PALADION
HIGH SPEED CYBER DEFENSE

www.paladion.net

Whitepaper

MSSP or MDR - Know the Difference and Choose the Right Partner

Author:

Vinod Vasudevan

CTO

Executive Summary

With the changing threat landscape, enterprises need high confidence that their cyber security service provider can provide the necessary protection. New generation attacks and deep targeted attacks are outdoing the capabilities of traditional managed security services. Managed security service providers (MSSPs) and managed detection and response (MDR) providers offer different approaches to combating threats.

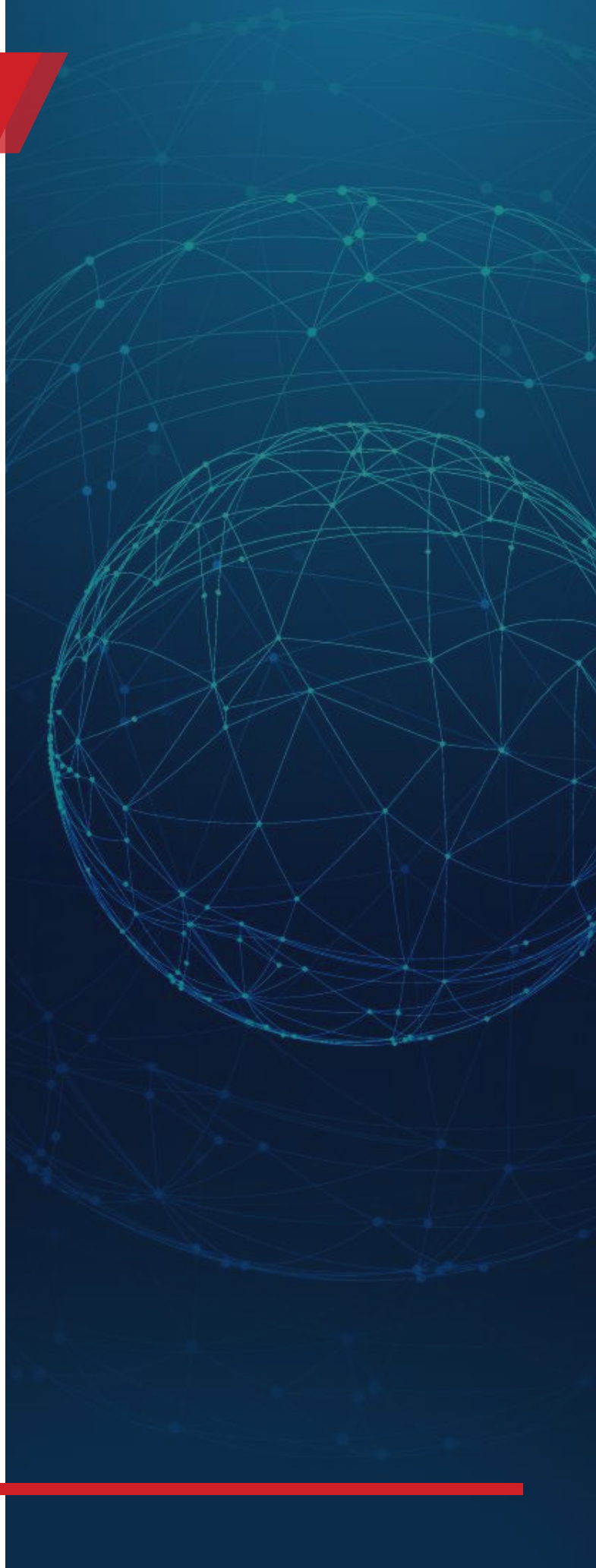
Shifting Categories of Security Service Providers.

Currently, there are two main categories of providers. The first, the Managed Security Services Provider (MSSP), offers remote monitoring of security-related events and data sources, the remote management of an enterprise's IT security technology, or both. The second, the Managed Detection and Response (MDR) Provider, offers 24/7 threat monitoring, detection, and response services. MDR services tend to be more 'low noise' to reduce unnecessary alerts yet more 'high-touch' (human contact) with greater support for responding to incidents and breaches.

