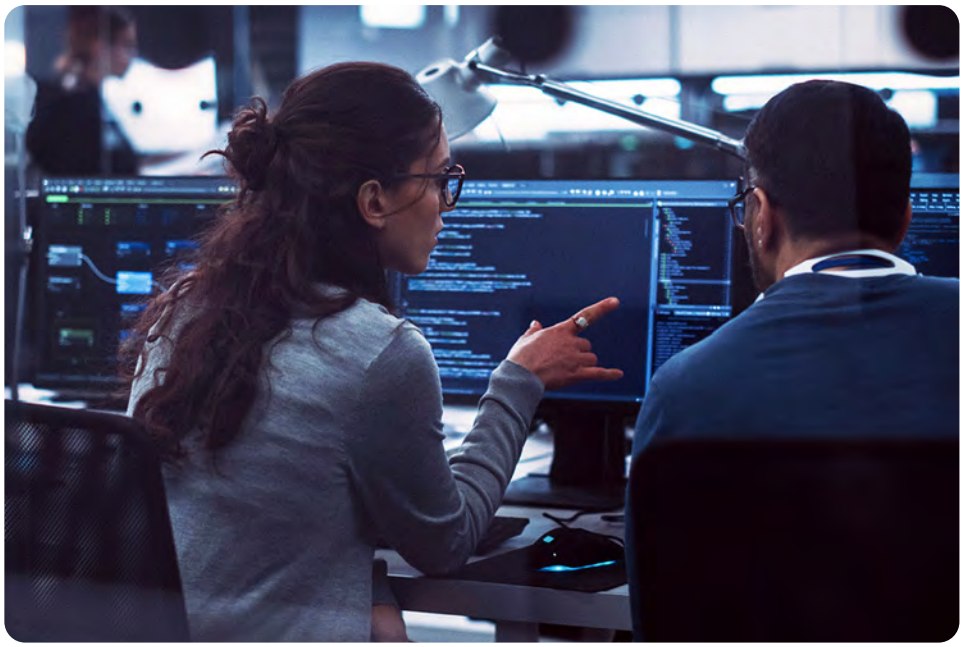
A buyer's guide

How to procure an MDR service that delivers real value

A practical guide for organisations seeking to procure an MDR service that effectively defends against today's (and tomorrow's) cyber threats.



Conscia
Secure progress

Contents

Introduction

Without effective security monitoring and response capabilities, organisations face escalating cyber risk. Modern threats are increasing rapidly in scale and speed, with attackers leveraging automation, identity-based attacks, and ransomware-as-a-service to cause significant business disruption.

At the same time, regulatory pressure is rising through frameworks such as NIS2, ISO/IEC 27001, and sector-specific regulations, increasing accountability for timely detection and response to incidents.

Many internal security teams are already stretched, operating under constant pressure with limited resources and skills shortages. As a result, delayed detection, slow response, and incomplete visibility can lead to prolonged outages, financial losses, regulatory penalties, and reputational damage. Many organisations therefore choose to outsource parts of their security monitoring and incident response to a Managed Detection & Response (MDR) service.

An MDR service is a fully managed, 24/7 expert-led lifecycle service that continuously detects, investigates, and actively disrupts cyber threats across an organisation's IT, cloud, identity, network, and OT environments. An MDR service goes far beyond traditional alert monitoring, combining advanced detection technologies with human security expertise and predefined response authority to rapidly reduce risk and limit business impact when attacks occur.

About this guide

This buyer's guide is designed to support organisations throughout their MDR service procurement journey. It helps you understand what a modern MDR service provider should deliver, what requirements to set, and how to avoid common mistakes. The guide explains the differences between traditional managed SOC and modern MDR services, outlines what a high-quality MDR service should include, and provides clear recommendations and a practical checklist to support your RFI, RFP, or tender process. The guidance is applicable to both private and public sector organisations.

Use this guide to define your needs and evaluate suppliers as part of a structured and outcome-focused sourcing process. It is intended for organisations that require an MDR service capable of protecting against both current and emerging cyber threats while meeting evolving legal and regulatory requirements.

This guide provides

- Key concepts to understand
- Guidance on the procurement process and key evaluation criteria
- A practical checklist for RFI and RFP processes
- Differences between a traditional managed SOC and a modern MDR service
- **A clear conclusion and next steps** →

Who this guide is for

This guide is written for C-level executives, procurement departments, and senior risk owners. It delivers practical guidance on designing a high-quality tender or sourcing process for MDR services, with a strong focus on outcomes, service quality, governance, and long-term value. The recommendations are based on real-world tender experience and proven selection criteria used by mature organisations.

Key concepts

Cybersecurity is filled with technical terminology. Below is a clear explanation of the key concepts used throughout this guide, focusing on what matters from a decision-making perspective.

SOC

Traditional Managed Security Operations Centre

A traditional managed SOC is an outsourced function that watches your environment 24/7, reviews alerts, manages core security tooling such as SIEM, and escalates suspected incidents to your team. Traditional managed SOCs are usually monitoring-centric, with little response authority and capability.

MDR

Managed Detection & Response

MDR is an outsourced detection and response capability delivered as a service, where detection, investigation, hunting, and active response are all handled by a provider. Unlike traditional managed SOC models, MDR focuses on direct action to contain and disrupt threats, not just alerting.

XDR

Extended Detection & Response

The core technology underlying a modern MDR service. XDR collects and correlates data across endpoints, identities, networks, and cloud environments, enabling faster detection, better context, and most importantly, integrated response and containment actions.

EDR / NDR

Endpoint / Network Detection & Response

Technologies that provide visibility and detection capabilities within specific domains: **EDR** focuses on endpoints such as laptops and servers. **NDR** monitors network traffic, particularly in environments where agents cannot be deployed (OT/IoT/IoMT). Together, they provide complementary coverage across the environment.

SIEM

Security Information & Event Management

A platform used for log collection, long-term storage, and compliance reporting. While valuable for auditability and retrospective analysis, SIEM is typically a supporting component rather than the primary detection and response engine in modern MDR architectures.

SOAR

Security Orchestration, Automation & Response

Primarily a provider technology that automates and standardises security processes. SOAR enables faster and more consistent response by executing predefined workflows and supporting analysts during investigations.

TI

Threat intelligence

Insights into threat actors, techniques, and emerging attack patterns. In a mature SOC, threat intelligence is operationalised into detection logic and response playbooks, not just consumed as static reports.

MITRE ATT&CK

A globally recognised framework that categorises how attackers operate, based on real-world attack techniques. It is used to evaluate detection coverage, identify security gaps, and ensure that threats are detected based on attacker behaviour, not just individual alerts.

Detection coverage

The extent to which an MDR service can detect relevant attacker techniques across your environment. High coverage means the ability to identify threats across endpoints, identities, networks, and cloud, and not just isolated events.

Detection use cases

Defined detection logic that identifies specific attacker behaviours or suspicious patterns. Mature MDR services continuously develop and refine use cases based on threat intelligence and real incidents to improve detection quality.

Containment

The actions taken to stop or limit an active threat. This may include isolating endpoints, disabling user accounts, or blocking network traffic. Effective containment is critical to reducing business impact.

False positives & alert fatigue

False positives are alerts that do not represent real threats. High volumes of such alerts create alert fatigue, reducing efficiency and increasing the risk that genuine threats are overlooked. A mature MDR service prioritises accuracy over volume.

MTTD

Mean Time to Detect

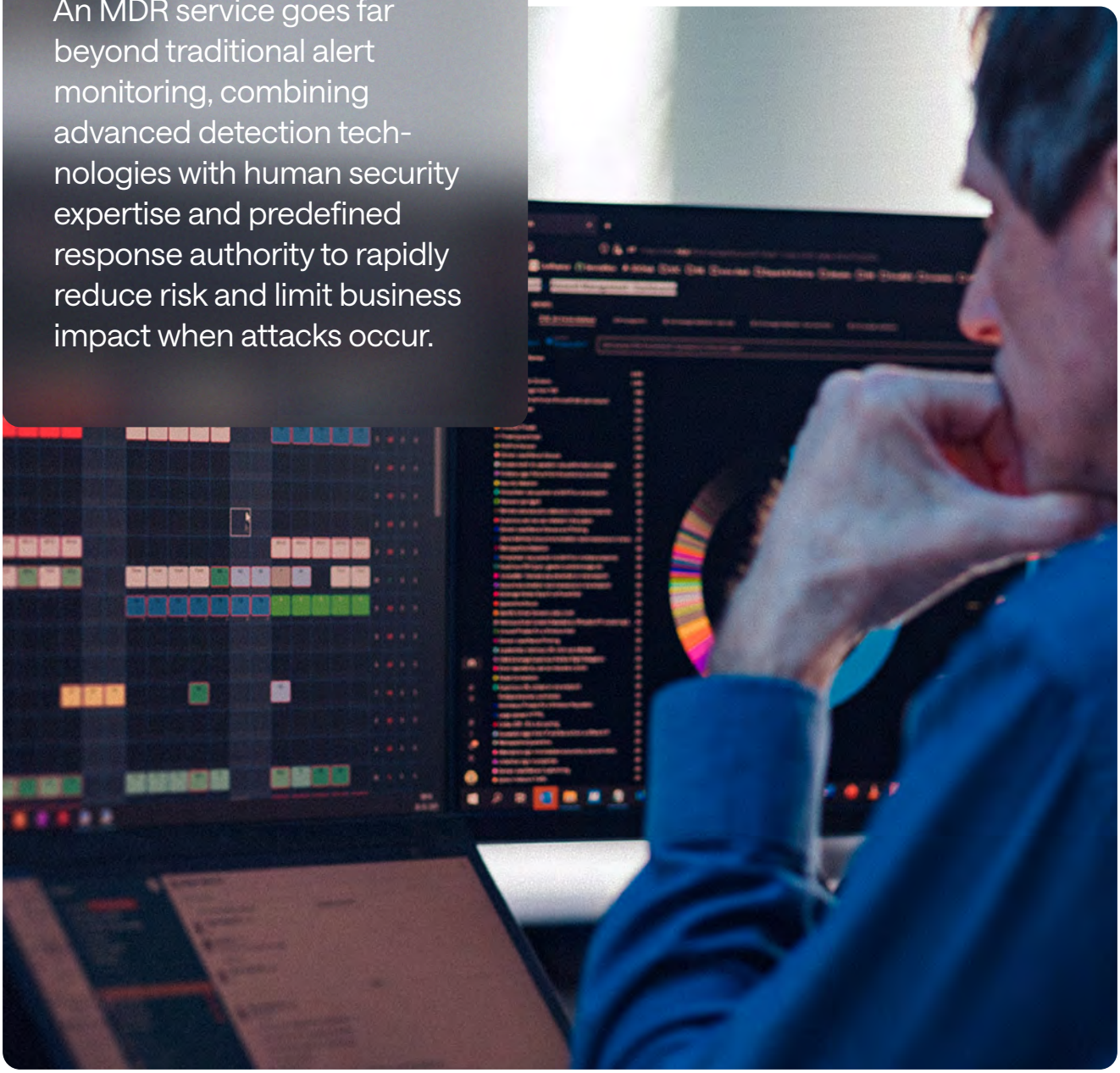
The average time it takes to identify that a security incident or threat has occurred.

