IDC MarketScape

IDC MarketScape: Middle East Managed Detection and Response 2025 Vendor Assessment

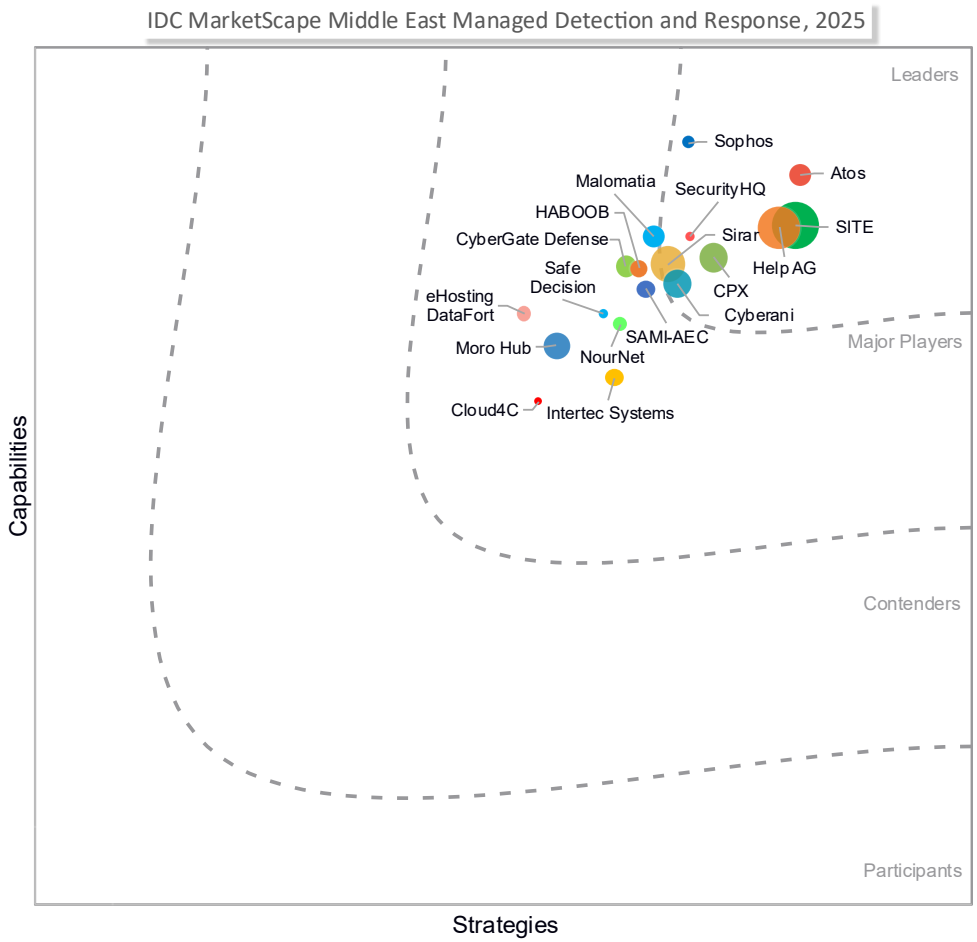
Shilpi Handa Shahin Hashim Yesim Arac Ozturk

This Excerpt is for Help AG

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Middle East Managed Detection and Response Vendor Assessment



Source: IDC, 2025

October 2025, IDC #META53011825

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

IDC OPINION

The Middle East managed detection and response (MDR) market experienced profound transformations in 2025, driven by regulatory developments, technological advancement, and the growing sovereign technology imperative. This year marked a pivotal shift in how organizations approach MDR services, with new licensing frameworks, AI-powered capabilities, and sovereign-focused strategies reshaping the cybersecurity landscape.

Regulatory Landscape Changes

Saudi Arabia's National Cybersecurity Authority (NCA) introduced a groundbreaking tiered licensing model for managed security operations center (SOC) services that fundamentally altered the managed security service provider landscape. The two-tier system requires all organizations providing SOC services to obtain proper licensing, with Tier 1 licenses mandating a minimum capital of SAR 50 million for providers serving government entities and critical national infrastructure. This regulatory framework emphasizes data localization, with all physical facilities, staff, and data required to remain within Saudi Arabia.

