IDC TECHNOLOGY SPOTLIGHT

Sponsored by: Pondurance

The managed security services marketspace has been rife with confusion. This paper intends to break up that confusion and provide a clear path forward for customers to meet business needs now and into the future.

Clearing Up the Managed Security Services Confusion

November 2021

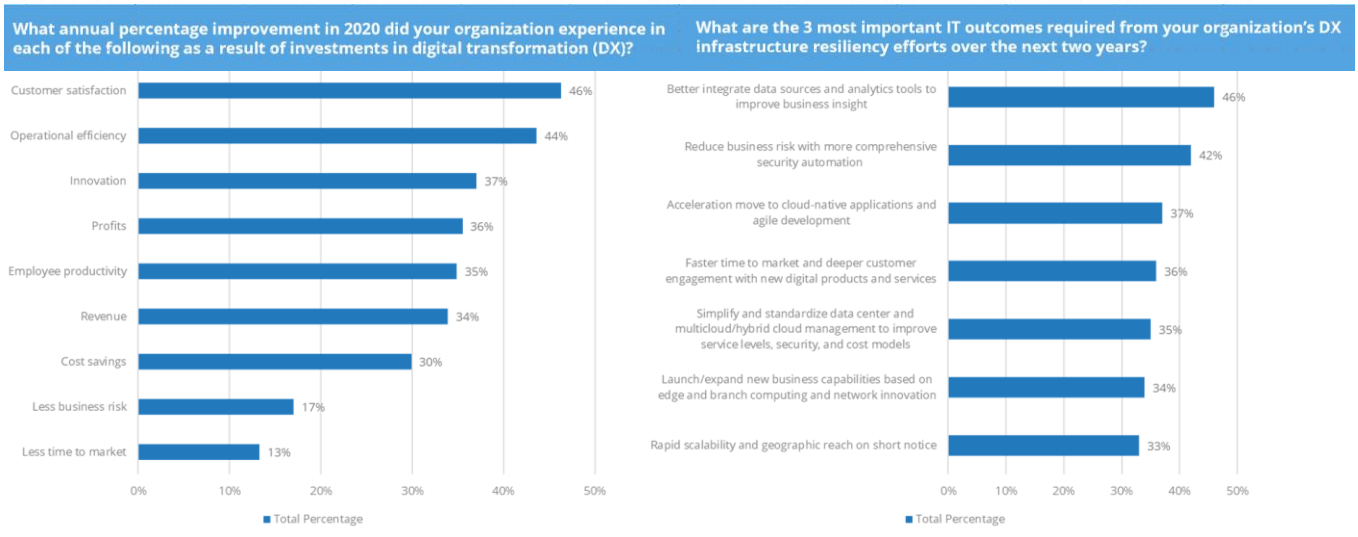
Written by: Philip D. Harris, Research Director

Introduction

Organizations, from the start of the pandemic to today, continue to work diligently to protect their IT environments, but this is becoming more difficult since the advent of several key factors: work from home, the Internet of Things (IoT) explosion, IT/operational technology (OT) security challenges and the expanded attack surface. These factors are largely the result of organizations racing to implement their digital transformation strategies and, as shown in Figure 1, organizations were willing to accept greater risk in the process.

It is a challenge for businesses to keep up with the sophistication of attacks, as the adversaries are always one step ahead. Security teams are always looking for that one silver bullet to solve all their security problems, but we know that does not exist. Add to this the lack of skilled cybersecurity professionals and a need for an optimized security operations center (SOC). These add to the overall cost of a security program as salaries move higher and higher and organizations are unable to invest in the necessary equipment, skilled staff, and even allocation of the space needed.

FIGURE 1: ***Why Is Cybersecurity Risk Management Lagging with Digital Transformation?***



IDC #US47988920 (June 2021)
Source: Future Enterprise Resiliency & Spending Survey, IDC, May 2021, N=832Source: IDC

To address this, many organizations look to managed security services providers (MSSPs) to take on the operational activities of security log correlation and monitoring, alert generation, incident response support, incident containment, remote security management, etc. Some MSSPs only perform the logging and monitoring aspect, and some perform both the logging and monitoring and the management of security solutions for organizations. To add more confusion to the mix, there are now providers offering comprehensive managed detection and response (MDR) either as a separate service or in addition to the traditional MSSP.

