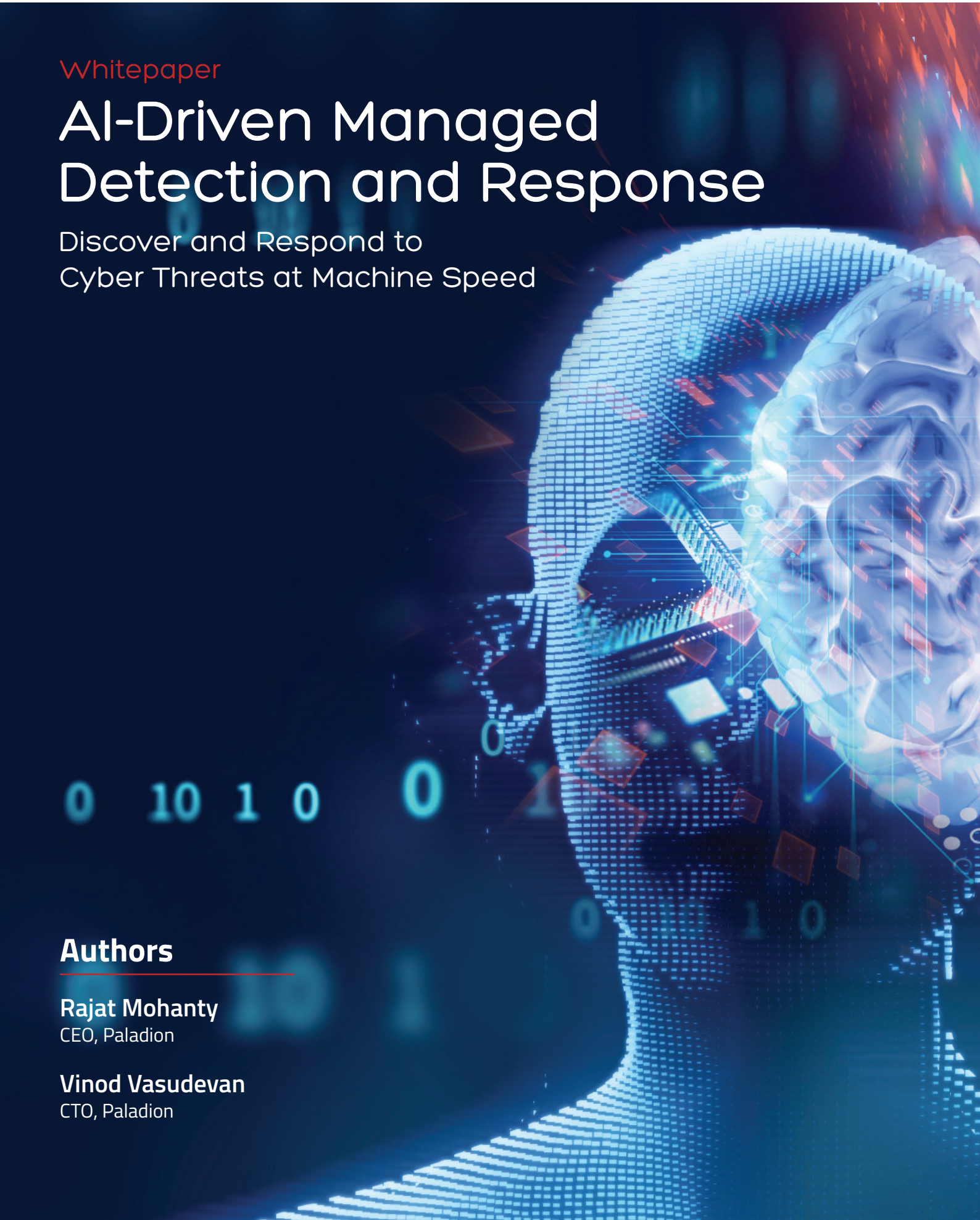
PALADION
HIGH SPEED CYBER DEFENSE

ahornloesungen
deutschland gmbh

Whitepaper

AI-Driven Managed Detection and Response

Discover and Respond to Cyber Threats at Machine Speed



Authors

Rajat Mohanty
CEO, Paladion

Vinod Vasudevan
CTO, Paladion

Executive Overview

To successfully manage current cyber threats, you must bridge the gap between the speed of attack and the speed of defense. AI based MDR services can deliver high speed cyber defense that match the speed of attacks.