The licensing system also introduced mandatory certification requirements for SOC analysts, creating new pathways for talent development while ensuring service quality standards. This approach aimed to leapfrog national cybersecurity maturity while driving ecosystem development through a broader, regulated market for managed SOC services.

The UAE Cybersecurity Council unveiled significant policy developments in 2025, announcing three new cybersecurity policies focusing on cloud computing and data security, Internet of Things (IoT) security, and cybersecurity operations centers. The Dubai Electronic Security Center (DESC) launched innovative projects including zero trust guidelines for government networks and the advanced "Ethaq Plus" platform for safeguarding digital transactions.

AI and Large Language Model Integration by Managed Security Service Providers

Managed security service providers (SPs) across the Middle East have significantly leveraged large language models (LLMs) in 2025, with most building proprietary AI solutions for threat detection, customer portals, threat hunting, and SOC operations.

AI-powered managed security SPs now use real-time data and machine learning to continuously learn and evolve, recognizing patterns and detecting anomalies with unprecedented accuracy. Behavioral analytics has become a key capability, enabling systems to learn normal behavior patterns for users, devices, and applications, and then detect suspicious activity early.

Automated Threat Hunting and Response

The integration of AI-driven threat hunting has transformed how managed security SPs approach proactive security. LLMs are now being used to accelerate threat hunting workflows, with some implementations reducing the initial classification time of security events by up to 99%. These systems leverage threat intelligence, behavioral analytics, and machine learning to identify advanced, stealthy threats that may evade traditional security controls.

Modern managed security SPs are implementing AI-powered chatbots and conversational interfaces that serve as command centers for security operations, enabling analysts to trigger automated workflows, fetch context, and coordinate responses without leaving their communication platforms. This ChatOps approach has significantly improved response times and collaboration across security teams.

Sovereign Technology Focus

There has been an unprecedented focus on digital sovereignty among Middle East organizations in 2025, with most companies emphasizing the localization of talent, resources, and infrastructure. This sovereign focus extends beyond data residency to encompass complete control over AI systems, deciding where data is stored, how it is processed, and which technologies are used without dependency on foreign vendors or infrastructure. A notable development in 2025 was the emergence of managed security SPs moving toward actual technical sovereignty by launching their own extended detection and response (XDR) products.

Evolution Beyond Traditional Monitoring

In 2025, Middle East managed security SPs have evolved far beyond basic threat monitoring to provide comprehensive, AI-powered security ecosystems. The essential capabilities now include:

- **Advanced Automation and Orchestration:** The integration of security orchestration, automation, and response (SOAR) platforms enables efficient threat response at scale, with automated quarantine, isolation, and remediation workflows. Digital forensics and incident response (DFIR) capabilities provide call-off remote or deployable staff for deep dive incident analysis.
- **Sovereign-Focused AI Chatbots:** AI-powered chatbots have become central to the delivery of managed security services, providing 24 x 7 availability, centralized security conversations, and improved visibility across security operations. These systems operate around the clock, instantly notifying team members and executing predefined playbooks for efficient threat mitigation.
- **Enhanced Analytics and Threat Intelligence:** Middle East MDR solutions leverage integrated data lakes, consolidating diverse data sources to create comprehensive security views. Telemetry coverage now extends to identity and email collaboration tools, IoT and operational technology (OT) device monitoring, and cloud services.

- **Compliance and Regulatory Expertise:** Given the evolving regulatory landscape, MDR providers must demonstrate expertise in navigating compliance requirements, including knowledge of NCA and Saudi Arabian Monetary Authority (SAMA) regulations in Saudi Arabia and Information Security Regulation (ISR) frameworks in the UAE.
- **Comprehensive Security Portals:** Managed security SPs provide intuitive, comprehensive customer portals offering real-time visibility into organizational security postures. Key features must include detailed threat mapping to visualize attack vectors and affected assets, dashboards providing threat intelligence overviews, incident alerts, and investigation status updates. The integration of AI-powered interfaces has transformed how organizations interact with managed security SPs. Conversational AI systems now interpret text commands, fetch context from threat intelligence, and trigger remediation instantly while keeping all stakeholders informed. This approach eliminates console-hopping and manual lookups, significantly improving operational efficiency.

