RelianceCyber

Cyber Incident Response Services (CIRS)

Expert protection for when the inevitable occurs

reliancecyber.com

INTRODUCTION

Every organisation needs a contingency

The digital world is full of security risks. Any business, no matter its size or industry, might face cyber threats. This makes it necessary for organisations to always be ready for a possible attack.

39% of UK businesses identified a cyber-attack in the last 12 months, with 83% of these businesses reporting phishing attempts.

Because of this, it's critical for companies to have a strong plan in place for responding to incidents. This plan should aim to reduce damage, make defenses stronger, and have a backup strategy for dealing with cyber threats. Reliance Cyber focuses on shifting from just reacting to threats to actively preventing them, keeping your business secure.

We partner with:

Google Cloud

paloalto NETWORKS

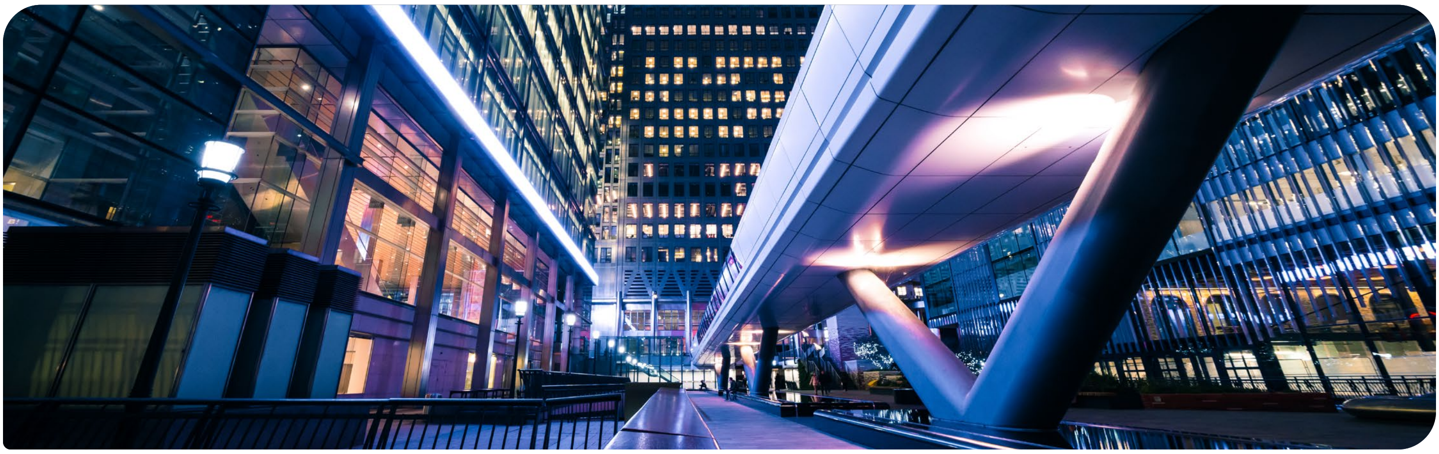
Microsoft

CHECK POINT

CROWDSTRIKE

CISCO

FORTINET



WHAT IS IT?

Comprehensive incident response

Effective incident response goes beyond technical solutions to include swift, accurate, and well-coordinated efforts across various fronts:

- **Containment and eradication of threats:** This involves quickly identifying and isolating affected systems to prevent further spread of the cyber threat. Following containment, the next step is to completely remove the threat from the environment, ensuring that all traces of the malicious actor are eradicated. This process is critical to restoring the integrity and security of your IT infrastructure

- **24/7 on-call support:** Our dedicated team ensures your safety around the clock, with analysts ready to respond immediately to incidents, offering you peace of mind

- **Understanding the impact of events:** Analysing the scope and scale of the incident is crucial. This includes determining which systems, data, and operations have been affected and to what extent. Understanding the impact helps in prioritising the response efforts and in planning the recovery process to minimize downtime and financial loss

- **Gathering and analysing forensic data:** Collecting and examining forensic evidence is essential for uncovering how the breach occurred, identifying the perpetrators, and understanding their methods. This step not only aids in resolving the current incident but also plays a key role in preventing future breaches by highlighting vulnerabilities and informing the development of stronger security measures