Traditional security monitoring services are slow to detect attacks and slow to respond to them. They are built to meet compliance requirements and detect known attacks by using pre-defined rules. This approach cannot detect advanced attacks and insider threats that are often hidden and bypass such rules. And with such security monitoring services, organizations are left to respond to threats themselves, where lack of automation and orchestration means mitigation can take days or even weeks.

Paladion's Managed Detection and Response Service (MDR) differs from traditional MSSP services. It combines machine learning, security automation, and human intelligence to swiftly detect advanced threats and respond to them rapidly, so that an offensive campaign is interrupted before its objective is achieved. Advanced machine learning provides early detection of advanced threats and our security automaton helps in faster response. We bring in the critical human intelligence with our 1000+ security analysts and engineers.

Paladion's MDR is a next generation AI based managed security, delivered from the cloud by leveraging Paladion's own big data security analytics & response orchestration platform, and our mature distributed security operations centers (SOCs) with proven track records going back 17 years.

Achieving High Speed Cyber Defense with our MDR Service

Paladion's MDR offering helps you anticipate and hunt for cyber threats, going beyond passive security monitoring.

It also provides response services from alert validation to incident management and breach management. A brief description of each part of our offering is given below.

Threat Anticipation

From Security News to Protection within Hours

This is threat intelligence in action. It applies global threat intelligence in your specific context to enhance your protection.

Every day we read or hear about a new security threat that has already claimed multiple victims. After an initial success, attackers typically repeat their attack against other targets across industries and geographies. A key part of the MDR service from Paladion is to gather data and intelligence on threats and attacks worldwide, and to then distil the information to identify which customers might be affected.

We then detail specific actions for each customer to protect their digital assets before such attacks can be launched. This tailored threat anticipation goes far beyond traditional passive threat intelligence feeds available so far. Instead of the days traditionally needed to move from news to protection, Paladion's MDR service can make it happen in just a few hours.

> *Paladion's AI-Driven MDR has drastically enhanced our threat visibility. Our customers data is important to us as an organization, and they feel more secure knowing that we are proactive when it comes to incident and threat analysis. It has been a crucial partnership for Stratus Video.*

- Chris Downing, Vice President
Engineering at Stratus Video

“Gartner Says Detection and Response is Top Security Priority for Organizations in 2017”

We continuously collect threat data from a variety of threat feeds, news, blogs, social media, and dark web resources in our proprietary threat intelligence platform. The data is analyzed in the context of each organization to see how likely it is for such threats or similar ones to materialize. If a threat is likely to occur, measures are put in place for detecting those using rules and analytical models, and responding to them with response playbooks.

How this helped an MDR Customer:

When Shadow Brokers made exploit tools and several CVEs public, our Threat Intelligence team analyzed the threats and vulnerabilities in the context of each MDR customer, removed vulnerabilities, and created analytical models and rules to detect any attack attempts.

