Integrity360

your **security** in mind

Aegis MDR

Eliminate threats across your organisation with enterprise-grade MDR Service from the European cyber security leaders

Introduction

Aegis MDR is Integrity360's open vendor detection and response service, designed for organisations seeking enterprise-grade protection against evolving cyber threats.

Combining expert-led threat detection, automation, and threat intelligence, the service delivers continuous detection and response — without the noise or operational overhead.

It integrates seamlessly with your environment, not disrupts it, and is backed by experienced analysts who understand context, not just indicators.

According to ENISA, Europe faces a cyber security talent shortage nearing 1 million professionals — underscoring the need for effective solutions that elevate security maturity and reduce risk without increasing pressure on in-house teams.

The problems

1. **Evolving business requirements meet evolving threats** – new and multi-vector threats that bypass defences and evade detections – this requires constant evaluation and enhancement of threat detection capabilities.
2. **High cost to build a mature 24x7 SOC** - with all the necessary specialised skills like threat hunting and threat content development, security analysts and incident response specialists.
3. **Pressure and load on in-house resources due to large volumes of alerts and who usually wear too many hats** - where alerts and incidents triage, investigation and escalations can overwhelm them, leaving limited capacity for more strategic initiatives.
4. **Stalled projects and slow technology adoption with competing priorities and urgencies within the organisation,** it's common to see projects freezing midway through, or never reaching the finish line, leading to security gaps, complex workflows, overspending and suboptimal operations.
5. **Compliance and regulatory demands continue to grow** – such as DORA and NIS2.
6. **Cyber security skill gap** – increasingly difficult to hire and maintain the right talent.
7. **Tool sprawl, too many suppliers, too many services** – consolidation of tools, technologies, and services is essential to reduce operational inefficiencies and procurement complexity.

Integrity360 Managed Threat Detection & Response Services

Aegis MDR service provides around-the-clock threat detection, investigation, and response across your digital environment. Built based on a layered architecture of telemetry, analytics, automation, and expert-led operations, it delivers real-time visibility into malicious activity and supports rapid containment and remediation.

The service integrates seamlessly with existing infrastructure including current threat detection solutions and leverages threat intelligence, behavioural analytics, and automation to reduce noise and prioritise threat alerts. With coverage across cloud, endpoint, network, and identity layers, MDR helps organisations stay ahead of evolving threats without the operational complexity.

Modular

We integrate modern threat detection technologies into one consolidated service, to build the widest threat detection coverage by bringing together EDR, NDR, CDR, ITDR, XDR and SIEM capabilities into a powerful, modular service that scales with your business requirements, risk posture, and budget constraints – without the operational overhead on your teams.

Transparent

Our MDR service provides you with all the assurance you need to be confident of the level of protection and coverage your organisation receives - access tickets, cases drill-down, detections data and metrics, and SLAs, ongoing insights, and even pricing model.

Always evolving

Dedicated detection engineering and threat content development, new detections to keep up with evolving threats, new platform features, continuous development to the service scope and capabilities, and defence improvement and advisory delivered as part of the service to help you strengthen your security controls, fill detection gaps, and improve your overall risk posture.

