CyberOne

# Cyber Incident Response

## G-Cloud 15

### Service Description

# Service Description
# Cyber Incident Response

This Schedule forms part of Schedule 3 to the Agreement between Customer and Provider and sets out a description of the Services and Service Levels for the Cyber Incident Response Service ("CIR Service") as specified in a Service Order.

## 1. Additional Definitions

The following definitions apply in this Schedule

**"Additional CIR Services"** Additional blocks of CIR Service Hours, which can be purchased in addition to the CIR Service Hours detailed on the Customer's existing Service Order(s).

**"CIR Service Hours"** The annual allocation of hours which the Customer can utilise in provision of the CIR Services that are specifically stated on a Service Order and prepaid as part of this CIR Service.

**"Incident Manager"** Provider appointed individual chosen to coordinate provision of the CIR Services to Customer when a Security Incident has arisen.

## 2. Additional Commercial Terms Relating to the CIR Services

2.1 The CIR Service Hours must be used within the Initial Term or any Renewal Term in which they are allocated. If during the Minimum Term or any Renewal Term, the Customer does not utilise the full annual allocation of CIR Service Hours, then 20% of the remaining balance may be rolled over and utilised by the Customer as professional services at rates given in the Agreement within the next Renewal Term.

2.2 Should the Customer require additional Services beyond the CIR Service Hours then the Customer must purchase a block of additional time at the agreed rates. Any additional CIR Service Hours must be utilised within 12 months of purchase.

2.3 All Services will be performed remotely, from the Provider's premises or at the Customer's site(s) as determined by the Provider. The Customer agrees to be responsible for any additional costs, travel and out-of-pocket expenses incurred by the Provider related to providing the Services at a Customer site.

## 3. Additional Customer Obligations Relating to the CIR Services

Obtain a software license for Microsoft Defender for Endpoint from the Service Commencement Date and maintain it for the duration of the Term of the CIR Service.

## 4. CIR Service

CIR Services shall comprise the following:

### 4.1 Proactive Service

One Remote onboarding workshop with a Provider Incident Manager and a subsequent high level incident plan detailing:

i. Key contacts
ii. Incident invocation protocol
iii. Incident briefing and Customer escalation protocols
iv. Provider access protocol
v. Standard operating procedures and response playbooks
vi. Special considerations
vii. Engagement closure protocol

Additional incident planning can be arranged via the CIR Incident Manager at the Customer's request. Note that this will consume CIR Service Hours.

### 4.2 Reactive Incident Response

Upon notification by the Customer to the Provider of a Security Incident requiring usage of the CIR Service Hours the Provider shall provide the following incident response services in line with the Service Levels stated in Clause 5 below:

**4.2.1 Assess:** Appoint an Incident Manager to conduct an initial review of the Security Incident, provide an initial incident assessment and conduct an initial briefing with the Customer.

**4.2.2 Investigate:** The Incident Manager will assemble a remote team that is proportionate to the needs of the Customer. The Provider may need to rotate the Incident Manager and/or members of the remote team during a Security Incident due to staff shift patterns or other circumstances. Guided by the Incident Manager, the assembled team will identify and investigate threat activity according to the incident scope, using live device forensics, threat intelligence, threat hunting and malware analysis. The assembled team will conduct these activities using defined service technologies, and within the constraints of their access. All key evidence and analysis will be documented in the case management system. Executive check-ins are provided daily. At any time during the investigation, if a finding is deemed an urgent finding, the Incident Manager will escalate to the designated Customer contact.

**4.2.3 Assist:** The assembled team will work with the Customer to attempt to contain/eradicate the threat from Customer's environment. The assembled team will conduct these activities using defined service technologies, and within the constraints of their access. All key activities will be documented in the case management system.

**4.2.4 Advise:** After concluding the incident, the Provider will provide the Customer with an optional incident report that contains an executive summary of the incident investigation, an incident timeline, key facts, remediation recommendations and an appendix with technical information e.g. indicators of compromise.

**4.3 Data Retention Periods**
Unless a specific retention period has been agreed on a Service Order, the Provider shall retain all evidence collected during the investigation of a specific Security Incident (including but not limited to malware samples, log samples and other evidence provided by the Customer) for a period of thirty (30) days from the date of the engagement closure for that particular Security Incident investigation ("Retention Period"). Subject to any applicable statutory requirement to retain information, after the expiry of the Retention Period, the Provider shall permanently delete all such evidence collected or provided by the Customer to the Provider during the course of the investigation.

## 5. Exclusions

**5.1 Monitoring:** The provider will not actively monitor the Customer's environment as part of the CIR Service

**5.2 Remediate/Recovery:** Remediation of the Security Incident and recovery of affected assets to live production status or building of new production environment are excluded, but the Provider may, on request, provide an estimate of time and costs for this work.

5.3 Only the activities, deliverables, and responsibilities expressly detailed within this Service Description are included. Any service elements not specifically stated are excluded from the scope unless agreed in writing by both parties.