In this paper, we will look at the managed security services (MSS) marketplace confusion to bring clarity and provide a path forward for customers to make the right choice based upon their business needs and requirements, their place in the threat landscape and their business appetite for risk.

Marketplace Confusion

There is confusion not only from professionals new to the security field but also from seasoned experts as to what the various options are and how these affect their overall architecture, support bolstering their security posture and deal with addressing their residual risks.

As these markets continue to evolve and become saturated, there's a certain amount of confusion around the dizzying array of vendors offering managed security services (MSS) and what the various categories of offerings are today. It becomes difficult for organizations to decide what to choose to address their security operational needs.

There continue to be several buzzwords that have explicitly entered the security services market. While some mean well and have value, others have become misleading. Terms such as machine learning (ML), artificial intelligence (AI), endpoint detection and response (EDR) and big data analytics all seem to be overused. Of course, all can't be game changers alone without the right coordination and integration of the various components. Additional services such as MDR and SOC as a service (SoCaaS) bring even more confusion into an already confused market.

Clearing Up the Confusion

So, let's break this down among the three most common managed services: MSS, MSSP and MDR. One thing that should become very clear to the reader is that IDC views this as an evolution of MSS as opposed to just a bunch of vendors trying to differentiate among themselves with fancy (cumbersome) services and naming conventions. To this end, IDC has designated this evolution as MSS 1.0 (MSS), MSS 2.0 (MSSP) and MSS 3.0 (MDR), and, in the rest of this section, this will be made apparent. Figure 2 below encapsulates and illustrates this evolution.

MSS evolved to include more capabilities since its introduction into the market well over 10 years ago, with many providers forced to offer more than just basic device hygiene. From IDC's perspective, the first generation of MSS, classified as MSS 1.0, provided the management of traditional security devices such as firewalls and intrusion detection and prevention systems. Additionally, log collection, alert management, alert guidance and recommendations were offered, but the services generally stopped there, where in-depth capabilities were needed.

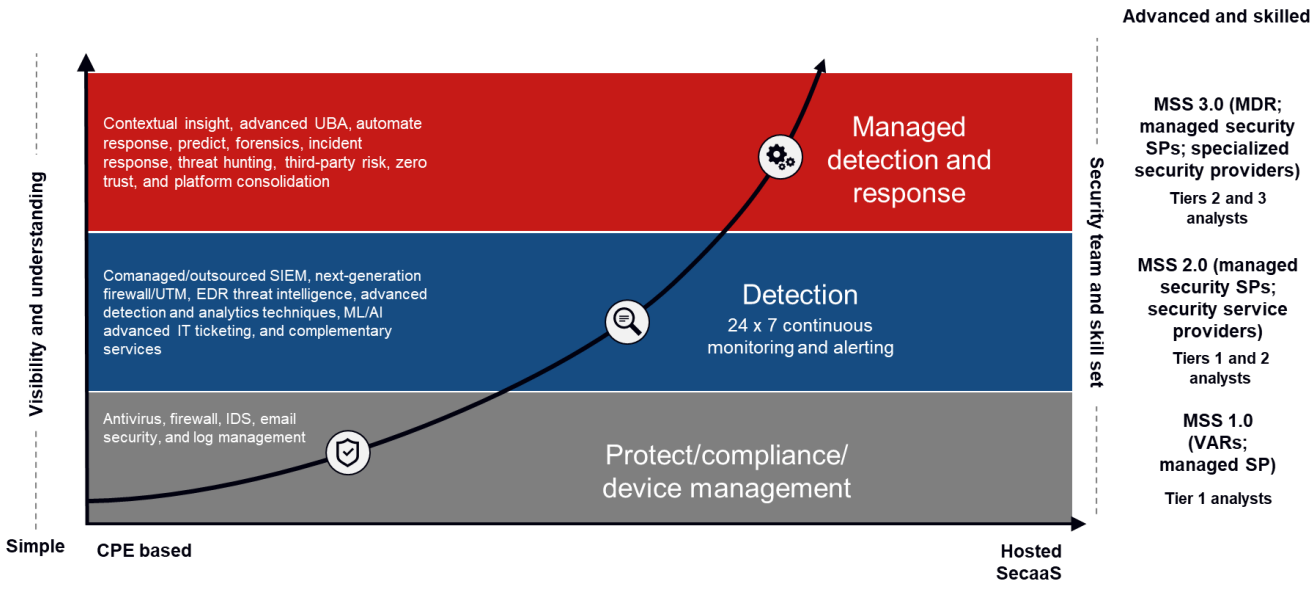
MSSPs also offered MSS 1.0 services. However, as time and vendor maturity have progressed, these providers have moved up the stack to MSS 2.0, where they started offering advanced security capabilities and services. As the attack surface grew due to organizations undergoing digital transformation, visibility became increasingly more important. The need to ingest more log sources and provide more advanced capabilities became necessary. This forced service providers to accelerate their adoption of new security technologies, such as ML/AI, automation and orchestration, and utilize SIEMs to aggregate and correlate logs and offer compliance reporting.