- **Clear communication with stakeholders:** Effective communication is key during a cyber incident. This involves keeping internal stakeholders, such as employees and management, informed about the situation and the steps being taken to resolve it. Additionally, it may be necessary to communicate with external stakeholders, such as customers, partners, and regulatory bodies, in a transparent and timely manner to maintain trust and comply with legal requirements

- **Navigating legal proceedings:** Cyber incidents often have legal implications, including compliance with data protection regulations and potential liability issues. Navigating these legal waters requires a thorough understanding of the legal framework, as well as coordination with legal counsel to ensure that the response efforts are compliant with relevant laws and regulations. This may also involve working with law enforcement if the incident is of a criminal nature

24/7

Our team is available around the clock, keeping your organisation's digital assets safe, giving you peace of mind when an incident occurs.

Rebuild with resilience: Recovering from a cyber incident is not only challenging but also critical for maintaining your organisation's integrity. Our service offers a strategy that extends beyond recovery to enhance your defenses against future threats. Rooted in resilience, our approach ensures that recovery efforts also bolster your business's security framework. This way, your organisation doesn't just recover; it evolves to become more robust and prepared for the digital challenges ahead

By addressing these aspects, an effective incident response plan ensures not only the technical recovery from cyber threats but also the operational, reputational, and legal resilience of the organisation.

Tailored incident response actions

In the wake of an incident, it is critical to have immediate access to diverse expertise. Reliance Cyber's highly experienced, multidisciplinary teams are perfectly equipped to respond to and manage incidents. Our expert teams cover all common elements of response including:

- **Triage:** Rapid assessment and decisive action to mitigate immediate threats, including malware removal and data recovery
- **24/7 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:** We partner with specialists to provide end-to-end recovery services designed to restore your operations to normalcy with minimal downtime and data loss

Why Reliance Cyber stands apart

Reliance Cyber is a leader in the cyber security domain, with a vast experience in responding to real-world incidents. Our holistic understanding of cyber threats and mitigation strategies ensures your organisation is in capable hands.

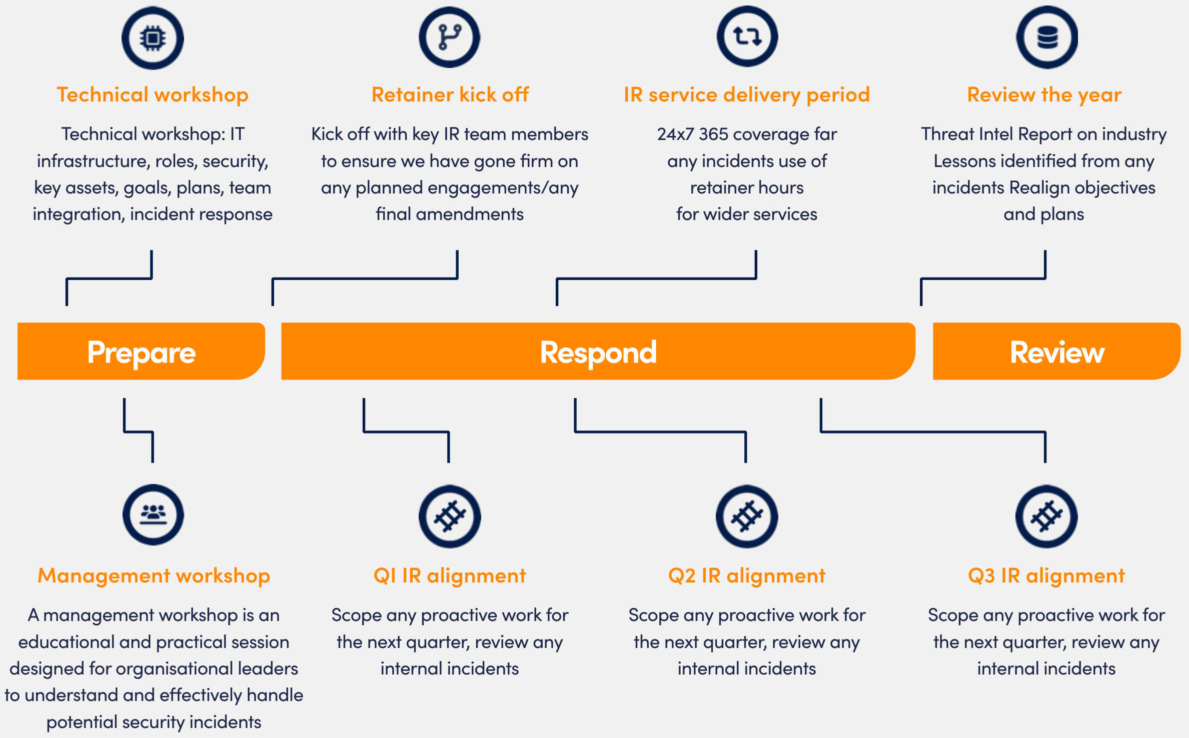
- **Post incident, follow-on services:** We partner with you along your journey by continuing to safeguard your organisation beyond an event
- **Advanced threat intelligence:** Our capabilities in identifying various types of attacks mean we can tailor our response efficiently, ensuring clear communication with stakeholders
- **24/7 SOC:** Our Managed Detection and Response (MDR) service ensures that there's always someone ready to assist you, regardless of when an incident occurs
- **Vendor-agnostic approach:** With the liberty to choose the right tools for every job, we address incidents comprehensively, from triage to law and reputation management

