-time for security threats, vulnerabilities and incidents.

Staffed by cybersecurity professionals, a SOC is usually structured around a tier system where the number of tiers can vary depending on the size and complexity of the organization. The more tiers a SOC has, the more specialized and advanced the support and expertise will be at each level.

For example:

- **Tier 1:** Initial triage and response to security incidents
- **Tier 2:** More advanced investigations and support
- **Tier 3:** Highly specialized expertise and support for complex or critical incidents

In general, each tier is responsible for providing progressively more advanced support and expertise, depending on the specific needs and capabilities of the business. **The end goal of the SOC is to protect the organization and its assets from cyber threats and other security risks.**

However, it is not uncommon for a SOC team to be part of an organization's IT department. This means SOC analysts, in addition to identifying, deploying, configuring and managing their security infrastructure, may also be called upon to address non-security related matters like support tickets and network administration.

An MDR offers continuously responsive, adaptive security protection that helps organizations keep their networks and systems secure by minimizing the impact of cyber threats and reducing the risk of data breaches and other security incidents. While not all security operations processes can

be fully outsourced, an MDR provides additional resources and expertise to help an in-house SOC stay ahead of emerging threats and effectively respond to them by reducing the time between detection and response. It does this by complementing the real-time efforts of the SOC with ongoing assistance and support, including:

- **Continuous monitoring**
- **Threat detection**
- **Rapid response**



MDR services grew out of SOC-as-a-Service, providing continuous monitoring and detection of security events. While a SOC team is still a component of an MDR, modern MDR services now also provide a remediation path to those security events.

According to a Gartner® report, it is important to "Define specific required outputs (incident ticket structure, reports) and goals that address defined use cases, before engaging with a provider. As with any outsourcing initiative, if outcomes are not defined, regardless of what service provider is used, the chance of success will be lessened."

—Gartner® [Market Guide for Managed Detection and Response Services](#). Published 14 February 2023. By Analyst(s): Pete Shoard, Al Price, Mitchell Schneider, Craig Lawson, Andrew Davies

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved



Introduction (continued)

Benefits of integrating SOC and MDR

An effective MDR service is ever vigilant, providing a level of hyperawareness to emerging threats and threat actors that a SOC alone can't offer. It creates personalized, organization-specific playbooks unique to each customer to monitor better an organization's network and systems for signs of compromise or malicious activity and covers a predefined technology stack, including Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) tools, Security Information and Event Management (SIEMs) and network and cloud services.

If a threat is detected, the MDR service alerts the organization's SOC team. It provides them with additional information about the threat and either resolves the threat on behalf of the SOC or provides recommended response measures. The efficacy and efficiency of the in-house SOC to identify and mitigate security breaches is boosted by the expertise provided by the MDR service and its human analysts.

Why integrate SOC and MDR?

Effective cybersecurity is an ecosystem of symbiotic relationships that work together to thwart bad actors and ever-emerging threats. Think of a home armed with a security system where the system continuously monitors for suspicious activity on its own but can reach out to the security company for additional support and backup if needed.

Like an organization with an in-house SOC, a home with a security system is good. But just as a home with a security system backed by ongoing support and assistance from an outside security company is better than one without such aid, so is an organization with an integrated SOC and MDR service better together.

However, as we know from experience and customer feedback, finding the right cultural and professional fit for your SOC team is imperative when creating a trusted, viable partnership to help you mature your security posture and better allocate your team's resources. To learn more about finding the right fit and successfully integrating your SOC team with your chosen MDR service, we invite you to consider the following best practices.

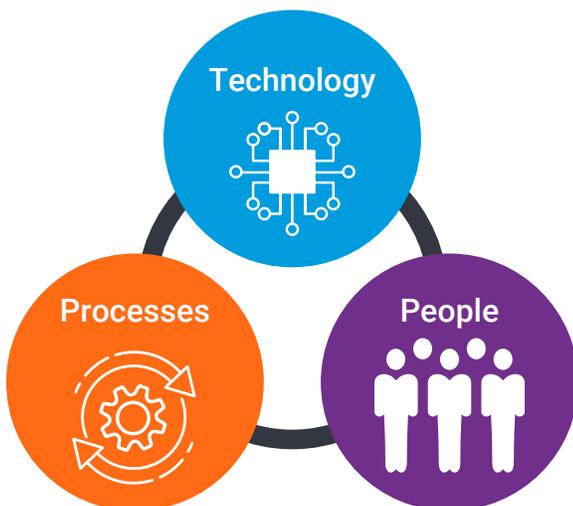


Figure 1: Effective cybersecurity is an ecosystem of symbiotic relationships that work together to thwart bad actors and ever-emerging threats.