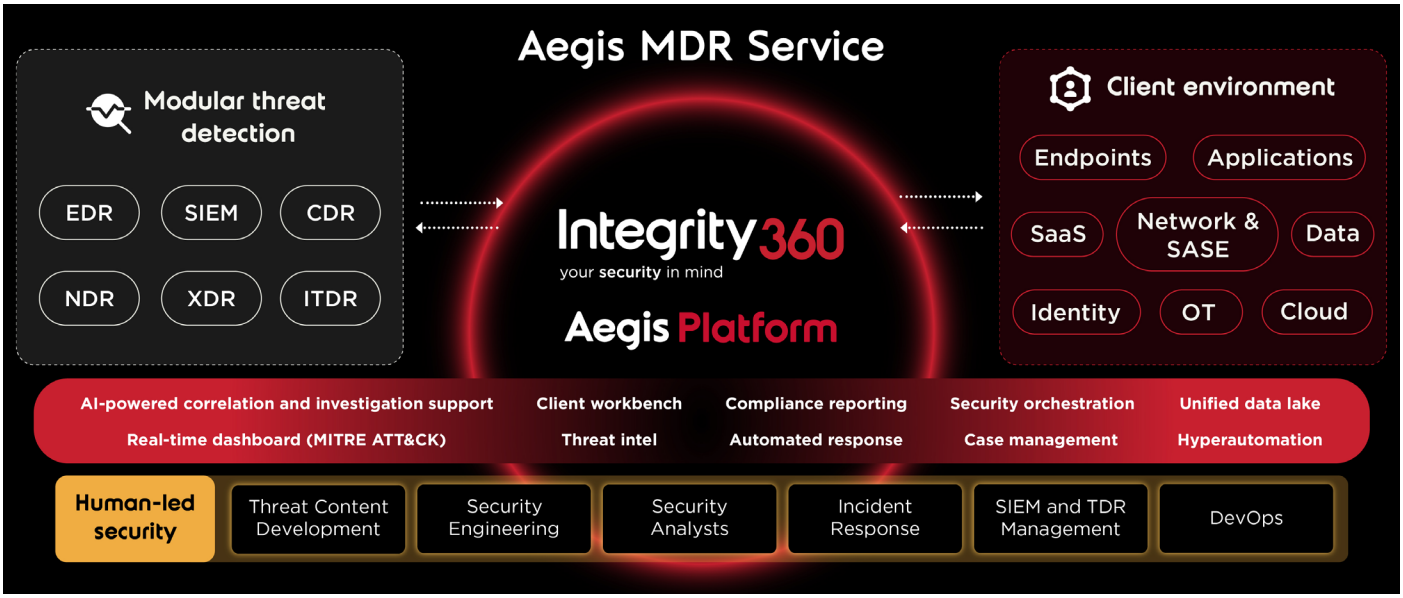
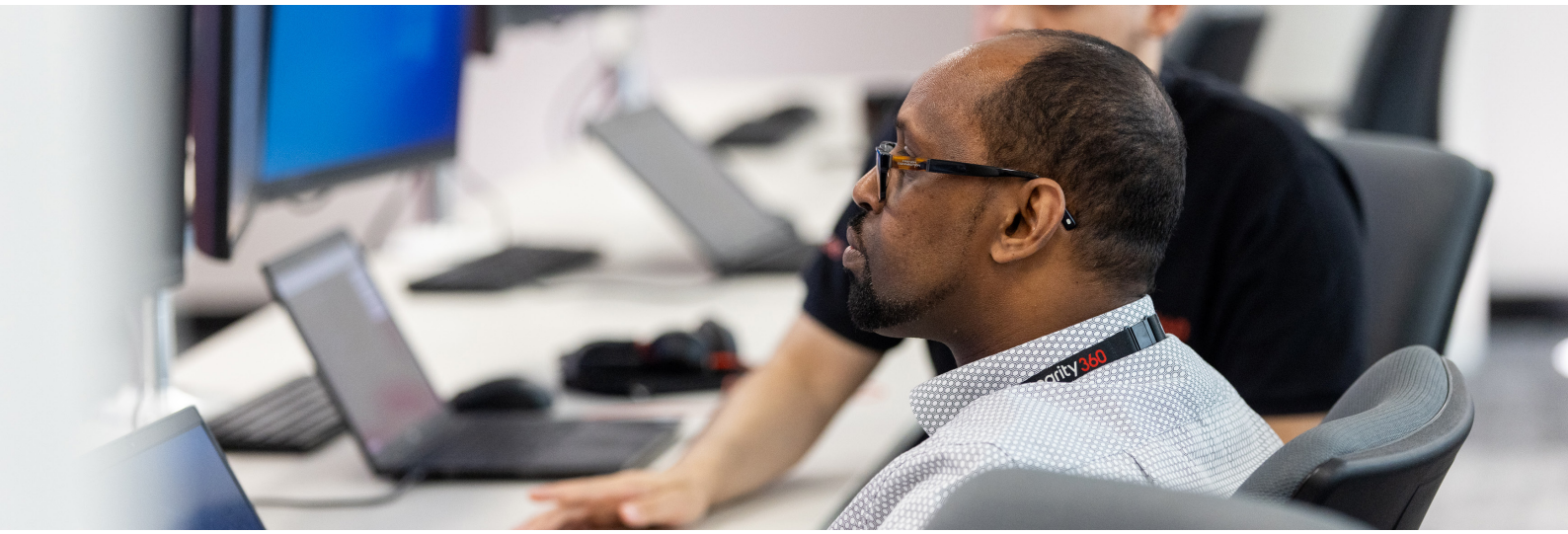


Figure 1: MDR service overview

Benefits of Aegis MDR

- **Enhanced threat visibility and protection:** Gain continuous insight into malicious activity across endpoints, cloud, network, and identity layers — without relying on fragmented tools or manual correlation.
- **Faster response times:** Automated workflows and expert-led triage reduce the time between detection and response, helping limit the impact of threats.
- **Reduced operational burden:** Security teams avoid alert fatigue and manual investigation overhead, freeing up time to focus on strategic initiatives.
- **Context-rich investigations:** Threats are analysed with environmental context, enabling more accurate prioritisation and reducing false positives.
- **Seamless integration:** The service works with your existing infrastructure and telemetry sources, avoiding disruption and accelerating time-to-value.
- **Continuous coverage:** 24/7 monitoring and response ensures threats are addressed regardless of time zone or internal resource availability.
- **Security maturity acceleration:** Organisations benefit from advanced capabilities such as threat hunting and behavioural analytics without needing to build them in-house.
- **Compliance support:** Detailed reporting and audit trails help meet regulatory requirements and demonstrate effective security controls.