Within this evolution, it became evident that MSS was not only about managing devices but also the data that these devices contain. The consulting arm grew in this era for many MSS providers expanding their offerings to security assessments, investigations, forensics, incident response and full SOCs. This has led to a further evolution of MSS 2.0 (see Figure 2) by service providers offering SoCaaS capability.

With organizations needing more help in advanced security functionality, especially around SIEM, organizations were forced to have either an in-house security team do its own SIEM tuning, configuration and updates or turn to a service provider that could provide a managed SOC. A managed SOC is a central component that combines a team of security experts and 24/7/365 support of around-the-clock monitoring and management of threats. Organizations can outsource a set of security capabilities to a managed SOC team, such as SIEM, vulnerability management, endpoint security and other detection and response tools. Managed SOC models can be deployed as a co-managed or fully managed/outsourcing of security.

In a managed SOC or SoCaaS, the "as-a-service" piece sometimes alludes to the fact that first, it's a service, and second, it is a cloud-based platform and/or cloud-hosted or multitenant service. That is not to say that the provider would not manage and monitor a customer's on-premises-based (CPE-based) equipment, but the monitoring and response pieces would be done by a MSSP (including managed SOC or SoCaaS).

FIGURE 2: ***Evolution of MSS***



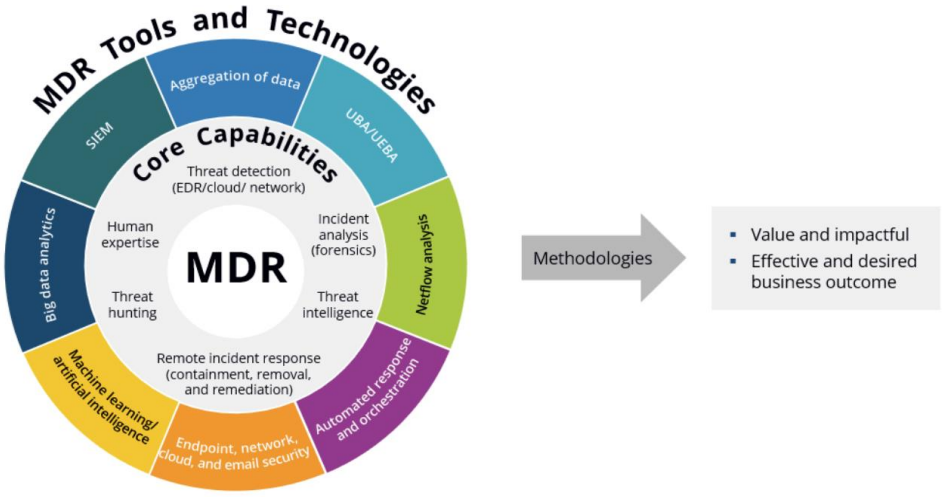
The next evolution of MSSP now brings in detection and response capabilities, known as MSS 3.0, which is where MDR really starts to shine as the next generation of security operations. This is also where the Pondurance MDR service brings forth all the elements that will be described later. To have this complete life cycle of services as stated, for example, in the National Institute of Standards and Technology to Cybersecurity Framework with the identify, protect, detect, respond, and recover framework functions, a new MSS model was needed. MSS 3.0 is the natural evolution that encompasses MDR. MDR is an extension of and includes both MSS and MSSP capabilities and services, and combines the tools, technologies, procedures methodologies and people used to provide full cybersecurity life cycle of capabilities for an organization (see Figure 3 below). With this in place, MSS 3.0 service providers can effectively work hand-in-hand with

their customers to not only alert on incidents conduct investigations and make recommendations but also take on the remediation steps through an EDR solution, tiered support analysts and full incident response services.