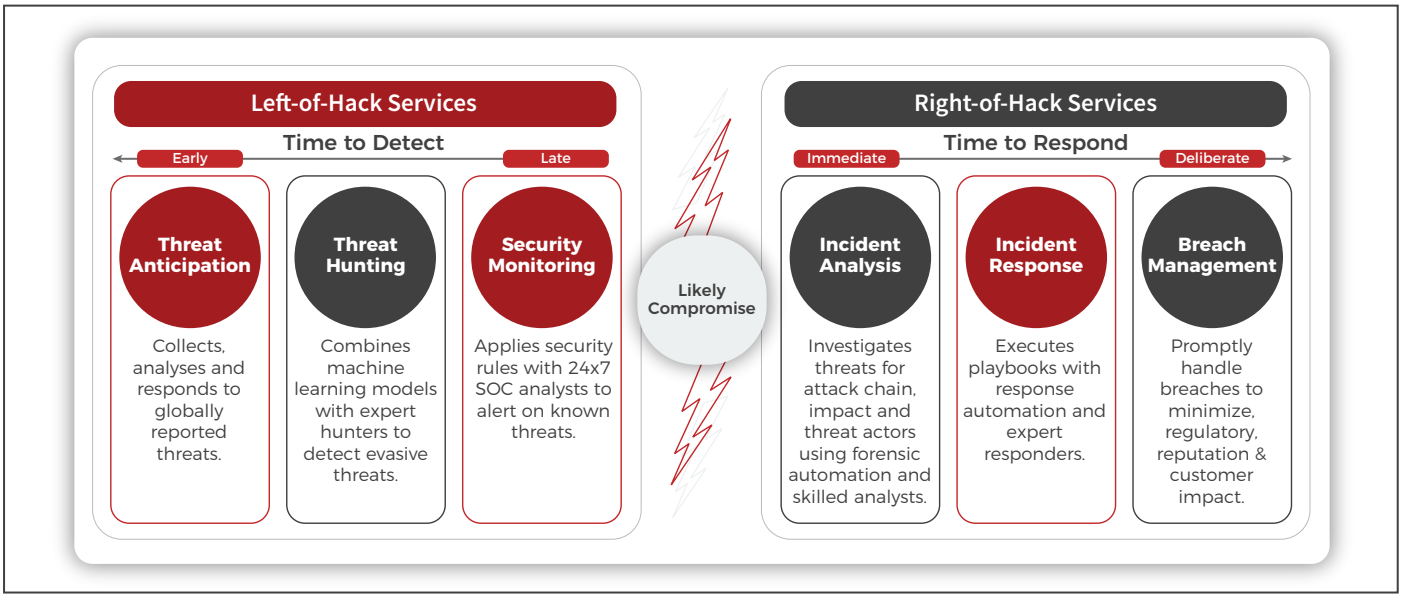
Threat Hunting

Don’t wait for alerts to show up; hunt them

This is security analytics in action: we apply data science and machine learning models to network, user, and machine data to proactively hunt for unknown and hidden threats in your environment.

Our platform uses data science models and machine learning algorithms to detect suspicious and anomalous activities. A specialized hunting team then analyzes these outputs and queries the data further to detect threats that may have bypassed other security controls.

Figure 1 : Components of Paladion’s MDR offering



Our threat hunting covers all five scenarios of security analytics:

Managed endpoint threat analytics

An oil and gas company was able to thwart an attack on distributed field systems controlling oil field pumps, thanks to endpoint analytics.

Managed user behavior analytics (UBA)

A financial institution put a timely end to the exfiltration of data after suspicious user activity was spotlighted using UBA.

Managed network threat analytics (NTA)

Thanks to the NTA in Paladion's MDR service, a government agency stopped an attack campaign designed to bring down its entire network of routers.