Service deliverables

1. Threat detection & monitoring

- 24/7 monitoring of client environments across endpoints, cloud, network, identity, data, and more domains
- Continuous detection engineering to stay ahead of evolving threats
- Behavioural analytics and anomaly detection to identify threats beyond signature-based methods
- Triage and investigation of security incidents by experienced analysts

2. Incident response

- Automated and semi-automated response actions and support to mitigate active threats
- Wide range of response actions covering endpoints, network connections, accounts, and cloud configuration changes
- Our NCSC CIR assured incident response service included in the service as standard

3. Threat intelligence

- Integration of global and proprietary threat intelligence sources
- Enrichment of alerts with contextual threat data to improve prioritisation
- Continuous updates to detection logic based on TI feed

4. Threat hunting

- Proactive threat hunting based on hypotheses and indicators of compromise (IOCs)
- Focused threat hunting to investigate a specific area of concern or based on intel
- Collaboration with client teams to validate findings and improve detection coverage

5. Platform management

- Remote administration for the TDR platforms and/or SIEM as part of the service
- Covering configuration and policy changes, and change and problem management
- Regular updates and patching and best practice assessment

6. Reporting & insights

- Scheduled reporting on threat activity, incident trends, and service performance
- Executive summaries and technical deep dives tailored to stakeholders needs
- Access to Integrity360 client workbench for real-time visibility into MDR operations, dashboards, threat intel reports, and more

Service and platform architecture

Aegis MDR reference architecture

Wide compatibility with your existing technology investments

Our MDR service doesn't require you to throw away significant investments you have already made – you can "bring-your-own-tech" due to the following key characteristics of our service architecture:

Open vendor ecosystem supporting the industry leading threat detection platforms.

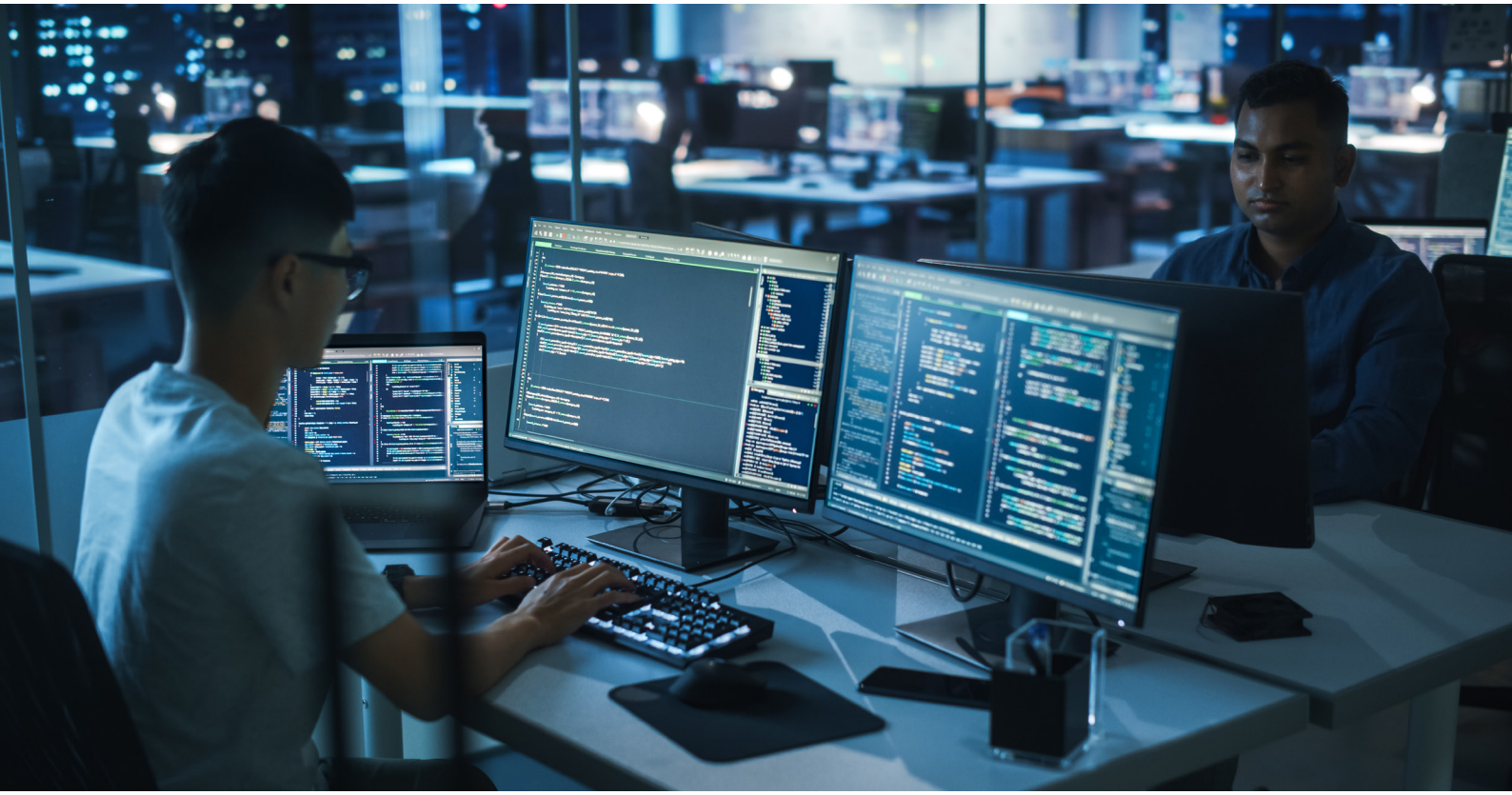
Platform service flexibility giving you the choice of letting us fully manage your platform or keep the platform support in-house.

