Digital Forensics Incident Response (DFIR) Service

Fast, Precise, and Committed Incident Response

DATASHEET

When a security incident occurs, the clock starts ticking, giving you a small window to respond. In a crisis you need an incident response team that can act swiftly, with precision, and seamlessly leverage your existing tools. That's where Adarma's Digital Forensics Incident Response (DFIR) comes in.

Always ready, our DFIR 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 DFIR 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 and often basic containment at best from their Managed Service or MDR 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 teams to deliver seamless and effective incident response. When every second counts, you need a team of experts to move through the gears quickly and seamlessly, end to end, to limit the impact.

The Power of Adarma DFIR

Our expert incident response team are trained to assist with forensic investigation and incident response. We support you with:

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

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

By combining the Adarma Threat Management Platform with a skilled team of experienced responders, we deliver a comprehensive DFIR service.

Here is what it includes:

Adarma Incident Response Retainer

Adarma's DFIR service offers an Incident Response Retainer that provides pre-paid blocks of hours for specialised incident response and recovery services. With flexible options for both proactive and reactive services, we prioritise rapid response times, providing you with direct access to our highly skilled incident response professionals. Any unused hours are not lost, they can be easily used against Adarma's range of consultancy services.

1 **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.

2 **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.

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

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

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

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

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

BENEFITS OF CHOOSING ADARMA DFIR

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 SLA is 3 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 detection 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.

Engage with Adarma DFIR

To learn more about our DFIR service and to discuss how we can address your specific requirements, we welcome you to connect with an Adarma Client Director or email hello@adarma.com. Visit adarma.com/incident-response/ for additional information.

Trust Adarma to deliver exceptional results in your incident response and fortify your cyber resilience efforts.

About Adarma

We are Adarma, leaders in detection and response services. We specialise in designing, building and managing cybersecurity operations that deliver a measurable reduction in business risk.

Our team of passionate cyber defenders work hand in hand with you to mitigate risk and maximise the value of your cybersecurity investments. Powered by the Adarma Threat Management Platform and optimised to your individual needs, we deliver an integrated set of services that improve your security posture.

We operate with transparency and visibility across today's hybrid-SOC environments to ensure your business is protected as you transform, innovate and grow.