The Middle East MDR market's evolution in 2025 represents a fundamental shift toward sovereign, AI-powered, and highly automated cybersecurity services. With regulatory frameworks driving market maturation, technological sovereignty requirements reshaping service delivery, and AI capabilities enabling unprecedented threat detection and response speeds, the region has positioned itself at the forefront of global cybersecurity innovation. Organizations that embrace these transformations while addressing talent development and regulatory compliance will be best positioned to navigate the evolving cyberthreat landscape.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

To be included in this 2025 IDC MarketScape for Middle East MDR services, providers had to meet the following criteria:

- **Portfolio of MDR Services:** The security service provider must offer managed services for threat detection and response. These could include any or all of the following:
  - Pure-play MDR/managed extended detection and response (MXDR)
  - Managed endpoint detection and response (EDR)
  - Managed threat hunting
  - Managed security information and event management (SIEM)
- **Revenue:** The provider's worldwide MDR revenue must have been AED/SAR 5 million or above for the year 2024.
- **Middle East Footprint:** The MDR service provider must have at least one MDR platform hosted in the Middle East region.

ADVICE FOR TECHNOLOGY BUYERS

Organizations evaluating MDR services should focus on the following key decision factors when selecting a service provider:

- **Security Model and Provider Scope:** Decide between sovereign managed security SPs (data residency, local compliance) and Middle East scale providers (broader regional coverage).
- **AI Strategy Alignment:** Choose between vendors with high levels of AI adoption for ML-driven detection and automated response or traditional vendors that rely on rule-based methods.
- **Core MDR Capabilities:** Ensure 24 x 7 threat detection, remote response, indicator of compromise (IoC)-based hunts, and customizable playbooks. Look for AI-enhanced anomaly detection, behavioral analytics, and real-time correlation across endpoint, network, identity, cloud, IoT, and OT telemetry.
- **Threat Intelligence and Reporting:** Select providers with robust threat-research capabilities and clear, business-aligned reporting.
- **Response and Remediation:** Confirm the ability to identify and contain threats; plan internal processes for full remediation. Consider add-on incident response retainers.
- **Customer Portal and Generative AI (GenAI):** Prioritize interactive portals with customizable dashboards, audit reports, and GenAI query features.
- **Compliance and Sovereignty:** Verify data residency support, privacy controls, and separate log retention for regulatory compliance.

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and opportunities.

Help AG

Help AG is positioned in the Leaders category of this 2025 IDC MarketScape for Middle East managed detection and response services.

Help AG, the cybersecurity arm of e&, is a provider of advanced cybersecurity services. HelpAG has been providing cybersecurity services in the region for more than two decades now. It operates SOCs across the Middle East and works with both private and government organizations across multiple sectors. The company's focus is on ensuring data sovereignty and meeting regulatory compliance requirements in the region. Headquartered in Dubai, with offices in Abu Dhabi, Riyadh, and Cairo,

Help AG delivers 24 x 7 x 365 managed security services through a team of 280+ cybersecurity experts operating a federated SOC model for regional coverage.

The company's MDR service combines automation, AI, and threat intelligence. At its core, its MDR service is powered by a centralized SOAR layer, complemented by client-specific SIEM deployments for visibility, control, and real-time threat monitoring.

The proprietary "Unicorn" platform is leveraged for the deployment of threat detection content. Automation spans the full detect-to-respond cycle — with Level 1 (L1) fully automated, Level 2 (L2) partially automated, and AI-driven incident summarization accelerating analyst decisions. Response automation as a service (RaaS) further enables centralized incident response across a wide range of customer assets, with the flexibility to integrate through APIs and custom connectors.