Best-of-breed security integration so you don't need to replace your own EDR or CDR, for example.

Efficient security telemetry with optimised log ingestion from your estate, ensuring full detection coverage without excessive data collection.

Response action integration with security solutions you already have to enable effective response.

Security orchestration & automation focused on conducting effective threat response actions.



Aegis MDR platform

A centralised platform is pivotal to provide a single standardised environment for our security analysts to monitor and investigate detected threats, collaborate with wider team members in our SOC and with the customers, provide standard playbooks for different use cases, automate and streamline incident investigation and ultimately facilitate the response and remediation of incidents for faster MTTD and MTTR.

Integrity360 Managed Detection & Response offers the widest cross-platform compatibility in the industry. This is enabled by abstracting the advanced service capability from the underlying detection and response service through integration with our leading MDR platform.

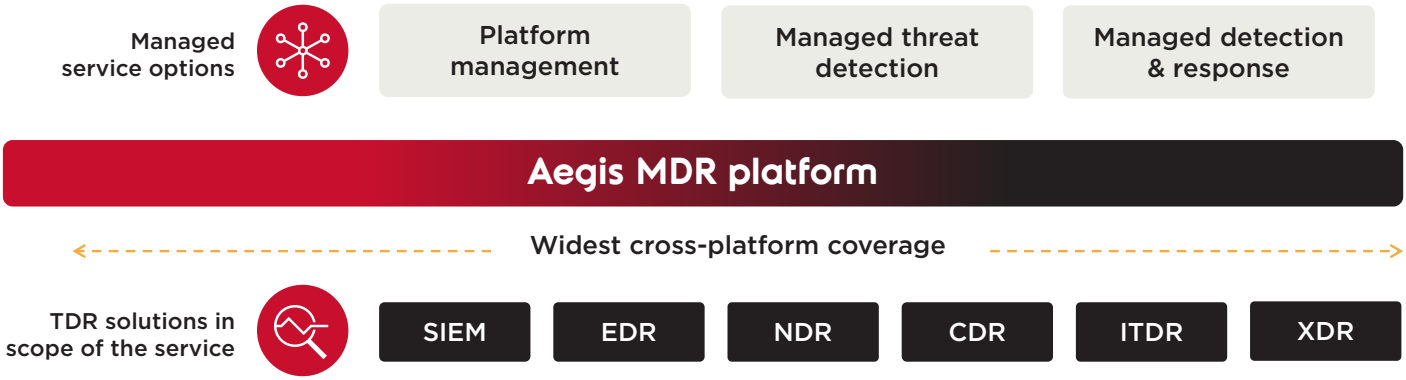
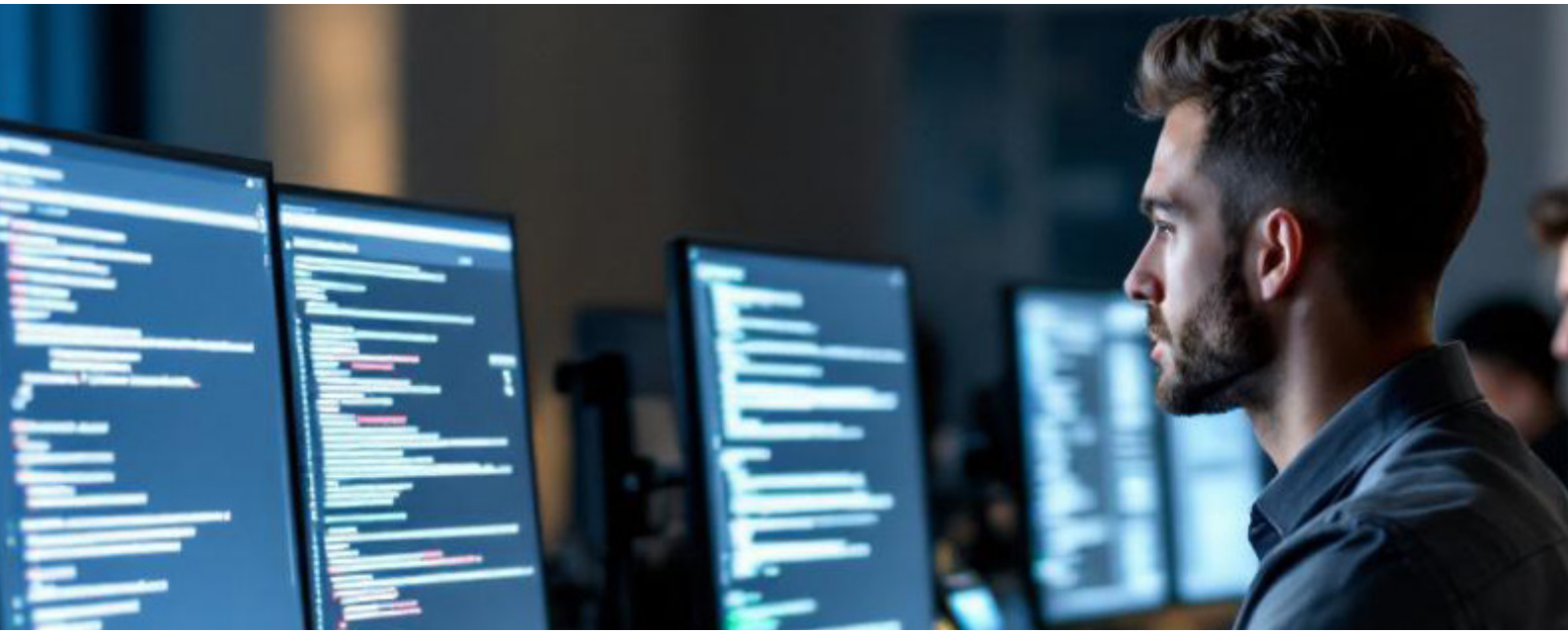


