PALADION
HIGH SPEED CYBER DEFENSE

Managed Detection and Response (MDR) with Artificial Intelligence

Discover and Respond to Cyber Threats at Machine Speed

Authors:

Rajat Mohanty
CEO, Paladion

Vinod Vasudevan
CTO, Paladion

Gartner Research:

Toby Bussa
Research Director, Gartner, Inc.

Craig Lawson
Research VP, Gartner, Inc.

Kelly M Kavanagh
Principal Research Analyst, Gartner, Inc.

Sid Deshpande
Principal Research Analyst, Gartner, Inc.

Gartner

In this issue

Executive Overview 3

Achieving High Speed Cyber Defense with our MDR Service 4

- Threat Hunting 5
- Security Monitoring 7
- Alert Response 8
- Incident Remediation 8
- Breach Management 9

Key Differentiators of Paladion's MDR 9

Conclusion 13

Research from Gartner:
Market Guide for Managed Detection and Response Services 14

About Paladion 24

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.

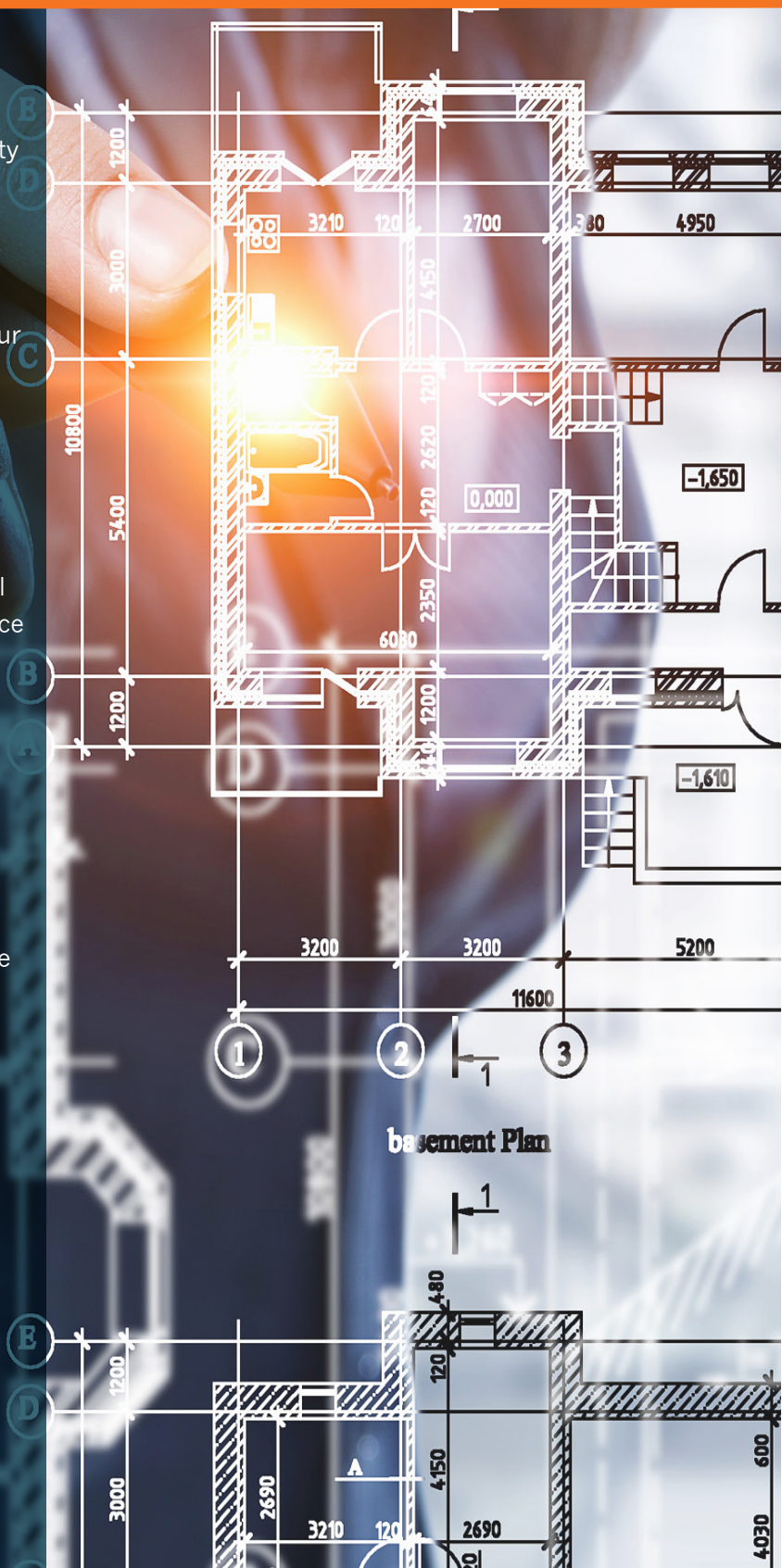
Threat Anticipation

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.