Any business, no matter its size or industry, might face cyber threats. This makes it necessary for organisations to always be ready for a possible attack.

Bringing peace of mind

Reliance Cyber provides immediate incident response services and proactive retainer options. Our retainer service ensures you are prioritised and prepared, with pre-paid hours and an established service-level agreement. We also assist clients with investigations and effective incident support.

Retainer service: A typical year



Technical workshop

Technical workshop: IT infrastructure, roles, security, key assets, goals, plans, team integration, incident response

Retainer kick off

Kick off with key IR team members to ensure we have gone firm on any planned engagements/any final amendments

IR service delivery period

24x7 365 coverage far any incidents use of retainer hours for wider services

Review the year

Threat Intel Report on industry Lessons identified from any incidents Realign objectives and plans

Prepare | **Respond** | **Review**

Management workshop

A management workshop is an educational and practical session designed for organisational leaders to understand and effectively handle potential security incidents

Q1 IR alignment

Scope any proactive work for the next quarter, review any internal incidents

Q2 IR alignment

Scope any proactive work for the next quarter, review any internal incidents

Q3 IR alignment

Scope any proactive work for the next quarter, review any internal incidents

Proactive support & prevention:

- **Always ready:** Our team is on standby to tackle issues immediately, emphasizing preventive strategies to avoid problems before they occur. We conduct in-depth risk assessments, routine system evaluations, and employ advanced early detection methods to minimize risks and safeguard your operations

Preparedness and reaction services:

- **Crisis scenario testing:** Engages leadership teams in desktop wargaming to strategise and prepare for potential crises
- **Cyber breach readiness assessments:** Assesses your preparedness for cyber breaches, identifying vulnerabilities and recommending enhancements
- **Incident response planning:** Offers a suite of services focused on both prevention and effective response to incidents, ensuring comprehensive coverage

PACKAGES

Standard incident response offering

Standard package

Our standard incident response offering provides you with 24/7 365 support from our experienced and 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 analysts all hold security clearance to deal with the most confidential information, giving you peace of mind when it comes to your data.

