1. Service Overview

We provide access to a 24x7 Cyber Security Incident Response ("CSIR") Service to assist you with high priority incidents and emergency mitigation advice in the event that a cyber-attack has been identified or suspected within your environment.

The Service provides access to Cyber Security Incident Responders ("IRs") who will assist with the evaluation of incidents and to understand the issues and the impact they may have on your organisation. Following prioritisation, we will engage appropriate resources to provide advice and guidance to contain and remove the relevant issues.

Our incident response team is contactable 24x7 and can provide advice with the technical and non-technical aspects of a cyber breach. Our CSIR Service can be incorporated into your incident response procedure and act as an extra capability or support for your in-house team.

2. Service Features

The CSIR Service provides access to our Cyber Security Operations Centre ("CSOC"), to request advice and assistance should you suffer or suspect a cyber breach. The Service gives you access to trained IRs who will capture key information about your incident, ascertain the potential impact and priority, and provide instruction for a course of responsive actions to contain or remove the issue and allow business continuity.

Once the issue has been contained or removed and BAU has resumed, we can provide further consultancy engagements to assist with understanding how the issue occurred, check there are no known remaining threats and provide 'lessons learned' around the incident to assist you with the prevention of repeat occurrences. Additional consultancy is charged at our standard rates and can be agreed according to your requirements.

The Service provides you pre-approved access to our CSIR resources as well as process and authorisation plans to activate the Service.

Details of service implementation, as well as information about your environment, are captured during onboarding sessions with you. These sessions are designed to gather sufficient information on your infrastructure and processes, which we will make available to our CSIR team to optimise the response time should you need to raise a CSIR request.

2.1 Incident Types and CSIR Response

Our CSIR Service is designed to assist with the following types of incidents:

Incident Types	CSIR Response
Malware	We will identify the malware to understand its payload, behaviour, threat level and recommend counter measures.

Virus	We will identify a suspected virus and provide information around steps to take to protect you against it.
Suspicious Files	We will review suspicious emails or files to determine whether they are harmless or malicious (*e.g.* email with a document attached).
DDoS Mitigation Attack	We will provide advice and suitable response in the event of suspected DDoS attack.

Incident Types	CSIR Response
Brand Protection	We will request the removal of phishing sites or report attacking sites from the internet.
Forensic Response	We will arrange a visit to your site to seize, image and analyse systems for forensics purposes.
Attack Response	We will conduct a penetration test to identify any weaknesses and recommend further countermeasures.
Virus Outbreak	We will assist in remediation after a virus outbreak.

2.2 Incident Response

Our reactive CSIR Service will give you access to a 24x7 incident response telephone number and a monitored email address to report a suspected incident.

After receiving your report of an incident or suspected breach, our analysts will undertake a brief evaluation of the incident to determine its nature and the threat that it poses to your organisation's operations. The purpose of this initial assessment is to gather necessary information about the incident; however, our analyst will not perform any technical analysis at this stage.

Typically, this initial assessment will lead onto the following actions:

(a) Further technical investigation performed by you or our IRs;

(b) Remote technical analysis, subject to your ability to provide secure access to our IRs;

(c) We will advise on the deployment of countermeasures that you can perform;

(d) We will evaluate the countermeasures and advise on who should be responsible to perform them (either you or our security team); and

(e) Provide post incident technical analysis and lessons learned.

NOTE: At any stage of the incident response, we may determine that the threat does not require further response action (e.g. it is a False Positive or deemed low risk).

Please note that the above list of actions may vary depending on the incident and will be confirmed following the evaluation of the incident. As a standard, we will perform fifteen (15) minutes of incident triage for every incident reported to our CSIR. Within this timeframe, we aim to provide you an update of what has occurred and advise on the proposed next steps.

Following the initial fifteen (15) minutes of incident triage, we may recommend to you to procure additional triage time or additional resources to investigate further and agree a remediation plan.

2.3 Incident Response Time

We offer additional triage time in blocks of fifteen (15) minutes, which can either be pre-purchased or requested by you as and when needed. We will charge you a fixed Fee for each additional block of fifteen (15) minutes at the rate contracted with you and detailed in your Order Form and/or SoW.