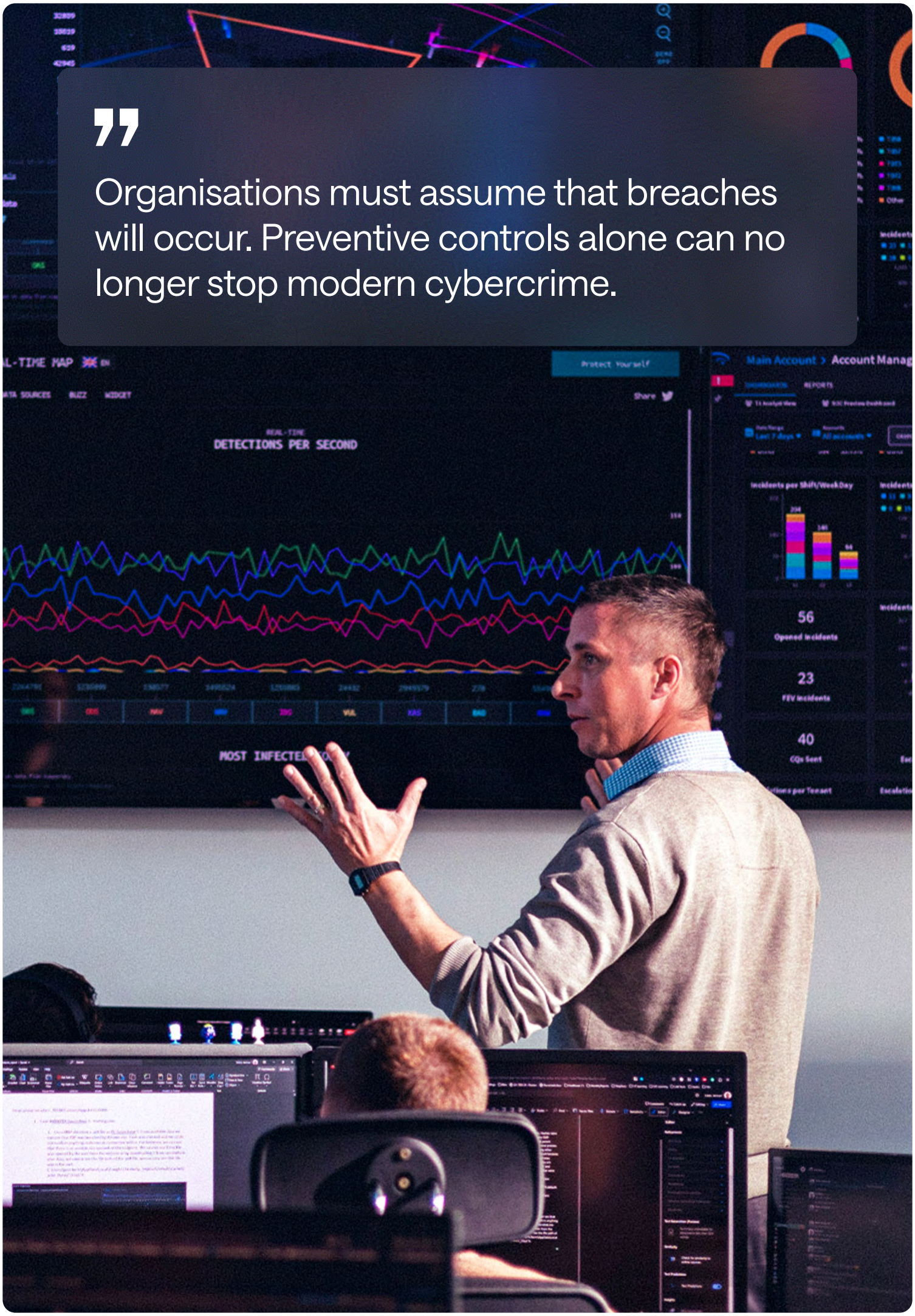
MTTR

Mean Time to Respond

The average time it takes to contain and remediate a confirmed security incident after detection.

> An MDR service goes far beyond traditional alert monitoring, combining advanced detection technologies with human security expertise and predefined response authority to rapidly reduce risk and limit business impact when attacks occur.




Organisations must assume that breaches will occur. Preventive controls alone can no longer stop modern cybercrime.
DETECTIONS PER SECOND
Protect Yourself
Main Account
56
23
40

Understanding the landscape

Why the market shifted from traditional managed SOC to MDR services

Attackers have become significantly faster and more automated. The acceptable time to detect and respond has therefore decreased dramatically – organisations increasingly recognise that detection alone is insufficient if response actions cannot be executed immediately. This evolution has driven the market toward MDR services. An MDR service explicitly includes both:

Detection: Continuous monitoring and advanced threat detection.

Response: Active containment and remediation actions performed by the provider.

An MDR service uses technology stacks that go beyond traditional SIEM platforms and include response and automation capabilities (e.g. SOAR, EDR/XDR integrations). These tools enable providers to:

Contain threats faster

Reduce attacker dwell time

Act within predefined response playbooks

Many organisations now deliberately choose an MDR service as a result, because response responsibilities are increasingly delegated to the provider, ensuring faster action and reduced operational burden for internal teams.

Why is an MDR service essential for today's security strategy?

Organisations must assume that breaches will occur. Preventive controls alone can no longer stop modern cybercrime, which operates faster, more covertly, and more effectively than traditional security models can manage. An MDR service addresses this reality by prioritising early detection, expert investigation, and rapid containment of genuine attacks.

1

Prevention alone is no longer sufficient in today's threat landscape

Preventive controls remain essential to reduce attack surfaces, but they cannot detect all attacker behaviour. Firewalls, antivirus tools, multi-factor authentication, and zero trust architectures often fail when attackers exploit gaps between controls, abuse legitimate identities, or deliberately evade automated defences.

Most successful breaches occur in this grey area, where only human-led investigation can reliably identify and stop malicious intent.

2

Attack speed has outpaced traditional response models

Cybercrime operates as a professional and highly monetised industry. Attacks can escalate from initial access to material business impact within minutes or hours. Security teams that operate only during business hours cannot respond at the required speed.

An MDR service delivers 24/7 detection, investigation, and response, closing the critical time gap between compromise and business damage.

3 Detection without response does not reduce risk

Alerting alone does not stop attackers. Many organisations already collect large volumes of security data but lack the expertise or capacity to act decisively.

An MDR service reduces risk because it includes active threat disruption. Confirmed threats are contained through actions such as endpoint isolation or disabling compromised identities. The ability to stop attacks in progress is what converts monitoring into measurable risk reduction.

4 Organisations lack the resources to build this internally

Operating a mature 24/7 MDR service requires skilled analysts, established processes, and modern XDR tooling. The cost and complexity make this difficult to sustain and scale. Many organisations experience alert fatigue, staffing shortages, and inconsistent response quality.

An MDR service provides enterprise-grade detection and response as a service, without the operational burden of building and maintaining internal capability.

