RelianceCyber

NCSC-Assured CREST Digital Forensics Incident Response (DFIR) Retainer

Service Definition

G-Cloud 15

Lot 3: Cloud Support

Contact Details

Email: contact@reliancecyber.com

Contact Number: +44 (0) 845 519 2946

Emergency Incident Hotline: +44 (0) 20 3872 9052

Assured Service Provider

in association with National Cyber Security Centre

Cyber Incident Response: Standard Level

CREST

Assured Service Provider

in association with National Cyber Security Centre

Cyber Incident Exercising

Contents

1 Incident Response Overview

Reliance Cyber's Digital Forensics Incident Response (DFIR) retainer provides immediate hands-on remediation, ensuring your team is supported during a cyberattack. Our retainer service includes immediate access to our experienced National Cyber Security Centre (NCSC) CIR Standard-assured, Security-Cleared (SC) DFIR Responders. This team will help to limit the damage caused by malicious actors and support speedy recovery, maximising the opportunity to emerge stronger and more secure.

This annual retainer service provides the reassurance that should an incident occur, you have immediate access to a team of experts ready to support you, taking both proactive and reactive steps to combat threats. The retained hours purchased will be used for both emergencies, such as a breach, and for unused hours to actively improve your security posture through incident-preparation workshops, simulations and training with our in-house experts.

1.1 Features

- 24x7x365 access to CREST (Reliance Cyber | crest-approved.org) registered, NCSC-assured incident responders.
- Preventative onboarding and threat modelling workshops, optimising monitoring, minimising weak points and providing recommendations before malicious actors can exploit these, maximising coverage from service outset.
- Proactive incident simulations to test against incidents ranging from common to complex scenarios.
- Remote incident response within a matter of hours, with optional on-site support available.
- Hands-on support to guide your team through the incident, with the key aim of minimising financial, reputational and operational damage caused to the business.
- In-house threat intelligence that is used by the DFIR team to assist in ongoing monitoring, rapid response and reporting.
- Legal and communications support referrals, specialising in the management of response activities across employees, customers and public relations during cyber incidents.
- Digital forensic investigation and analysis to understand the scope and impact of the intrusion.

1.2 Benefits

- Immediate access to incident response support capabilities and emergency response.
- Cost-effective and scalable capabilities available throughout the contract term, with the option to purchase more hours without the risk of price increases.
- Ability to repurpose unused time through either our incident response team or additional professional services.
- Enhanced visibility through log and network traffic examination to identify encrypted or exfiltrated data, determining its value and potential impact.
- Expert guidance throughout the response and recovery process, collaborating with internal teams and third-party contractors.
- Access to strategies encouraging ransom avoidance, allowing you to protect against ransom payment through assessment of data value and facilitating board decisions.

1.3 Outcomes

- **Timely recovery**: Swift restoration of public services and business operations following a cyber incident, minimising downtime and financial losses.
- **Data security**: Ensuring the security of citizen and sensitive data through swift expulsion of adversaries and implementation of protective measures.
- **Cost savings**: Avoiding costly ransom payments using public finances through expert assessment of data value and informed decision-making.
- **Compliance assurance**: Ensuring compliance with data protection regulations through thorough incident investigation and reporting.
- **Risk minimisation**: Identifying and addressing vulnerabilities to prevent future incidents and strengthen cybersecurity posture.
- **Confidence building**: Restoring stakeholders' confidence by demonstrating a proactive approach to incident response and preparedness.
- **Peace of mind**: Providing assurance and peace of mind through proactive incident response, ensuring readiness for any eventuality.
- **Improved preparedness**: Enhancing clients' readiness to handle future incidents through protecting what's vital and being resilient to incidents affecting non-vital assets.

2 Methodology

Reliance Cyber takes a proactive approach to incidents. During the onboarding phase of the retainer contract, identification and possible remediation steps are highlighted to reduce the risk of a cyber incident. Exercises are conducted to familiarise key stakeholders with the incident process. These exercises help identify contact and communication flows to streamline and mitigate the risk of process failure during an incident. Throughout the engagement, our incident responders are on standby to tackle issues and maximise our responsiveness.