"Gartner Says Detection and Response is Top Security Priority for Organizations in 2017"[1]

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.

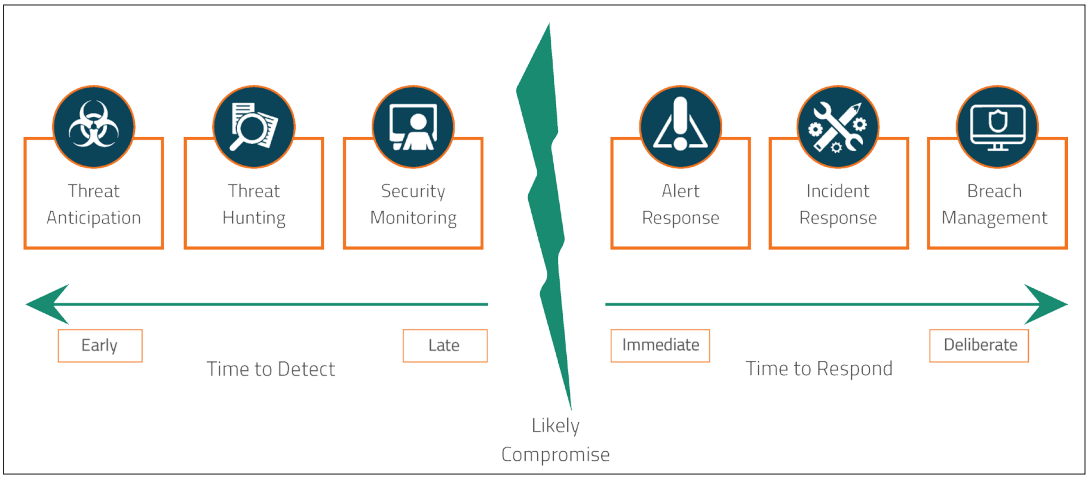
Threat Hunting

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



Source: Paladion

[1]Gartner Press Release, http://www.gartner.com/newsroom/id/3638017, 14 March 2017

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.

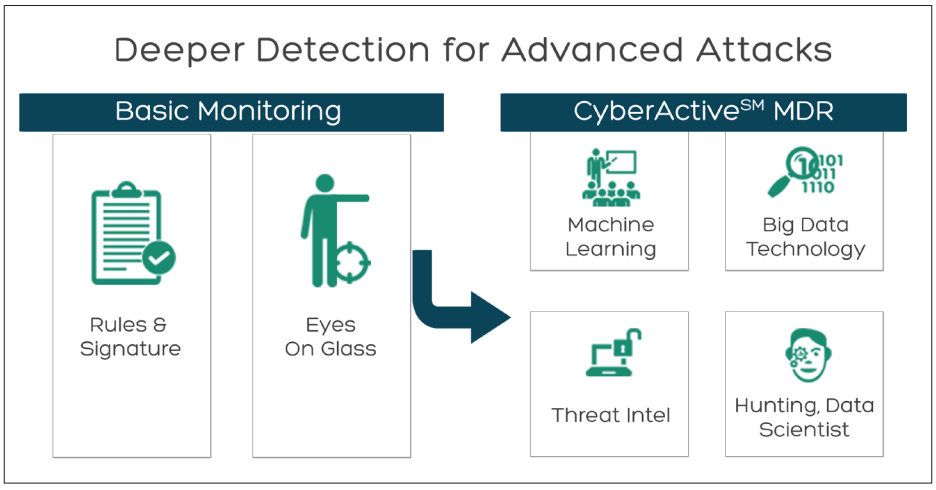
- **Managed application threat analytics (ATA)**