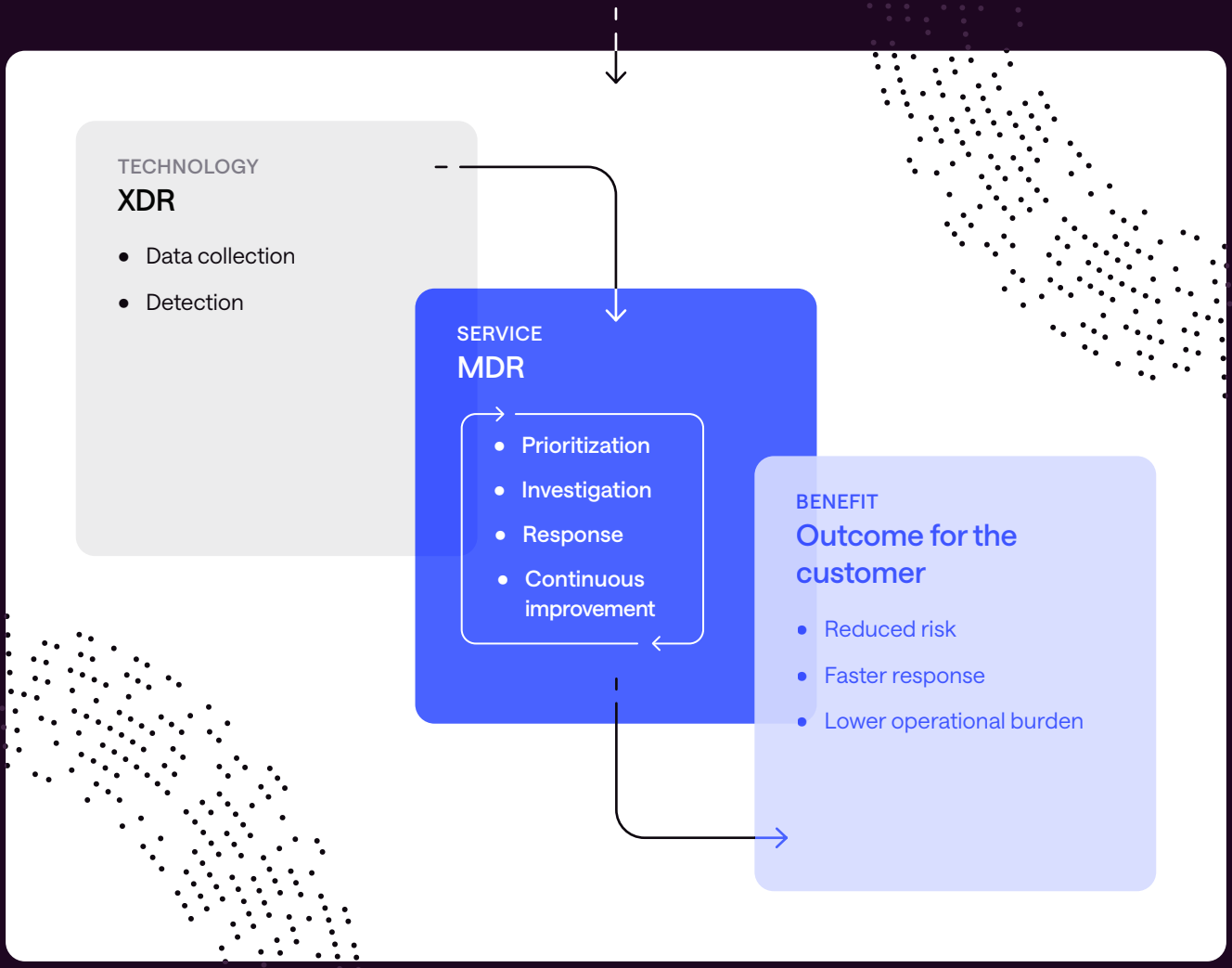
5 Human expertise is critical for modern threats

Automated tools accelerate detection, but they cannot assess intent, context, or attacker tradecraft on their own.

An MDR service provides continuous access to experienced security analysts who interpret weak signals, conduct threat hunting, and make informed decisions during high-pressure incidents. Human judgement is the primary reason an MDR service consistently outperforms tool-only approaches.

6 An MDR service aligns security with business risk

Security strategy is now driven by business risk rather than technology alone. An MDR service prioritises incidents based on asset criticality, exposure, and potential impact, ensuring response capacity is used where it matters most. The objective is not fewer alerts, but smaller incidents and minimal business impact.



What good looks like

What an MDR service must deliver

A modern MDR service is a fully operational security function. It continuously detects, investigates, and stops threats rather than simply operating security tools. An MDR service delivers value only when technology, human expertise, and clearly defined processes work together as a single, outcome-driven capability. Tools alone do not provide protection. The following elements are essential.

24/7 operational capability

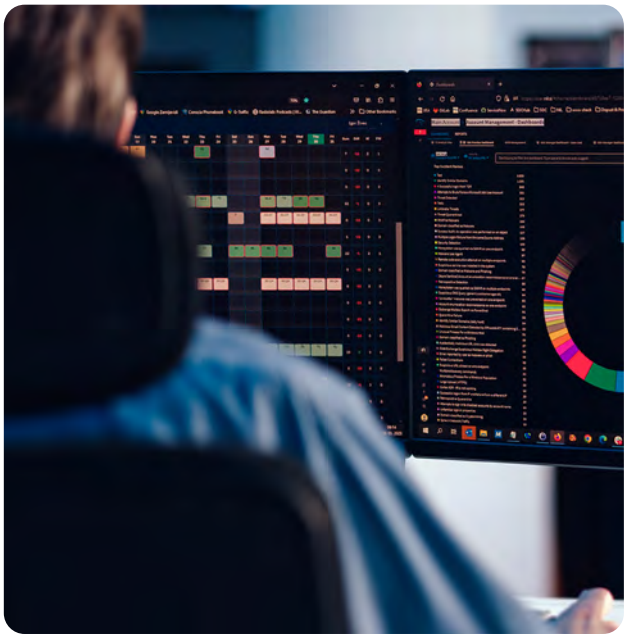
An MDR service must operate continuously, with real-time monitoring performed by dedicated security analysts at all times. This requires:

- **Fully staffed 24/7 operations** – not on-call coverage or follow-the-sun handovers
- **Continuous analysis** of security events across all relevant systems
- **Immediate investigation** of suspicious activity, regardless of time or day

Threat actors operate without time constraints. Effective security operations must do the same. The service must cover the full lifecycle of a security incident, from initial detection to final resolution. This includes:

- **Continuous detection** across endpoints, identities, cloud, network, and OT/IoT environments
- **Human-led investigation** until a clear, validated conclusion is reached
- **Structured** remediation guidance and recovery support

Services that cover only parts of the incident lifecycle introduce gaps. These gaps create delays that attackers can exploit to increase impact.



Active response & containment

The service must include active response capability. Detection alone does not reduce risk if action cannot be taken immediately.

The provider must be able to contain confirmed threats and limit business impact through actions such as:

- **Isolating** compromised endpoints
- **Disabling** compromised user accounts
- **Blocking** malicious network activity

The ability to act – not just alert – is what transforms security monitoring into effective risk reduction.

End-to-end threat lifecycle coverage

Skilled analysts and operational expertise

Technology enables detection, but expertise enables decision-making. A high-quality MDR service is built on:

- **Experienced, multi-tiered** analysts and incident responders
- **Strong certification** and continuous training *(e.g. SANS GIAC or equivalent)*
- **Access to senior expertise** for complex or high-impact incidents

The quality of analysis directly impacts both detection accuracy and response speed.

Low operational burden for your organisation

A core objective of an MDR service is to reduce the workload on internal IT and security teams. This requires:

- **Autonomous investigation** and triage by the provider
- **Escalation of only** validated high-confidence incidents
- **Minimal reliance** on customer-team analysis or tool management

The service should act as an extension of your organisation, and not an additional operational burden.

Continuous improvement & measurable outcomes

An MDR service must evolve continuously to remain effective against changing threats. This includes:

- **Ongoing development** of detection use cases based on real incidents and threat intelligence
- **Regular reporting** with actionable recommendations
- **Measurement and improvement** of key metrics, such as detection & response time

The objective is not just to handle incidents, but to reduce the likelihood and impact of future attacks.

Modern technology & integrated architecture

Technology is a critical enabler, but only when applied correctly. A modern MDR service should:

- Be built on **XDR platforms for real-time** detection and response
- **Use SIEM** as a complementary component for log retention, compliance, and niche detection cases
- **Integrate seamlessly** with existing security tools and environments
- Support both **IT & OT/IoT/IoMT** use cases where required