2.1 Service Onboarding

To onboard and prepare your organisation for an incident, we conduct in-depth risk assessments, conduct routine system evaluations and employ advanced early-detection methods to minimise risks and safeguard your operations and services.

Onboarding will consist of:

- **Technical Workshop**. We will work with your technical teams to understand your entire IT infrastructure and create an overview of your roles, security, key assets, goals, plans, team integration and incident response protocols.
- **Management Workshop**. This is an educational and practical session designed for your organisational leaders. This aims to provide leadership with an understanding of how to handle potential security incidents effectively should they occur, as well as the process for contacting us.
- **Retainer Kick-Off**. Our incident response team will organise a kick-off meeting to introduce themselves to the key individuals within your organisation. This kick-off will finalise any planned engagements, such as requested workshops or simulations, that utilise your retained hours.
- **Supply of Emergency Contact Details**. We will supply the necessary contact information should an emergency occur, whilst documenting all key contact details from your organisation that we may need throughout the service lifetime.

We will also recommend using retained hours to take preparedness measures whilst onboarding and throughout the service's lifetime. Our experience has shown that proactive threat mitigation can reduce the number of emergency hours needed to respond to incidents.

2.2 Ongoing Support

Throughout the service, you will receive complete coverage of any incidents that may occur. Alongside this, we will work with your internal teams to understand how best to utilise any unused hours when no incident occurs.

Typical ongoing support throughout the service will consist of:

- **Ongoing Incident Management**. Our incident response team will be contactable 24x7x365 for any incidents that may occur. We will provide reactive incident response support to nullify the incident and begin recovery activities, with the aim of minimising disruption and damage to the wider environment.
- **Quarterly Alignment Reviews**. We will plan and schedule incident response-related work or additional services over the next quarter. This ensures the service's objectives align with the organisation's ongoing needs.
- **End of Year Review**. An objective review covering previous incident lessons, any outstanding or ongoing recommendations and corresponding action plans. A threat intelligence report highlights Reliance Cyber's vision to change the threat landscape, tailored for the UK public sector.

2.3 Incident Support

Should an incident occur, our multidisciplinary teams are equipped to respond to and manage incidents. Our expert teams cover all elements of response, including:

- **Triage**: Rapid assessment to determine the best decisive action to mitigate immediate threats and prioritise mitigation actions.
- **24x7 threat containment & monitoring**: Round-the-clock identification, containment and ongoing vigilance during incidents to ensure constant protection. This includes comprehensive strategies for all types of threats, from overt attacks to sophisticated breaches, preventing further system damage.
- **Post-breach analysis and forensic investigation**: Thorough data preservation and analysis to determine the incident's root cause, nature of the breach and risk to your data.
- **Decision making**: Critical decisions during incidents, like ransomware attacks, are informed by expert consultation.
- **Legal and insurance cooperation**: Collaboration with legal and insurance firms to support investigations and provide expert testimony.
- **Recovery**: Reliance Cyber will partner with your specialists or can provide recommendations on end-to-end recovery services designed to restore your operations to normalcy with minimal downtime and data loss.

2.4 Service Level Agreements

Specific service level agreements will be defined throughout Onboarding. The following table illustrates our standard Incident Response service levels.

Level	Description	Update Within
1	Initial Incident Response Call-Back.	2 hours
2	Incident Response, on-site or remote support to conduct	24 hours

3 Service Options

We have two key incident response retainer services built to ensure you receive the service that you're looking for. This includes:

	Standard IR Retainer	Enhanced IR Retainer
Summary	Our standard incident response offering provides 24x7x365 support from our experienced, certified team of digital forensics and incident response (DFIR) specialists. We will help you contain, investigate and remediate any cyber incidents that may affect your business operations, reputation or compliance. Our standard incident response offering provides a reliable, cost-effective solution for your cyber security needs.	Our Enhanced Response Retainer provides you with access to a comprehensive suite of services designed to protect your business and minimise the impact of cyber incidents, going beyond traditional incident response. Our Enhanced retainer provides trusted referrals for crucial legal and public relations support to navigate the complexities of post-incident response. This ensures that not only are the technical aspects of a breach addressed, but also the legal and reputational considerations that are critical to maintaining your business's integrity and customer trust.
Coverage	24x7x365	24x7x365
Initial Call Back SLA	2 hours	2 hours
On-site or remote support SLA	24 hours	24 hours
Minimum hours	40	120
Minimum contract length	12 months	12 months

