Incident Response Retainer Service

Fast, Precise and Committed Incident Response

When a security incident occurs, the clock starts ticking, giving you a small window to respond. In a crisis, you need an expert team of incident responders who can act swiftly, with precision, and seamlessly leverage your existing tools. That's where Adarma's Incident Response service comes in.

Always ready, our incident response team of dedicated incident response specialists are prepared at a moment's notice to support you in defending your digital estate and to help you minimise the impact of a cyber incident. Backed by an experienced multidisciplinary team of Security Operations Centre (SOC) experts, our Incident Response service provides you with dedicated cyber defenders.

Addressing the Gap in Incident Response

Traditionally, organisations have only had two options to choose from; expensive incident response consultants, or, limited containment from their Managed Security Service Provider. Even having both options can leave organisations suffering an incident with a worrying gap in their response speed and capability.

Our approach is different. We unite our Managed Security and Incident Response into a single, coordinated capability – so when a threat emerges, our experts can act fast, minimise disruption, and take control from start to finish.

Incident Response Expertise

Our elite incident response team will support you with:

- Onboarding and Incident Planning
- Incident Tracking and Coordination
- Briefings, Daily Updates and Urgent Findings
- Threat Hunting
- Threat Containment
- Malware Sample Analysis
- Malware Eradication
- Incident Reporting and Closure

Our team is also backed by continuous monitoring from our UK-based SOC.

By combining the Adarma Security Operations platform, Socket®, with a skilled team of experienced responders, we deliver a comprehensive incident response service.

Incident Response Retainer

Adarma's Incident Response Service offers a retainer that provides pre-paid blocks of hours for specialised incident response and recovery support. With flexible options for both proactive and reactive services, we prioritise rapid response times and give you direct access to our highly skilled incident response professionals. Any unused hours are not lost – they can be easily applied to Adarma's wider range of consultancy services.

What's Included in Adarma's Incident Response Service

Pre-Incident Planning:
Proactive planning with an Adarma Incident Manager, and the publication of a shared incident plan acts as a guide during major events. We do this as part of the onboarding process, and it doesn't eat into your contracted hour allowance.

Technical Incident Management:
Our team takes charge of the technical aspects of incident response, ensuring a swift and efficient response to mitigate the impact effectively.

Threat Intelligence:
Our robust threat intelligence capabilities augment your incident response and proactively identify potential threats and adversaries' next steps.

Hunting:
Integrated proactive threat hunting helps to identify and neutralise potential threats and combat new adversary activity before they inflict significant damage.

Investigation:
Expert in-depth investigation and analysis, supported by our SOC team brings clarity to the root cause of incidents. This allows us to deal with the problem at source and adapt to new challenges to gain the edge.

Containment and Eradication:
Taking immediate action to contain the incident and eradicate any existing threats.

Reporting:
We provide comprehensive incident reports that encompasses key findings, lessons learned, and recommendations for future incident response improvements.

Why Adarma for Incident Response?

Speed and Efficacy:
Our highly skilled team and proven methodology enable faster and more efficient incident response, minimising business disruption and costs. Our maximum initial response time service-level agreement is three hours.

Intelligence-led Response:
Our incident response team is supported by an experienced multidisciplinary SOC capability comprising analysts, hunters, security engineers, and threat intelligence experts, ensuring a swift and effective containment of incidents through a knowledge-driven approach.

Personalised Approach:
We collaborate with you to develop a customised plan that aligns with your operational needs, existing investments, and internal resources.

Augmenting People and Process:
We leverage your existing technology infrastructure, adding our technical response capabilities, incident recovery support, hunting, forensics, and containment expertise, which are supported by our Threat Intelligence and SOC teams, enhancing your overall cyber defences.

Cybersecurity Experts:
As industry-leading specialists in threat detection, investigation and response services, we are committed to mitigating risk and maximising the value of your cybersecurity investments. Our team of dedicated cyber defenders work hand in hand with customers to deliver measurable results, ensuring your organisations stays protected and resilient.

Meet the team

Philip Ridley

Head of Security Response

With over 20 years of experience in cybersecurity and incident response, Philip leads Adarma's incident response capability. Drawing on his background in cybercrime investigation and threat management, he works closely with customers during high-stakes security incidents to deliver fast, effective response and long-term resilience.

Connect with Philip on LinkedIn

> **In incident response, speed and context are everything. At Adarma, we bring clarity to chaos – helping our customers act fast, stay informed, and emerge stronger."**

Who We Are

Adarma is a trusted partner in security consulting and co-managed security operations. We work as an extension of your team to help simplify operations, build resilience, and deliver measurable outcomes.

We specialise in 24/7 threat detection, investigation and response, security consulting, and engineering support for large, complex organisations in high-risk sectors. Our platform, Socket, enhances automation, insight, and orchestration – empowering teams to act faster and more decisively.

Technology-independent and customer-led, we integrate with platforms like Microsoft, Splunk, CrowdStrike, and Google SecOps to maximise the return on your security investments. Together, we build stronger business resilience and deliver measurable security outcomes that matter.

Engage with Adarma Incident Response

Book a strategy session with one of our solution consultants and receive a complimentary Threat Landscape Report tailored to your industry.

Book a consultation