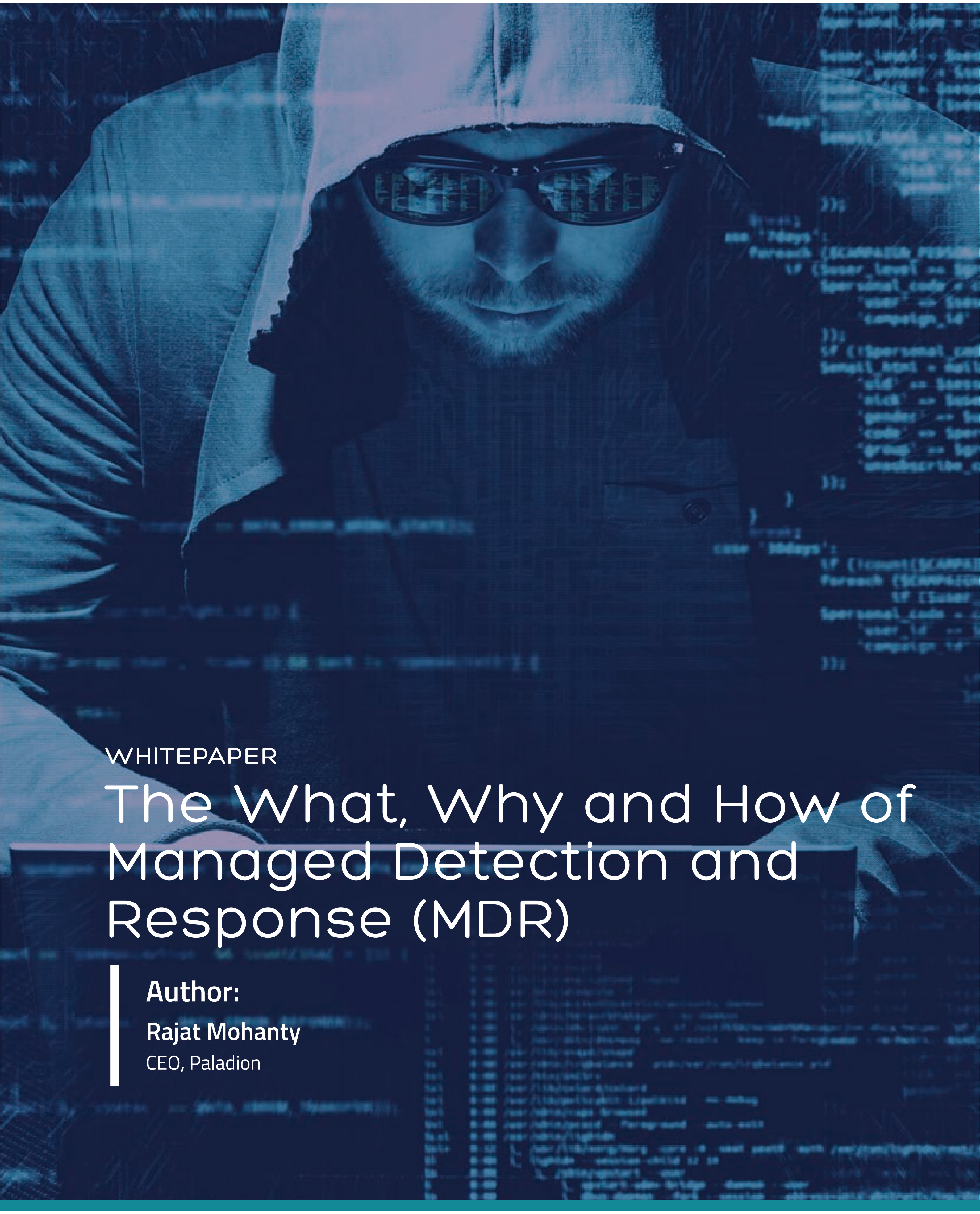
PALADION
HIGH SPEED CYBER DEFENSE



WHITEPAPER

The What, Why and How of Managed Detection and Response (MDR)

Author:

Rajat Mohanty
CEO, Paladion

Managed detection and response services are becoming increasingly popular. Gartner estimates that the number of organizations using MDR services will grow 15 times in the next 3 years.