  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



Source: Paladion

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

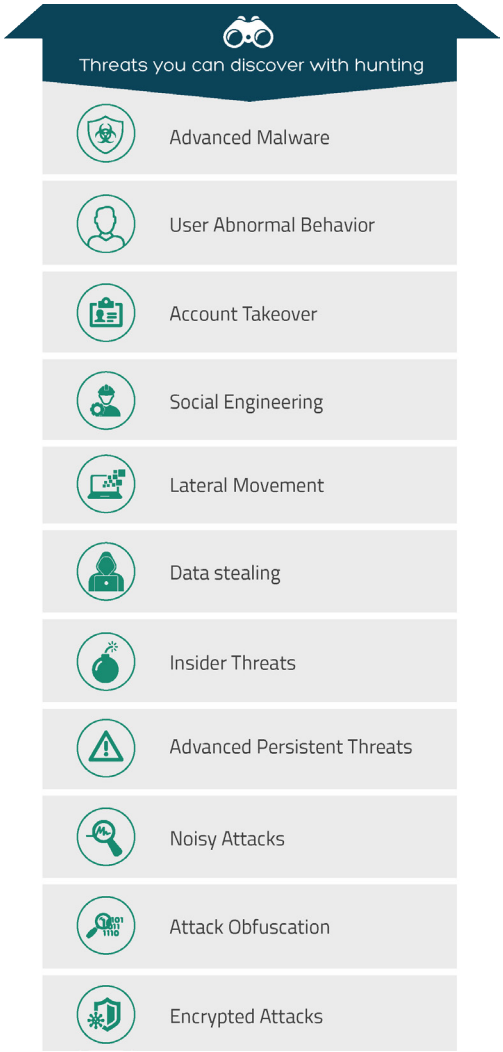
This is SIEM in action: we apply real time rules to logs and security events to detect known attacks.

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



Source: Paladion

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 minutes instead 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.

Source: Paladion

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.

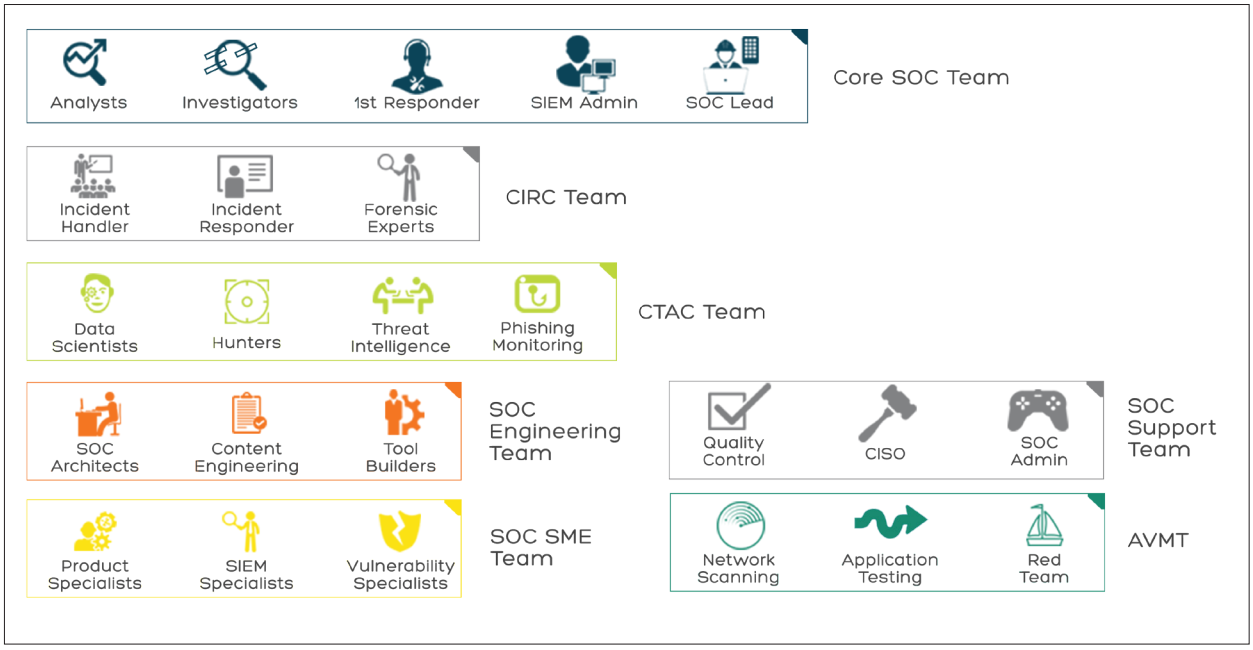
High Human Touch, High-Performance Systems

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. The managed detection

and 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.

