Datasheet

# Adarma MDR Service

### You're already a target.

Adversaries are monetising their assets:  selling credentials, methods – and infrastructure. Ransomware-as-a-Service demonstrates that even individuals can now act at scale: it's not just the biggest names in the crosshairs.

Opportunistic attacks against organisations of all sizes are now a valid business model for adversaries. Ongoing headlines show that protective controls don't offer guaranteed safety against cyber threats; and when protection fails, damage is measured by time taken to detect and contain. The longer your exposure, the greater the incident impact.

Our Managed Detection and Response (MDR) service works with you to give assurance – and reassurance – that your organisation has effective controls in place to reduce the risk of a major cyber incident.

It provides 24x7 expert monitoring, investigation, and containment, minimising the time taken to detect, investigate and contain threats by up to 80% over traditional MSSP approaches.

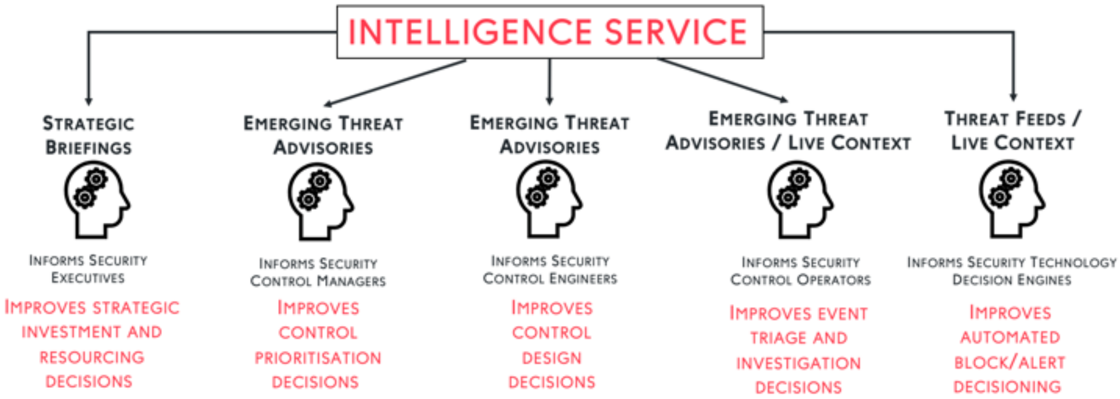
## Adarma MDR Service

Adarma offers a pre-defined, rapidly deployed MDR capability derived from the NIST framework. Designed, built, and refined by industry veterans to minimise your effort and maximise operational effectiveness. Four components working together to provide detection and response:

### 24x7 Threat Intelligence

Strong intelligence is the foundation of an effective security service, providing material crucial to the effective operation of each system component. Adarma's centralised intelligence improves security decision-making – sorting, selecting, and curating via multiple sector sources from the state level through to your individual organisation.

Powered by cross-industry expertise, our strategic briefings, operational advisories and technical threat assessments present a current view of your threat landscape, while curated machine-readable threat intelligence (MRTI) feeds supply up-to-the-minute information on known adversary infrastructure and malware.


INTELLIGENCE SERVICE
Strategic Briefings
Informs Security Executives
Improves strategic investment and resourcing decisions
Emerging Threat Advisories
Informs Security Control Managers
Improves control prioritisation decisions
Emerging Threat Advisories
Informs Security Control Engineers
Improves control design decisions
Emerging Threat Advisories / Live Context
Informs Security Control Operators
Improves event triage and investigation decisions
Threat Feeds / Live Context
Informs Security Technology Decision Engines
Improves automated block/alert decisioning

"The purpose of INTELLIGENCE is to INFORM – it's OBJECTIVE to IMPROVE cyber security DECISIONS."

Datasheet

# Adarma MDR Service

## 24x7 Monitoring

The longer it takes to detect a threat, the longer it takes to make your organisation safe… and the greater the damage to your assets. Operating from within our ISO 27000 accredited Security Operations Centre, our analysts monitor around-the-clock against all forms of cyber threat to your organisation and business sector.

- We're flexible and accommodating: we understand your processes and architecture are unique, and we're ready. We can integrate with any log, feed, or data source — on premises or in the cloud.
- We focus on accuracy and transparency: rapidly identifying threats amongst legitimate activity. Every outcome helps adapt to threats and enhance our controls, reducing potential harm by driving down time to detection.
  - Every action we take to protect your business is visible to you. You can watch us deliver on our promises in real time.
- We've got the talent: our team draws on decades of experience with security monitoring design, setup and operation.
- We constantly improve the service: reviewing and refine our controls based on the general and specific threat landscapes. They're hand-crafted by experts - rigorously defined, ruthlessly tested, and swiftly deployed via in-house Adarma technologies.
  - All the logic, controls, and tuning remain under your control and available to use — forever.

An MDR service that lives up to promises requires expertise and experience across a range of cyber security disciplines, a rare combinaton of knowledge and intuition.

**MONITORING & DETECTION**

Distinguishing threats among legitimate activity and following IOC traces to the target requires skill, knowledge, and precise judgment. Doing it quickly and accurately takes expertise.