Why This Rapid Rise in Adoption?

Cyber threats are rising in both volume and sophistication. Beyond a certain point, investments in prevention technologies show diminishing returns. Organizations therefore look to add strong detection and response capabilities to quickly identify threats and respond before they turn into breaches.

Traditional security monitoring is built around limited log collection and rule based analysis is no longer sufficient. While it is good for compliance use cases and visibility into common attacks, it is ineffective against newer forms of attacks. The next generation of security operations need other technologies beyond traditional SIEM (security information and event management) and newer skills beyond eye-on-glass monitoring. – See our e-guide on building an adaptive, future ready security operations center.

Building such next generation capabilities for threat detection and response is not feasible for most organizations. An MDR provider can help bridge this gap by delivering advanced detection and response as- a-service, thereby removing the complexity and cost of building in-house next generation security operations.

What is MDR?

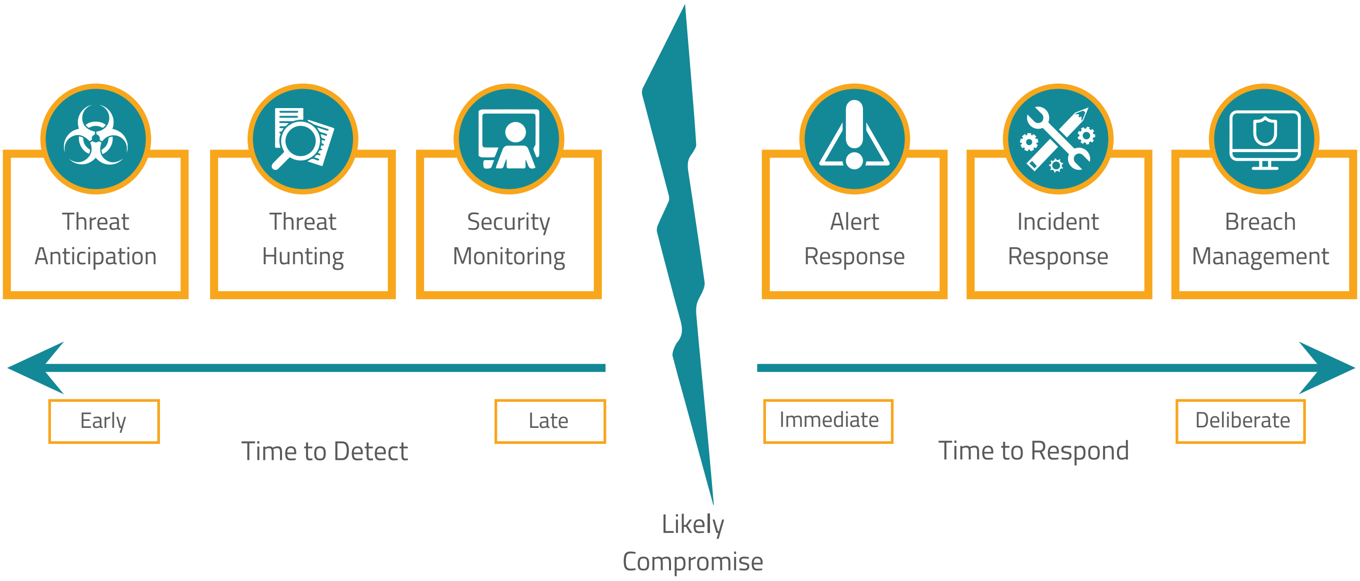
Managed detection and response is a combination of technology and skills to deliver advanced threat detection, deep threat analytics, global threat intelligence, faster incident mitigation, and collaborative breach response on a 24x7 basis.

However, MDR services are not a replacement of traditional managed security services (MSS) such as log management, log monitoring, vulnerability scanning, and security device management. Both solutions have a role to play; MDR enhances MSS services with focus on detecting and responding to breaches by bringing in complementary technologies and services on security analytics, response orchestration, and threat intelligence.

MDR services can be delivered by specialized vendors focused only on threat management or by an existing MSS provider with MDR capabilities. For many organizations, the best value comes from working with a single provider who has integrated MSSP and MDR services.

How is MDR Delivered?

At Paladion, we have designed our MDR offering to have the six outcomes described in the diagram and the table below.