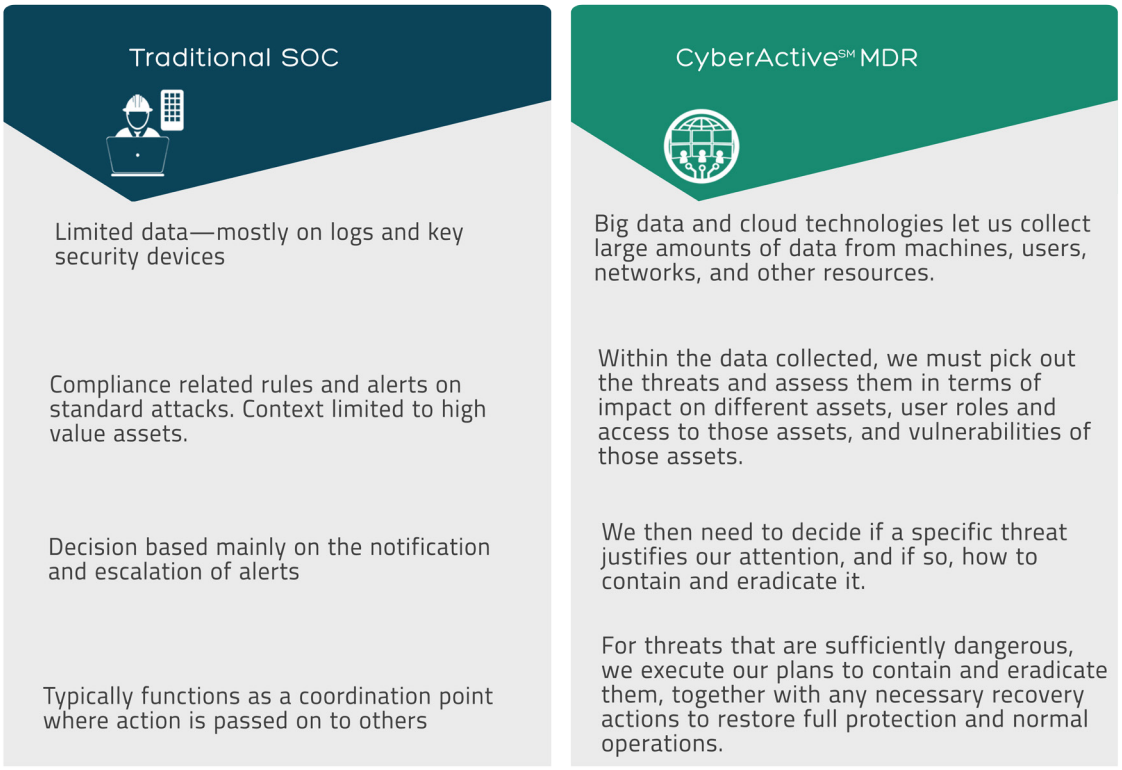
Figure 4: SOC staff build on the MDR model



Source: Paladion

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



Source: Paladion

Source: Paladion

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

Additional Reading:

Whitepaper

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

E-Book

Taking Your SIEM to the Next Level with Managed Detection and Response

E-Book

How to Build an Adaptive, Future Ready Security Operations Center

Whitepaper

Upgrade your SOC with Security Analytics and Orchestration

Whitepaper

Use Cases for Security Analytics

Source: Paladion

Research from Gartner:

Market Guide for Managed Detection and Response Services

Managed detection and response improves threat detection monitoring and incident response capabilities via a turnkey approach to detecting threats that have bypassed other controls. Security and risk management leaders need to understand this service and its implications for their environments.

Key Findings

- Organizations are looking to improve real-time threat detection and incident response capabilities; however, they often struggle to invest limited resources in the required people, processes and technology.
- The managed detection and response service market is evolving, and vendors take varied approaches to delivering their services, making it challenging for buyers to compare providers.
- MDR vendors target two primary groups of buyers: (1) small or midsize businesses and small enterprises with minimal investments in security tools/staff; (2) well-invested enterprises that are investing in people and tools, but are looking for partners to augment their capabilities.
- MDR providers are adding the ability to contain threats to existing remote incident response capabilities, primarily driven by SMB organizations that lack security teams and 24/7 IT.

- The overlap between managed security services and MDR is increasing, which is adding to the confusion in the market and making it difficult for buyers. MSS and MDR still have distinct characteristics that buyers need to understand.

Recommendations

IT security and risk management leaders involved with security monitoring and operations should:

- Use MDR services to implement threat detection and incident response capabilities when they don't exist or are immature, or when approaches such as MSS haven't met expectations.

- Use MDR services when a turnkey service is the goal, and decisions on technologies, expertise and processes are left to the provider. Scrutinize how potential vendors are delivering services to ensure the technology stack will fit the IT environment — e.g., SaaS and infrastructure as a service coverage.

- Evaluate providers offering MDR-type services that can improve their incident response capabilities now or in the future, when requirements point toward using an MSS provider over an MDR service provider.

Strategic Planning Assumptions

By 2020, 15% of organizations (see Note 1) will be using services such as MDR, which is an increase from fewer than 1% today.

By 2020, 80% of worldwide managed security service providers (MSSPs) will offer MDR-type services.