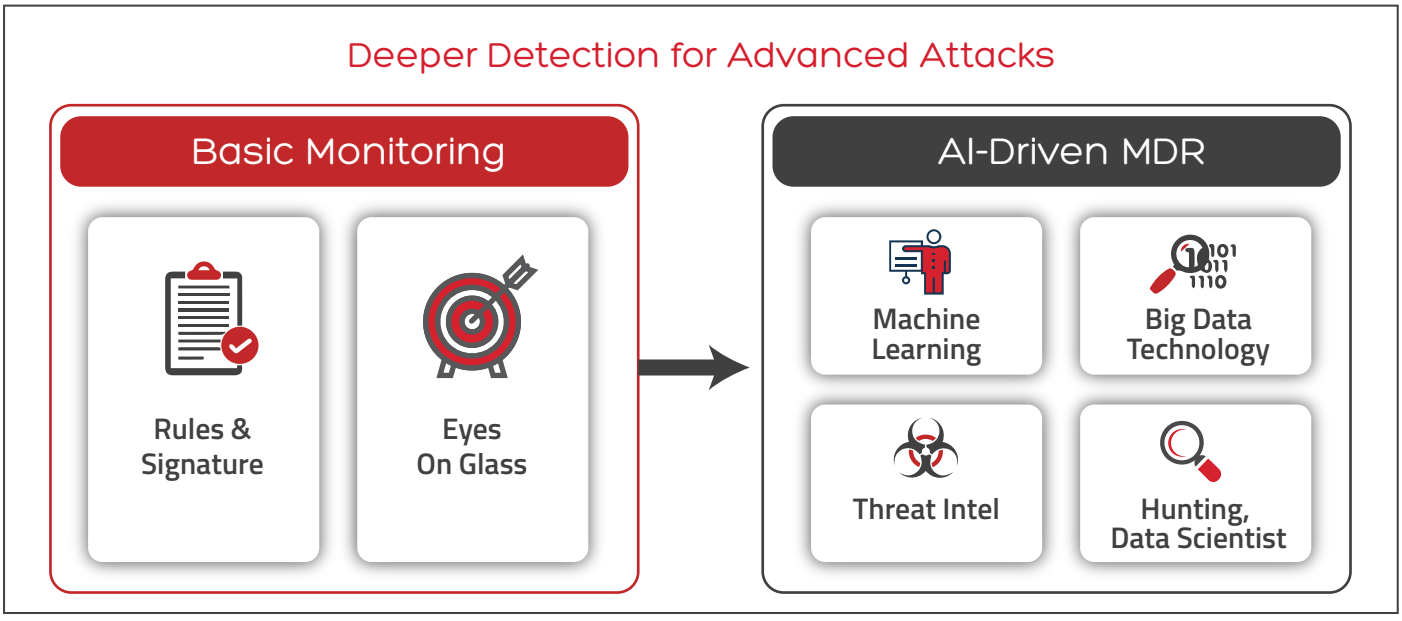
Managed application threat analytics (ATA)

A pharmaceuticals company detected and eliminated an attempt to steal confidential data from its R&D test management application.

Managed breach analytics

With Paladion's assistance in establishing compliance status and orchestrating a rapid response to an attack, a hospital avoided both data loss and regulatory fines.

Figure 2: Deeper detection for advanced attacks



How this helped an MDR Customer:

MDR threat hunting models helped unearth an advanced attack campaign in progress in a large financial institution within a few weeks of deployment. The attackers were in the network for more than a year using stealth malware. Machine learning models to detect malware beaconing and lateral movement were the initial triggers, and in combination with end point threat analytics the full campaign was unearthed before the attackers succeeded.