Service providers can deploy MDR services utilizing a mixture of clients' existing capabilities, cybersecurity partners' supplied tools or services and private intellectual property. This partnership forms a powerful combination of advanced EDR/extended detection response (XDR) solutions, human expertise, threat intelligence, threat hunting, enhanced consoles, dashboarding and reporting and various forms of intellectual property developed by the MDR service provider (see Figure 3). The following are brief descriptions:

- The utilization of EDR endpoint protection solutions, such as Carbon Black, CrowdStrike and Sentinel One, or even proprietary EDR solutions is a typical addition for MDR providers with a heavy focus on monitoring and protecting endpoints. XDR is also an evolution of EDR systems that have access to a greater universe of telemetry data such as the network, the endpoints, logs, cloud instances and messaging systems that can be used in place of an EDR system. Combined with traditional MSS and MSSP services, MDR also empowers the MDR service providers team to manage much of the remediations directly as organizations allow.
- Human-based expertise is crucial for MDRs to provide a well-trained team of cybersecurity experts in a 24/7/365 SOC, remote coordinated incident response for containment and removal of threats, and threat hunting capabilities that leverage threat intelligence, risk analysis, defined playbooks and even automation.
- Additionally, integration of various threat intelligence feeds from sources, such as endpoints, dark web intelligence forums, open source and commercial service feeds and vertically focused threat intelligence feeds, is critical. MDR service providers also offer web-based consoles and dashboards, that enhance monitoring, alerting, updating, and reporting of indicators of compromise (IOCs) and generate service tickets.
- Intellectual property includes the methodologies, practices, procedures and various forms of automation, intelligence, response, and orchestration that pull together the human and technology-based capabilities into a set of services providing greater value than if the end customer were to take this on alone.

FIGURE 3: ***An Effective MDR Solution***

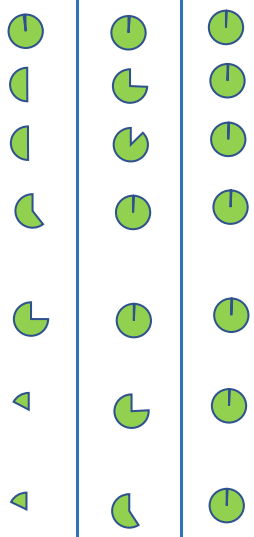


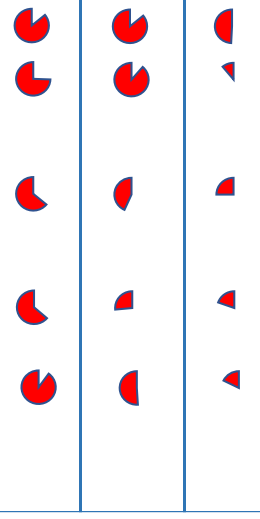
Source: IDC, 2020

Advantages and Disadvantages

There are several ways to view the advantages and disadvantages of the above-mentioned approaches between MSS 1.0 (MSS), MSS 2.0 (MSSP) and MSS 3.0 (MDR). Figure 4 breaks out the advantages and disadvantages.