Figure 2: Service modules and coverage

Compatibility of new platforms can be achieved by inbound alert integration and outbound response integration, usually in the form of standard APIs, or other similar mechanisms. This enables the MDR service to take advantage of best-of-breed detection and threat content developments and avoids customer having to abandon previous significant investments in order to avail of the service. Typical platform categories compatible with Aegis platform include:

- **Security Information & Event Management (SIEM):** Most of the major SIEM platforms used for log ingestion, security event correlation and advanced threat analytics. SIEM ingests and correlates log and telemetry data from across the client's environment, then by applying advanced analytics and rule-based logic, it identifies anomalous behaviours, policy violations, and potential indicators of compromise in real time. Our threat content development team continues to develop new SIEM detection rules based on threat intel, while our security engineering team looks after the platform and detections tuning.

- **Endpoint Detection & Response (EDR):** All leading solutions to detect and respond to threats on endpoints (workstations and servers, whether appliance based, virtual or in the cloud). EDR is considered a fundamental element of any organisation's threat protection solutions, and the most widely deployed.
- **Network Detection & Response (NDR):** Platforms designed to automatically baseline normal traffic flows in the network (whether encrypted or unencrypted) and using advanced AI and Machine Learning to recognise and alert on anomalous traffic flows, in addition to recognise suspicious tunnelled connections, and other network based IoCs.
- **Cloud Detection & Response (CDR):** A cloud-native security capability that delivers real-time threat detection, investigation, and automated response across public, private, and hybrid cloud environments. Unlike traditional tools designed for static, on-premises infrastructure, CDR is purpose-built to address the dynamic, ephemeral nature of cloud workloads, APIs, containers, and serverless functions, in addition to identifying cloud users suspicious behaviours and other cloud related threats.
- **Identity Threat Detection & Response (ITDR):** Solutions that focus on digital identities - the current perimeter in modern enterprise environments. ITDR continuously monitors identity systems such as Active Directory, Entra ID, and cloud identity providers to detect Identity related threats, such as lateral movement and compromised accounts. ITDR focuses on behavioural anomalies in user and machine identities, enabling real-time detection of compromised accounts and insider threats.
- **Extended Detection & Response (XDR):** Platforms that collect and automatically correlate data across multiple security layers – email, endpoint, server, cloud workload, and network to provide a more holistic and integrated threat detection capability. XDR platforms usually include embedded SIEM capabilities, covering multiple areas of the client environment.



Service highlights

Threat hunting ensures that threat detection capability provided by the technology solution is augmented with proactive, human-led threat hunting to unearth threats that may have managed to bypass all existing threat prevention and detection mechanisms. There are three main types of threat hunting conducted: proactive, reactive and focused.