Market Definition

Managed detection and response (MDR) providers deliver services for buyers looking to improve their threat detection, incident response and continuous-monitoring capabilities. These services are delivered by providers using approaches that do not fit the traditional managed security service (MSS) model. Security event monitoring in many organizations is focused on internet and network perimeter, ingress-egress traffic only, rather than lateral (east-west) movement, once an attacker is inside the organization. MDR providers' services leverage two or more of the five styles of advanced threat defense, along with security analytics, which can be expensive, difficult to obtain and hard to sustain for many organizations, especially small or midsize businesses (SMBs) and small enterprises.

MDR services are characterized by the following attributes:

- A focus on threat-detection-only use cases, especially attacks that have bypassed preventative security controls. Compliance use cases are not a focus, and are not usually addressed.

- The delivery of services using the provider's curated technology stack, deployed on a customer's premises, which may include one or more tools, usually focused on network- and host-based solutions:

    - These vendor-provided tools are not only positioned at internet gateways, but are inward-facing to detect threats missed by traditional perimeter security technologies.

    - These tools are managed and monitored by the provider.

- The types of tools and detection methods used by the providers vary in the use of logs, network flows and network traffic (e.g., full packet capture), endpoint activity through the use of endpoint detection and response-type tools and deception technologies. Some vendors rely solely on network security monitoring; others rely on endpoint agents only and many leverage a combination of these technologies in their "stack."

- Few MDR providers rely solely on logs generated by a customer's security tools to monitor and detect threats. They require some component of their technology stack to deliver the service to curate the type of logs fed into their analytics platform.

- Security event management and analysis technology that commonly uses threat intelligence and advanced data analytics is at the core of these services. The data management and analytic platforms are fed events from the vendor's technology stack (and, in some cases, customer-owned technologies as well). MDR providers increasingly emphasize the need to curate the data required to ensure that incidents are detected with higher fidelity, and, more importantly, that the right type of event and contextual data is available to the provider's analysts. This is visible to the customer as richer information and targeted, action-oriented advice, when alerted to a potential security incident.

- 24/7 monitoring, analysis and customer alerting of security events with incident triage performed by a person (e.g., not relying just on automation to add some context to an event). There tends to be more direct communication with security operations center (SOC) analysts and less emphasis on using a portal for alerting, investigation, case management and workflow activities.

- Incident validation and remote response services, which may include one or more actions, such as identifying indicators of compromise (IOCs), sandboxing and reverse engineering malware, and consulting on containment and remediation are included in the service, without the need for an incident-response-specific retainer or agreement. Retainers are reserved for significant circumstances and may be performed remotely (if feasible and time-critical) or via on-site breach response services.

- Assistance with remediation actions in bringing the environment back to some form of "known good" is sometimes included or may be available as an additional service. During the past year, containment of a threat has become visible in the offerings from several providers (and is addressed in more detail in the Market Direction section).

Market Direction

MDR is still an emerging market, as Gartner observes new entrants coming into the market (and anticipates additional provides entering the market during the next several years), combined with significant variability across the providers' approaches. MDR services can take a variety of forms, and we continue to see new approaches being introduced. With the introduction of the concept of MDR services, the number of providers that offer services that align to the MDR market definition, rather than the definition of an MSSP (see Table 1), has become more visible during the past 12 months. Several of these MSSPs leaned more toward MDR, while providing only a few elements associated with MSSs. Increasingly, MSSPs, both global and regional, have added MDR-type services to their portfolios.

Table 1: Differences Between MDR and MSS

Characteristic	MDR	MSS
Security event log and context sources	Proprietary technology stack provided by the provider and deployed at the customer's premises, which is included in the service price	Event-source-agnostic. Data sent to the provider is determined by the customer.
Remote device management	Only for their own technology stacks	Yes. Vendor-agnostic for most common security controls — e.g., firewalls, intrusion detection systems (IDSs), intrusion prevention systems (IPSs) or web gateways — or tools deployed with MDR-type services.
Compliance reporting	Very rarely	Yes
Interface to service	Rely on more-direct communication (voice, email) to analysts, rather than portals.	Portal and email acts as the primary interface, with secondary access to analysts provided via chat functions and phone.
Incident response support	Lightweight, remote, incident response support typically included in basic services. On-site incident response provided by retainer.	Both remote and on-site provided by a separate retainer.
Incident containment	Provided using provided technology stack or customer-owned technologies, leveraging scripts and APIs to programmatically make changes.	When remote, full management of security controls is managed for a customer and MDR-type services are offered — e.g., managed endpoint detection and response (EDR).
Provide service-level agreements (SLA) for incident detection and response	Rarely	Yes
Source: Gartner (May 2017)		

Demand from the SMB and small-enterprise space has been particularly strong, as MDR services hit a "sweet spot" with these organizations, due to their lack of investment in threat detection capabilities. Within the SMB and small-enterprise buyer space, we see some MDR vendors specifically focusing on the small business and smaller midsize organizations (e.g., up to 300 employees) with small IT teams and minimal investment in security. Other providers are targeting organizations from 500 to 2,000 employees that have some security controls and, possibly, a couple of full-time security analysts.