Help AG has developed proprietary AI/ML models for incident summarization, alert prioritization, threat advisory creation, and IoC extraction, as well as a compliance engine for log normalization. Data sovereignty and regulatory compliance are core strengths of Help AG's service model. All platforms and client data remain within the country of operation, and services are delivered by locally based teams familiar with regulations such as National Cybersecurity Authority (NCA), Saudi Arabian Monetary Authority (SAMA), Information Security Regulation (ISR), and Unified Information Access (UIA). The SOCs are certified to ISO27001, ISO22301, and ISO20000 standards, and Help AG's SOC operations have achieved SOC-CMM Level 3 maturity. Continuous workforce development is a priority, with analysts trained annually and 800+ active certifications maintained across the team.

Threat intelligence is offered both as a standalone service and fully integrated with MDR. Help AG's Cyber Threat Intelligence (CTI) team follows a structured life cycle of planning, collection, processing, and dissemination. Automated IoC-driven threat hunting is included by default, while tactics, techniques, and procedure (TTP)-based hypothesis threat hunts are offered as an add-on service. The proprietary Threat Intelligence Platform (TIP) ingests open, closed, and internally sourced feeds, including DFIR data, providing context-rich intelligence outputs. AI is increasingly being leveraged to enhance threat advisory generation and automate hypothesis development.

Analytics capabilities are built on trusted, industry-leading vendor platforms and enhanced with proprietary and third-party AI/ML models. These systems support functions such as incident summarization, anomaly detection, and behavioral analytics. Future development focuses on distributed ML for detection, generative AI for detection portability, and predictive analytics for proactive defense.

Beyond MDR, Help AG provides a broad portfolio of managed security services. These include cloud workload protection, secure access service edge (SASE)/security service edge (SSE), network and email security, endpoint protection, vulnerability management, identity and access management, application security, web

application and API protection (WAAP), distributed denial-of-service (DDoS) protection, public key infrastructure (PKI) services, and digital risk protection. Its consulting practice includes more than 150 specialists in compliance, risk, architecture, incident response, penetration testing, and emerging areas such as quantum-safe encryption and cyber-risk quantification. DFIR services are fully in-house, CREST and DESC certified, and delivered through flexible retainer models.

Client engagement is supported by a cloud-hosted service portal that provides real-time updates, dashboards, ticketing integration, executive reporting, and visualization features such as MITRE ATT&CK mapping.

Help AG's commercial model is based on value- and outcome-driven pricing, adjusted to factors like data volume, deployment type, service scope, and SLAs. The company maintains high customer retention rates and strong satisfaction scores, supported by dedicated service delivery managers and a verticalized go-to-market alignment with e&'s broader sales strategy.

Help AG operates primarily in the UAE, Saudi Arabia, and Egypt, with a strong presence across customer environments in Türkiye, India, Australia, APAC, and parts of Central and Eastern Europe. The company plans to expand its operations into Qatar, Morocco, South Africa, and additional European markets. Through its collaboration with Vodafone International, Help AG extends its reach to multinational clients across the Middle East, Africa, and APAC regions.

Strengths

Help AG has built extensive automation capabilities, with routine SOC workflows fully automated and proprietary AI/ML models enhancing incident analysis, alert prioritization, and content generation. Its SOC operations are certified to SOC-CMM Level 3 and multiple ISO standards. The company's service is deeply rooted in data sovereignty and regulatory alignment, delivered through locally based cybersecurity experts who understand and operate within regional frameworks such as NCA, SAMA, ISR, and UIA.

Help AG boasts strong customer satisfaction and retention levels. Critical incidents are resolved quickly, meeting or exceeding response time commitments. Ongoing investment in research, innovation, and AI-based service development, supported by e&'s data science expertise, helps Help AG sustain its position in regional cybersecurity and service quality.

Challenges

Help AG has established its presence in the UAE and is scaling its presence in Saudi Arabia, yet there is an opportunity to further replicate its success in other regional markets. Building on its progress with proprietary AI-driven platforms, Help AG's opportunity lies in evolving these innovations into wider cybersecurity frameworks.

Continued investment in scaling proprietary solutions like Unicorn, as well as maintaining interoperability with evolving third-party technologies, will support service consistency and innovation. Maintaining and growing specialized talent, particularly in AI and advanced threat analysis, will remain critical as the footprint expands.

