Incident Response Retainer

SERVICE DEFINITION FOR THE G-CLOUD 15 FRAMEWORK

Overview

Even in the most secure environments, security incidents are unavoidable. With an ever-accelerating arms race between attackers and defenders, being ready to respond quickly and effectively is key to recovery.

Our Incident Response Retainer service is designed to ensure that when the worst happens, you can call on the expertise you need to recover effectively.

We're experts in business, and we're pragmatists at heart. Throughout any incident, we'll make sure your business objectives are properly considered. You might want to get systems up and running again as quickly as possible, establish accountability, or conduct a wide-ranging analysis of indicators of compromise to determine the extent of a breach. We'll help you meet your goals.

- Experts in defence. We understand how your adversaries operate, which makes us highly effective in containing and responding to their actions.
- Pragmatic approach. We understand the importance of a fast recovery.
- Get everyone on side. We make sure stakeholders are engaged during an incident. Experience has taught us that keeping the relevant parties informed helps reduce the stress of an emergency.
- CREST member. We're fully accredited to provide Cyber Security Incident Response services.

Our Service

Our Cyber Security Incident Response Retainer provides access to our Incident Response Team (IRT) with a service level agreement providing guaranteed response times when an incident occurs, and fixed incident response rates.

In an emergency, the Cyberis Incident Response Team (IRT) can be deployed to provide expert consulting and technical advice to help you handle a security incident from initial detection to closure. Whatever the size of the incident - from a simple breach of policy to an estate-wide compromise - we can manage the incident from start-to-finish, or work as part of your own incident response team. The Cyber Security Incident Response (CSIR) Retainer consists of an allotment of hours you may apply towards assistance from our IRT in the event of a cyber security incident.

Cyberis Limited
Unit E, The Courtyard, Tewkesbury Business Park, Tewkesbury, Gloucestershire, GL20 8GD
T: +44 1684 353514 | E: info@cyberis.com | W: cyberis.com

Benefits

- Guaranteed access to our Incident Response Team with defined SLAs – giving you access to the expertise you need quickly in an emergency.
- 24x7x365 incident reporting
- Initial triage within 4 hours
- Remote support within 8 hours
- Onsite assistance within 24 hours
- 40 hours of inclusive incident response as standard (additional inclusive hours can be negotiated at retainer initiation, or additional response time can be purchased as needed when an incident occurs).
- Unused hours can be used against our standard scheduled services at the end of the retainer period

Approach

Integration project

Before we start our retainer with you, we will conduct an integration project with you. This allows us to gather relevant information about your organisation, systems and processes so that when you call our Incident Response Team, they have all the background and access they need to hit the ground running.

Remote access

We can deploy our zero-configuration remote VPN device to your networks, so that our responders can access your systems remotely when you need help. Our solution is configured to connect securely from your network to our cloud systems, and access is controlled via robust certificate-based authentication restricted to our IRT for accountability.

When an incident occurs

We use our industry experience in incident response management and analysis as well as proven industry guidance and frameworks provided by CREST, the NCSC and NIST. The typical incident response lifecycle will start with you contacting Cyberis to inform the IRT of an incident. We'll respond with a technical call back to verbally triage the incident. Detailed incident triage, identification, containment and recovery will then follow, via remote support, and if required an onsite presence.

Regular reviews

After responding to an incident, Cyberis will schedule a review meeting. The agenda for this will include reviewing the incident that Cyberis has responded to, confirming that the zero-config VPN device is still operating, the utilisation of hours purchased, discuss any improvements that can be made, and understand any post-incident organisational or process changes.

Unused hours

At the end of the 12-month retainer period, when outstanding hours remain, there is a three-month grace period in which outstanding hours from the retainer may be used for the delivery of our standard scheduled services – including our supporting incident response services and penetration testing.

Retainer overview

An overview of our retainer process and SLAs is illustrated below:

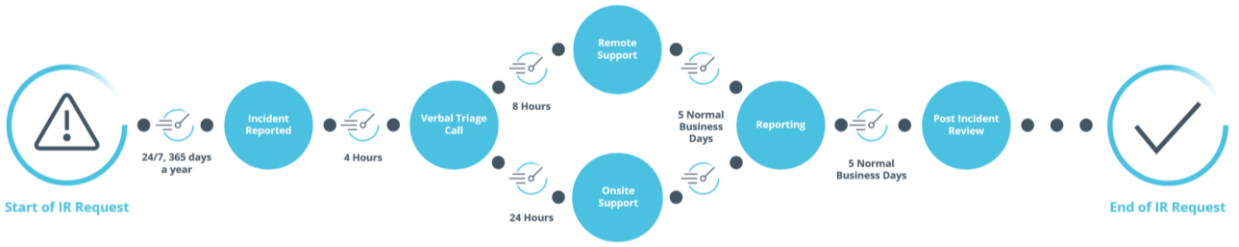

Figure 1: CSIR retainer overview

Service Management

We operate a service management process that is integrated with our ISO 9001 Quality Management System.

All projects are assigned a lead consultant and a project manager throughout delivery of the testing. We operate an escalation procedure in the event of unresolved client dissatisfaction; at the time of G-Cloud 15 submission, this procedure has never been used.

Service Constraints and Levels

An overview of our standard SLAs is provided above. Our retainer services are tailored and agreed in each 'Statement of Work' within a proposal.

Financial Recompense

We do not have a formal recompense model; as part of our ISO 9001 certification and commitment to customer service, we monitor the quality and delivery of all testing services very carefully.

Training

Training is offered in several of the testing service disciplines we offer; we are happy to discuss training options with our customers.

Ordering and Invoicing Process

Our normal process is to produce a 'Statement of Work' within a commercial proposal and once acceptance is given (through a signed order form or purchase order) we will commence the scheduling process.

Fixed price projects are invoiced on acceptance of the deliverables of each work task. Projects undertaken on a time and materials basis are invoiced monthly in arrears. We are happy to discuss the ordering and invoicing process with our customers.

Termination Terms

Refer to the separate 'Terms and Conditions' document.

Data Restoration / Service Migration

Data restoration and service migration is not included in our price.

Customer Responsibilities

All customer responsibilities will be defined in the 'Statement of Work' for each engagement/project.

Technical Requirements

All technical requirements and service dependencies are discussed with the client during scoping, as in most cases each project has different requirements. Technical requirements and testing pre-requisites will be documented in the 'Statement of Work' within the proposal.