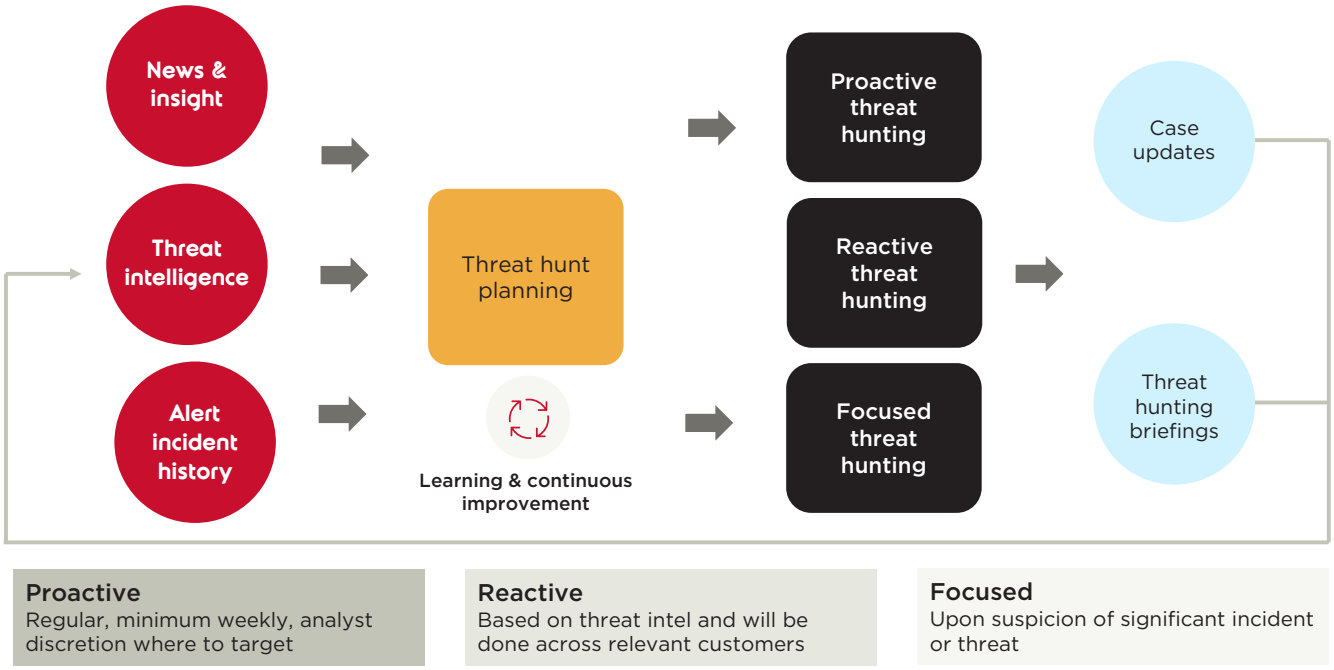


Figure 3: Threat hunting process

Aegis client workbench: Complete transparency for your internal teams

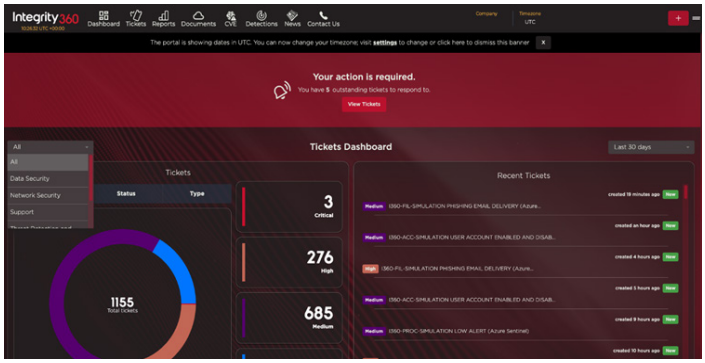
Transparency is one of the core advantages offered by our service. Integrity360 provides your security team with complete transparency over our security teams' activities via the client workbench, showing real-time dashboards, where users can view alerts and reports on security incidents, cases and service activities, giving you total visibility across our service engagement.

For example, **you can monitor the state of the MDR service in real-time through an online security posture dashboard or service overview dashboard.**

You also get access to threat intel briefings, detections catalogue, MDR service reports, and an expanding collection of security resources

Other information you can view through the dashboard includes:

- Alerts by product (source)
- Cases by stage and by severity
- Top alerts detected
- Top MITRE ATT&CK tactics detected
- Top alerts by host
- Top alerts by network or action



AI-powered security operations

Our MDR service integrates AI across the security incident lifecycle

- **Detections:** Multiple detection technologies that use Machine Learning and a combination of LLMs and SLMs for telemetry analysis to refine detection reliability.
- **Triage:** We accelerate triage phase by using an AI security assistant that adds further context and insights to cases during triage.
- **Investigation:** We use AI agents to increase the analysts efficiency and expedite the investigation process.
- **Response:** Gen AI can be used to produce remediation steps and/or scripts for specific use cases.

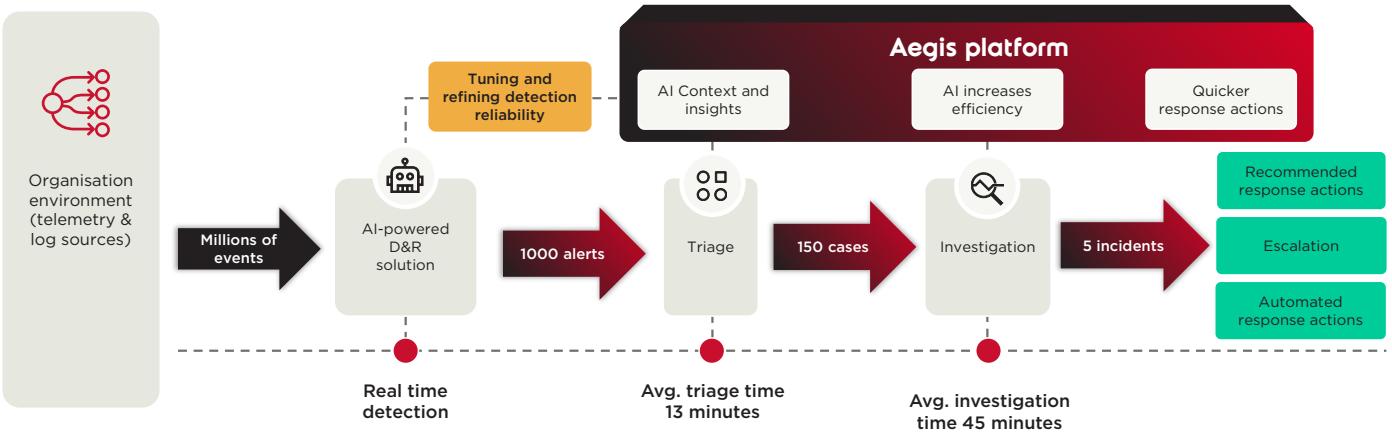


Figure 4: AI enhanced incident lifecycle example

Six weeks time-to-value

Aegis MDR service onboarding approach is designed to deliver fast time-to-value. In as little as six weeks, the base MDR service, with endpoint threat detection, alerting, and response can be up and running and delivering security value to your organisation.