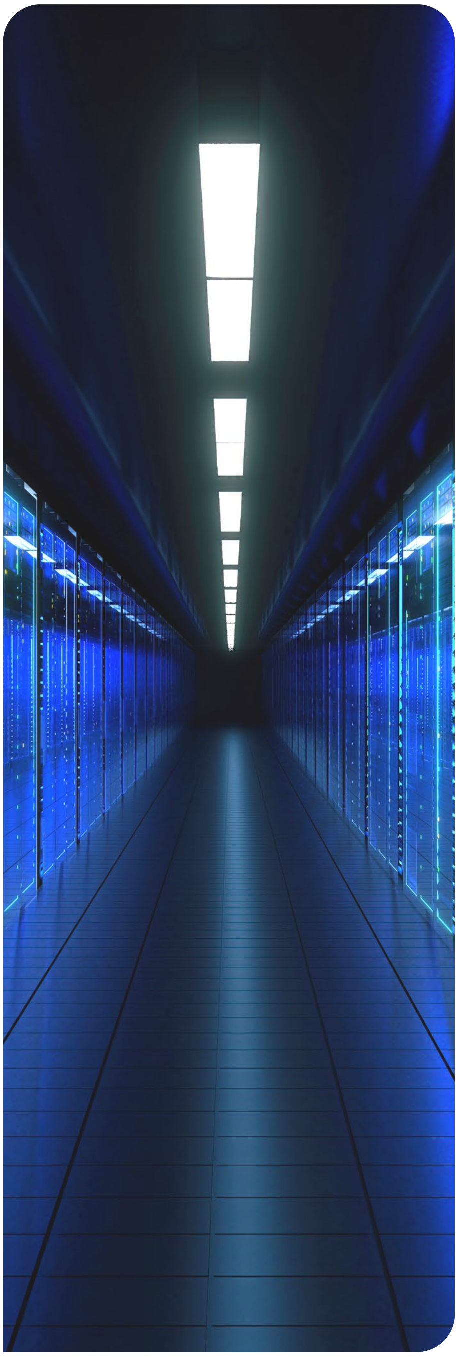
What's included in the package?

- A guaranteed 2-hour response time from our on-call DFIR Analysts

With our standard package, you will get the following benefits:

- A standard onboarding process that includes:
  - Team alignment and kick-off meeting to establish roles, responsibilities, and communication channels
  - IR handbook development to document your incident response plan, policies, and procedures
  - A flexible pool of hours that can be used for any DFIR service, such as threat hunting, malware analysis, digital forensics, incident management, business email compromise investigations, crisis simulation & tabletop exercises
  - A preferential rate for any additional hours beyond the standard package

Our standard incident response offering is designed to provide you with a reliable and cost-effective solution for your cyber security needs. That still provides you with the coverage you expect from an incident response retainer.



Get in touch

Contact us today to find out more or to sign up for our standard package.

Contact us at
+44 (0)845 519 2946 or email
contact@reliancecyber.com

PACKAGES

Incident response retainer package: Enhanced

Protect your business from cyber threats with our comprehensive and flexible service

Cyber incidents can have devastating consequences for your business, such as data breaches, reputational damage, legal liabilities, and operational disruptions. That's why you need a reliable and experienced partner to help you prepare for, respond to, and recover from cyber incidents. With our improved incident response retainer package, you get all the services you need to protect your business and reduce the damage of cyber incidents from the first containment to the forensic investigation and legal and public relations support.

What's included in the package?

The incident response retainer package – enhanced includes everything from our standard package, plus the following additional features:

- **Enhanced on boarding:** We will conduct a technical workshop and a management workshop with your team to assess your current security posture, identify your key assets and risks, and define your incident response plan and procedures. We will also provide you with a security roadmap that outlines the best practices and recommendations on how to use your hours to improve your security maturity and resilience before a breach happens

- **Hours can be used for any professional service:** You will have access to a pool of hours that you can use for any of our professional services, such as vulnerability assessments, penetration testing, threat hunting, security awareness training, and more. You can choose the services that best suit your needs and priorities

- **80% of hours can be carried over to Q1:** If you don't use all of your hours in Q4, you can carry over up to 80% of them to Q1 of the next year. This way, you can optimize your budget and plan your security activities accordingly

- **Access to legal support from leading law firm:** In the event of a cyber incident, you will need expert legal and communications advice to navigate the regulatory and reputational challenges. That's why we have partnered with leading law firms that specialise in cyber law and crisis management

- **Best hourly rate:** By choosing our incident response retainer package – enhanced, you will get the best rate for our services. This is a significant saving compared to our standard rate