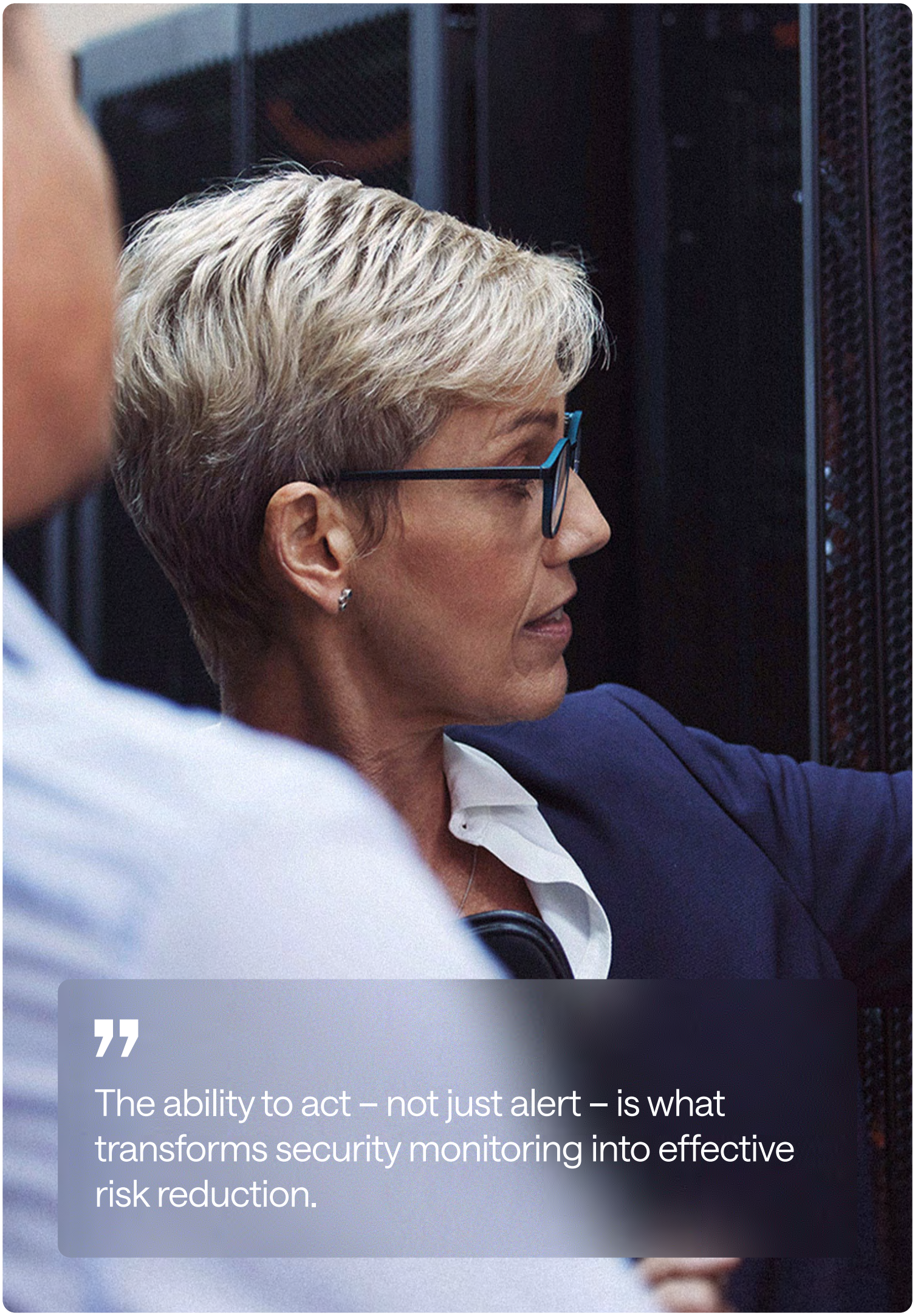
The focus should be on detection quality, response speed, and scalability.

Summary

A high-value MDR service is defined by its ability to:

- Operate continuously
- Cover the full threat lifecycle
- Minimise internal workload
- Act immediately on confirmed threats
- And continuously improve over time

These capabilities form the foundation for effective, outcome-driven security operations.


”
The ability to act – not just alert – is what transforms security monitoring into effective risk reduction.

XDR or SIEM?

What should sit at the foundation of a modern MDR service?

SIEM & its features

Limited visibility

SIEM platforms collect logs, but they often struggle to correlate activity across identity systems, networks, email, cloud platforms, and endpoints. This limitation creates blind spots in critical parts of the environment, particularly where attacks span multiple domains.

High workload & low precision

SIEM platforms often generate high volumes of alerts, many of which are false positives. Analysts can become overwhelmed by noise, increasing the risk that genuine threats are delayed or missed entirely.

Manual configuration & maintenance

SIEM solutions require continuous rule tuning, interpretation, and maintenance. This approach assumes access to experienced internal security teams – a capability many organisations do not have or cannot sustain.

Slower response

Most SIEM platforms detect events but lack built-in mechanisms for immediate action. The time between detection and response therefore increases, allowing attackers more opportunity to escalate activity.

Advantages of building on XDR

Broad & unified coverage

XDR correlates telemetry from endpoints, networks, identity systems, email, SaaS applications, and cloud platforms within a single, coherent view. This enables visibility across the full attack surface.

Automated correlation & contextual understanding

XDR prioritises incidents rather than isolated alerts. Structured incident views show the full attack chain, improving both detection speed and analytical precision.

Fewer but more relevant alerts

XDR platforms reduce noise by filtering low-value signals and prioritising risk. Analysts focus on verified threats rather than raw event volume, increasing operational efficiency.

Faster containment

Many XDR platforms support direct response actions, such as isolating endpoints, disabling compromised accounts, or blocking malicious traffic. This shortens the time from detection to containment.

Strong foundation for threat hunting & improvement

Structured and enriched XDR data supports proactive threat hunting and continuous improvement of detection logic. This enables the MDR provider to evolve based on real attack behaviour, not static rules.

The role of SIEM as a complement

SIEM continues to serve an important role within a modern MDR service for some customers, particularly for:

Log retention and compliance

Customised reporting

Long-term forensic analysis and auditing

In this role, SIEM can support real-time detection and response operations for rare use cases not supported by XDR, such as custom application log analysis. The primary detection and response capability should however reside within XDR to ensure speed, context, and action.

SIEM vs XDR - key differences	SIEM	XDR
Visibility	Log-based analysis with limited coverage of initial attack stages	Detailed telemetry for holistic attack chain view with broad coverage
Automation	Limited, often manual	High, with built-in response
Alert quality	High volume, lower relevance	Fewer alerts, higher relevance
Response time	Slower, manual actions	Faster, integrated response
Primary use	Compliance and log retention	Detection, response, and threat hunting

Recommendation

Choose a provider that has built its MDR service around XDR, with SIEM used as a complementary platform for compliance and long-term log management.

This approach is particularly important for organisations in regulated sectors such as healthcare and financial services, where rapid response and strong auditability are both essential.

Additional capabilities to consider

A modern MDR service is more than monitoring and alerts. To address today's threat landscape effectively, it should form part of a broader security ecosystem that can expand as your needs evolve. Here are additional capabilities that can significantly strengthen your protection.

Continuous Customer Improvement

A mature MDR service should provide their customers with a constant stream of recommendations to improve the customers hygiene and security maturity, based on evidence gathered during security operations.

Threat hunting

Proactively searching for signs of compromise that have not triggered alerts. This is particularly important when attackers use new or tailored techniques designed to evade standard detection.

Digital forensics & incident investigation

Major incidents often require deeper technical analysis. A well-prepared MDR service should have access to digital forensics and incident response (DFIR) specialists – either in-house or through a trusted partner – to support investigation, evidence collection, and recovery.

Exposure management

Services that identify vulnerabilities, exposed systems, and misconfigurations can reduce your overall attack surface. This is especially valuable for organisations with distributed environments, legacy systems, or complex supply chains.

Detection of data leaks & brand misuse

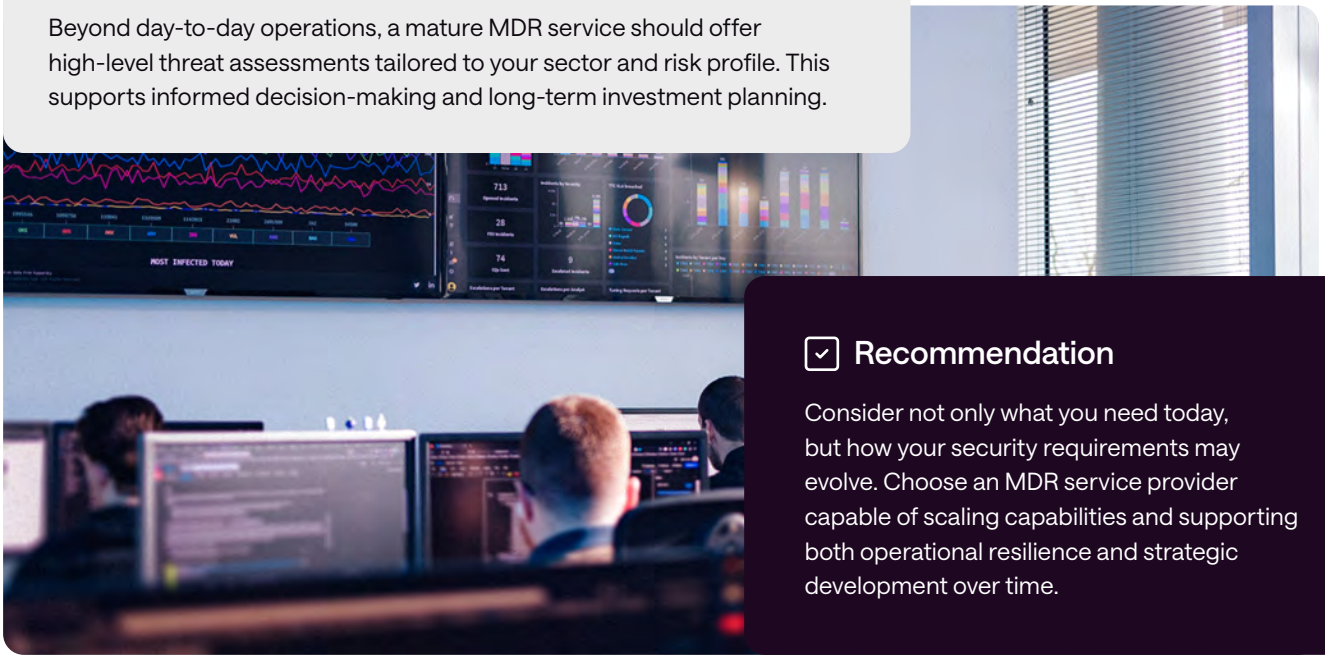
Monitoring open sources and the dark web – areas of the internet not indexed by traditional search engines and often used by criminal actors – can provide early warning of leaked credentials, phishing campaigns, or identity misuse targeting your organisation.

