Cyber Incident Retainer Service Definition

Document title	Cyber Incident Retainer Service Definition		
Reference No.	IF-SER-012	**Version**	1.0
Author	Holly Jackson, Cyber Manager		
Reviewed by	Lisa Washer, Head of Cyber		
Issue date	23/07/2026		

Cyber Incident Retainer Service Definition

Document Control

Version	Name	Comment	Date
0.1	Holly Jackson	Initial draft	19/01/2026
0.2	Lisa Washer	Review and amendments	23/01/2026
1.0	Holly Jackson	Final review and amendments	23/01/2026

Correlation Chart

Clause	FSR Code of Practice v2	ISO/IEC 17025:2017	ILAC-G19 :06/2022	ISO 9001:2015	ISO/IEC 27001:2022
Review of Requests, Tenders and Contracts	16	7.1	4.1, 4.7	8	4.2

Cyber Incident Retainer Service Definition

Contents

1. Cyber Incident Retainer Service

1.1 Service Overview

1.1.1 The Cyber Incident Retainer provides organisations with rapid, expert support in the event of a cyber security incident. It ensures pre-agreed access to specialist incident responders, forensic investigators, and advisory resources to help contain, eradicate, and recover from cyber threats.

1.1.2 The service is designed to reduce the impact of cyber incidents by ensuring preparedness, minimising downtime, and enabling swift, coordinated action. It is suitable for organisations seeking assurance that qualified support is immediately available when needed, without the delays associated with ad-hoc procurement.

2. Service Features

2.1.1 Below is a list of the core capabilities and characteristics of the service:

- **Guaranteed Response Availability -** Pre-contracted incident response hours for use during cyber incidents.
- **24/7 Incident Reporting Hotline –** Always available communication channel to initiate incident support.
- **Priority Access to Investigators -** Direct access to trained Digital Forensics & Incident Response experts.
- **Threat Intelligence Briefings -** Regular updates on emerging threats and industry-relevant risks.
- **Retained Advisory Hours -** Hours can be used for preparation, tabletop exercises, readiness assessments, or incident support.
- **Annual Incident Readiness Review -** Review of incident response plans, communication procedures, and escalation paths.
- **Documentation & Evidence Handling -** Support in maintaining the chain of custody and evidence integrity during investigations.
- **Post Incident Reporting -** Detailed technical and executive-level post incident reporting.

3. Service Benefits

3.1.1 The key benefits of this service are outlined below:

- **Reduced Business Impact -** Faster containment and recovery significantly limits operational disruption.
- **Cost Certainty -** Pre-agreed retained hours and rates eliminate emergency procurement costs.
- **Improved Preparedness -** Readiness assessments and tabletop exercises strengthen resilience.
- **Expert Support on Demand -** Immediate access to highly skilled cybersecurity professionals.
- **Regulatory & Compliance Support -** Assistance in meeting industry obligations (PCI DSS, GDPR, DPA, etc.).
- **Enhanced Decision-Making -** Clear, structured advice during high-pressure situations.
- **Trusted Accredited Delivery -** Delivered by CREST and SANS-accredited specialists operating as an NCSC CIR-accredited provider.

4. Scope of Service

4.1.1 Defines what is included and excluded within the service. This should clearly set boundaries around activities, systems, users, and deliverables.

4.2 In-scope activities

4.2.1 The scope of the service includes the following activities:

- Incident triage, assessment, and initial containment guidance
- Digital forensics and evidence acquisition
- Malware analysis and behavioural review
- Network and endpoint compromise analysis
- Log review and artefact investigation
- Incident communications guidance (internal/external)
- Post-incident root cause analysis
- Participation in tabletop exercises
- Access to retained advisory hours

4.3 Out-of-scope activities

4.3.1 The following activities are not included as part of the service scope. However, the organisation can provide support for these activities through additional services or established partner arrangements, subject to separate agreement:

- Full network rebuilds, IT recovery operations, or infrastructure restoration
- Cyber insurance negotiations or legal representation
- Development of full security architecture or long-term remediation projects
- Tools or technologies not provided through the retainer
- Activities exceeding retained hours without prior agreement

4.4 Assumptions and dependencies

4.4.1 Delivery of the service is subject to the following assumptions, constraints, and dependencies, which influence scope, timelines, and outcomes.