## 6. CIR Service Levels

In relation to the CIR Services the following service levels shall apply.

| Service Component | Availability, Response Times & Procedure |
|---|---|
| **Notification:** Security Incident requiring CIR Service | Provider SOC available 24x7.<br><br>Logging of Ticket by Provider and initial response to Customer within fifteen (15) minutes of Ticket Open.<br><br>Appointment of Incident Manager with one hour of Ticket Open. |
| **Assess:** Initial Scope Assessment | Within a maximum of 2 hours from Ticket Open. |
| **Assess:** Initial Briefing | As agreed with Customer on completion of Initial Security Incident scope assessment. |
| **Investigate:** identify and investigate threat activity according to the incident scope, using live device forensics, threat intelligence, threat hunting and malware analysis | Service performed 24x7x365. |
| **Assist** | Service performed 24x7x365. |
| **Advise** | Service performed 0900-1800 Monday-Friday. |
| **Advise:** Incident Report | Incident of up to 50 hours: Report to be provided within 3 Working Days from the conclusion of the investigation.<br><br>Incident of 50-200 hours: Report to be provided within 10 Working Days from the conclusion of the investigation.<br><br>Over 200 hours: Report to be provided within 15 Working Days from the conclusion of the investigation |

CyberOne

# Cyber Incident Response

## Don't Just Respond. Recover.

## Incidents Commonly Resolved:

- Ransomware & Malware Attacks
- Data Breach
- Phishing & Social Engineering Attacks
- Business Email Compromise
- Intellectual Property Theft
- Employee Misconduct & Insider Threats
- Distributed Denial of Service Attacks
- Cloud Security Incidents

**As a leading NCSC Cyber Incident Response Assured Service Provider, CyberOne believes effective recovery is as crucial as the initial response. When under attack, stemming the bleed is the number one business priority, but this quickly pivots from stopping the attack to initiating the recovery.**

Our 'Defend at Speed' philosophy extends beyond rapid defence to encompass comprehensive recovery, ensuring business continuity and fulfilment of business needs.

In the current threat landscape, a robust Cyber Incident Response and recovery plan is essential for organisations in all sectors. CyberOne's commitment to rapid threat neutralisation, operational restoration and the strengthening of security posture underscores the pivotal role of recovery—it's not an afterthought, but a critical phase in the incident lifecycle.

Our comprehensive approach ensures recovery is seamlessly integrated into the Cyber Incident Response process, enabling Organisations to not only bounce back but also emerge stronger and more resilient.

## Our Approach

**Quick Identification**
Our advanced threat intelligence systems provide early detection to stay ahead of threats.

**Efficient Detection**
Our systems swiftly identify breaches, preventing them from escalating into larger issues.

**Authoritative Response**
We offer a decisive response to contain and eradicate threats while preserving crucial evidence.

**Strategic Protection**
We guard essential assets with cutting-edge security protocols, keeping your operations secure.

**Damage Limitation**
Our experts act quickly to contain and reduce the impact of cyber security incidents.

**Minimised Network Access**
We ensure any unauthorised access is promptly detected and blocked to maintain network integrity.

**Reduced Recovery Time**
Our streamlined processes get your operations back up with minimal downtime.

**Robust Recovery**
We ensure operations are restored with minimal disruption, reinforcing your defences for future challenges.

# Cyber Incident Response: Ready When You Need Us

At CyberOne, Cyber Incident Response is more than a procedure; it's a commitment to operational continuity and cyber resilience. Once a breach occurs, our structured approach kicks in: we ascertain the what, how and who of the breach, assessing the scope of impact and ensuring increased resilience.

## CyberOne Objectives

### Limit the Damage

Immediate actions to contain and minimise the impact.

### Efficient Restoration

Reducing the time and effort required to bounce back from an incident.

### Accelerate Recovery

Streamlining the restoration of services for a swift return to business as usual.

### Restrict Attacker Access

Cutting short the attacker's reach to safeguard your network integrity.

## Why Choose CyberOne Cyber Incident Response Services?

**Direct Access to Cyber Security Experts**
Benefit from unlimited access to CyberOne's experienced team of experts.

**Immediate Analyst Response**
Upon breach report, we dive into action to contain the threat.

**Covert Surveillance Services**
Discreetly monitoring to pre-emptively detect and address cyber threats.

**Malware Reverse Engineering**
Analysis to determine the depth of compromise and prevent repeat occurrences.

**Regular Progress Updates**
Stay informed as the investigation unfolds, with comprehensive communication throughout.

**ISO27001 Compliant Services**
Our operations conform to the highest international security management standards

**NCSC Cyber Incident Response (Standard Level) Assured Service Provider**
Recognised at handling substantial cyber incidents.

**Around-the-Clock UK-Based SOC Analysts**
Ready 24x7 to respond as soon as a breach is detected.

**Insider Threat Investigations**
In-depth probing to resolve and mitigate internal security breaches.

**Incident Classification and Impact Assessment**
Swift determination of attack type and scope for targeted response.

**In-Depth Reporting**
Post-incident analysis outlining security gaps, consolidating learning and reinforcing security.

**Bespoke Plan Design (Optional)**
Craft and implement a plan that aligns with your unique needs.

## About CyberOne

CyberOne is a Microsoft Security Solution Partner and member of the Microsoft Intelligent Security Association (MISA). We deliver one of the UK's most advanced AI-augmented Managed eXtended Detection & Response (MXDR) services, recognised with Microsoft-verified Managed XDR solution status, enabling organisations to move with confidence from risk to resilience. Powered by Microsoft's market-leading security technologies and realised by CyberOne's accredited experts, we help businesses anticipate and contain modern threats so they can thrive.

With 24x7x365 Global SOC coverage, NCSC accredited Cyber Incident Response, CREST SOC and Penetration Testing accreditations and guaranteed SLAs, CyberOne combines Microsoft Security with expert consulting, professional and managed services to protect operations, achieve compliance and build lasting resilience.

## Accreditations & Certifications

CyberOne's services are backed by the world's leading standards bodies including NCSC, CREST and ISO as well as our key technology partners, whilst our experts are backed by industry-leading certifications, cementing our role as leaders in cyber security.


CyberOne

hello@cyberone.security

+44 (0) 3452 757575

cyberone.security