FIGURE 4: **Advantages and Disadvantages of MSS 1.0 (MSS), MSS 2.0 (MSSP) and MSS 3.0 (MDR)**

Advantages	MSS 1.0 (MSS)	MSS 2.0 (MSSP)	MSS 3.0 (MDR)
	The Larger the Pie, the Greater the Advantage		
• **Cost Savings** - Service providers provide a reasonable fee or subscription for the entire organization by leveraging the same experts across their entire customer base. • **Security Expertise** - With the availability of security professionals in high demand, this easily deals with the security skills shortages being experienced today. • **Customer Support** - Service providers provide real-time support in the event of issues or incidents that arise. This also includes working with experts to resolve technical issues based upon recommended remediations. • **Compliance** - In today's environment with expanded attack surfaces, work-from-home and IoT explosion, and privacy concerns, service providers today must demonstrate compliance to security regulations or frameworks to support customers. Often times, end customers will request audit or certification-type reports that demonstrate the service provider is compliant. • **Business Risk** - In today's world of digital transformation and the movement to the cloud, organizations need to ensure they are online all the time and cannot be subject to disruption of any kind, whether from an attacker or other form of disruption. Leveraging a service provider can significantly reduce the risk of any kind of disruption. • **Modernization** - Some organizations may not have the staffing, budget or time to upgrade security processes and solutions to address evolving risks. Service providers can offer an easier means by which organizations can modernize by outsourcing to a service provider. Some MDR service providers offer the ability to migrate to next-generation technologies such as EDR or XDR solutions. • **Incident Management** - MSSPs may offer some form of incident response capability. MDR service providers offer various incident response capabilities so that organizations can immediately address incidents the moment they are identified.			

Disadvantages	MSS 1.0 (MSS)	MSS 2.0 (MSSP)	MSS 3.0 (MDR)
	The Larger the Pie, the Greater the Disadvantage		
• **Security Costs Don't Go Away** - Organizations will still need to maintain some form of security presence even if it is with a single person, chief information security officer or otherwise, to ensure the service provider is performing against the service-level agreements. • **Sensitive Data Concerns** - Not so much a concern today with many service providers that either strip sensitive data from log sources or tokenize or otherwise sanitize sensitive data prior to receipt. However, this could be an issue if not fully investigated with your service provider. Ensure they do not have access to sensitive data or, at the very least, ensure there are contractual obligations that protect you. • **Lack of Control** - Like anything you hand off to someone else to manage for you that is outside your organization, you lose some measure of control over processes, procedures, communications, staff, etc. The key here is making sure you have in place the appropriate control structures to monitor the performance of the service provider. • **Transparency** - Some service providers may state that their capabilities are completely proprietary and are not able to tell you exactly how they will provide their service to you. Be wary of service providers that are not willing to share how they will perform their services to your satisfaction. • **Business Justification** - There are times when the internal security organization may not have provided enough justification for pursuing either of these approaches. Service providers should support their customers by aiding in building that justification.			

Source: IDC, 2021

What Should the Decision-Making Approach Be?

IDC recognizes that some blurring is occurring in the security services market, and the line between MSS, MSSP, MDR and SoCaaS can be quite confusing. In fact, my colleague also wrote a market perspective titled "Blending Together/Overlap of Consulting and MDR," (US46232520) which discusses how consulting, MSS and MDR providers are overlapping and offering a wider array of services.

Organizations should steer away from getting caught up in all the different buzzwords occurring in the market. Instead, focus on what type of security assistance you need. This will help you derive the requirements, which will make the decision much easier.

For example, are you looking for an extension to your IT or security team that includes 24/7/365 support across the full life cycle of your cybersecurity needs? Is your business in the crosshairs of the attacker community and need more advanced technologies, expertise, and response capabilities? Think about what type of business outcome you are trying to achieve and what offerings will meet your IT and security requirements. It is also essential to think about the value in what the service provider brings to the table. What different levels of support are offered that will elevate your cybersecurity maturity? What security technology stack is the provider bringing to the table? Do they have the experts you need from Tier 1 to threat hunters to IR investigators? Does the MDR service provider comply with required security frameworks and/or regulations.

In the end, organizations should focus on the people, process and technology that will help them reach their long-term goals for improving and maturing security with their business needs.

FIGURE 5: ***Terms of Importance When Selecting a Third-Party Security Service Provider***

Green = managed, red = professional, and black = mixed
n = 400

Green = managed, red = professional, and black = mixed

Notes:

See *Pricing Considerations Rank at the Bottom of the List When Choosing Third-Party Security Service Providers* (IDC #US45364819, July 2019) for details.

