CLOUDGUARD

PROTECT +

Incident Response Retainer Service (IRR)

Supporting organisations in higher performance Incident Response Management

Service overview

CloudGuard operates 2 levels of Incident Response (IR) for customers. **Incident Response Retainer** (IRR) offers a number of key benefits to customers when experiencing a major cyber incident.

The IRR service is critical to ensuring the highest levels of responsiveness to any incident, **24 hours** a day with access to highly skilled and experienced cyber specialist who focus on minimising exposure and business disruption whilst maximising containment and focus.

Over **69% of businesses** experienced a significant cyber incident in 2025. The CloudGuard IRR service provides businesses with the reassurance that, whatever and whenever an event occurs, a highly skilled team will be engaged and protecting the business within **60 minutes**.

High performance Incident Response is more than how quickly can the right resources be engaged. The CloudGuard IRR proactively focuses on **3 key areas** even before an incident occurs:

- **Readiness** – ensuring the processes & tested plan to engage at speed.
- **Responsiveness** – every minute counts when minimising business exposure, risk and disruption.
- **Resilience** – testing, improving and rehearsing response actions to ensure highest performance when needed

Service overview

Incident Response Retainer (IR) commits to the following outcomes:

- Appropriately skilled cyber incident resources engaged and working on the incident within 60 minutes, 24 hours a day
- To identify and lead technical communications in relation to the IR
- Work with all customer 3rd parties required to contain, manage, response and remediate the Incident
- Work with and advise the customer on all aspects of a major cyber incident
- To involve the response team where required
- To provide the initial 10 hours of a response within the IRR service charge
- To continually update the Incident Response plan and test this at least every 12 months

Why this matters now

Threats are real and increasing for every business. Without a **regularly tested** and proven Incident Response plan, most businesses underperform in terms of response when critically tested. Tested and updated plans provide proven evidence in how a business will respond and coordinate all available resources to minimise business disruption and impact.

CLOUDGUARD

IRR Service scope

Our Incident Response Retainer service aligns to the five core best practice pillars:

Resource Response to SLA
CloudGuard expert Cyber Incident Responders will be actively working on the customer incident within 60 minutes. The initial 10 hours of IR time are included in the IRR Service charge in any 12-month period.

Incident Management & Reporting
The team will establish technical incident leadership, an open incident bridge and 30-minute updates to the Customer.

Operational Resilience and Readiness Planning
The IRR service includes a best practice, fit for business Incident Response plan and strategy. Working with each customer, this will include a clear event management and containment structure as well as contact details.

Third-Party Collaboration
CloudGuard will engage with any Customer 3rd parties to ensure all aspects of an incident are contained to industry best practice management standards. This includes working with all Cyber insurers.

Readiness & Resilience Testing
Review of IRR Roles and Responsibilities, reporting structures, continual improvements, policies and regulatory awareness.

Our approach

Delivered through a collaborative and supportive engagement:

1. Identify & Validate cyber-Incident
2. Invoke appropriate Service Response
3. Establish Customer communications
4. Follow IR plan with technical updates every 30 minutes
5. Contain, Protect & Manage Incident in Technical leadership role
6. Complete all necessary forensic investigations as required
7. Confirm any data leakage or exfiltration
8. Engage all necessary 3rd parties and authorities as required
9. Complete Root Cause Analysis
10. Review and continually update Incident Response plan
11. Over communicate at all times

Why CloudGuard

CloudGuard delivers enterprise-grade cybersecurity for growing businesses. Combining automation-led technology with UK-based experts, we provide 24/7 protection, without the complexity or cost of traditional platforms. Our fully managed approach simplifies detection, protection and improvement, so you can focus on growing with confidence.

Get in touch