MDR services augment the capabilities of the in-house SOC by offloading:

- Tier 1 and Tier 2 support
- Eliminating false positives
- Simplifying investigation
- Expediting the response process
- Providing additional dedicated tools and resources

By partnering with an MDR service, in-house teams have more room to focus on real and emerging cyber threats and provide enhanced protection for their respective organizations.





Five areas to consider when planning the integration of your SOC with an MDR service.

Once you've decided to integrate your SOC with an MDR service, the next steps will be to:



Assess the current state of your SOC



Identify any potential challenges or barriers to integration



Define the goals and objectives of the integration



Clarify the roles and responsibilities of both teams



Develop a roadmap for the integration process





Assessing the current state of your SOC

SOCs are dynamic, with people, technology and processes evolving over time to meet the security needs of the company.

The current maturity level of your SOC team and the number and type of security systems your organization has in place all play a role in determining how much support your team will need from an MDR service.

Take the time to assess what manual processes you have in place and where inefficiencies prevent your SOC from reaching its full potential. Think about how Artificial Intelligence (AI) and Machine Learning (ML)-powered tools that augment (but don't replace) human reasoning can help remove friction and increase the efficiency of your team.



The inclusion of human reasoning is specifically called out because the right MDR service will use a balance of automation and human awareness to provide the best possible results. For example, having two-person integrity on actions that could disrupt your organization, such as isolating a host, banning a hash, automating changes and more.





Identifying any potential challenges or barriers to integration

Your industry and your organization's internal structure are two potential challenges to successful integration.

Incident response teams often collaborate broadly across multiple groups within an organization, some of which are outside of security, like operations, risk, legal and firewall/network administrators. This is especially true in high-risk industries targeted by persistent threats, which necessitate orchestrating higher numbers of response steps with external teams.

Anticipating and maintaining communication and coordinating activities with these other groups can impede a SOC-led initiative to integrate with an MDR service. Avoid this by performing a thorough assessment of the technical capabilities of the MDR service and mapping how it aligns with the charter policy within your organization which clearly defines the role/authority of security. Carefully list out all business units that need to be onboarded and share this information with your MDR vendor.

Aligned correctly across teams, an MDR service can help centralize actions and minimize the need for your team to toggle between stakeholders, workflows, the types of threats it can detect and the methods it uses for incident response.

If transparency is a concern, find out if the MDR provider will integrate into your current infrastructure and provide your team with insight into what their analysts see, allowing your team to understand what is going on and how outputs are determined. For example, investigation procedures need to show exactly what steps the MDR SOC analysts took when investigating alerts.

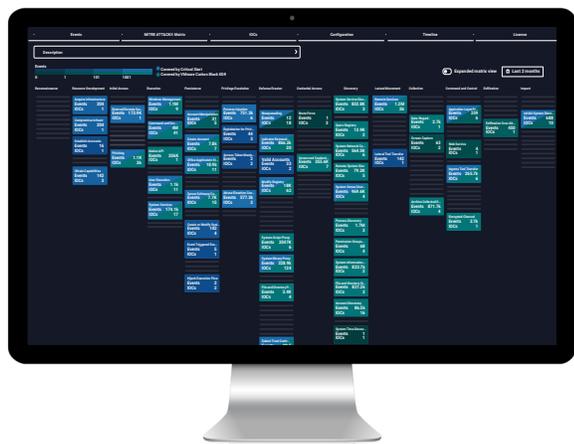


Figure 2: Map threat detection content to the MITRE ATT&CK® Framework

Additional functionality essential for delivering comprehensive SOC services includes:

- Security value dashboards and SLA tracking and notification of Time to Detect (TTD) and Median Time to Resolve (MTTR) for every alert
- Longer retention periods of metrics and audit logs around both teams SOC operations
- Allowing multiple people on your team to directly communicate to the MDR SOC to ask questions and request response actions
- Workflow for notification schedules and escalation
- Proving detection utilization and improvement of MITRE ATT&CK® Framework coverage
- Single Sign-On (SSO) across multiple systems, application of least privilege principles and avoiding shared credentials
- Analyst threat investigation enrichments (OSINT, Sandbox Capabilities, Base 64 Decode) and automation included in the investigation details for reference
- Multi-level hierarchy for business units, geographic divisions and other organizational groups
- Reduced dwell times with remote investigation and response across mobile devices using native iOS and Android applications

An MDR that applies information learned from other customers to improve your investigation and response times and that uses a centralized platform providing analytics and data retention capabilities, plus the added functionality listed above, will give your team complete visibility across all alerts, improve coordination and streamline the response processes across the SOC and MDR.