The components that may require more time to build, complete integrations, and further tuning (such as SIEM or XDR) run as a parallel workstream, so that the full service comes into effect once all have been completed.

We understand that onboarding to an MSSP can be an extra workload for you in the short term. For this reason, we ensure that you have full visibility of dependencies during onboarding so they can be managed. To ensure the successful delivery of the service stand-up and an efficient time-to-value, project management and governance are included as part of our service.

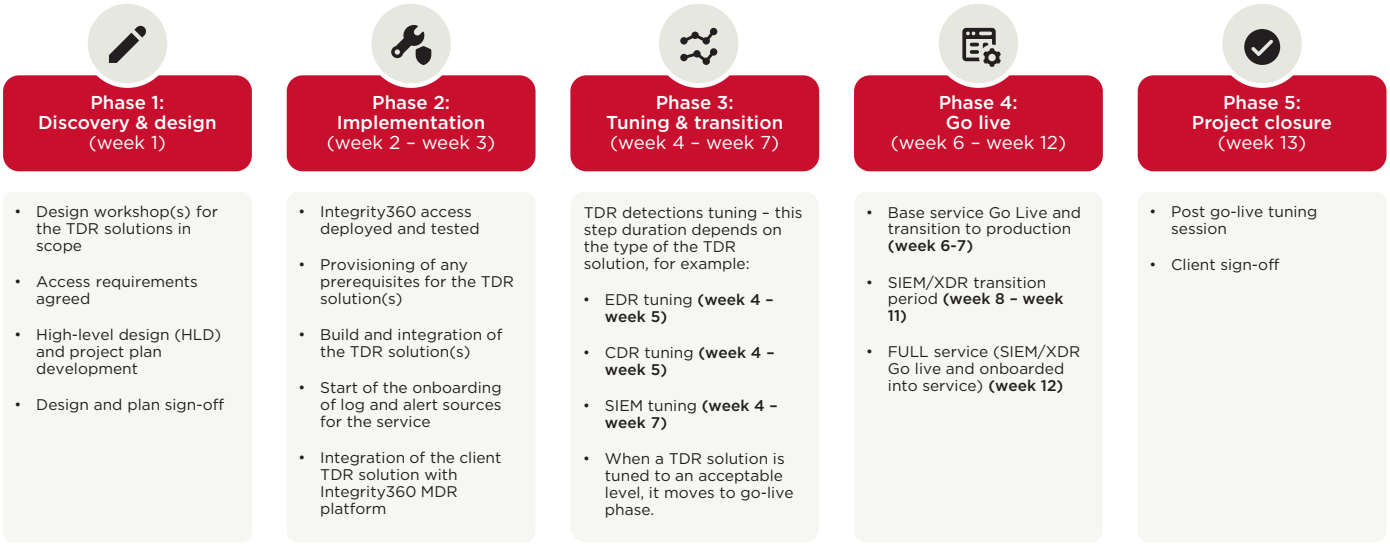


Figure 5: Onboarding standard plan

Continuous improvement

Defence improvement and MDR advisory – both are standard service deliverables – highlight weaknesses or areas of improvement in our clients' security controls and detection coverage, for continuous risk posture improvement.

Service Delivery Management (SDM) act as a single point of contact from onboarding and throughout the entire service lifecycle to ensure we deliver maximum value as part of the service. The SDM is responsible for the assurance of service deliverables, service innovation and continuous improvement, client escalation management, value demonstration and facilitation of service reviews to ensures that each customer's individual requirements are fully addressed.

The Integrity360 MDR difference

Wide compatibility with existing investments: We can layer the service over your existing security technology investments.

Quick time-to-value: Our onboarding approach is designed to deliver fast time-to-value in as little as 6 weeks.

Simple transparent cost model: Easy to understand, track and predict costs.

Continuous improvement: Regular reviews to highlight opportunities to improve your security posture and detection capabilities.

Breadth of security expertise: Threat intelligence, threat hunting, threat content development and incident response expertise as part of the service.

Security partnership: We act as an extension of your team, working as your security partner and advisor, from design and procurement to 24/7 security operations.

Risk-oriented use cases: Protect against the most material threats to your business, based on your threat profile and utilising threat-informed defence.

End-to-end security specialist: We are a pure-play cyber security organisation. Cyber security is our core focus, with cross-portfolio synergies.

Next steps

As security threats grow more complex, your organisation needs to be at the top of its game to stop them. Integrity360's MDR service provides your security team access to people, processes and technology, so that they have everything they need to detect and respond to advanced threats in and outside of business hours.