Mean rating is based on a scale of 1-10, where 1 = not important and 10 = very important.

Source: IDC's *MSSP Survey*, 2019

Benefits

As you can see from figures 3 and 4 and the discussions that surround these, there are a variety of benefits a customer can derive from choosing the right MSS. What customers need to keep in the forefront of any decision is the threat landscape and how susceptible their organizations are to attack or exposure. This will help customers determine the best route for choosing the right MSS. Also, consider the fact that as organizations continue to push the envelope of digital transformation, more advanced managed services capabilities will be needed to meet both the current and future security needs. Having a leg-up on the business means security organizations may be viewed as a business partner instead of a business inhibitor.

There is a compelling case for many security service providers that choose not to offer a full breadth of services. The argument that a firm is sticking to its core competencies, as one example, is not without merit. IDC recognizes that spreading the providing firm's capabilities too broadly and without the proper bench strength to call upon when resources are stretched thin is a relevant point. The overriding principle that service providers need to keep in mind is they need to take care of their customers. The domino effect of taking care of each customer's specific business needs by offering up the guidance and capabilities that are within the service providers core competencies will result in higher trust and stickiness from its client base.

Sometimes that means having the right partnerships in place to recommend or partner with a competitor to fill a specific need. CISOs will respect and remember the service provider that does not overpromise or falsely state its own capabilities, but instead is seen as that trusted advisor that is willing and able to recommend the services and capabilities of competitors when that is the best course of action. Taking care of the customer, even when that means deferring business, is always better than trying to deliver capabilities that are not readily available or matured enough to provide for a client to rely upon.

The concept of a cyber fusion center for SOCs has been in vogue in recent years. One of the core reasons for this concept is that virtual and physical walls have been put up between SOCs and the businesses that they are tasked with protecting. Unfortunately, tribalism can often occur within the confines of security service providers as walls are put up between the teams that provide the critical security functions and other organizational departments. Opportunities are plentiful for MDR and MSS teams to keep their ears open for engaging the consulting teams on ways to improve their clients' cybersecurity postures. The opposite is true for consulting engagements, as they also can look at opportunities to offer up their MDR or other MSS offerings.

Technical training is always a good idea in retaining scarce cybersecurity talent, but a brief portion of any company-provided training might be well suited to provide sales training to the best sales team a service provider might have: the very people who provide the human intelligence in any security service offering.

Considering Pondurance

Business and security leaders face a variety of challenges when trying to secure their digital assets and operations from cyber threats, and in the post-pandemic world, this becomes especially problematic with the race toward digital transformation. To compound the challenges, security professionals are in high demand, creating a wildly competitive market for security talent that is expensive to hire and hard to retain.

In the latter part of 2008, Pondurance was established with a mission to ensure that every organization can detect and respond to cyberthreats — regardless of size, industry, or current in-house capabilities. The Pondurance team believes

that AI, automation, and security technology products alone cannot stop motivated attackers. Attackers aren't machines; they are people, and you need ingenious human intelligence, experience, and expertise to go head-to-head with adversaries. Pondurance combines its advanced platform with decades of human intelligence to speed detection and response and contain cybersecurity threats quickly to ultimately decrease risk.

Pondurance has built an organization that utilizes a combination of human intelligence and the Pondurance SCOPE platform to aid customers in stopping security incidents with 24/7/365 detection and response, enabling customers to maximize internal resources and security investments, improving customer compliance needs and accelerating security program maturity, all with the intention to lower the total cost of ownership for security. See Figure 6 for a high-level view of the Pondurance MDR framework.

The Pondurance people, framework, platform, and services all combine to both take the mystery out of the managed security space and provide a simple, but powerful, next-generation MDR (MSS 3.0) capability to enable customers to accelerate their business strategies with confidence (see Figure 6).

Pondurance differentiates itself from the competition in the following critical ways:

- 24/7x365 U.S.-based SOCs

  Pondurance MDR is powered by analysts, threat hunters and incident responders who utilize an advanced cloud-native platform technology to provide customers with continuous cyber risk reduction. Pondurance has been instrumental in aiding law enforcement at the state and national levels to track down cybercriminals and expose numerous zero-day vulnerabilities.