Finally, be aware of geographical legislation that informs data protection, residency and privacy regulations with which your MDR vendor must also comply. A vendor with a solid industry reputation and with documented experience across a varied customer base will be able to help you identify these sometimes-overlooked areas of concern and ensure nothing is missed.





Defining the goals and objectives of the integration

“Not knowing where to start” can stall an integration indefinitely, but a good MDR service will help you break down each integration stage into manageable steps.

Thinking about when, where and how you want MDR service support is an excellent way to help define the goals and objectives of the integration. Decide the level of customizable threat detection use cases relative to your environment you need and if the MDR service can provide that level of personalization.

Remember to evaluate additional capabilities that will help your team meet its goals and objectives, including:



Consider the contractual agreements within your SOC and how an MDR can support those with its features and functionality, including the MDR’s Service Level Agreements (SLAs) and response times and its ability to scale with your organization.

THREAT DETECTION	THREAT RESPONSE	ADDITIONAL TOOLS & SERVICES
<ul style="list-style-type: none"> • 24x7x365 alert monitoring and custom, curated and community threat detection using vendor-provided and proprietary Indicators of Compromise (IOCs) • Analysis and investigation of security alerts using industry best practices and processes and resolution playbooks • Dedicated threat detection engineering team for adding customer detections to your instance • Threat intelligence team to obtain, interpret and investigate new and emerging threats for your protection 	<ul style="list-style-type: none"> • Rapid response and active containment or disruption of threats vs. response guidance • Guaranteed one-hour Service Level Agreement (SLA) which includes Time to Detect (TTD) and Median Time to Resolve (MTTR) for all alerts • Automated security functions, orchestration and incident response workflows • Resolution of every alert, regardless of criticality 	<ul style="list-style-type: none"> • 24x7x365 access to a security expert • Access and support from a dedicated Customer Support team member • Mobile app • A registry of trusted behavior to help reduce false positives • Alert enrichment for additional context • Custom playbooks • Logging platform user activity for audit and compliance purposes • Ability to map threat detection content to the MITRE ATT&CK® Framework • Centralized reporting • Platform health monitoring • Incident Response services in the event of a breach • Spend-related support • Risk assessments • Support to better understand your risk profile and increase your cybersecurity maturity





Clarify the roles and responsibilities of both teams

Both your organization and your chosen MDR provider have a role to play in ensuring the success of the MDR services, beginning with the implementation and continuing through the triage, investigation and remediation of any identified threats. Understanding and documenting the rules of engagement are good places to start.

Both teams will divide responsibilities in three main areas:

- **Implementation**
- **Monitoring, investigation, response and escalation**
- **System management**

Don't let the fact that a SOC is a component of an MDR service create concern around the potential redundancy of roles and responsibilities. Unlike an in-house SOC team that may be hampered by additional duties, an MDR service provides a dedicated SOC team whose overarching goal is to reduce other companies' risk and attack surfaces.

Risk stems from a combination of threats (malicious actors who target companies and mean doing them financial or, in the case of medical companies, possible physical harm) and vulnerabilities (weaknesses in an IT environment) that can overwhelm a SOC team in the form of alert fatigue.

To support the in-house team, an MDR SOC is comprised of a rotating team of analysts and engineers with an increasing level of specific responsibilities aligned with their assigned tier, as in this example:



Mapping out the roles and responsibilities of your team in the context of what the MDR SOC provides and enforcing process discipline will optimize your team and help ensure it gets the help it needs to allow it to focus on the security priorities that matter for your business.





Developing a roadmap for the integration process

When mapping out the integration process, remember to include additional support your team will need after the initial onboarding, configuration and deployment of the MDR service.

Find out if training and continuing education are available and if the vendor offers regular security assessments to help identify potential vulnerabilities as your SOC evolves.