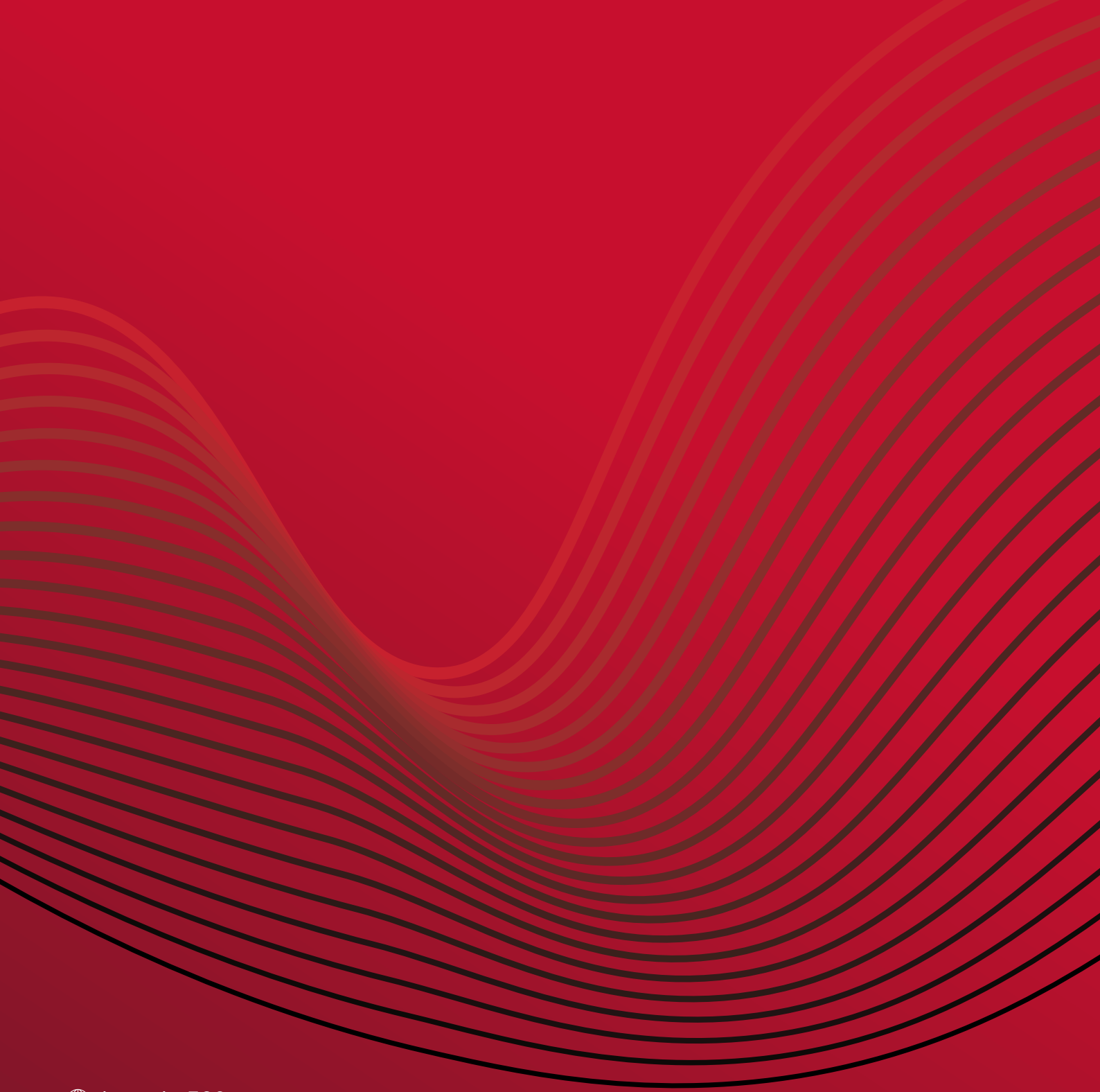
Our team will help you to identify the risks specific to your environment and develop a detection and response strategy to mitigate those risks. We will also provide you with complete visibility over the real-time effectiveness of the service so that you can rest assured that your environment is kept secure.

Why choose Integrity360?

Choosing a cyber security provider is a critical decision for any business. Here are just a few reasons why you should choose Integrity360:

Integrity360 is Europe's leading cyber security and PCI specialist, with offices across the UK, Ireland, Bulgaria, Italy, Sweden, Spain, Lithuania, Ukraine, across Africa, and the Caribbean. **The company operates six Security Operations Centres (SOCs) in Madrid, Dublin, Sofia, Stockholm, Rome, and Cape Town.**

With over 700 employees and an expert team of over 500 dedicated cyber security professionals, **Integrity360 offers a full suite of professional, support, and managed security services.** These services cover every aspect of cyber risk management, from identification and prevention to detection, response, and recovery. Whether working independently or alongside an organisation's internal teams.



integrity360.com

info@integrity360.com

Dublin, Ireland
+353 1 293 4027

Ludwigsburg, Germany
+49 71 414 879 980

Sofia, Bulgaria
+359 2 491 011 0

Cape Town, South Africa
+27 21 100 377 4

London, UK
+44 2033 973 414

Madrid, Spain
+34 910 767 092

Stockholm, Sweden
+46 8 514 832 00

Johannesburg, South Africa
+27 860 625 673

Kyiv, Ukraine
+38 504 701 125

Zurich, Switzerland
+41 44 4213 336

Paris, France
Rome, Italy
Vilnius, Lithuania