- The client provides timely access to systems, logs, and relevant personnel
- The client maintains current contact details for escalation
- Remote access to affected systems is enabled where required
- Third-party suppliers cooperate as necessary

5. Onboarding

5.1.1.1 The onboarding process begins with contract initiation and the recording of all service entitlements, ensuring that the client's retained hours, response commitments, and support provisions are formally captured and available to the delivery team. Once this is complete, a dedicated account manager is assigned to act as the primary point of contact and oversee the service.

5.1.1.2 A kick-off meeting is then held to confirm key stakeholders, establish communication routes, define escalation paths, and gather initial information about the client's environments, systems, and operational context. Following this, the team proceeds with the configuration of all communication channels, including secure email, phone line details, and any other secure access methods required to support incident engagement.

5.1.1.3 Finally, the onboarding phase includes further information collation to support the retained service, ensuring that all relevant documentation, diagrams, contacts, system lists, and security processes are captured. This enables the service team to respond quickly and effectively should an incident arise.

6. Service Delivery Model

6.1.1 The incident response retainer service is delivered through a structured and flexible engagement model that enables rapid support during cyber incidents. Where call-off hours are not utilised for incident response activities, they may be applied to agreed proactive security and preparedness services. All services are delivered in accordance with recognised incident response and digital forensic investigation practices and are tailored to the nature, severity, and complexity of the engagement.

6.2 Onboarding

6.2.1 Information is collated and validated to enable rapid activation of the retainer, including organisational context, technical environment details, and key contacts.

6.2.2 Establishment of communication protocols, escalation paths, and engagement procedures to support informed and timely decision-making during an incident.

6.3 Incident Activation

6.3.1 When the service needs to be activated to support an incident the following activites take place:

- **Onboarding** – Information collation to ensure smooth and informed decision making.
- **Initial Triage and Scoping -** Rapid assessment to confirm incident type, scope, severity, and immediate priorities. This phase includes review of initial indicators, validation of incident status, and confirmation of investigation objectives.
- **Investigation and Analysis -** Detailed forensic investigation of in-scope systems, accounts, and data. Activities may include endpoint, server, cloud, network, and log analysis, evidence preservation, and reconstruction of attacker activity.
- **Impact Assessment and Advisory Support -** Assessment of business, operational, and data impact, including potential regulatory considerations. Advisory support is provided to inform containment, remediation planning, and recovery decisions.
- **Reporting and Close-Out -** Delivery of technical and executive reports detailing findings, timelines, conclusions, and recommendations. A close-out discussion is held to review outcomes and next steps of each incident (s).

6.4 Proactive Services

6.4.1 Proactive services are delivered as part of the incident response retainer to ensure the client derives ongoing value throughout the contract term. Where incident call-off hours are not utilised, they may be applied to agreed proactive activities designed to reduce risk, strengthen response capability, and improve decision-making. Services are delivered through a structured, phased approach aligned to recognised incident response and

security best practices, ensuring the retainer provides measurable and practical benefit beyond reactive incident support.

- **Discovery & Prioritisation** - Review of the organisation's environment, threat profile, and existing controls to identify and prioritise proactive activities. Scope, objectives, and use of available retainer hours are agreed.
- **Readiness & Planning** - Development or refinement of incident response documentation, playbooks, escalation procedures, and communication plans. This phase may include gap analysis against recognised incident response and security frameworks.
- **Threat-Led Assessment** - Targeted assessments based on current threat intelligence and organisational risk, which may include compromise assessments, log and telemetry reviews, and validation of detection and response capabilities.
- **Exercise & Validation** - Delivery of tabletop exercises, simulations, or technical validation activities to test incident response processes, decision-making, and coordination under realistic scenarios.
- **Advisory & Improvement** - Provision of strategic and technical advisory support to address identified gaps, enhance resilience, and strengthen preparedness. Outputs may include recommendations, roadmaps, and implementation guidance.
- **Reporting & Review** - Delivery of summary outputs detailing activities performed, findings, and recommendations, followed by a review session to confirm outcomes and agree next steps for ongoing improvement.

6.5 Typical Timescales

6.5.1 The incident response retainer is provided under an annual contract, enabling support to be activated as required during the term. When an incident is reported and accepted, incident triage will commence within two (2) hours. Delivery timelines thereafter are determined by the incident's complexity, scope, and data availability. Initial triage activities are typically completed within the first 24–48 hours of activation. Investigation and analysis may extend from several days to multiple weeks, depending on the severity and scale of the incident. Reporting is delivered in accordance with agreed timescales following completion of investigative activities.