If you require additional assistance outside of the incident response or as part of a non-emergency follow up (e.g. onsite attendance to retrieve data for forensic analysis), we can provide you with professional service time which would be charge at our standard rates.

Following the initial fifteen (15) minutes of incident triage and before committing to additional time and effort, we will seek consent from your nominated contact(s) to proceed in dealing with the incident. If you provide such consent, the time taken to deal with the incident will be deducted from your contracted allowance and/or billed according to the time spent in resolving the incident.

We will endeavour to provide you details of the time we anticipate would be needed to resolve the incident and the associated costs, however this data would be an estimate only and may vary.

If authorised to proceed, we will raise a ticket to record the time spent by our analyst to deal with the breach and the actions and time taken during such event. Once the ticket has been closed, we will invoice you for the time recorded on the ticket or, if you have a pool of pre-purchased support time, we will deduct the time spent by our analyst from such pool, in which event the ticket will detail any remaining time in your pre-purchased pool.

2.4 Additional Features

As part of this Service, we will provide you the following:

(a) Approximately six (6) to twelve (12) Cyber security Threat Flash reports per year; and

(b) Invites to and priority access for our Cyber Security Workshop sessions (approximately two (2) events per year).

These items are provided in addition to our standard CSIR Service; however, they are not subject to any additional Fee. You can opt out of these services at any time during your contract term.

3. Service Implementation

3.1 Service Onboarding

Our Service implementation team will contact you to discuss your Service and complete the onboarding process. Onboarding ensures that the CSIR team have the core information necessary to provide the Service to you.

During the onboarding process, our representative will document information about how your infrastructure is set-up, the security controls that are in place, and request architecture diagrams from you. All information received from you will be securely stored and made available to our CSIR team.

After order acceptance, we will implement the Service as follows:

Service Implementation	Us	You
We will provide a dedicated 24x7 monitored email address and telephone number.	•	
You will provide the list of your contacts authorised to instigate the CSIR Service.		•
We will provide you with escalation contacts and a PIN number for confirming your identity.	•	
You will ensure you are able to provide us remote access to your affected infrastructure as and when needed.		•
We will enable our systems to be able to provide ticketed detail for each incident.	•	

Implementation work will be carried out during Business Hours. We will invoice additional charges for any work undertaken out of hours. We reserve the right to charge additional fees for any change in your requirements occurring after the implementation of the Service and outside the scope of the contract (as described in the MSA).

3.2 Ready for Service

The Ready for Service Date will be the date when we (acting reasonably and properly) notify you via email that the onboarding process is completed and that we are ready to provide the CSIR Service.

4. Billing

The Service will be billed as a Recurring Fee and a Non-Recurring Fee as described in our Billing Guide.

The Recurring Fee is related to the provision of access to the CSIR Service; whilst any additional time used and the pre-purchase of any additional time blocks will be charged as a Non-Recurring Fee.

Any additional support time used in accordance with Section 2.3 is charged in increments of fifteen (15) minutes at the rate contracted in your Order Form and/or SoW. We will bill you for the Service post incident, based on the time spent by our analyst.

You are able to pre-purchase, eight (8) hour, or sixteen (16) hour CSIR time blocks at any time. Pre-purchased time is valid for twelve (12) months from the date of the relevant Order Form, which you must sign before using any CSIR time block. If you have pre-purchased CSIR time, we will deduct from your allowance any time spent by our analyst in the resolution of an incident. Please note that if you have any unused purchase time at the end of the relevant contract term, you won't be able to carry over such allowance during successive contract terms, unless expressly agreed with us in writing.

If you exhaust your allowance during an incident investigation process, we will notify you and seek your consent to proceed with the investigation, which we will charge in increments of fifteen (15) minutes as described in Section 2.3.

You will be able to purchase additional CSIR time blocks at any time during the term of your Service. You will be able to use such additional CSIR time blocks for a period of twelve (12) months following the date of purchase (as documented in either a variation to your original Order Form or in an additional Order Form). Please note that if you terminate your Agreement for CSIR Service with us, you will not be able to use any pre-purchase CSIR time.