Consider Help AG When

Help AG is well suited for medium-sized and large enterprises and private and government organizations in the Middle East that require comprehensive MDR services, strong regulatory compliance, and local data residency. Its mature automation platform and proprietary AI/ML tools deliver operational efficiency for organizations seeking advanced security without building internal capabilities. Help AG's expertise in managing multi-technology environments and partnerships with vendors enables unified security operations across diverse stacks. The company's SOC-CMM Level 3 certification and regulatory experience make it a strong choice for regulated industries needing high-fidelity threat detection and compliance reporting. With scalable, cloud-native security services and a proven record of reliable, 24 x 7 x 365 operations, Help AG supports organizations undergoing digital transformation and cybersecurity modernization.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis (or strategies axis) indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

Managed detection and response (MDR), as a subset of managed security services (MSS), combines the tools, technologies, procedures, and methodologies used to provide full cybersecurity detection and response capabilities for an organization. Service providers can deploy MDR services utilizing a mixture of customers' existing capabilities and partner-supplied tools or services and private intellectual property. MDR services are typically supplied by a provider's well-trained cybersecurity staff working in one or more 24 x 7 x 365 remote SOCs.

Strategies and Capabilities Criteria

This section includes an introduction to market-specific weighting definitions and weighting values (see Tables 1 and 2).

TABLE 1

Key Strategy Measures for Success: Middle East Managed Detection and Response

Strategies Criteria	Definitions	Weight (%)
Cost normalization strategy	▪ The vendor's strategy to normalize service delivery costs with standardization, service tiering, and automation.	5
Customer portal strategy	▪ The vendor's road map to improve the capabilities of its customer portal.	8
Functionality or offering strategy	▪ The vendor's investment in growing the size of its security team, expanding geographically, and acquiring SOC certifications. Own IP gets a higher score — very high focus on technical sovereignty this year. ▪ Future investments and partnerships aimed at enhancing/adding to the capabilities of the MDR service across security domains. Vendors that have a road map for enhancements across endpoint, network, cloud, identity, and other threat detection and response score	28

TABLE 1

Key Strategy Measures for Success: Middle East Managed Detection and Response

Strategies Criteria	Definitions	Weight (%)
	higher. Investments in R&D for risk-based security operations, improved service delivery, and support for newer threat vectors (e.g., AI model threats, synthetic identities). ▪ Future investments for curation, normalization. and administration of threat intelligence to enhance the value of MDR service to clients. ▪ R&D investment and service enhancement road map — IP, mergers, acquisitions, investments.	
Future outlook	▪ The vendor's strategy to grow revenue and number of customers.	6
Go-to-market strategy	▪ The vendor's investments and efforts in improving market messaging, increasing outreach, and building awareness for the brand through regional campaigns, targeted marketing, or digital channels. The vendor's investment in improving sales across segments, region, and industries. ▪ The vendor's strategy to drive channel engagement and growth. Strategy to add new managed SP/managed security SP partners or service resellers. ▪ New initiatives to drive customer engagement at an operational, as well as executive, level.	14
Growth	▪ Future investments in threat hunting capabilities and automation. Other strategies like tiering the vendor's threat hunting offering to further solidify the MDR service in the future.	7
Innovation	▪ Future investments in security analytics and AI/ML to improve detection fidelity, investigation, and overall risk reduction for MDR customers.	9
R&D pace/productivity	▪ The vendor's initiatives to reduce time to value	4
Range of services strategy	▪ The vendor's road map to grow its portfolio of managed and professional security services.	6
Security outcomes strategy	▪ SLA improvement road map and other metrics for service improvement,	5
Talent management strategy	▪ The vendor's initiatives to improve/maintain the quality of security talent. ▪ The vendor's initiatives to attract and retain niche security talent.	8
Total		100