Hours	A pool of hours that can be used for any IR service, such as threat hunting, malware analysis, digital forensics, incident management, business email compromise investigations, crisis simulation, etc.	A pool of hours that you can use for any of our professional services, such as vulnerability assessments, penetration testing, threat hunting, cloud architecture review, security awareness training and more.
Surplus hours	N/A	In any contract year, up to 80% of Service Hours that are not used can be shifted to other Professional Services that the Reliance Cyber offers (except for more retainer services), as long as those Professional Services are provided in the same contract year or within the first three (3) months after it.

3.1 Emergency Retainer

Reliance Cyber also offers SLA-guaranteed emergency DFIR support for major incidents, with a 24x7 hotline for real-time remediation of ongoing issues. This retainer enables you to purchase retainer hours and use them immediately to remediate critical breaches.

Think that you're experiencing a breach? Call our emergency incident hotline for hands-on, NCSC-assured support: +44 (0) 20 3872 9052.

4 Why Reliance Cyber?

Reliance Cyber is a Managed Security Services Partner (MSSP), dedicated to fortifying our clients through cyber security. With a rich legacy spanning 20 years, Reliance Cyber has emerged as a trusted and innovative MSSP, continually reinvesting to ensure our clients receive the best security support on the market. This has enabled us to recruit the best SC specialists and develop market-leading capabilities focused solely on cyber security.

Operating 24x7x365, we prioritise collaboration, transparency and long-term trust-based relationships with clients to navigate the ever-evolving landscape of cyber threats.

4.1 Core Capabilities

Reliance Cyber's core services are structured around three strategic pillars, reflecting our holistic approach to cyber threat management across managed, proactive and reactive services.

- **Managed Services** – We deliver enhanced security operations through continuous monitoring, proactive threat detection, and rapid remediation. Operating 24x7 on our clients' behalf, our managed services include Managed Detection and Response (MDR), Managed Endpoint Detection and Response (EDR), Managed Secure Access Service Edge (SASE), Phishing Monitoring and Vulnerability Management.
- **Proactive Consulting Services** – We support clients in identifying and addressing vulnerabilities before threat actors can exploit them. Our proactive security offerings include Cyber Threat Intelligence, Crisis Simulations, Compromise Assessments and a range of bespoke solutions tailored to meet each client's unique risk landscape.
- **Reactive Consulting Services** – When incidents occur, we provide expert incident response and recovery support. Our services are delivered using methodologies certified by CREST and aligned with guidance from the National Cyber Security Centre (NCSC). Leveraging deep digital forensics expertise, we help clients contain, investigate, and recover from cyber incidents swiftly and effectively, minimising impact and enabling lessons learned to strengthen future defences.

RelianceCyber

Additional Services That Compliment DFIR

Where Incident Response serves as your organisation's reactive defence against threats, our supplementary services extend this security shield. Whether integrated as bolt-on features or standalone services, they prioritise pre-emptive measures to safeguard your network.

Reliance Cyber Managed Detection and Response (MDR)

While DFIR reacts to a breach, our MDR service works to ensure one never takes hold. By combining 24x7 threat hunting with advanced analytics and threat monitoring, we identify and neutralise attackers before they can escalate. With our 24x7x365 UK-based Security Operations Centre (SOC) monitoring your environment in real-time, we provide deep visibility, rapid containment and the proactive intelligence needed to stop before they can escalate.

Cato Managed Secure Access Service Edge (SASE)

When traditional VPNs and fragmented tools fail to secure your remote workforce, our Managed SASE service provides a unified, cloud-native architecture. We combine SD-WAN with comprehensive security-as-a-service to deliver seamless connectivity and consistent policy enforcement. With our experts managing your edge, we provide secure web gateways, zero-trust access and real-time threat protection for every user, regardless of location.