MDR Outcomes	Description	How We Deliver
Threat Anticipation	This is **Threat Intelligence in Action:** global threat intelligence on attacks and attackers is applied in the context of each specific organization. Going beyond the generic data of threat intelligence providers, our MDR service converts threat intelligence data into actionable tasks, anticipating what could happen and how to stop it, if it happened.	We continuously collect threat data from a variety of threat feeds, news, blogs, social media and dark web resources in our threat intelligence platform. The data is analyzed in the context of each organization to see how likely such threats or similar ones will materialize. If a threat is likely to occur, measures are put in place for detecting them (rules and analytical models) and responding to them (response playbooks).
Threat Hunting	This is **Security Analytics in Action:** data science and machine learning are used with security, user and IT data to enable the detection of unknown and hidden threats.	We input your data from your log files, network traffic, packets, user access, application and endpoints into our big data analytics platform.

MDR Outcomes	Description	How We Deliver
Threat Hunting Contd.	There are now multiple security analytics technologies in market, including network threat analytics (NTA), user behavior analytics (UBA), endpoint threat analytics/endpoint detection and response (EDR), and application threat analytics (ATA). Our MDR service converts such analytics into actionable outcomes of detecting potential threats that have bypassed traditional security controls.	Our platform uses data sciences models and machine learning algorithms to detect suspicious and anomalous activities. A specialized hunting team then analyzes these outputs and queries the data and systems further to detect threats that may have bypassed other security controls.
Security Monitoring	This is **SIEM in Action:** the application of rules to logs and security events to detect known attacks.	We collect your logs and security events for analysis on our big data SIEM platform.

MDR Outcomes	Description	How We Deliver
Security monitoring Contd.	Different SIEM technologies are available to organizations, but they can be hard to operationalize. Our MDR offering produces the SIEM outcome for detecting known threats, policy, and compliance violations.	Instead of a static approach, we build and constantly fine tune the rules for detecting threats and non-compliances. We then monitor the alerts on a 24x7 basis and notify you according to the severity of these alerts.
Alert Response	This is **the bridge between alert notification to incident response plan and activation:** triaging the alerts to focus on the most relevant threats and then investigating them to attack chain, blast radius and potential impact to assets. Not every alert needs an incident response plan to be activated. The alerts need to be investigated for who, what, when, and how to the determine extent of the impact.	Our incident analysis platform has models and rules for fast triage of all your alerts, applying your contextual information, our threat intelligence, and observed kill chain behavior. Our incident analysts review these triaged threats and conduct deep incident analysis, using models for investigation integrated into our platform.

MDR Outcomes	Description	How We Deliver
Alert Response Contd.	Our MDR offering validates the threats using our incident analysis platform. Specialized incident analysts then provide the most relevant alerts and threats to be dealt with.	We then produce a highly curated incident analysis report that describes the entire attack campaign going beyond the current isolated alert, together with detailed mitigation steps.
Incident Response	This is **Response Orchestration technology in Action:** Carrying out rapid, coordinated activities for containment, remediation, and recovery. Response orchestration technologies have emerged for automating incident response but they need organizations to build up a considerable knowledge base and hire the requisite skills to utilize them.	We use our response automation platform with its response work flows, case management, forensic tools, and playbooks for a variety of incidents. Our responders collaborate with your distributed teams to contain, mitigate and recover from major incidents leveraging our platform and our knowledge base.

MDR Outcomes	Description	How We Deliver
Incident Response Contd.	As a practical alternative, our MDR offering provides you incident response as a service in a collaborative approach between your team and our specialized responders via our response orchestration technology platform.	Our team also builds and updates the response playbook as new incidents emerge or existing playbooks are found inadequate.
Breach Management	When an incident results in the breach of protected data (PCI, HIPAA, PII, or other) or customer confidential data, our MDR service assists in the entire breach management.	We provide services for breach forensics, evidence collection and retention, assessment of impact on compliance with regulatory requirements, and best practices for breach notifications.

MDR is a new industry segment and continues to evolve. This is our vision of MDR and how it can help organizations handle threats and vulnerabilities effectively. What is your vision? Add a comment below / Share your thoughts with us; we'd love to hear what MDR means to you.