6.5.2 Investigation effort is determined by the nature and severity of the incident and confirmed through initial scoping. As a guide, the following approach is used:

- **Low Severity** (1–2 days): Phishing analysis, suspicious login activity, single-endpoint malware alerts, or user error reviews.
- **Moderate Severity** (3–5 days): Confirmed malware infections, business email compromise, limited data exposure, or internal misuse affecting a small number of systems.

- **High Severity** (6–10 days): Ransomware incidents, confirmed data breaches, privileged account compromise, or multi-system intrusions.
- **Critical / Major Severity** (10–20+ days): Enterprise-wide ransomware, advanced persistent threat activity, large-scale data exfiltration, or incidents requiring regulatory or legal reporting. A 30-day post-incident monitoring period is recommended to confirm effective recovery. All investigations are supported by a dedicated Cyber Incident Response Specialist, Cyber Incident Manager, and Account Manager.

6.5.3 Proactive services are delivered throughout the term of the annual incident response retainer and are scheduled by mutual agreement to ensure optimal use of available call-off hours. Timescales for proactive activities vary depending on scope, complexity, and organisational readiness.

6.5.4 As a guide, discrete proactive activities such as planning workshops, advisory sessions, or targeted reviews are typically delivered over several days to a few weeks from agreement of scope. Larger or multi-phase activities, including readiness programmes or exercise delivery, may be delivered over longer periods and phased to align with operational priorities.

6.5.5 Delivery timelines are confirmed during the discovery and planning phase for each proactive engagement and may be adjusted to ensure effective outcomes and maximise client value from the retainer.

6.6 Delivery Modes

6.6.1 The service may be delivered remotely, on-site, or through a hybrid approach, depending on incident requirements, data sensitivity, and client preference. Remote delivery is used where secure access can be provided, while on-site support may be required for sensitive environments, evidence handling, or operational constraints.

7. Support Model

7.1.1 The incident response retainer provides the client with continuous 24×7 access to specialist incident response and digital forensics support for the duration of the annual contract. Support is available on a call-off basis for both incident response activities and agreed proactive services.

7.1.2 Incident reporting and activation are available at any time. Upon notification of an incident, triage will commence in accordance with the agreed response times, and an incident response lead will be assigned as the primary point of contact. The incident response lead is responsible for coordinating technical investigation, advisory support, and communications throughout the engagement.

7.1.3 During active incidents, support is delivered through a structured escalation model, enabling rapid mobilisation of additional specialist resources based on incident severity and scope. Regular status updates are provided, and investigative and advisory activities are conducted in line with recognised incident response and digital forensic best practices.

7.1.4 Outside of active incidents, the 24×7 support model enables scheduled access to advisory and proactive services, ensuring the client derives ongoing value from the retainer and maintains a state of readiness throughout the contract term.

7.2 Escalation Paths

7.2.1 Operational escalation is managed by the Incident Manager, who coordinates resources and resolves issues impacting investigation progress. Strategic or commercial escalation is managed by the Account Manager. Escalation to senior technical specialists or management occurs where incident severity, regulatory risk, or complexity increases.

7.3 Optional Support Services

7.3.1 In addition to the core investigation service, optional specialist support services may be provided subject to separate agreement. These include executive-level briefings, regulatory-focused reporting, extended post-incident monitoring, expert witness support, and follow-on incident response or remediation advisory services. Further specialist services may also be provided to support broader incident response and recovery activities, including eDiscovery services to support Data Protection Officers (DPOs) and data breach analysis, malware analysis, threat hunting, penetration testing, and wider cyber security consultancy services. Services may be delivered directly or through established partner arrangements, depending on scope and requirements.

8. Service Level Agreements

8.1 Availability

8.1.1 The incident response retainer provides 24×7, 365-day access to incident response and digital forensics support for the duration of the annual contract term.

8.2 Incident Reporting

8.2.1 Incidents may be reported at any time via the agreed communication channels. An incident is considered accepted once acknowledged by the service provider.

8.3 Response and Triage

8.3.1 Upon acceptance of an incident, initial incident triage will commence within two (2) hours, regardless of day or time. As part of the triage process, a kick-off call will be conducted with relevant stakeholders to confirm the sequence of events, review activities completed to date, validate initial indicators, and agree immediate priorities and next steps. Triage activities include confirmation of incident status, initial scoping, and alignment on investigation objectives.