Source: IDC, 2025

TABLE 2

Key Capability Measures for Success: Middle East Managed Detection and Response

Capabilities Criteria	Definitions	Weight (%)
Customer portal	▪ The vendor offers its customers a service portal that is easy to use, has an intuitive UI, and organizes information well for different personas. Includes AI-driven chatbots offering 24 x 7 personalized support, adaptive dashboards tailored for different user personas, self-service analytics powered by natural language queries, and contextual resource recommendations based on user roles and signal patterns. Advanced portals may also feature multilingual support, built-in gamified learning paths, and seamless authentication with predictive security and privacy controls, continuously evolving the UI based on behavioral analytics for optimal ease of use. ▪ Pre-defined reporting capabilities, persona-based reporting, and customizable reporting options. Operational, executive, and compliance reporting capabilities. AI-powered report generation that adapts to operational, executive, and compliance needs with persona-based dashboards automatically offering different levels of insights. Predefined, role-tailored templates, drag-and-drop custom report builders and natural language queries for non-technical users to explore data with ease. Automated regulatory mapping, and scheduled, context-aware summaries.	8
Customer satisfaction	▪ Relationship management and initiatives to drive customer delight. IDC's independent *CXO Survey* will be leveraged.	5
Customer service delivery	▪ The vendor has a demonstrated ability to ease and accelerate the onboarding of new clients to reduce time to value. Usage of AI, rapid onboarding, and using AI to automate migration of data, configuration, and alert rules for new clients. Unique features that boost time to value include guided setup wizards, instant integration with third-party tools, automated detection tuning, and AI-driven recommendations for configuration and response workflows. Personalized dashboard creation and real-time feedback on deployment effectiveness.	4
Customer service offering	▪ Breadth and depth of telemetry sources across endpoint, network, cloud, identity, email, SIEM, and others. Coverage of cloud and OT environments. The vendor has demonstrated a capability to consume these telemetry sources for third-party providers. The vendor has also demonstrated an ability to create custom detection rules and not just rely on out-of-the-box detection capabilities of the security solution. Custom logs from web applications, business-specific APIs, proprietary systems, or OT/ IoT devices. ▪ The vendor has demonstrated response capabilities across security domains (endpoint, network, identity, etc.). AI usage to be an important criteria.	14
Functionality or offering	▪ The vendor has demonstrated that it has essential capabilities to service clients in the Middle East. Essential capabilities include the size of security team, geographical coverage, and number of SOCs,	24

TABLE 2

Key Capability Measures for Success: Middle East Managed Detection and Response

Capabilities Criteria	Definitions	Weight (%)
	plus their spread around the region and their certifications. The ability of the vendor to handle data sovereignty concerns of clients is also considered to be an essential capability. Number of SOCs, size of team at each SOC, threat hunters, and incident response (IR) team size. The technology being leveraged. The level of integration available in platform. The automation rate. Net promoter scores where available. IDC benchmarking of capabilities across Middle East providers. ▪ The vendor has demonstrated extensive capabilities for proactive and reactive threat hunting within the MDR offering. Usage of AI. Big team for advanced human expertise, data analytics platform, data lake for deep analytics powered by vast data, and up-to-date threat intelligence. The vendor automates collection and analysis from deep and dark web sources for early threat warnings, uses behavioral AI to counter advanced attacks with instant rollback and deep forensics, seamlessly integrates data from diverse security tools for unified detection, prioritizes threats based on specific organizational assets, and delivers proactive, real-time intelligence and automated incident response for fast, compliant action. ▪ The vendor has a demonstrated ability to aggregate, curate, normalize, and enrich threat intelligence and administer it for threat detection and validation. Usage of AI, real-time aggregation from dark web, open web, and proprietary sources; automated contextual enrichment of alerts; seamless integration with SIEM, XDR, and SOAR platforms; AI-powered threat actor profiling; predictive modeling of emerging threats; tailored intelligence for specific industries; and automated response and playbook workflows for rapid incident mitigation. ▪ Vendor utilizes advanced security analytics, including AI/ML use cases for threat detection and investigation. Usage of AI analytics platforms, data lakes, AI-driven anomaly detection, automated correlation across multiple data sources, real-time threat scoring and visualization, seamless integration with cloud and on-premises environments, and continuous behavioral profiling for users and devices. The vendor provides customizable machine learning models, fast query capabilities for massive data sets, predictive risk analytics, automated incident response, and highly interactive dashboards for proactive decision-making. 12 months of log retention — with 3 months immediately available for analysis.	
Go to market	▪ Marketing capabilities of the vendor across channels (e.g., account based, regional, industry based, digital). Vendors that are active in digital marketing, have excellent websites, and run regional campaigns score higher. Vendors that are very visible in the market will score higher. ▪ Channel and partner management to drive indirect sales. Vendors that have a wide network of services resellers and managed	7