**Our analysts are experts.**

**INVESTIGATION & HUNTING**

Going from detection to discovery takes expertise.

Proactively hunting for live threats is an artform. It combines deep knowledge of threat tactics and techniques with a familiarity diverse enterprise technologies and logs, while performing ad-hoc data analysis at scale.

**Our analysts are artists.**

## 24x7 Threat Hunting & Investigation

Automated detection controls aren't always be sufficient for novel threats or areas where controls have not yet been deployed. Adarma's analysts provide ad-hoc investigative capability in order to determine what needs escalation, and what can be noted and closed.

But investigation goes beyond known threats and incidents. Proactive hunting further reduces the risk of long-term infiltration or compromise of your systems. We regularly undertake exploration of activity inside systems and endpoints, searching for unknown threats, proposing hypotheses and creating new detective controls as an output.

SOAR tooling is a crucial part of our rapid investigative capability, but we know automation is a tool, not a replacement. We detect at machine speed — we execute with human insight and oversight.

### 24x7 Incident Response

When a threat is identified, we're already on hand to shut it down. Combining the machine speed of SOAR and the expertise of analysts, we can instantly take whatever action is needed to contain the immediate threat - disabling accounts, isolating devices, modifying firewall or proxy policies. Our custom tooling integrates with hundreds of technologies for containment, driving time to response down even further.

And once the threat's contained, we're there to support your next steps, providing context, information, and guidance to help you understand the incident and the impact – then organise your response until the incident's resolved. We're never more than an IM, call, or email away.

Together, these components give you expert round-the-clock monitoring, investigation, and containment.  Significantly reducing time to detect threats, minimising their opportunity to do harm. Doing everything possible to reduce risk to your organisation and assets, making sure being a target doesn't mean becoming a victim.

> THE greatest advantage a **defender** has over an **attacker** is superior knowledge of their environment.
>
> It's easy to **miss the value** of possessing direct, relevant intelligence about your organisation to **defeating attacker** activity.
>
> David Calder, Chief Product Officer

## Deploying and Managing the Service

During the initial enrolment period we work collaboratively to define and agree on the scope of intelligence and monitoring requirements, threat response procedures and reporting.  We deploy detection engineering and controls, onboarding the data feeds to be monitored. We'll maximise the value of your data and ensure the best fit of controls against your threat profile, bounding performance via agreed SLAs and KPIs.

- Our technical quality and attention to detail is unmatched – we onboard new customers and bring them under protection quickly without compromising either.
- Our bespoke control management system gives full visibility into all deployed controls, and our self-service reporting feature lets you track performance against service SLAs and KPIs - including changes to these metrics over time.
- We take care of the management of the service over the lifetime of the agreement. Platform and agent management is as vital as threats management – as targets, endpoints, and threats change over time, controls and configurations can drift into failure.

Datasheet

# Adarma MDR Service

## Why Adarma?

**Full transparency. True collaboration.**

We don't just ask you to trust us with your defence: we demonstrate 24/7 why you can. Everything we do is fully visible. Totally transparent. Entirely accountable. There's auditable, evidential, meaningful data for every piece of information our analysts generate. Nothing's locked away inside a black box.

Cross-industry experience: Our experience crosses boundaries across industries, verticals, and enterprises.

> **"Security relies on trust.**
>
> We operate our security operations function in partnership with Adarma - their commitment to transparent and collaborative working is one we can rely on. As our business grows and our threat profile changes, we need a partner we can trust to change and adapt with us."
>
> – Clarks

Organisational Agility: We're large enough to deliver excellence, and robust enough to offer proven methodologies for success. But we'll never be too big to understand each customer as an individual and adapt as necessary to meet your needs.

Flexibility: Adarma's services fit to your people, processes and technology rather than demanding you change operations to fit our service. Our team works with yours to ensure we understand your particular configuration, enabling us to integrate and monitor any log, feed, or data source, on premises or in the cloud.

Passionate Expertise: our analysts and engineers come from dedicated security backgrounds. and their passion to go beyond the boundaries of their discipline achieves a deeper, broader security perspective than you'd find in typical MSSPs. Growing their skills isn't an empty exercise. It's because working to keep your assets secure helps fulfil the Adarma mission: making the world a safer place.

UK based: Our entire operation is based in the United Kingdom, keeping your supply chain short and increasing your cyber resilience. If you ever need to drop in and see the service running for yourself – you can.

If you are considering how best to protect your organisation and would like to know more, our expert advisory team would be delighted to talk to you: enquiries@adarma.com

### About Adarma

We're one of the largest independent security services companies in the UK. A business formed and run by experienced senior security leaders, we know security and how to deliver real value in the real world. This is why our clients are successful FTSE 350 organisations from all industry sectors.

Adarma delivers innovative tailored solutions for some of the world's biggest companies. Our teams are a diverse group of technical experts and consultants, all with the same objective and united by the same goal: to help our clients prepare for attack and stand side-by-side with them when it happens.

Helping make the world a safer place.

www.adarma.com