Get in touch

Contact us today to find out more about our enhanced package.
Contact us at **+44 (0)845 519 2946** or email **contact@reliancecyber.com**

Comparison

	◎ Standard package	◎ Enhanced package
Summary	Our standard incident response offering provides you with 24/7 365 support from our experienced and 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 analysts all hold security clearance to deal with the most confidential information, giving you peace of mind when it comes to your data. Our standard incident response offering is designed to provide you with a reliable and cost-effective solution for your cyber security needs. That still provides you with the coverage you expect from an incident response retainer.	Our Enhanced Response Retainer Package goes beyond the foundational offerings of the standard retainer, providing you access to a comprehensive suite of services designed to protect your business and minimise the impact of cyber incidents that go above and beyond tradition incident response. We recognise the multifaceted nature of cyber incidents; our Enhanced package provides access to crucial legal and public relations support through our partners 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. By choosing our Enhanced Response Retainer Package, you're securing a robust defence mechanism for your organisation, equipped to tackle the immediate challenges of a cyber incident and manage its longer-term repercussions.
Coverage	24/7 365	24/7 365
SLA	2 hours	2 hours
Minimum hours	40	120
Onboarding	A standard onboarding process that includes: Team alignment and kick-off meeting to establish roles, responsibilities, and communication channels. IR handbook development to document your incident response plan, policies, and procedure.	The enhanced onboarding includes everything in the standard plus: A technical workshop and a management workshop with your team to assess your current security posture, identify your key assets and risks, and define your incident response plan and procedures. We will also provide you with a security roadmap that outlines the best practices and recommendations on how to use your hours to improve your security maturity and resilience before a breach happens.
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 & Tabletop exercise.	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. You can choose the services that best suit your needs and priorities.
Surplus hours	N/A	80% of hours can be carried over to Q1: If you don't use all of your hours in Q4, you can carry over up to 80% of them to Q1 of the next year. This way, you can optimize your budget and plan your security activities accordingly.
Hourly rate	A preferential rate for any additional hours beyond the standard package.	By choosing our enhanced incident response retainer package, you will get the best rate for our services. This is a significant saving compared to our standard rate.

Why choose us?

We are a trusted and experienced provider of cyber security services, with a proven track record of helping clients across various industries and sectors.

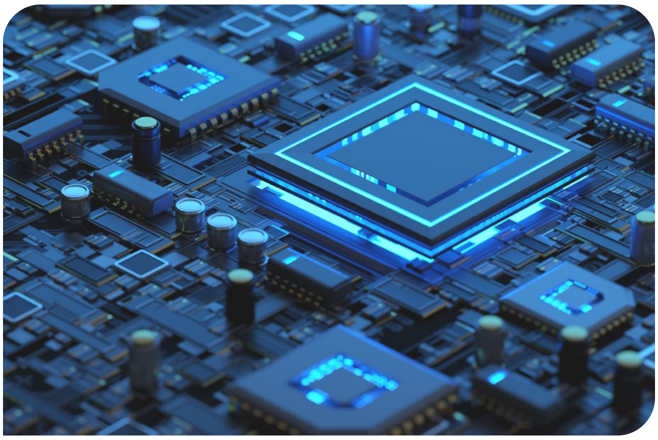
We have a team of certified and qualified professionals who have the skills and expertise to handle any type of cyber incident. We use the latest tools and technologies to detect, contain, analyse, and remediate cyber threats. We also offer a holistic and tailored approach to cyber security, taking into account your business objectives, challenges, and environment. We are committed to delivering high-quality and cost-effective solutions that meet your expectations and requirements.

How to get started

If you are interested in our incident response retainer package - enhanced, please contact us today to discuss your needs and get a quote.

You can reach us by phone, email, or online form. We will be happy to answer any questions you may have and provide you with more details about our service. Don't wait until it's too late - secure your business today with our incident response retainer package - enhanced.

Want to find out more? Enquire at **contact@reliancecyber.com**



! Experiencing a cyber incident?

Contact our emergency hotline:
+44 (0) 203 872 9052

RelianceCyber

Get in touch

+44 (0)845 519 2946

contact@reliancecyber.com

reliancecyber.com