Log management & compliance

Proper log collection and retention are essential for both forensic investigations and regulatory compliance. An MDR service that manages log architecture as part of its service reduces administrative burden and compliance risk.

Strategic threat assessments

Beyond day-to-day operations, a mature MDR service should offer high-level threat assessments tailored to your sector and risk profile. This supports informed decision-making and long-term investment planning.



Recommendation

Consider not only what you need today, but how your security requirements may evolve. Choose an MDR service provider capable of scaling capabilities and supporting both operational resilience and strategic development over time.

Structuring your procurement

Define your scope first

Unclear scope is one of the most common root causes of failed MDR service engagements. If inputs are incomplete or ambiguous, providers will make assumptions – and those assumptions will later turn into contractual friction.

To receive meaningful and comparable proposals (and less questions in Q&A rounds), the tender should clearly **describe:**

- A high-level architecture overview (diagram)
- Number of endpoints and servers
- Identity landscape *(AD/Entra ID)*
- Key applications and SaaS platforms
- Existing security tooling
- Desired future state and onboarding expectations

You should also clarify

- Cloud strategy *(cloud-first, hybrid, on-prem)*
- Compliance drivers *(e.g. NIS2, sector regulations)*
- Risk assessments already performed
- Your organisational structure, if MDR services should be tailored to specific business units.
- Phased versus full-scope onboarding expectations

Choose the right tender strategy

Selecting an MDR service provider is a risk transfer and continuity decision, not a standard IT sourcing exercise. It has a direct impact on business operations, regulatory compliance, and reputational exposure. The tender strategy your organisation adopts therefore plays a decisive role in determining the quality of outcomes.

A poorly structured tender leads to superficial comparisons, unclear responsibilities, and implicit assumptions around response authority, escalation, and accountability. A well-designed tender, by contrast, establishes transparency from the outset and reduces operational and contractual risk later in the engagement.

Avoid “open for everyone” tenders

Launching a fully open or public tender as a first step frequently leads to:

- A high number of responses with widely varying maturity levels
- Significant evaluation effort for procurement and subject-matter experts
- Proposals that are difficult to compare due to different interpretations of the scope

From a buyer’s perspective, this increases the risk of selecting a provider based on presentation quality rather than operational capability.

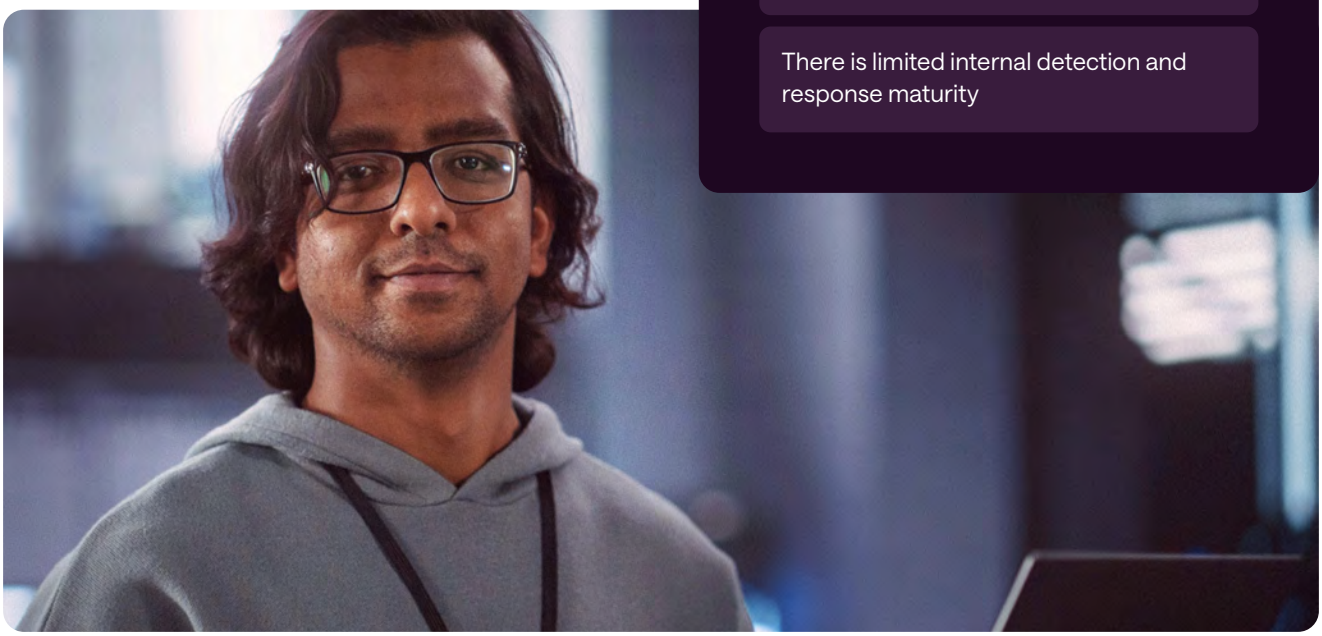
Recommended tender types

Depending on regulatory context and procurement obligations, suitable tender models include:

- **Limited tenders** based on a shortlist of qualified providers for organisations with procurement flexibility
- **Single supplier engagement** where continuity, speed, or existing dependencies are critical
- **Competitive dialogue,** which is strongly recommended for complex or highly regulated environments

Competitive dialogue is particularly effective when:

- The provider is expected to take responsibility
- Existing security architecture is complex or hybrid
- There is limited internal detection and response maturity



Define the right evaluation philosophy

How proposals are evaluated is just as important as what is requested. An evaluation philosophy that places excessive weight on tools or price often obscures meaningful operational differences between providers.

Focus on outcomes, not tools

From a procurement and executive standpoint, prescribing detailed technical implementations introduces unnecessary risk.

Instead, your organisation should:

- Define business and security outcomes
  (e.g. detection coverage, response time, escalation handling)
- Allow providers to propose how those outcomes are achieved
- Set only essential boundary conditions
  (e.g. required platform support or regulatory constraints)

This approach encourages innovation, makes providers accountable for results, and prevents vendor-driven technology lock-in too.

Pricing evaluations based on Total Cost of Ownership (TCO)

MDR services vary significantly in pricing structure. Comparing monthly service fees alone rarely reflects the true cost.

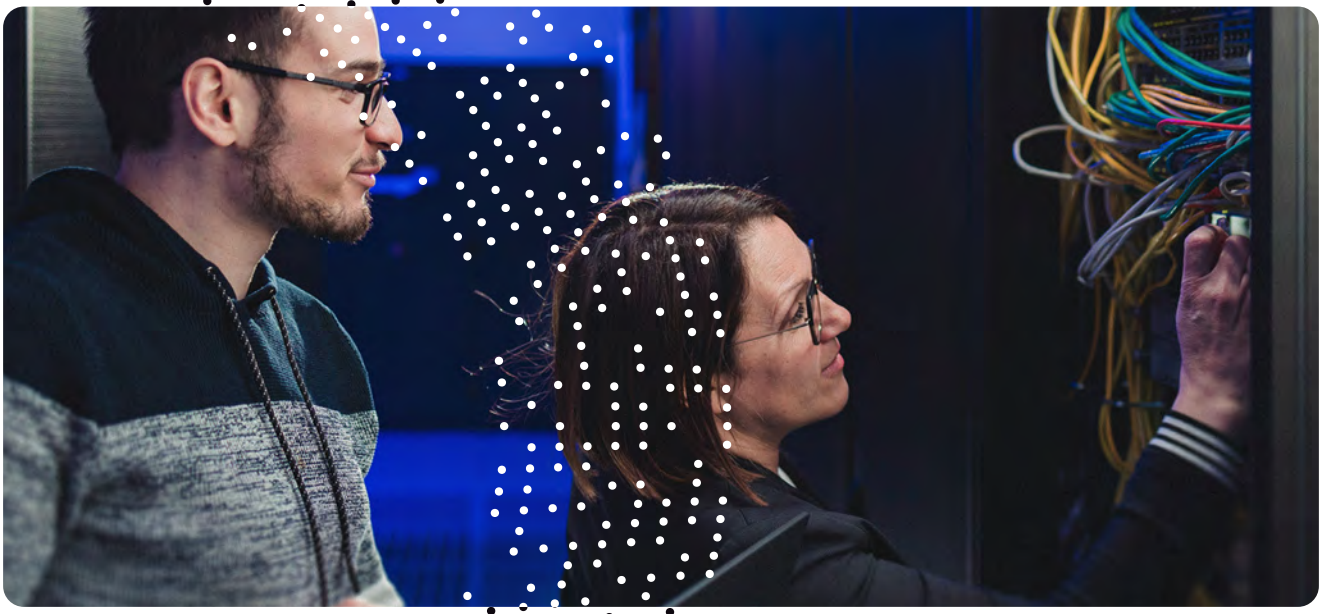
Best practice for your organisation:

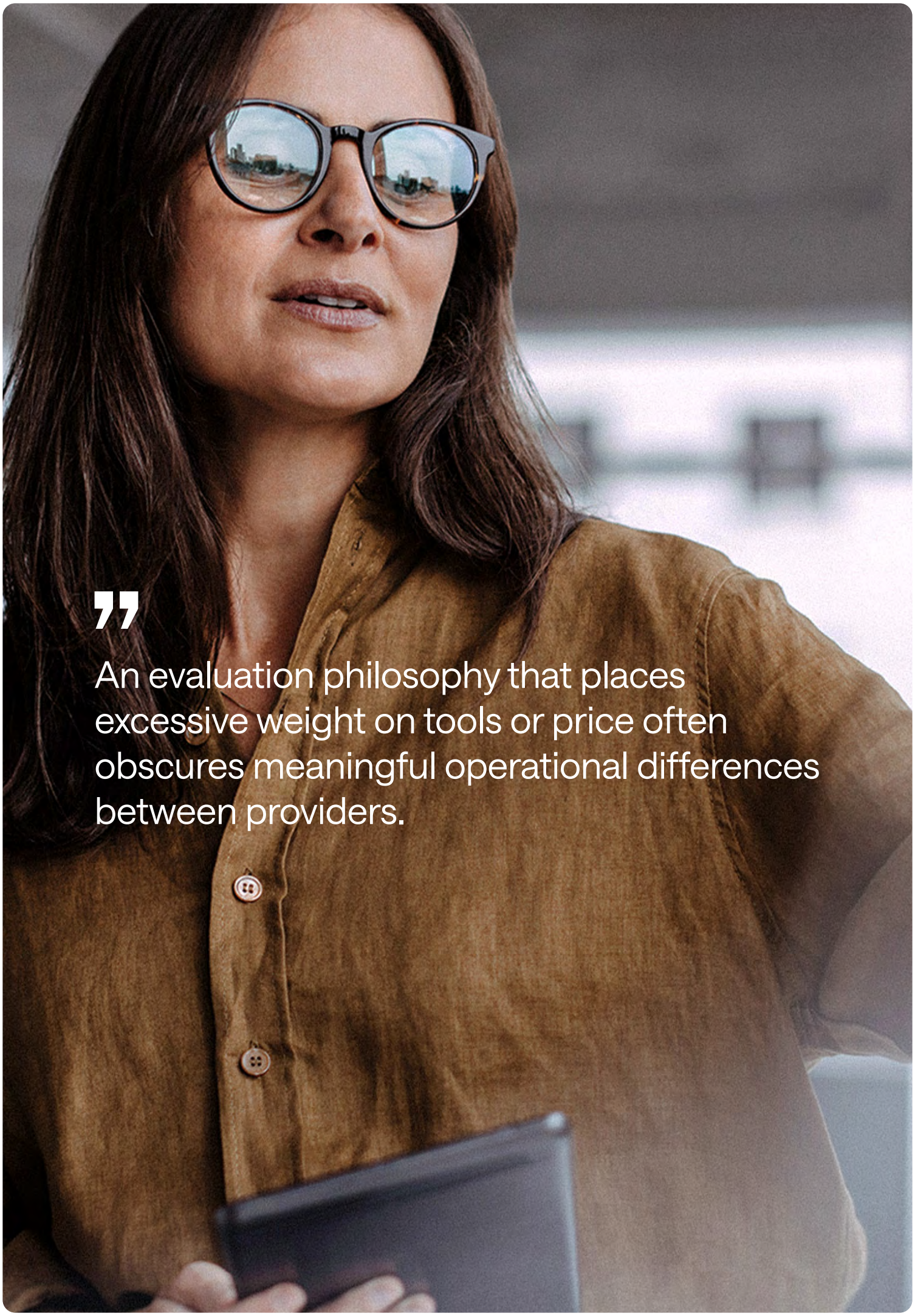
- Use a mandatory pricing template for all bidders

Distinguish clearly between:

- Service fees
- Technology or license costs
- Variable components
  (e.g. log volume, data retention, response activities)

Evaluation should be based on TCO over the contract period, including realistic growth scenarios. This prevents cost surprises after contract signature.




”
An evaluation philosophy that places excessive weight on tools or price often obscures meaningful operational differences between providers.

Evaluating providers

Quality & selection criteria (shortlist phase)

Quality and selection criteria are the primary means of reducing long-term operational and governance risk, not merely a scoring mechanism.

Security operations rarely fail because of tools alone; they fail due to insufficient expertise, unclear ownership, or immature processes. The criteria in this chapter are designed to help buyers distinguish between providers that can theoretically deliver a service and those that can consistently operate it under real-world pressure.

Analyst capacity & expertise

The capability of the provider is one of the strongest indicators of an MDR service quality. The size, composition, and skill level of analysts directly affect investigation depth, response speed, and incident outcomes.

Mature tenders typically assess:

- The number of dedicated analysts and the 24/7 staffing model
- The availability of Tier 1, Tier 2, and Tier 3 expertise
- The level of relevant security certifications *(for example, SANS GIAC)*

In practice, insufficient analyst capacity results in delayed investigations, shallow analysis, and slow response during peak demand or large-scale incidents.

Certifications & control frameworks

Certifications provide assurance for procurement and risk owners by demonstrating that security operations are controlled, auditable, and repeatable rather than serving as basic hygiene measures.

Requiring standards such as ISO 9001, ISO 27001, and preferably ISAE 3402 Type II helps ensure that processes are documented and consistently applied, controls are independently audited, and deviations or incidents can be traced, reviewed, and clearly explained.

This is particularly important in regulated sectors, where organisations must be able to demonstrate effective governance and control over outsourced security operations.

MDR maturity

Maturity models such as SOC-CMM, or equivalent frameworks, provide an objective way to assess MDR provider quality. They allow buyers to evaluate operational capability beyond marketing claims.

Higher maturity levels typically indicate:

- Proactive detection use-case management
- Integrated use of threat intelligence
- Increasing use of automation for detection and response

A maturity assessment reduces reliance on subjective claims and supports a more evidence-based evaluation of provider capability.

Relevant experience & references

Relevant experience significantly reduces onboarding and delivery risk. Providers that have operated in comparable environments are more likely to anticipate challenges and respond effectively.

Buyers typically assess:

- Experience in similar sectors or regulatory environments
- A comparable scale and complexity of monitored assets
- Verifiable customer references

This helps confirm that the provider understands not only the technology, but also the operational, regulatory, and organisational context in which the service must function.

Portfolio breadth & strategic fit

Many organisations score providers higher when they can support future security needs beyond core MDR service delivery, such as consultancy services, vulnerability assessments, attack surface management, and managed red teaming or penetration testing.

While these capabilities may not be required from day one, they indicate whether a provider can act as a long-term security partner capable of supporting evolving requirements as the organisation's threat landscape and maturity develop.

This does not imply that all services must be contracted immediately, but it indicates whether a provider can act as a long-term security partner rather than a narrowly scoped service supplier.

Vision & future readiness

Many organisations score providers higher when they can support future security needs, such as:

- Consultancy services
- Vulnerability assessments
- Attack surface management
- Data leakage detection (dark web monitoring)
- Managed red teaming and penetration testing

This does not imply that all services must be contracted immediately, but it indicates whether a provider can act as a long-term security partner rather than a narrowly scoped service supplier.

> Quality and selection criteria are the primary means of reducing long-term operational and governance risk, not merely a scoring mechanism.

Operational success criteria

With unclear operational governance, even a well-selected provider might fail to deliver real value. But what is the criteria for operational success? This chapter focuses on the conditions required for sustained, predictable service delivery.

Governance model

A clear separation of responsibilities is essential within a good governance model. Your organisation retains ownership of security policy, compliance interpretation, and business risk decisions, while the provider is accountable for detection, analysis, and response actions within clearly agreed boundaries.

Such a distinction ensures effective decision-making, accountability, and smooth collaboration during security operations and incidents. Responsibilities become blurred during incidents, leading to delays and escalation confusion without this important separation.

Cooperation with preventive teams

Reducing false positives is a shared responsibility and cannot be achieved the provider on its own. Therefore, strong security outcomes depend on close collaboration between the MDR provider and your organisation's IT teams, who manage preventive controls across the network, cloud, endpoints, and application landscape.

By working together and adjusting controls based on real incident feedback, recurring false positives can be systematically eliminated, leading to more efficient investigations, faster response times, and a higher overall quality of service.

Dedicated team

Having a clearly defined delivery team that includes account management, service delivery, and senior analysts reduces reliance on individual people and helps ensure consistent service delivery. This team-based approach supports continuity during security incidents, staff changes, or periods of increased workload, giving your organisation confidence that the service will remain stable and reliable when it matters most.

Transparency & service management

Operational transparency enables trust and executive oversight.

