NTT Security

Whitepaper

Augmenting traditional security monitoring with Managed Detection and Response (MDR)

If you are looking to improve your threat detection and incident response capabilities, but are concerned about budget squeezes and resource availability, you're not alone.

A growing number of organizations are not only struggling to accurately detect and respond to advanced threats as they arise instead of hours, weeks or months later; but also to find cost-effective solutions that make the most of existing investments.

With new threats emerging so fast that organizations cannot keep up, many businesses are now asking how they can augment their existing security monitoring capabilities without significant cost increases. Managed Detection and Response (MDR) is emerging as a service offering that builds on existing MSS services to enable organizations to improve traditional threat detection and response capabilities, without the expense of investing in additional staff. Gartner estimates that by 2020, 15% of midsize and enterprise organizations will be using services like MDR, up from less than 1% in 2016.

By 2020, 15% of midsize and enterprise organizations will be using services like MDR, up from less than 1% today.

Gartner

Challenging times require a fresh look at security services

Today's advanced targeted threats are leaving organizations struggling to deploy, manage and use an effective combination of expertise and tools to detect and respond to threats. And traditional signature-based anti-malware tools are no match for detecting threat actors that use complex evasion techniques. Many organizations, facing skills shortages and looking to be cost-efficient, may already be using MSSPs to manage complex solutions, analyze high volumes of alerts and achieve compliance. However, in order to detect and quickly respond to previously unknown threats, these organizations should now be looking to the market for new services to match their evolving requirements. These include contextual threat intelligence, hunting for threats moving laterally within the network, endpoint detection and response, and critical incident response.

MDR - more than traditional Managed Security Services

Typically, organizations find that many MSSPs will offer basic detection and alerting services, only for it to fall to the client organization to provide additional analysis and response. With attacks becoming more frequent and complex however, organizations are finding it impossible to manage this workload around the clock, and detect advanced threat actors using traditional detection methods. The need to have an advanced detection and response capability to act quickly and accurately is critical in order to limit risk.

Definition of Managed Detection and Response (MDR)

A focus on enhanced 24/7 monitoring, advanced and unknown threat detection using advanced analytics and contextual threat intelligence, remote, rapid incident validation and actionable recommendations or remediation guidance. This is supported by traditional Managed Security Services, Consulting and a Critical Incident Response program in case a breach does occur.

Aware of these challenges, some existing and new providers are responding by offering MDR services - advanced security services that include advanced analytics capabilities, contextualized threat intelligence, threat hunting and human validation. They may also offer consulting services for remediation guidance. In some cases MDR services can mean that decisions around which tools and methods to use for security monitoring and response are passed to the provider and away from the organization, and in other instances, providers offer services using the organization's existing infrastructure and technology. There are pros and cons with both setups, so organizations should look for a solution provider that includes an initial consultation to assess their existing infrastructure and maturity level and recommend the best possible solution to maximize existing capabilities.

MDR services can be offered in a number of ways, depending on the changing needs of the organization, from augmenting their SOC with advanced detection and response services to implementing traditional MSS controls with advanced MDR capabilities. But it is important to remember that having traditional MSS is an essential foundation to take full advantage of MDR. Advanced detection and response of threats will be most effective if there is a broader threat monitoring solution already in place.

Consider managed security service providers (MSSPs) that offer MDR-like services when device management and compliance use cases are required.

Gartner

The differentiator in MDR is the complementary use of contextualized threat intelligence and advanced analytics that feature anomaly detection techniques such as machine learning or behavior modeling in addition to traditional methods such as signature and perimeter-based defences. The advantage is that the gap between detection and response is being shortened and the accuracy is increased.

Another significant differentiator between traditional MSSP and MDR is how the service is delivered. Typically the MDR provider will deploy and manage detection tools at both perimeter and endpoints, using logs, endpoint activity and network traffic to ensure that the organization's threat detection ability is improved.

It's important to remember that the full benefits of MDR can only be realized if the organization takes a full-service approach (see Figure 1) – this means starting with a consulting assessment to enable the organization to fully understand their risk posture and provide a tailored roadmap; getting the basics right in the right place with a traditional MSS; building in advanced MDR capabilities, and supporting with a critical incident response service in case a breach does occur.

Figure 1 Full Service Approach to MDR

Looking for MDR services? Seven questions you need to ask

It is worth asking a handful of questions as part of any due diligence when selecting a partner:

- Does the MDR provider offer strategic consulting services such as MSS assessment and Critical Incident Response planning to ensure that the MDR service forms part of your overall security strategy rather than a bolted-on service?
- Does the provider offer traditional MSS services to support their MDR services?
- Does the MDR service look beyond the endpoints to monitor the network, servers, applications, as well as devices?
- Can the provider demonstrate expertise in using tools for threat hunting, threat detection, threat response, advanced analytics and network behavior analysis to identify and respond to attacks?
- Is the MDR provider also a threat intelligence provider, and if so, what types of threat intelligence do they provide? Will they rely only on publicly-available commercial threat intelligence services, or do they generate their own threat intelligence?
- Will the provider offer 24/7 monitoring, analysis and alerting, and how does the provider use experts (rather than just automation) to add context?
- Does the provider have a rapid response team that can respond when advanced threats are found?

Conclusion

Over the coming years, traditional MSSP providers will reshape their existing offerings to meet customer demand for MDR but there are those who have already been investing in and offering these capabilities for some time along with strategic and technical security consulting. Don't jump at the first sales pitch – look for a provider who can offer MDR that is supported by consulting, traditional MSS and Critical Incident Response for breach readiness and post-breach incident management. A full service offering from one provider will ensure that your MDR solution is supported by managed security, consultancy and technical expertise. The need to integrate your MDR provider with the overall mission of the business and your risk management strategy is critical; as they can assist in education, securing funding and alignment of their advancements to help meet your company's short and long term goals.

About NTT Security

NTT Security is the specialized security company of NTT Group. With embedded security we enable Group companies (Dimension Data, NTT Communications and NTT DATA) to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of consulting and managed services for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more.

To learn more about NTT Security and our unique services for information security and risk management, please speak to your account representative or visit: **www.nttsecurity.com** for regional contact information.