Ask about the customer support process, including when and what type of access is available (web, phone, email, etc.). Also, inquire about the information you may need to show your executive leadership and other stakeholders to prove the success of the integration and ongoing partnership as well as to answer questions as they arise. This may include:

- **RFIs**
- **Weekly intelligence summaries**
- **Threat advisories**
- **Threat detection content**

A standard implementation starts with integrating your product into the MDR provider's analytics platform. This first step is imperative to establish a well-defined baseline environment configuration. At this point, the product configuration is evaluated to ensure compliance with best practices (such as a hardened environment) and properly configured policies.

Next, the provider will work with you to tune the events generated by your security tools, helping to adapt the MDR service to the unique profiles of your environment and uncover any latent suspect activity within your network requiring further investigation. A standard implementation typically includes the following actions:

- **Recommendations for configuration changes and any updates to your security products as recommended by the technology vendor and the MDR experts**
- **Recommendations for additional deployment of your security products as necessary to achieve your business objectives**
- **Guidance on your security products' testing plan and deployment processes (if needed)**
- **Customizing threat detection content to facilitate the identification of threats**
- **Baselining of network activity to help eliminate false positives and known good behaviors**
- **Integration with your organization's support processes or ticketing system**
- **End-user training**
- **Ensuring the MDR service continually monitors, triages and responds to security alerts and that their response to identified threats will be to escalate to your team for mitigation and remediation (unless otherwise specified)**

To ensure comprehensive coverage, take inventory of your security ecosystem to ensure all endpoint devices in your environment (endpoint deployments) and relevant log sources are included, and all parsers are completed during your onboarding and implementation. Before transitioning into a production state, ask your MDR service to conduct a final health check of your supported security products and their configuration to ensure they're ready for continuous monitoring. Only if your teams agree that your supported security products are ready and that processes are in place to mitigate or resolve any security alerts should you transition to a production state.



Manage expectations around time to deployment (you want a service that can be up and running in weeks, not months so that you can see an immediate reduction in alerts and accelerated return on your investment) and clarify if there is a centralized communication platform (like a chat or ticketing system) that will help streamline communication as your teams move further into the process.





Seven best practices when implementing the integration of SOC and MDR

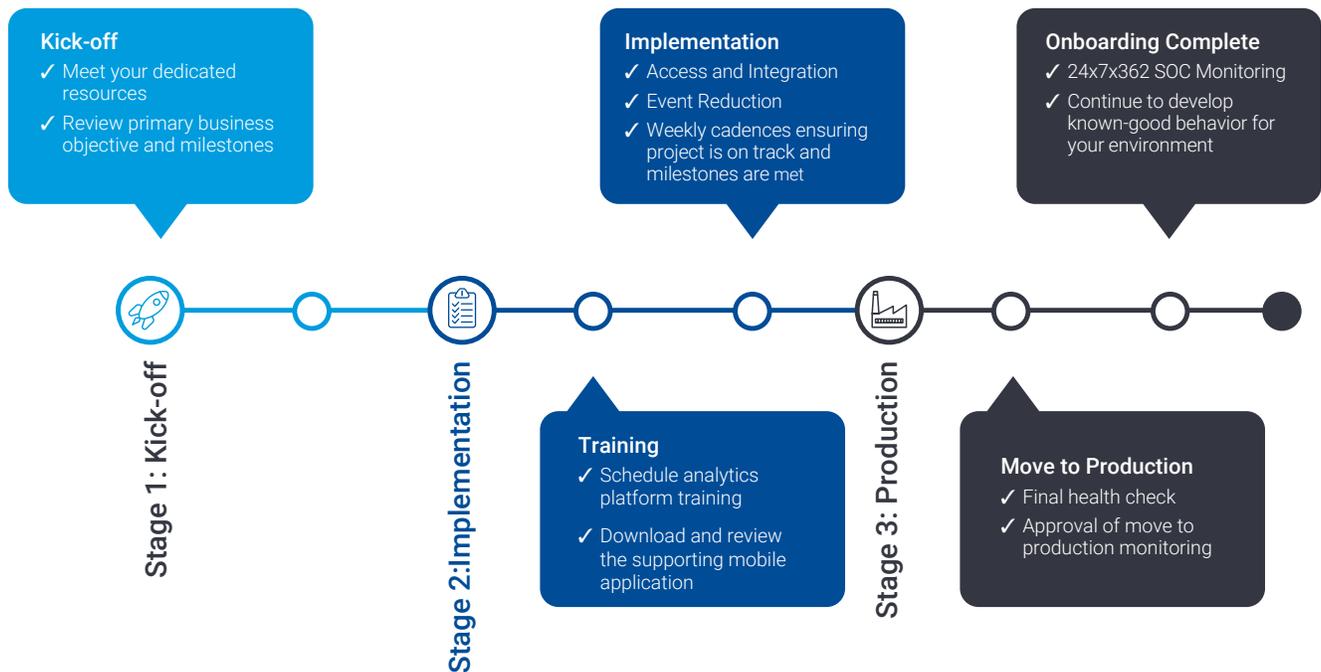
The time to discuss how your SOC team and the MDR service will align on best practices is during the onboarding process, before moving to production. During this phase, establish cross-team communication channels and educate the MDR provider about your organization, team, network and priorities.