What MSSPs Do

Historically, MSSPs have used rules and signatures to protect their customers. Automation and shared services are characteristics of MSSPs, relying more on a standard one-size-fits all approach and less on customer context-based detection or response to serve their market. Typically:

- MSSPs take in their customers' security data and send them threat alerts. An MSSP will pull customer security logs and alerts into its security incident and event management (SIEM) platform and notify customers about threats if certain rules and signature match.
- MSSPs apply internal rules of thumb to select which alerts they will bring to their customers' attention. These are not tuned to customer environment.
- Customers will need to investigate these alerts for any impact or relevance. MSSPs may provide additional log information based on customer requests.
- If a customer has a potential incident, an MSSP may provide additional professional services for incident management. However, these additional services are not always deployed fast enough to keep up with the response requirements for effectively managing the incident.
- MSSPs provide customers with commodity threat intelligence feed on malicious IPs, ports, URLs and file signatures. These data are machine readable. Customers can integrate them into their SIEM, intrusion protection system (IPS), firewall or URL filters.
- MSSPs offer management of security devices. This provides a preventive layer of protection by pre-configuring rules to block known attack scenarios. This is a manual layer that is not integrated in real time to the detection process. There are usually separate teams working to provide security monitoring as one offering and security device management as another offering.



Missing pieces in the MSSP Security Jigsaw

While rules and process driven MSSPs can demonstrate efficiency in their activities, they may not be effective against today's cybercriminals.

- MSSPs may miss over 70% of threats because they only take in system security data and apply generic rules for threat detection.
- Mid-size and larger enterprises can easily face thousands of cybersecurity threats every day. MSSPs do not have enough human resources to evaluate all these alerts for customers. They limit their selection of alerts to forward to customers based on their top use cases. Consequently, there is a higher chance that a critical alert is overlooked, simply because it did not meet a top use case.
- MSSPs cannot fully investigate and analyze alerts for a customer, because they lack the context for the customer's environment. They do not provide investigation as part of their monitoring service. They cannot answer key questions about a customer's alerts, such as: Is there an impact? Are the alerts benign? Are they currently indeterminate? What steps must be taken to further determine their impact?
- MSSPs do not provide continuous incident management services. They often cannot contain an attack that is spreading fast, nor execute a playbook for incident recovery, nor conduct root cause mitigation while working seamlessly with a customer's internal team.

MSSP services were sufficient before the advent of deep targeted attacks and in a world of low attack volumes. In a more predictable world, an MSSP approach with rules and signatures for known attack use cases and preventive measures with management of security rules was sufficient. In a dynamic world of targeted attacks with new and changing attack vectors used by unknown attackers, the MSSP model fails. For many mid to large enterprises, their MSSP may be simply providing them a basic security monitoring service that is necessary, but insufficient in today's dynamic threat landscape.

The MDR Side of the Security Coin

MDR services are for enterprises that want to move beyond compliance requirements and boost their 24x7 threat detection and response capabilities. MDR service providers put greater emphasis on using AI to detect the new threat vectors, leverage customer context information to triage alerts, and have response automation to quickly contain threats. Salient features that enable MDR providers to solve problems that beat MSSPs are listed below:

- MDR services go beyond only looking at perimeter systems. They have a comprehensive approach to look at internal systems and end points
- MDR providers scale beyond conventional sources by including proxy, NetFlow, user activity for detecting advanced attacks
- MDR uses different types of AI algorithms to hunt for attacks at scale
- Mature MDR providers have a technology platform with multiple technology modules including threat hunting, threat intel, SIEM, endpoint threat detection and response (ETDR), user and entity behaviour analytics (UEBA), and incident analysis and response
- MDR providers take ownership of response with playbooks that define response activities and roles.monitoring as one offering and security device management as another offering.

The flip side is that not all MDR service providers offer the compliance reporting that MSSPs do and may also stop short of managing appliances like firewalls (network or web application firewalls) and intrusion detection and prevention systems (IDS/IPS). However, MDR providers who are also MSSPs offer such management along with advanced threat detection and response.