Security Monitoring

Detect known attacks and compliance violations at machine speed

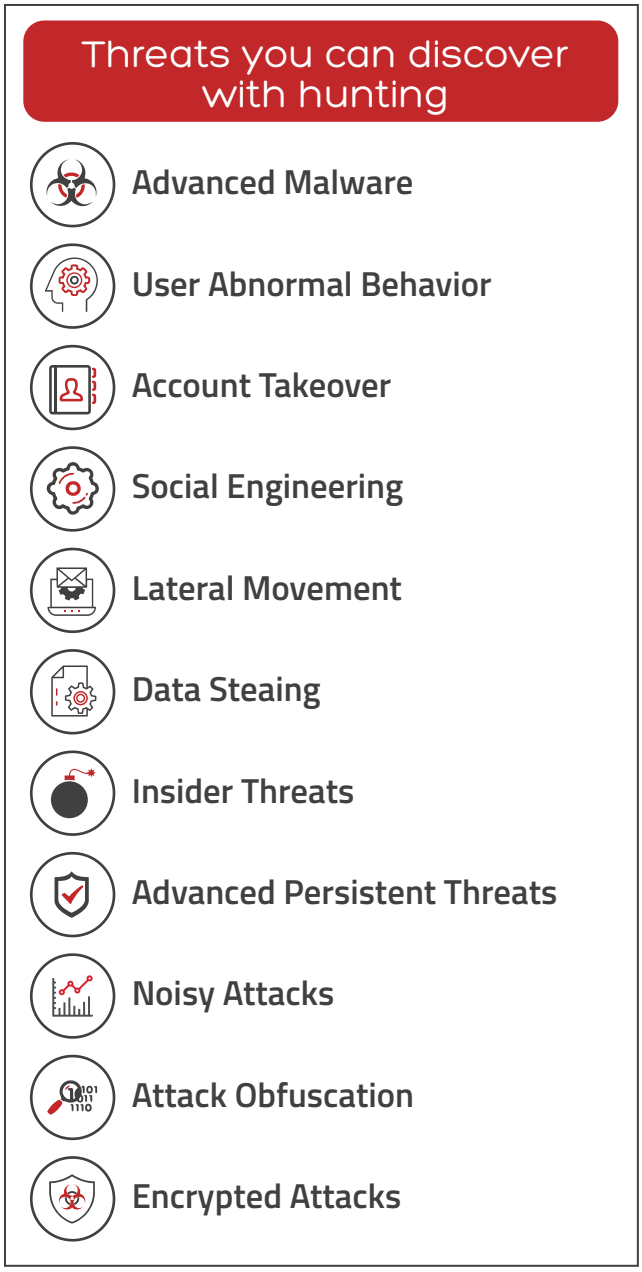
This is SIEM in action: we apply real time rules to logs and security events to detect known attacks.

A variety of SIEM technologies are available to organizations, but they can be hard to operationalize and maintain in-house. Our MDR offering delivers the SIEM outcome for detecting known threats, policy, and compliance violations.

We collect your logs and security events for analysis on our big data SIEM platform. 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.

We extend security monitoring to hybrid and pure cloud infrastructure. Connectors along with use cases enable detection of attacks to cloud consoles including Azure and AWS. Monitoring also enables protection of cloud infrastructure for all types of deployments including PaaS and SaaS. Deep connectors and specialized use cases enables detection of new age attacks on cloud apps. Comprehensive cover is provided for Azure Office 365 components including email, DLP, Sharepoint, Intune, and Dynamics.

Figure 3: Threats you can discover with hunting



How this helped an MDR Customer:

A large manufacturing company with hybrid in-house datacenters on Azure infrastructure and Office 365 had invested in cloud security technologies for end point protection and URL filtering. Paladion's MDR provided 360 degree visibility and protection across the hybrid infrastructure with a combination of cloud connectors and use cases on the big data MDR platform, which was supported by a team that understood new age attacks on the cloud.

Alert Response

Not every alert is an incident and not every incident a single alert

This is the bridge between alert notification to incident response and activation: triaging the alerts to focus on the most relevant threats and then investigating them to establish if there is a security incident. It converts alerts into more significant information such as the 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 MDR offering validates the threats and provides deep incident analysis combing our platform with specialized incident responders.

The incident analysis platform has models and rules for fast triage of all your alerts, applying 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. They then provide the most relevant alerts and threats to be dealt with.

How this helped an MDR Customer:

Alert validation at a leading financial institution had reduced from hours to seconds two weeks after MDR was implemented. Alerts were triaged against 20 plus parameters by applying contextual information, threat intelligence, and observing kill chain behavior.

Incident Remediation

Activate curated remediation in minutes to contain incidents

This is our Response Orchestration technology in Action; with the execution of rapid, coordinated activities for containment, eradication, 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. 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.

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. Our teams also build and update response playbook as new incidents emerge or existing playbooks are found inadequate.

How this helped an MDR Customer:

A leading e-commerce giant that took weeks to analyze incidents and remediate threats subscribed to Paladion's MDR service to enhance their incident response capabilities. Within 3 weeks of implementation, incident analysis was completed in minutesinstead of weeks and threats were contained in near real-time.

Breach Management

Get Back to Business Operations -Fast

When an incident results in the breach of protected data (PCI, HIPAA, PII, etc.) or customer confidential data, our MDR service assists in the entire breach management. We provide services for breach forensics, evidence collection & retention, assessment of impact on compliance with regulatory requirements, and best practices for breach notifications.