Minimum expectations typically include:

A named Service Delivery Manager (SDM)

Clear escalation processes

Real-time dashboards and portals for insight into incidents, performance, and secure communication that include information such as:

- Incident information (also historic)
- Threat intelligence information
- Secure communication channel to share documents
- Regular tactical and strategic service reviews

Transparency to enable oversight without micromanagement

Reporting

Reporting should go beyond metrics. Strong reporting combines performance data with interpretation and recommended improvements, for example:

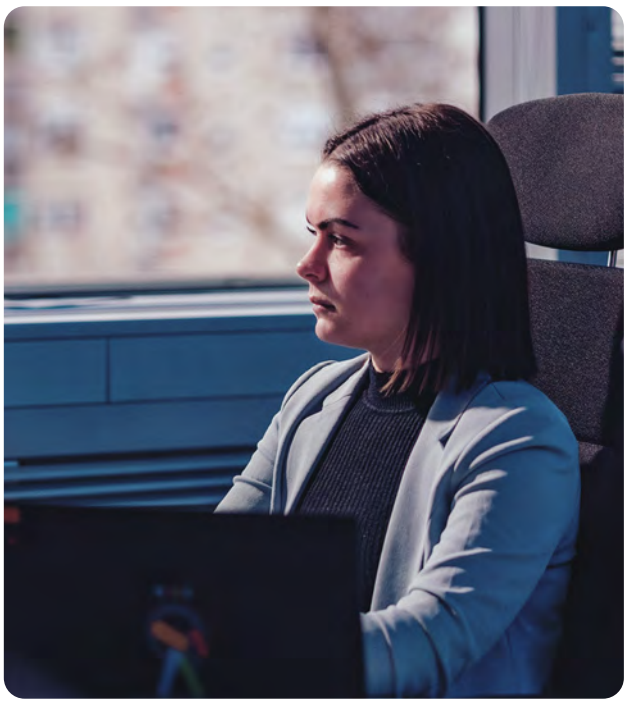
Executive summaries	Trend analysis
Recommendations for improvement	Contextual threat information

This enables MDR services to function as a driver for continuous security maturity improvement, and not only reactively.

Functional & platform requirements

Platform requirements should not dictate architecture – they should support outcomes. From a buyer's perspective, the platform is an enabler of detection quality, response speed, and governance transparency, not just a goal.

In many tenders, insufficient attention to platform capabilities results in services that technically collect logs but fail operationally due to alert overload, slow response, or lack of insight for executives. That means that modern operating models increasingly require automation and orchestration, given the volume of events that must be analysed and correlated.



Functional capabilities

From an executive and procurement standpoint, functional capabilities determine whether the service can be operated reliably, compliantly, and at scale over the contract term.

Key capabilities include:

Secure data handling and segregation: In multi-tenant or multi-participant environments, it must be demonstrable that log data and cases are strictly segregated per organisation.

Log retention and forensic readiness: The provider should advise on retention aligned with regulatory drivers and support investigations weeks or months after an incident without data gaps.

Use of threat intelligence: Mature operations enrich detections with relevant threat intelligence to improve context, reduce noise, and support prioritisation.

These functional requirements directly influence auditability, investigation quality, and the ability to explain incidents to regulators and boards.

Platform capabilities

Platform capabilities determine whether analysts can act fast enough in a real incident and whether the organisation retains visibility and control.

Minimum expectations typically include:

Automation and orchestration (SOAR) to standardise repeatable actions, accelerate containment, and reduce analyst overload

Incident and case management to support structured investigation, documentation of analyst actions, and clear escalation paths

Dashboards and reporting that support both operational collaboration and executive oversight

Alignment with MITRE ATT&CK to support transparency, maturity assessments, and structured improvement of detections

Finally, it is vital to explicitly address false positive management. For this, the platform and process you are using should support tuning, feedback loops, and continuous optimisation rather than static rule sets.

Common pitfalls to avoid

Key differences between MDR services are often obscured by similar presentations and marketing language. Avoid the following common mistakes, as they can have significant long-term consequences.

Continuous Customer Improvement

A mature MDR service should provide their customers with a constant stream of recommendations to improve the customers hygiene and security maturity, based on evidence gathered during security operations.

Selecting a technology provider without operational security expertise

Security operations require specialist skills beyond technology management. An MDR service is a security function, not an IT operations service. Require proven expertise in incident handling, threat analysis, and adversary behaviour.

Underestimating the workload placed on internal teams

Some providers escalate large volumes of unfiltered alerts with limited context. This approach transfers operational burden back to your internal teams and reduces the value of outsourcing. Demand effective triage and validation before escalation.

Focusing on license models rather than outcomes

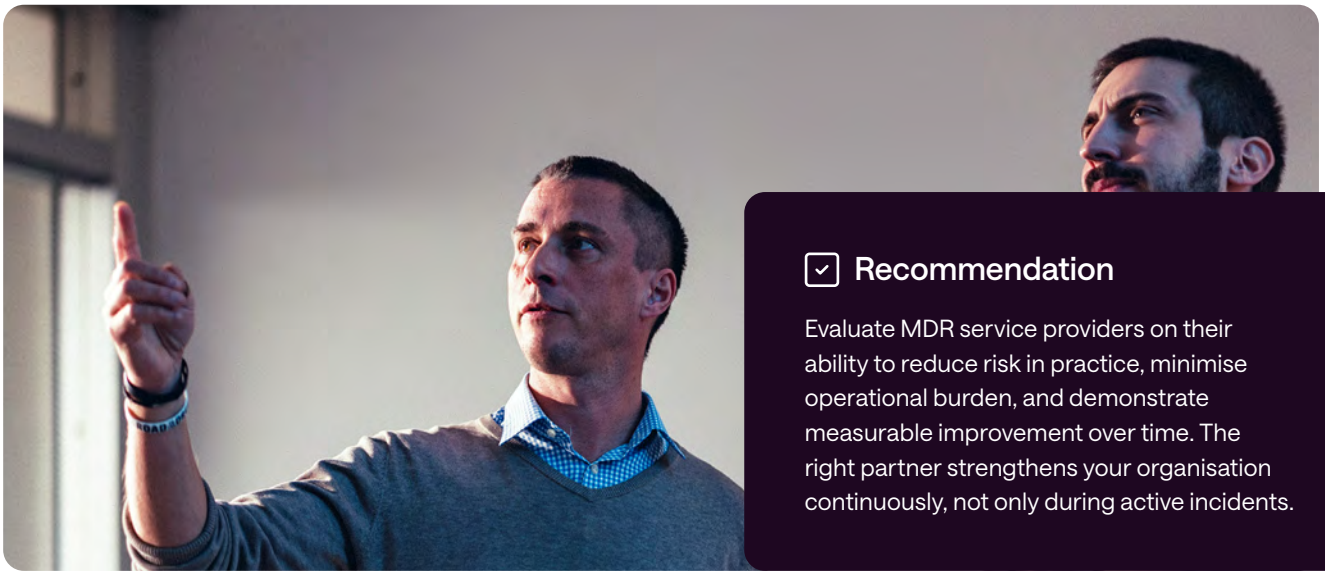
Pricing based on logs, users, or endpoints has little value if the service does not reduce risk. Prioritise detection quality, response speed, and threat coverage over licence structures or unit costs.

Overlooking continuous improvement

A capable MDR service does more than resolve incidents as they arise. It actively strengthens your security posture through structured follow-up, detection improvement, and measurable risk reduction. Without this, security maturity will stagnate.