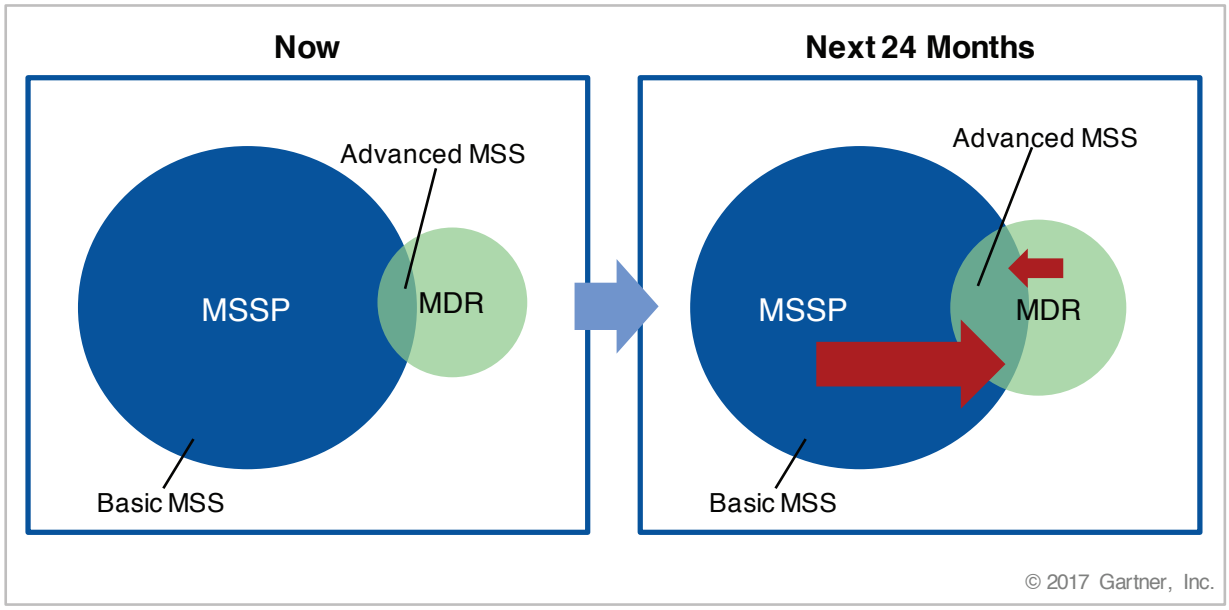
As anticipated, during the past 12 months, we are seeing buyers demand even more incident response capabilities from the providers, which are becoming visible in the market as "incident containment" capabilities. The SMB and small-enterprise buyers have been driving demand more than enterprise customers. This is expected, as larger enterprises generally have made the investments in security teams that are resourced to perform their own incident validation and coordinate response activities. Larger enterprises tend to be staffed 24/7 and to have more segmented IT responsibilities. Allowing a third party to make changes to security technologies on their behalf may conflict with IT culture, risk tolerance for changes being made that could affect business operations, or even policies and procedures in heavily regulated environments that prevent ad hoc changes from being made. SMB organizations tend to have fewer of these concerns and are more risk-tolerant (e.g., the risk of a business impact from a bad firewall change versus ransomware encrypting critical data).

Containment can take various forms, and there is not one dominant approach in the market. Example containment methods include programmatically changing firewall rules via APIs to block an IP address, isolating a process or a host from the network using an endpoint agent, locking user accounts in Active Directory, integrating with a customer's network access control (NAC) tool, and blocking network activity via DNS requests and TCP resets.

MSSPs are accelerating toward MDR, while MDR service providers are slowly adding more MSSP-type capabilities (see Figure 1). MSSPs have begun to enter the MDR market with offerings that supplement their existing services. These offerings tend to be purchased by buyers who have specific MSS requirements that cannot be met by MDR providers (e.g., device management, vulnerability management, compliance reporting) and want more "advanced threat detection," along with traditional MSSs. Accordingly, Gartner has updated the associated Strategic Planning Assumption, based on what has been observed in the market. We believe that 80% of all global MSSPs will have an MDR-type service offering by 2020.