How this helped a non-customer that reached Paladion for assistance:

A global manufacturing company was a victim of a ransomware attack and reached Paladion's incident response team for assistance. Paladion's team started incident analysis and detonated the ransomware sample in our labs, while another team reached ground zero to contain the attack. With expert coordination, all systems were back online in less than 4.5 hours.

Key Differentiators of Paladion's MDR

Cloud Delivered MDR

Our Cloud Delivered MDR offers scalability, affordability, one-click upgrades, state-of-the-art security technologies, and round-the-clock access to security experts. Get the scale and processing power of Cloud for high speed defense.

Single AI and automation platform for hunting, monitoring, and response

Paladion's MDR is delivered through its proprietary multi-source, big data analytics platform. Applying analytics concurrently to multiple sources of IT, network, users and business data, it helps visualize a single view of the attack. Being multi-source, the platform has the unique ability to link together individual attacks and identify an attack campaign. Modern attacks do not occur as a single event at a single asset. They are usually spread out across time and assets using a variety of individual attacks in cyber kill chain. Only the Paladion's MDR platform can provide a full view of various stages of kill chain and piece together the entire attack campaign, and orchestrate responses to mitigate the attack.

High Human Touch, High-Performance Systems

Cyber security excellence is achieved when both machines and human work in tandem. The speed and power from the machines, and the insights and experience from the human minds offer an unbeatable combination.

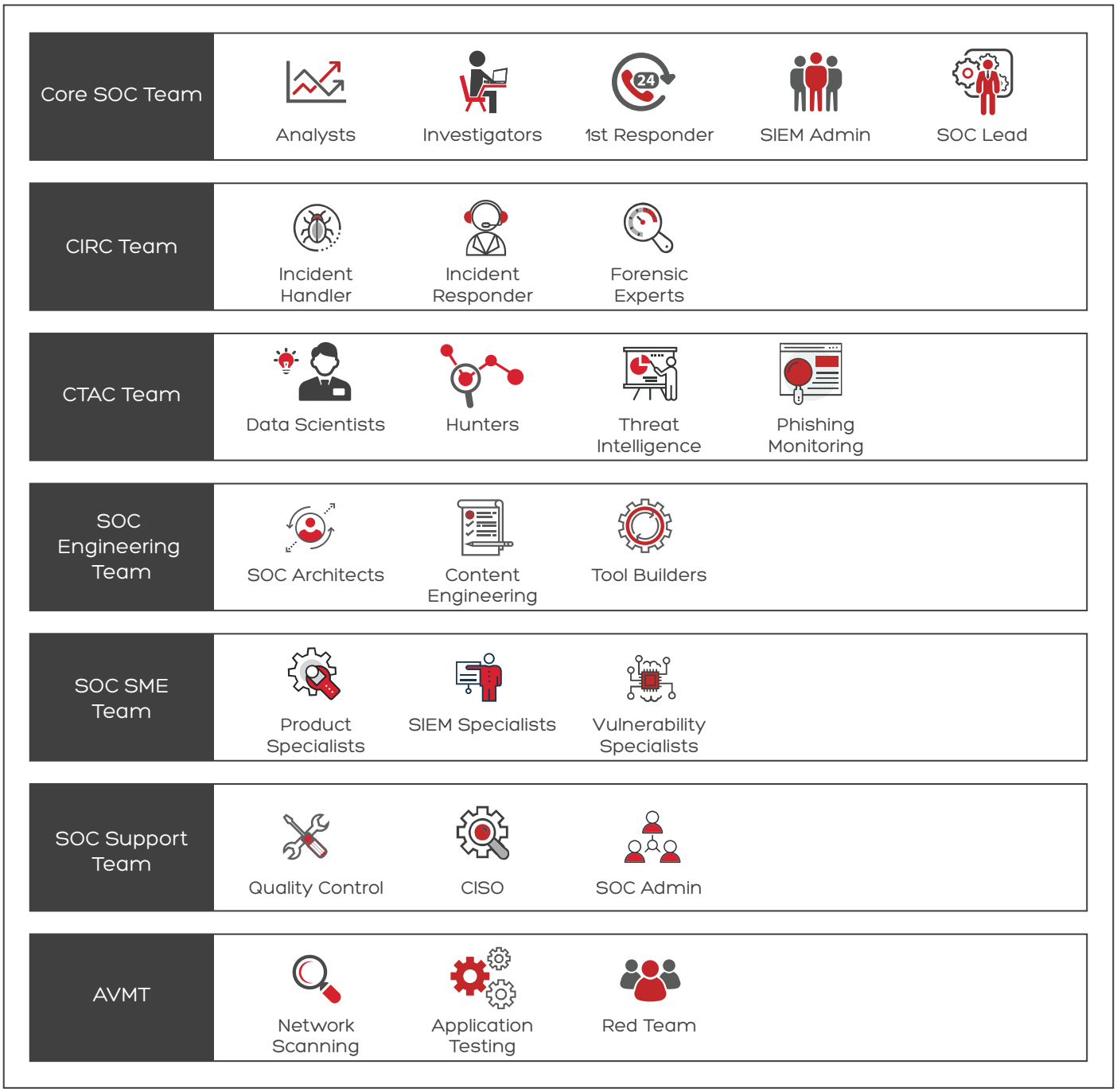
> *Paladion was able to swiftly deploy their technology and services across our vast network. We see a significant improvement in our threat detection maturity with their MDR threat hunting, and our in-house IT teams no longer need to spend their efforts analyzing and remediating complex cyber threats. Paladion has provided us the much-needed security assurance with their MDR service.*