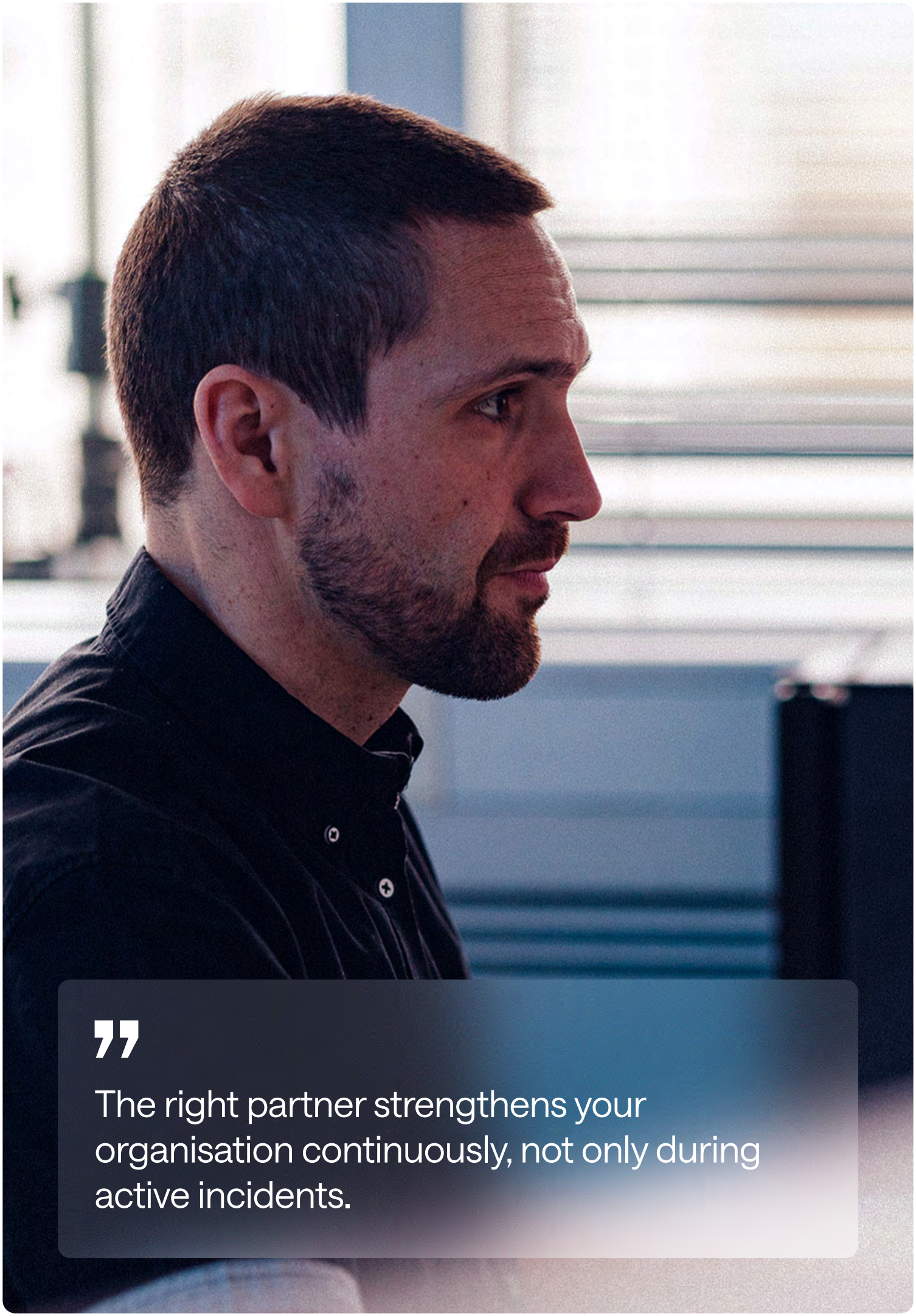
Treating SIEM as the sole foundation

SIEM remains valuable for log retention, reporting, and compliance. However, SIEM alone lacks the context, automation, and response capabilities required for modern threat operations. A modern MDR service must be supported by complementary technologies that can act – not only observe.



Recommendation

Evaluate MDR service providers on their ability to reduce risk in practice, minimise operational burden, and demonstrate measurable improvement over time. The right partner strengthens your organisation continuously, not only during active incidents.


”
The right partner strengthens your organisation continuously, not only during active incidents.

Making the decision

Checklist for procuring a modern MDR service

As has been shown throughout this guide, an MDR service requires operational, technical, and strategic consideration. Below is a practical checklist of requirements and capabilities that should be included in any serious procurement process. You can use this checklist as the foundation for an RFI or RFP process, or as an internal evaluation framework when reviewing existing or potential providers.

General MDR service capabilities

- [ ] Provides managed detection and response as a service, not just alerting or tool management.
- [ ] Covers the full incident lifecycle: monitoring, detection, investigation, response, and improvement.
- [ ] Designed for measurable risk reduction, not volume-based alert delivery.

Technology strategy: XDR over traditional SIEM

- [ ] Uses XDR first architecture for high-fidelity detection across endpoint, identity, cloud, and network.
- [ ] Uses SIEM only as a supporting component, not as the primary detection layer.
- [ ] Demonstrates how XDR improves detection speed and coverage versus log-centric SIEM models.

MDR expertise & skill level

- [ ] Operates a 24/7 staffed center with live analysts ("eyes on glass").
- [ ] Employs experienced, certified MDR analysts and incident responders.
- [ ] Can demonstrate longstanding MDR operational experience across multiple customers and sectors.

Service coverage: End-to-end MDR service

- [ ] Continuous monitoring and detection.
- [ ] Human led investigation and triage until verdict.
- [ ] Active response and containment, not only escalation.
- [ ] Ongoing recommendations and remediation guidance to reduce future risk.

24/7 "eyes on glass" operations

- [ ] Continuous monitoring is performed by live analysts, not on-call or follow-the-sun handovers.
- [ ] Clear proof that nights, weekends, and holidays are fully covered.

Governance, transparency & service control

- [ ] Clear service governance model with defined SLAs and responsibilities.
- [ ] Assigned points of contact (e.g. service management, MDR provider interface).
- [ ] Transparent reporting on incidents, performance, and service quality.

Regulatory & compliance awareness

- [ ] Demonstrable experience supporting regulated environments (e.g. healthcare, finance, public sector).
- [ ] Familiarity with relevant regulatory and compliance frameworks.
- [ ] MDR outputs (reports, processes) support audit and assurance needs.

Proven MDR experience & maturity

- [ ] MDR service has documented operational history, not a newly assembled service.
- [ ] Can demonstrate service maturity, continuous improvement, and case experience.
- [ ] Clear investment in MDR capabilities, tooling, and people over time.

CONTINUES ↓

Pricing model transparency

- [ ] Pricing model is clear and predictable.
- [ ] Costs are based on understandable drivers such as users or endpoints, not opaque log volumes.
- [ ] Ability to scale pricing as the organisation grows without complex recalculation.
- [ ] Quality over price weighting.

Must-have: MITRE ATT&CK alignment & threat coverage transparency

- [ ] The provider explicitly uses the MITRE ATT&CK framework as a foundation for detection engineering and threat coverage.
- [ ] Detection capabilities are mapped to MITRE ATT&CK tactics and techniques, not just individual alerts.
- [ ] The provider can demonstrate measured MITRE ATT&CK coverage (e.g. percentage of techniques covered), based on real detections and use cases.
- [ ] Threat detection prioritisation is aligned to attack behaviour and kill chain progression, not raw log events.
- [ ] Incident reports and dashboards provide ATT&CK based insights, clearly showing:
  - Which attacker techniques were observed.
  - How far the attack progressed.
  - Which techniques were blocked, contained, or mitigated.
- [ ] The provider uses MITRE ATT&CK to identify detection gaps and continuously improve coverage through new use cases and threat hunts.
- [ ] MITRE ATT&CK mapping supports board-level reporting, regulatory discussions, and risk-based communication.

Are you ready to take the next step?

Procuring an MDR service is a strategic decision that requires careful evaluation. A modern MDR service should:

Be built around XDR	Cover a broad attack surface
Enable automated and rapid response	Contribute to long-term improvement

Use the checklist in this guide to define clear requirements, avoid common pitfalls, and select a partner that operates as an extension of your organisation.

A structured procurement approach

For services like this, we recommend a two-stage process.

Stage 1: pre-qualification

Define baseline requirements for a provider. In addition to functional criteria, consider organisational certifications (e.g. ISO 9001, ISO 22301, and ISO 27001) and MDR-specific certifications (e.g. SANS GIAC).

Stage 2: detailed proposal phase

Shortlist three qualified providers and invite them to respond to detailed procurement documentation. This approach reduces administrative burden while improving proposal quality and final outcomes.

Suggested next steps

1. Define your requirements (for example, IT, IoMT and/or OT coverage, regulatory obligations).
2. Launch an RFI or RFP process using the checklist as your framework.
3. Request live demonstrations to assess practical delivery capability.
4. Engage security experts to explore how an MDR service can be tailored to your organisation.
5. Use customer references to assess your chosen provider before you sign a contract.

☑ Recommendation

Structure your procurement process to prioritise capability, measurable outcomes, and long-term partnership potential, not simply pricing or technical features.

Why consider Conscia's MDR service

When selecting a partner, the difference often lies in execution. Conscia delivers a modern MDR service built on measurable outcomes, deep technical expertise, and minimal operational friction. Our MDR service combines advanced detection and response technology with experienced analysts and clearly defined processes. Here is what sets us apart:

Rapid response & extensive coverage

Our detection and response capability covers more than 90 percent of the MITRE ATT&CK framework. Using leading XDR technology, we can act within minutes – not hours.

Proactive protection as standard

We focus not only on detecting attacks, but on stopping them. Our MDR analysts are authorised to act immediately according to predefined playbooks, reducing the risk of impact.

Low operational burden

You are not overwhelmed with unnecessary alerts. We provide fully analysed, relevant, and actionable insights – and involve you only when required.

Support for both IT & OT

Whether you operate in manufacturing, healthcare, or the public sector, we secure your entire environment – from cloud platforms to industrial networks.

Continuous improvement

You receive regular improvement recommendations, monthly reporting, and access to senior expertise that understands your environment. Our service evolves with you – not alongside you.

A complete security ecosystem

We also provide threat hunting, digital forensics, exposure management, log architecture services, and brand monitoring – allowing us to act as a comprehensive security partner when needed.

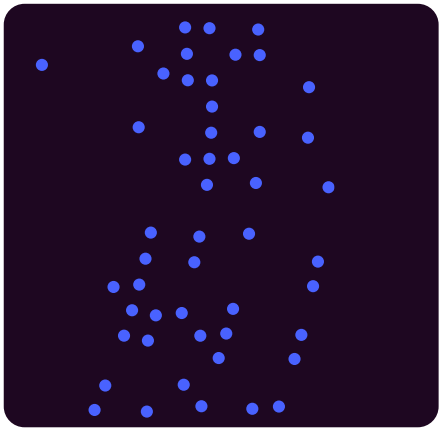
Clear delivery model

We deliver according to defined service levels, with dedicated service management and clear communication channels. Our services are designed to work in practice – not just on paper.

About conscia

Conscia designs, builds, secures and operates mission-critical infrastructures in cyber-security, networking, hybrid cloud and observability. With security as the foundation, we provide the conditions for sustainable digital development.

We call it *Secure progress.*



Conscia Headquarters
Conscia A/S
Kirkebjerg Parkvej 9, 2. sal
2605 Brøndby
Denmark

Contact
+45 70 20 77 80
conscia.com

Conscia
Secure progress