The overlap between most MSSPs and MDR providers is still limited to a couple of services — e.g., managed EDR and threat hunting. Clients should be wary of claims from traditional MSSPs on their ability to deliver MDR-like services. Delivering these services requires technologies not traditionally in scope for MSS, such as endpoint threat detection and response, network behavior analysis and network forensic tools. Those exploring MSSPs for these services should assess the MSSPs' expertise in running the technologies, using them to effectively identify and respond to breaches. They need to understand how MSSP incident response services that may provide some of these capabilities are integrated.

Figure 1: MDR Service Providers in Relation to MSSPs



Source: Gartner (May 2017)

Many MSSPs won't be viewed as competition against MDR services. Leading MSSPs will close the gap, but many won't, and those that try it may require a couple of years. Operating inside the network and doing response work is not the "traditional" mode of operation for most MSSPs. Thus, SOC staff skills and processes will need to be updated to bridge this gap. The difference between MSSPs and leading MDR providers is expected to continue to favor MDR-specific players for at least another five years, or perhaps longer.

Market Analysis

When Gartner defined MDR services in 2016, there was an expectation that the market was broader than what was visible on the surface. This turned out to be true (See the Representative Vendors section).

Three elements of the MDR market best define its current state:

- It is a dynamic market that is witnessing new vendors entering and trying to differentiate themselves against existing vendors, who themselves are adjusting their branding and offerings.
- Although the promised outcomes are usually the same (e.g., detect threats), the methods to deliver the service to customers, the level of incident response services provided and the target customers vary.

- There is some overlap with MSSPs, with an expectation that the MSSPs will react to these new MDR services providers by adjusting their offerings and adding new ones to compete.

MDR providers generally target two types of buyers:

- Those with minimal investments in security-monitoring expertise and tools

- Well-invested buyers that have reached a specific level of maturity, or have started investing, in people and tools, but are looking for a provider to augment current capabilities (e.g., fill a gap, while an internal SOC is being implemented)

The latter group is looking to provide a "second set of eyes" on internal security monitoring services, and to augment existing internal capabilities focused on detecting advanced threats against an organization.

The technology stacks employed by the MDR providers continue to evolve. The two primary approaches used — network and endpoint agent — remain the most common, but we continue to see more-comprehensive technology stacks that cover the gamut of the monitoring options being deployed. Providers that were oriented toward a single approach (e.g., internet ingress/egress network traffic monitoring only, or identified improvements in their technology stacks) have begun plugging those gaps:

- EDR agents are a common technology — especially those offering active response capabilities. Most providers are aligned with a single EDR vendor (especially if it's their own technology), but we increasingly see MDR providers adopt several providers, adjusting to customer demand.

- Increasingly network-monitoring capabilities using on-premises deployed sensors (physical or virtual) that already perform signature-based detections, full packet capture and deep packet inspection, are being extended to include other vectors, such as DNS traffic and netflow data.

- Email monitoring is slowly being incorporated to move monitoring up the cyber kill chain — e.g., to the delivery phase, rather than focusing solely on the command and control (C2) phase.

- Deception technologies are being offered by a few vendors to address such challenges as accelerating service implementation and concerns about deploying EDR agents onto endpoints in challenging geographies, such as Europe (due to privacy and user-monitoring concerns).

Another critical component observed with MDR services is reliance on advanced analytics in log analysis platforms. MDR providers have entered this market with the ability to leverage commodity big data analytics platforms, such as Hadoop, Elastic and NoSQL, along with a growing pool of data science talent. There are also many options available on the market for curated threat intelligence that can be purchased from third parties, if the intelligence is not generated in-house. This big data analytics approach takes the curated data out of the provider's technology stack and enables them to do more-precise, real-time threat detection, using advanced analytics (e.g., machine learning), supported by higher-fidelity threat intelligence.

The ability to collect large volumes of data also helps the MDR providers' incident investigation and response activities. Investment in log and data capture and analysis capabilities enables MDR

providers to invest in smaller teams of experienced analysts focused on incident investigation and response. It also allows many vendors to perform automated and manual threat hunting through their customers' logs and data, looking for IOCs.

However, some MDR providers have not invested in these analytic platforms and may leverage commercial, off-the-shelf systems, including traditional security information and event management (SIEM) solutions. This does not necessarily imply that a lack of advanced analytics and machine learning is an impediment to doing more-precise threat detection; however, buyers should ask potential vendors how they perform analytics, what tools and methods they employ, and how they differentiate their services from those of their competitors.