If this Service is part of a wider package of services that you have agreed to, other Fees may be included in a broader implementation charge that enables the delivery of your chosen services. All the services that you are procuring from us and the associated Fees will be indicated on your Order Form and/or SoW.

4.1 Additional Charges

We reserve the right to charge additional fees in the following situations:

(a) Implementation work carried out outside Business Hours; and

(b) Any change in your requirements occurring after the implementation of the Service and outside the scope of the contract (as described in the MSA).

5. Service Operations

The table below describes the process followed by our IR team when you inform our CSOC of an incident and request escalation to our CSIR team:

PHASE 1	Initial CSIR Request
1	Our CSOC analyst takes the details from you and creates the CSIR ticket, which will include the caller's name and number. This ticket will then be escalated to the CSIR triage.
PHASE 2	**CSIR Triage**
2	Once the details have been received from our CSOC, our CSIR team will contact your authorised contacts by phone call.
3	The target response time for CSIR triage is calculated from the time when the CSIR request is made by you to the CSOC, with CSIR triage having one (1) hour from the first contact with the CSOC to phone you (your CSIR requestor) back.

4	The aim of the initial phone call is to collect all the information necessary to understand the nature of the incident, carry out the initial triage (fifteen (15) minutes included) and to prioritise the incident accordingly. All incidents will be reviewed and prioritised within the initial fifteen (15) minutes of triage. Incident prioritisation will then drive the response targets as detailed in Section 9. If additional triage time is required, you must approve this in writing via email or via the IMS.
PHASE 3	**CSIR Response Plan**
5	The CSIR Response Plan is dependent on the incident priority and required CSIR team triage. Initial response times are detailed in Section 9.
6	We will send you the Response Plan within the CSIR ticket.
PHASE 4	**Support**
7	We will provide remediation support as detailed in Section 9, based on the incident prioritisation.
PHASE 5	**Analytical Response**
8	If our CSIR determines that further in-depth analytical work is required as part of your Response Plan, this work and applicable Fee will be agreed with you and this can be arranged and executed as BAU. There is no SLA for this work, however it's the CSIR Management Group's responsibility to ensure you are regularly updated about this work whilst Phase 5 work is ongoing.
PHASE 6	**Completion and Review**
9	Within ten (10) business days of a CSIR incident being completed, the CSIR Manager (when the incident is closed) will organise a review into the handling of the incident and whether any changes are required to our CSIR Response Process, change will be recorded in the IMS platform. Where appropriate, the CSIR Manager will invite you to attend this meeting.

6. Dependencies

We provide the CSIR Service subject to the dependencies listed below. Where CSIR forms part of a wider package of services that you are procuring from us, assistance or ownership of some of your obligations may be passed to our professional services implementation team or may be covered by a broader Managed Service package. Details of the services that are included in your contract will be detailed in your Order Form and/or SoW.

6.1 Client Obligations

(a) You will be available to allow the completion of the onboarding process and provide appropriate information as requested;

(b) You will provide us reasonable assistance in the performance of the Service, including, but not limited to, providing all technical and infrastructure information that we may reasonably require for performing the Service;

(c) You will provide us remote access and all credentials necessary for the performance of the Service;

(d) You will provide us with accurate and up-to-date information, including name, email, landline, and mobile numbers (if applicable) for all your authorised points of contact and your main office or contact address;

(e) You will notify us at least twenty-four (24) hours in advance of any systems maintenance or network or system administration activity that will (or has the potential to) affect our ability to perform the Service;

(f) You will actively work with our support team to resolve any logged calls or service requests requiring your inputs or action;

(g) You will manage and keep up-to-date any maintenance and technical support contracts with your software and hardware vendors for the environment in which the Service is offered;

(h) If you require any change(s) to the scope of your Service, you must raise your request before we commence any implementation activity for the Service;

(i) In the event of an incident, you will:

(i) provide all available evidence and credentials needed to access any affected host(s) that require investigation;

(ii) facilitate interviews with your relevant staff members as we may reasonably require to conduct the investigation; and

(iii) where possible, ensure that documentation of known activity and events is prepared prior to the escalation of the incident to our CSIR team.