-  **Clear Communication**
-  **Aligning Security Tools**
-  **Understanding roles and responsibilities**
-  **Defining incident escalation processes**
-  **Holding regular meetings and reviews**
-  **Clarifying the retention policy**
-  **Monitoring/measuring progress**



Seven best practices when implementing the integration of SOC and MDR (continued)

Manage expectations around time to deployment (you want a service that can be up and running in weeks, not months so that you can see an immediate reduction in alerts and accelerated return on your investment) and clarify if there is a centralized communication platform (like a chat or ticketing system) that will help streamline communication as your teams move further into the process.



ONBOARDING



Timeline



Management



Connection



Policies



Fine-Tuning



Seven best practices when implementing the integration of SOC and MDR (continued)

A good cultural fit is as important as ensuring your chosen service supports the tools in your security ecosystem.

Ask about:

- **How the service prioritizes your primary business objectives and goals during onboarding to ensure that ROI is trackable and how you will map the success of your goals to the MDR service**
- **The retention rate of the SOC employees and how individuals (and teams) are continually trained to deliver optimal service**

Understand how your supported security tools align with the capabilities of the MDR service and how they can integrate into a unified security management platform that allows for centralized monitoring, analysis and incident response. This can include integrating different security technologies such as firewall, intrusion detection and prevention systems, endpoint protection and SIEMs.

Next, your teams will identify key stakeholders and outline their incident response **roles and responsibilities** to help ensure the right people are involved in ticket escalation. Discuss how the security teams will collaborate remotely, have access to full audit trails, and be enabled to isolate a host, investigate an endpoint and effectively remediate threats.

These decisions must be communicated clearly to all teams, stakeholders and employees to ensure everyone knows who does what in case of an incident. **Establishing incident severity levels** will help teams determine the level of urgency required for a given incident and **defining clear, trackable escalation paths** will ensure incidents quickly and effectively get escalated to the right people. Preparing the response workflow processes and integrating with existing ticket management systems to ensure a business-centric response will ensure you get the most out of your MDR service.

Regular meetings and reviews are a place to discuss the latest security threats and what steps are being taken to protect against them, ongoing incidents, security metrics and statistics, vulnerabilities and remediation, security tool performance, changes to compliance or regulatory requirements, closed incident postmortem and training and knowledge sharing.

Remember to take time during these meetings to reinforce process discipline and occasionally test the incident escalation process to identify and address any issues and ensure the teams are prepared to handle incidents.

If, for whatever reason, you decide to end your MDR service, it helps to know beforehand what the retention policy is for any technical artifacts made specifically for your organization. For example, an MDR service may add custom detections and modify detections within your supported security tools to improve MITRE ATT&CK® Framework coverage. Typically, if a service should end, your organization would retain:

- **Custom detections and content added at your request**
- **Detections and IOCs developed from vulnerability research**
- **Detections and IOCs developed from threat intelligence research**
- **Detections and IOCs developed from incident response investigation**

Finally, measuring the success of the integration is the backbone of a successful SOC/MDR partnership, and why it is imperative to establish ongoing **monitoring and measuring of progress**. This can happen in several ways and will be discussed more in-depth in the next section.



Measuring the success of the integration

Understanding a security program's overall performance, effectiveness and efficiency are critical to maturing processes and practices.

To aid in the monitoring of your MDR service, ensure that the vendor provides reporting to pre-designated contacts and specialized, single-source-of-truth dashboards that include:

- Situation awareness and urgent actions
- Recent activity for security alert, investigation and response metrics
- Measurement and performance management improvements for your security analysts
- Performance indicators tracking MDR SOC efficiency and SLA metrics
- KPIs for technology effectiveness of the supported products
- Threat content and detection and open/closed alerts mapped to the MITRE ATT&CK® Framework



Tracking KPIs and incident data over time can help identify trends and patterns, while measuring the effectiveness of the incident management process (time taken to resolve incidents, number of false positives, etc.) will track the effectiveness of the integration.