- Mukund Dadarkar, Head IT and CISO
Quality Kiosk

The managed detectionand response service from Paladion uses these principles for a collaborative approach between specialized teams to tackle threats. Unlike a traditional SOC, our SOC is built on the MDR model and houses specially trained staff for the roles shown in the diagram below.

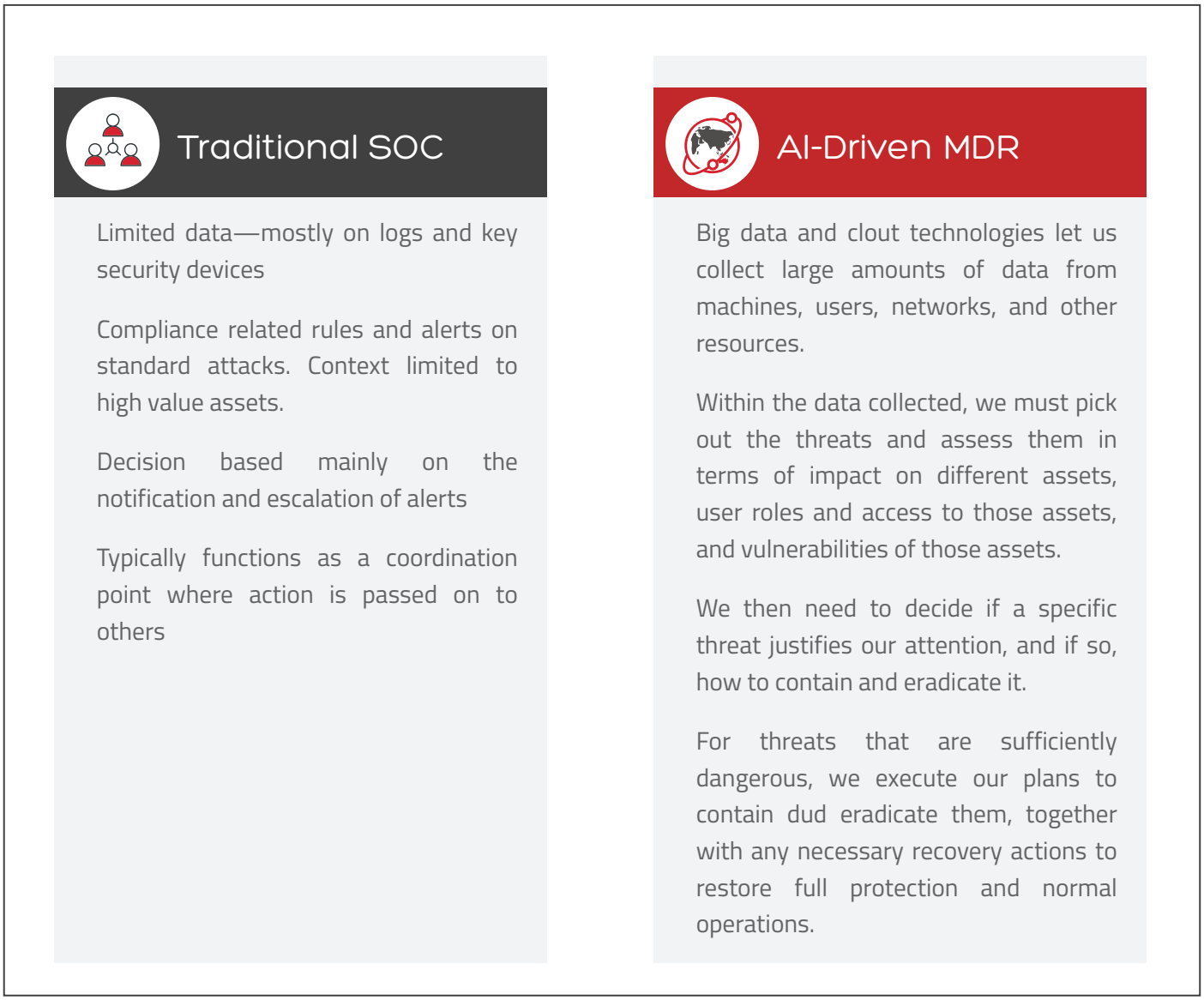
Customers using MDR with security monitoring get full access to our global team of experts and three times more resources per client than traditional managed security centers. Named resources are distributed across multiple skill sets.