- 360-degree visibility

  Pondurance detection and response brings together network (traffic analysis sensors), EDR, SIEM and cloud infrastructure (Amazon Web Services, Google Cloud Platform and Azure) to gain overall visibility of the customer environments and provide the necessary information to the SOC analysts to ensure that threats are identified and actioned immediately.

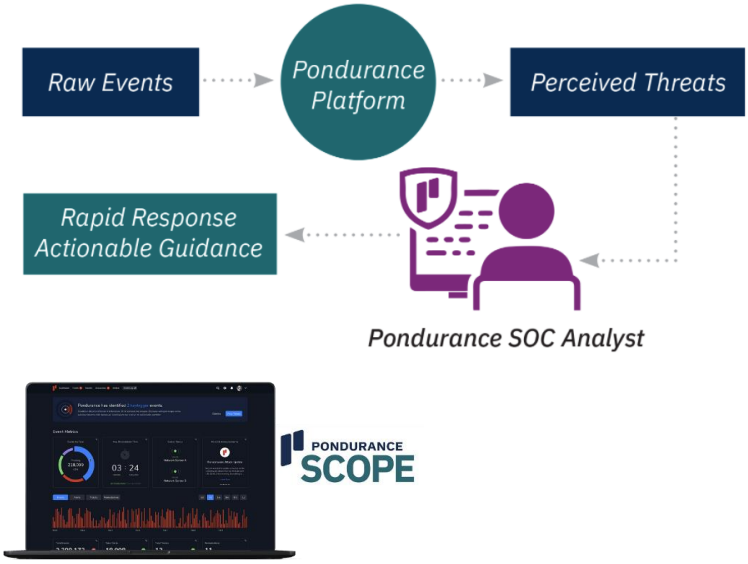
- Closed-loop incident response

  This aids customers in reducing the time it takes to respond to emerging threats through triage and incident response services. Pondurance believes that rapid human intervention is often the key difference between immediate containment and impact to the business.

- Integration with customer-existing infrastructure and control structures

  Pondurance has developed its platform to enable integration with existing security investments, whether cloud-based or on-premises security controls. This also includes providing connectors to various log sources that are not already part of their extensive library as part of their subscription.

FIGURE 6: ***Pondurance High-Level MDR Framework***



Source: Pondurance, 2021

Conclusion

Organizations, both during and post-pandemic, continue to look for ways to reduce risk and protect their IT environments. This has been a difficult proposition mainly due to businesses driving toward digital transformation and willingness to accept great risk from the key factors of work from home, the IoT explosion, IT/OT security challenges and the expanded attack surface. This continues to be a common theme between business and security, where the business needs to drive forward, but fear security will inhibit the forward progression.

Fortunately, with the evolution of MSS, service providers can now offer advanced solutions to make security a positive business driver. As we've seen above, organizations have had to deal with the confusion in the MSS marketspace rife with a variety of jargon, a variety of solutions and a confusing array of services. The good news is that this marketspace has been simplified and clarified as we see an evolution of MSS in the form of MSS 1.0 (MSS), MSS 2.0 (MSSP) and MSS 3.0 (MDR). What customers can now do is be very clear about their requirements and where the business stands in the threat landscape.

Since its inception, Pondurance has fulfilled the requirements of MSS 3.0 where the combination of humans, technology and services brings together a straightforward managed security service that customers can leverage to meet their needs and even future needs of their businesses.

About the Analyst

***Philip D. Harris, CISSP, CCSK**, Research Director, Cybersecurity Risk Management Services*

Phil Harris is the Research Director for CRMS. He is responsible for developing and socializing IDC's point of view on Governance, Risk and Compliance across people and process focused on creating a foundation of Privacy and Trust with enterprises, IT suppliers and service providers.

MESSAGE FROM THE SPONSOR

About Pondurance

Pondurance delivers world-class MDR services to industries facing pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements, and digital transformation.

Our advanced Pondurance SCOPE platform with our experienced team of analysts continuously hunts, investigates, validates, and contains threats, so your team can focus on what matters most.

Get real examples of how we help our clients in our case studies here: https://cybersecurity.pondurance.com/case-studies_idc

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com