8.4 Investigation and Support

8.4.1 Investigation and advisory support are delivered on a best-efforts basis in line with the incident's severity, scope, and complexity. The level of effort and resource allocation are confirmed during the initial triage and scoping phase.

8.5 Communications and Updates

8.5.1 During active incidents, regular status updates are provided at agreed intervals. Escalation procedures and primary points of contact are established at activation to support effective coordination and decision-making.

8.6 Reporting

8.6.1 Interim and final reports are delivered in accordance with agreed timescales following completion of investigative activities. Reporting includes technical findings, impact assessment, and actionable recommendations.

8.7 Exclusions

8.7.1 The SLA applies to response and triage commencement times only. Resolution timelines are not guaranteed and are dependent on incident-specific factors including data availability, system access, and client responsiveness.

9. Technical Requirements

9.1.1 Delivery of the service requires appropriate technical access, information, and resources to enable effective investigation activities. The following requirements apply and are confirmed during onboarding.

9.1.2 **Logging and Data Availability -** Access to relevant system, application, security, and network logs is required. The scope and depth of findings depend on log availability, retention periods, and data quality.

9.1.3 **System and Environment Information -** Provision of relevant technical documentation, such as network diagrams, asset inventories, system architecture, identity and access models, and security tooling in use, to support investigation planning and analysis.

9.1.4 **User and Stakeholder Availability -** Availability of system owners, administrators, and subject matter experts to support access provisioning, clarify system behaviour, and validate findings.

9.1.5 **Secure Communications -** Use of secure communication channels for information exchange, including file transfer and reporting, to protect sensitive investigation data.

9.1.6 **Forensic Handling Requirements -** Where forensic imaging or evidence preservation is required, systems must be made available in a manner that supports forensic integrity and minimises operational impact.

9.1.7 **Third-Party Platforms -** Access to cloud providers, software vendors, or external platforms may require additional approvals or legal processes and may impact investigation timelines.

10. Exit and Offboarding

10.1.1 The incident response retainer is delivered on an annual basis and may be renewed for subsequent terms by mutual agreement. Upon expiry or termination of the retainer where renewal is not agreed, an off-boarding process will be undertaken to ensure an orderly transition and closure of services.

10.1.2 All active incident response activities will be completed or formally handed over as agreed with the client. Any outstanding reports, deliverables, or agreed outputs relating to incidents or proactive services delivered during the retainer term will be finalised in accordance with contractual commitments.

10.1.3 Access to client systems, tools, and data provided for the purpose of service delivery will be securely removed. Evidence, investigation artefacts, and reports will be returned to the client or securely retained or destroyed in line with agreed data handling and retention requirements.

10.1.4 A close-out discussion may be conducted to review services delivered during the retainer term, summarise key outcomes, and identify recommendations for ongoing incident response capability and preparedness. Unused retainer hours do not carry over beyond the contract term unless otherwise agreed in writing.

10.1.5 Where requested, reasonable transition support may be provided to assist the client in transferring services to an alternative provider or internal capability.

11. Roles and Responsibilities

11.1.1 The following roles are defined to ensure effective governance, delivery, and communication throughout the Service.

11.2 Account Manager

11.2.1 Acts as the primary commercial and engagement contact for the organisation. Responsible for contract management, service coordination, and strategic escalation. Ensures the service is delivered in line with agreed scope and expectations.

11.3 Incident Manager

11.3.1 Provides overall operational leadership for the investigation. Responsible for incident coordination, prioritisation, decision-making, escalation management, and communication oversight. Acts as the primary operational point of contact throughout the engagement.

11.4 Cyber Incident Response (CIR) Specialist

11.4.1 Responsible for the technical investigation and forensic analysis. Conducts evidence collection, analysis, and documentation in accordance with recognised forensic standards. Provides expert input to support containment, remediation planning, and reporting.

11.5 Client Incident Lead

11.5.1 Acts as the organisation's primary point of contact for the investigation. Coordinates internal stakeholders, facilitates access to systems and information, and supports decision-making and escalation activities.

11.6 Client Stakeholders and Subject Matter Experts

11.6.1 Provide system access, technical knowledge, and operational context required to support investigation activities and validate findings.

*****END OF DOCUMENT*****