Figure 4: SOC staff build on the MDR model



While MDR can significantly increase IT security posture in a cost-effective way, it is also designed to augment traditional security systems, rather than replace them. Conventional security solutions such as SIEMs, anti-virus software, firewalls, and intrusion detection systems still have an important role to play. Their signature, rules, and policy based approaches allow them to filter out common and known threats. Our security monitoring team constantly fine tune the rules based on the latest threat intelligence and customer's profile, update signatures manually where needed, and ensure the technologies are updated to get the maximum return from these investments.

Figure 5: Traditional SOC Vs Managed Detection and Response



Conclusion

Our MDR differs from traditional security monitoring by detecting advanced threats early and responding to them faster. It brings an integrated security analytics platform built on big data that can sift through huge amounts of security data to identify incidents to focus on. The service also brings specialized, highly coordinated teams that hunt, investigate, and respond to threats. The integration of advanced technology and human expertise ensures threats are identified in near real-time and are validated in minutes. Containment and remediation of threats is completed within hours.

MDR from Paladion can be added to your existing security operations center or it can also be provided as part of a total managed security service that combines rule based solutions with the MDR service. Investments in existing solutions can be protected, allowing enterprises to also continue to maximize their return on investment for solutions already in place.

With Paladion's MDR you get:

- Continuous detection of advanced threats
- Increased visibility on assets, network, users
- Reduce dwell time from 90+ days to 1 day
- Respond in minutes & hours instead of days & weeks
- Swift, coordinated response to reduce business impact

> *Paladion's AI-driven MDR service has powerfully augmented our existing security posture. They tailored their security services to meet our specific needs and deployed their services quickly and simply. They both increased the speed of our detection and response, and done so with a very high-touch, people-first approach that our internal security team loves.*

- Chief Information Officer
Fortune 500 Manufacturing Company

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 Frost&Sullivan, Asian Banker, Red Herring, amongst others. For 18 years, Paladion has been actively managing cyber risk for over 700 customers from its 5 AI-Driven SOCs placed across the globe.

Please visit www.paladion.net for more information.

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