"Response" is the key element of the MDR. Many MSSPs offer basic detection and alerting services, and the customer's security team (which needs to have adequate resources) is responsible for providing additional incident, analysis and associated response activities. Gartner clients want more-comprehensive services than are typically provided by many MSSPs — customers often receive an alert of a suspected incident that has minimal information, and are then left to fend for themselves using the MSSP's portal capabilities. MDR services include varying degrees of "lightweight," remote incident response services as part of the core services. MDR providers favor dedicated incident response experts to man their SOCs, who validate potential incidents, assemble the appropriate context, investigate as much as is feasible about the scope and severity given the information and tools available, and make recommendations, so the customer can quickly start containment and remediation activities (if not done by the MDR provider).

MDR service providers, by virtue of their delivery approach (e.g., using their own technology stacks and machine-learning-driven analytic platforms) do not have to adapt to the technologies or data sources deployed by the customer. However, this often means customers have little input on refining the detection methods used by the MDR providers. For many customers, this is acceptable, because they want to rely on the provider's expertise to detect threats.

Gartner has seen pricing models that are based solely on the size of an organization, which is a common approach. However, there are also models that are based on a variety of factors, usually related to the technology stack employed, such as a combination of organization size, number of network appliances and EDR agents required. Some providers are more closely aligned with some MSSP pricing models, based on the volume or velocity of events generated and forwarded for analysis. Finally, some providers are employing approaches based on the number of incidents generated by a customer.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

- Alert Logic
- Arctic Wolf Networks
- Cisco
- CrowdStrike
- CSIS
- Cybereason

- Cynet Systems
- Datashield
- eSentire
- F-Secure
- FireEye
- Ingalls Information Security
- IronNet Cybersecurity
- K2 Intelligence
- Kudelski Security
- Mnemonic
- MWR InfoSecurity
- Morphick
- NCC Group
- Netswitch
- NetWatcher
- Paladion
- Proficio
- Rapid7
- Raytheon Foreground Security
- Red Canary
- Rook Security
- SecureLink
- UnitedLex
- Vigilant

Market Recommendations

- MDR buyers should tread carefully. The MDR services market is still new, in comparison with MSS. It lacks broad visibility with end-user buyers and does not yet have the battle scars other security monitoring approaches (e.g., SIEMs and MSSs) have collected as part of the assessment, use and validation by customers.

- Do not assume that all MDR vendors are the same. Choose a vendor that is oriented toward your organization's size, security maturity level, specific requirements, and existing threat detection and response capabilities. There is sufficient variability across offerings, delivery models, vertical expertise and pricing that can make direct comparisons challenging. Having a strong set of requirements at the beginning will ease the analysis and selection process.

- SMB and enterprise buyers should evaluate providers based on security technologies deployed and expertise in your organization, looking for those vendors who best meet requirements, while filling the gaps in tools and expertise coverage.

- Organizations that have not yet invested in detection and response technologies and internal capabilities should focus on MDR providers with comprehensive technology stacks that cover real-time threat detection and historic/forensic capabilities across networks and hosts.

- Enterprises considering implementing an SOC should not go it alone. Look to an MDR service provider as a partner that can augment your SOC as it is being implemented and matured. This allows you to quickly implement mature threat detection and response capabilities, rather than having to build from scratch. This can mean an SOC is operating at a greater maturity level in several months, rather than several years.

- Use proofs of concept to your advantage to validate claims and fit for purpose with your organization's requirements. Most MDR providers lack the vetting and decades of competition that MSSPs have faced. Therefore, there is an increased burden on the customer to perform sufficient due diligence on the MDR providers before signing a contract.

- If you have data residency and strong privacy or other compliance requirements, validate that the MDR providers can comply with them. For example, by operating within your geographic region or those using a data collection architecture in which your data remains on-premises and only metadata or event data is sent back to a central SOC, and by leveraging deception technologies, rather than deploying EDR agents across an organization.

Note 1. Organization Size Definitions

Gartner defines an enterprise business as one with more than 1,000 employees and more than $1 billion in annual revenue. Gartner defines a midsize business as "[a] business that, due to its size, has different IT requirements — and often faces different IT challenges — than do large enterprises, and whose IT resources (usually budget and staff) are often highly constrained." Midsize enterprises have 100 to 999 employees, with $50 million to $1 billion in annual revenue.

Source: Gartner Research Note G00308991, Toby Bussa, Craig Lawson, Kelly M. Kavanagh, Sid Deshpande, 31 May 2017

About Paladion

PALADION
HIGH SPEED CYBER DEFENSE

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 semi-autonomous cyber platform and managed services with leading security technologies. Paladion is consistently rated and recognized by 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 six cyber operations centers placed across the globe. It houses 900+ cyber security professionals including security researchers, threat hunters, ethical hackers, incident responders, solution architects, consultants and more. Paladion is also actively involved in several information security research forums such as OWASP, and has authored several books on security monitoring, application security, and more.

For more information, please visit www.paladion.net