TABLE 2

Key Capability Measures for Success: Middle East Managed Detection and Response

Capabilities Criteria	Definitions	Weight (%)
	SP/managed security SP partnerships to drive indirect sales score higher. ▪ Large distributed sales team and initiatives to drive customer confidence through the buying process. Customer spread across regions, segments. and industries.	
Range of services	▪ The vendor offers a suite of managed services that complement its MDR offering. Unique service bundles score higher. ▪ Portfolio of professional services, including strategic consulting and technical assessments, that complement the MDR service. Vendors with a broad suite of professional services score higher. ▪ Forensics and incident response retainer capabilities and the ability to perform DFIR in traditional computing as well as cloud environments, either through in-house offering or partner integrated. Vendors that offer full IR life-cycle support score higher. Cyber-insurance gets a higher score.	12
Security outcomes	▪ The vendor offers SLAs across several metrics like MTTD and MTTR, or goes beyond standard metrics to provide dynamic, context-aware SLAs. Unique features include self-adjusting SLAs based on incident risk and customer tier, predictive automation that reallocates resources to prevent potential violations, workflow integrations for compliance documentation, and transparent historical SLA tracking for continuous improvement. ▪ The vendor has shown improvements in MTTD and MTTR over time and its 2023 MTTD and MTTR is low compared to other vendors. Absolute comparison among participants, must evaluate individual improvement. ▪ The vendor offers several guarantees for incident scenarios. Tiered financial penalties scaled to breach severity, automatic "premium" support upgrades, or free enhanced services. Cyber-insurance policy contributions or automated regulatory compliance support after a breach event.	14
Service tiers	▪ The vendor offers tiered MDR services to target customers with different needs. Tiers suited to all types of industries. ▪ Flexible pricing options; pricing to suit all types of segments.	6
Talent management	▪ Tenure and training of the security employees. Local employee percentage. Certifications, trainings, tie-ups. ▪ Talent attainment and retention. Team size. Role in national talent building. University tie-ups, competition hosting, leading middle talent.	6
Total		100

Source: IDC, 2025

LEARN MORE

Related Research

- *IDC MarketScape: Middle East Governance, Risk, and Compliance Services 2025 Vendor Assessment* (IDC #META53726425, August 2025)

Synopsis

This IDC study presents a vendor assessment of emerging managed detection and response service providers in the Middle East. Using the IDC MarketScape model, 18 MDR service providers with operations and customers in the Middle East were evaluated. This process included interviewing one or more customers from each provider, while for one that did not actively participate in this study, the evaluation was based on IDC's knowledge of its security services offerings and capabilities. Providers were measured in terms of current capabilities and future strategies for delivering MDR services to customers in the Middle East.

"MDR remains the top cybersecurity investment trend in 2025, with the market hotter and more competitive than ever. Most managed security service providers now offer mature MDR services, intensifying competition. This year, we are seeing 'strategy wars' as MDR providers choose between technical sovereignty (regional, compliance-focused delivery) and global expansion (scalable, unified platforms). AI-powered automation, outcome-driven pricing, and sector-specific solutions are driving innovation. The market is defined by rapid growth, strategic differentiation, and ongoing activity around mergers and acquisitions. MDR is now the digital control plane for enterprise resilience." — Shilpi Handa, associate director, cybersecurity, Middle East and Africa, IDC

ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

IDC Middle East/Africa

Level 15, Thuraya Tower 1
Dubai Media City
P.O. Box 500615
Dubai, United Arab Emirates
+971.4.3912741
Twitter: @IDC
blogs.idc.com
www.idc.com