> *Over 70% of breaches today are not detected through traditional rules and signatures.*

Missing pieces in the MSSP Security Jigsaw

The table below captures the differences between MSSP and MDR.

#	Area	MSSP	MDR
1	Scope of assets	Perimeter devices	Perimeter devices, Internal systems and end points
2	Monitored Sources	Security devices, limited DMZ IT infrastructure including OS, webservers, network devices, databases	Security Devices. More comprehensive DMZ and internal IT infrastructure including OS, webservers, databases. Additional sources including proxy, NetFlow, user directories
3	Detection Technologies	Rules and signatures, threat intelligence, light weight analytics	AI (machine learning, deep learning, statistical anomalies), rules and signatures, threat intelligence
4	Detection Process	Eyes on the glass with limited hunting	Advanced hunting for attacks and eyes on the glass for triaged alerts
5	Integration of customer context information	Limited integration of assets, vulnerability information	Integration of assets, vulnerabilities, users for context
6	Response Process	Customer ownership with support for event information from service provider	Service provider ownership or joint ownership with well-defined playbooks on activities and roles
7	Response Technologies	None. Pre-configure rules & signatures through management of firewalls, IPS as a preventive mechanism for known attack scenarios	Dynamic auto containment through on-the-fly configuration of parameters in firewalls, IPS, end points, network access control (NAC)
8	Reporting	Compliance focused with wide variety of reports	Threat focused reporting, compliance is a by-product
9	Management of security device infrastructure	Core part of offering	Not a core service offering. Leverage security infrastructure as part of response
10	Technology platform for service delivery	SIEMs with support for rules. Payload/packet capture technologies matched against signatures.	Big data security platforms with SIEM, threat hunting, incident analysis, auto-containment and orchestrated response. ETDR and UEBA also integrated in to the offering.

Paladion's MDR

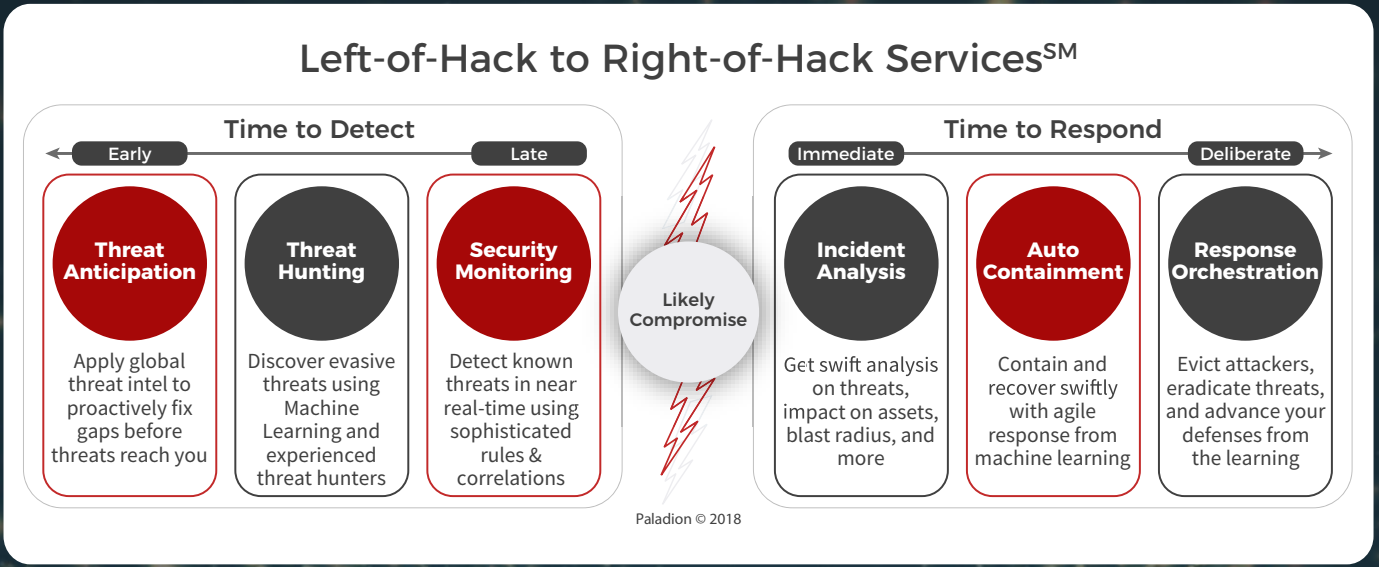
Paladion's MDR solution brings you the benefit of early detection and faster response to advanced threats. It leverages advanced technology including artificial intelligence, blending it with human expertise for gains in performance in handling alerts, responses, and recoveries.