7. Exclusions

The excluded items described below are outside the scope of this Service Description:

(a) The Service provides response capabilities and should be used as part of a wider approach to risk mitigation. We accept no liability for any damage or disruption caused by any malicious actor, threat, automated or manually operated process or entity carrying out any actions that damage, delete, corrupt or prevent access to systems and data, in part or in whole, either purposely or otherwise;

(b) The service is not provided as a Security Support or as a help desk Service. You are responsible for using the unlimited access to the included fifteen (15) minutes of initial triage in good faith and in a reasonable and proper way;

(c) Site attendance is not immediate. We will schedule any work requiring our attendance on site subject to resource availability at the time of the request;

(d) We will not perform any data destruction activity as part of this Service. Once forensic copies of target data have been taken, we will return all original media to you; and

(e) This Service is dependent on the security and resilience of your environment and your obligation to provide us with accurate and sufficient information on the incidents as we may reasonably require. We will make reasonable effort to prevent loss of data, systems or interruption to business, however we do not provide any warranty or guarantee that losses will not be incurred, and business activity will not be interrupted.

8. Definitions and Acronyms

8.1 Definitions

In this document “we” or “us” refers to the Supplier, and “you” refers to the Client.

The terms listed have the following meanings:

Term	Meaning
CSIR Management Group	The team who over-see the CSIR triage team, providing management guidance and support and assisting with assuring processes are followed.
CSIR Triage	The process of reviewing and understanding the incident, with view to measure impact and provide next appropriate and actionable steps.
False Positive	False alarm or security alert wrongly indicating that there is a threat or a vulnerability.
Incident Responder	Member of staff who is trained in incident response and able to guide and assist with the reported incident.
Response Plan	Agreed response to a CSIR incident, incorporating incident priority, related SLA and resources required to implement the fix.
Statement of Work	A document which defines project-specific or client-specific activities, deliverables and/or timelines for providing the services.

8.2 Acronyms

Acronym	Meaning
BAU	Business as Usual
CSIR	Cyber Security Incident Response
CSOC	Cyber Security Operations Centre
DDoS	Distributed Denial of Service
IR	Incident Responder
SoW	Statement of Work

9. Operational Targets

We will perform the fifteen (15) minutes initial triage as set out in the Cyber Security Incident Response Service Description and assign a priority to your incident. Where you require additional support from us following prioritisation, we will endeavour to respond in accordance with the targets set out in the table below:

Type 6	P1	P2	P3	P4
Response	1 hour*	8 hours*	1 Business Day*	N/A
Fix	Not applicable due to the nature of the Service.			
Hours of Support	24x7	24x7	Business Hours	Business Hours
Description	• High risk, including a suspected or high probability of system compromise; • Identification of an incident requiring urgent assistance.	• Medium risk, increased attack activity including high priority events that may require further investigation, no indication of compromise; • Identification of an incident requiring assistance.	• Low risk incidents indicating the need for increased vigilance and posing no immediate risk of compromise or exposure; • Identification of an incident requiring low priority assistance/support.	• Information only incidents which require no action; • Identification of a false positive.
Response	CSIR Responder will make reasonable effort to advise on the actions to remediate the incident as soon as possible but, in any event, will contact the client within one (1) hour from initial triage.	CSIR Responder will advise on the actions to remediate the incident within eight (8) hours from initial triage.	CSIR Responder will advise on the actions to remediate the incident within one (1) Business Day from initial triage.	N/A

* Calculated from the time we receive a request from one of your authorised contacts to provide further incident analysis following the initial fifteen (15) minutes triage.

10. Service Levels

The Service will be delivered within the target level set out below.

Core Service Component	Measurement	Period	Target
CSOC Operations – Initial CSIR Triage	Triage team response from initial notification of incident	24x7	Within 1 Hour
CSOC Operations – Initial CSIR Triage	Availability of the CSOC team for the provision of the CSIR initial triage.	24x7	99.9%