Proactively gather and analyze security data to understand the types of incidents encountered and the effectiveness of the security controls. Then overlay KPIs such as incident detection and response time and number of incidents a month to help your team measure overall performance and identify areas of improvement.

Using the reporting and dashboard capabilities from the incident management software provided by the MDR to regularly review and analyze the data to identify areas for improvement and to provide a comprehensive view of the incident management process to your stakeholders, including executive management and legal and compliance teams, can help ensure that everyone is aware of progress being made and any areas that need improvement. It also ensures that teams are aligned to perform adjustments as necessary to optimize the integration and its outcomes.

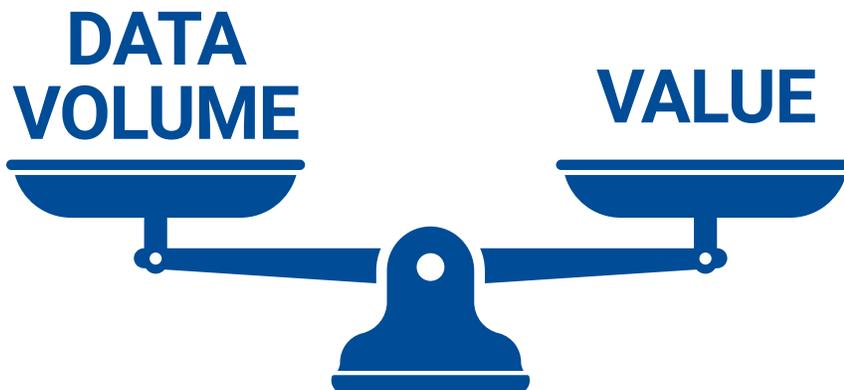


Figure 4: Regularly review and analyze the data to identify areas for improvement and to ensure you are getting your expected ROI



Conclusion

Your SOC plays a crucial role in your organization's security:

Mitigating risks and stopping breaches safeguards your customers' data (and sometimes even their lives) and protects your company's intellectual property and brand value. You know that partnering with an MDR service is a leading way to holistically approach the unique risks your team faces and increase your cyber resilience—you're just looking for guidance on how to get that partnership off to a good start and help make it thrive.

Following the best practices outlined in this white paper will help your team successfully integrate with an MDR service to eliminate risk acceptance and stay ahead of the increase in vulnerable attack vectors exacerbated by remote work, the shortage of skilled cybersecurity professionals and a high team turnover rate fueled by alert fatigue.

Take the time to map out where your SOC is now and how you expect it to grow and mature to find the right MDR provider to grow with you. Set your team up for success before implementation by requiring your SOC and your chosen MDR provider to:

- Align processes and procedures
- Establish clear communication channels
- Ensure all necessary tools and technologies are in place, and
- Provide training and onboarding to team members

Staying focused on the risks affecting your business and deciding upon the results your organization needs to achieve will ensure your integration succeeds and delivers the expected outcomes.

If you are unsure how to identify or prioritize these risks or are concerned you may be overlooking an area of importance, find an MDR provider that can help scope this information with you and your team.



Around-the-clock access to an MDR service with an experienced team with military, intelligence, security, public and private sector backgrounds will work closely with you to understand your organization and its unique needs. It will help you maximize your investment, including reviewing configuration and policies (if applicable) to help uncover and address any gaps in coverage and providing guidance and recommendations based on your business goals and priorities.

According to a Gartner® report, it is important to “Define specific required outputs (incident ticket structure, reports) and goals that address defined use cases, before engaging with a provider. As with any outsourcing initiative, if outcomes are not defined, regardless of what service provider is used, the chance of success will be lessened.”

—Gartner® [Market Guide for Managed Detection and Response Services](#). Published 14 February 2023. By Analyst(s): Pete Shoard, Al Price, Mitchell Schneider, Craig Lawson, Andrew Davies

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved



Allowing your internal resources to communicate openly with your MDR service is the key to maintaining collaborative relationships that are imperative to success. This open-door policy will ensure productive dialogue so that as your SOC grows and matures, you can continuously review and fine-tune the integration of your teams, which is critical to improving overall outcomes.





For more information, contact us at:
<https://www.criticalstart.com/contact/>