Paladion's MDR looks at data from the entire IT stack of the customer to provide unified analytics on threats. It also correlates data with intelligence on threats and attacks worldwide to see if a customer's organization might be affected. High speed response automation technologies enable quick mitigation to reduce attack dwell time from as long as months to as little as days.

Paladion's Left of Hack/Right of Hack MDR (2.0 Service Model). An MDR service provider can serve customers better by providing more comprehensive, modular services before (to the left of) and after (to the right of) a likely compromise or hack. From 'left of hack' through to 'right of hack', a schema for these services is the following:

- Threat Anticipation - Paladion's MDR offering collects, analyzes and responds to globally reported threats in the context of customer assets(application of threat intelligence).
- Threat Hunting - This combines advanced AI driven detection models with expert human hunters to detect evasive threats (Threat Hunters in action).
- Security monitoring - Paladion's MDR offering applies real time security rules to alert customers to known threats (leverage of SIEM systems)
- Incident analysis - Removes irrelevant noise and only flags likely incidents. Scores relevant data to prioritize alerts, and automates asset impact analysis, attribution, attack chain creation, and patient zero identification.
- Auto Containment.- Uses pre-integration with customer technologies to contain a threat in minutes using Firewall rules, network ACLs, end point reconfiguration, process termination, user deletion/disablement.
- Response Orchestration - Centralizes and orchestrates incident response to reduce attacker dwell time from weeks to under one day. Deploys hundreds of playbooks to automatically contain a threat. Paladion's AI.saac continuously learns (machine learning) to add new playbooks and effectively contain a threat in minutes.

Incident responders make sure attackers do not exploit the same vulnerability and adapt defenses, so attackers cannot use the same TTP (tactics, techniques and procedures) again.



Conclusion

MDR services can be used to add threat detection, incident response, and 24/7 monitoring to organizations, either as a full-service solution for midsize enterprises or to supplement existing capabilities in larger organizations. Compliance reporting requirements and basic security monitoring can be handled by an MSSP. A combination of two can be beneficial for certain organizations who want a single vendor for cost and delivery efficiency.

PALADION

HIGH SPEED CYBER DEFENSE

ABOUT PALADION

Paladion is a global cyber defense company that provides Managed Detection and Response Services, DevOps Security, Cyber Forensics, Incident Response, and more by tightly bundling its AI platform - AI.saac and advanced managed security services. Paladion is consistently rated and recognized by leading independent analyst firms, and awarded by CRN, Asian Banker, Red Herring, amongst others. For 17 years, Paladion has been actively managing cyber risk for over 700 customers from its five AI-Driven SOCs placed across the globe.

WW Headquarters: 11480 Commerce Park Drive, Suite 210, Reston, VA 20191 USA. Ph: +1-703-956-9468
Bangalore: +91-80-42543444, Mumbai: +91-2233655151, Delhi: +91-9910301180, London: +44(0)2071487475, Dubai: +971-4-2595526, Sharjah: +971-50-8344863, Doha: +974 33777866, Riyadh: +966(0)114725163, Muscat: +968 99383575, Kuala Lumpur: +60-3-7660-4988, Bangkok: +66 23093650-51, Jalan Kedoya Raya: +62-8111664399.

sales@paladion.net | www.paladion.net