National Cyber Security Centre
a part of GCHQ

Assured Cyber Incident Response Scheme

Enhanced Level

Scheme Standard

v1.0

December 2024

A review will take place October - December of each year for publication the following February.

Document owner

National Cyber Security Centre (NCSC). All material is UK Crown Copyright ©

Abbreviations/Definitions

Agreement	Means the “assurance ecosystem agreement” entered into between the NCSC and the Company, including all Schedules, as amended from time to time.
Attacker	Means a malicious actor who seeks to exploit computer systems with the intention of changing, destroying, stealing, or disabling information, and then exploiting the outcome.
Common Supported Operating Systems	Any version of Windows, MacOS or Linux which is currently supported by the vendor
Common Legacy Operating Systems	Any version of Windows, MacOS or Linux, for which vendor support ended in the last five years.
Company (and “Companies” shall be interpreted accordingly)	Means the company which is, or is applying to become, a member of the Scheme.
Customer	Means the organisation which contracts with the Company for the provision of CIR Services.
CIR Head Consultant	Means the person in the Company responsible for the technical delivery of CIR Services.
CIR Service Owner	Means the person in the Company with overall responsibility for the provision of CIR Services.
CIR Service(s)	Means cyber incident response service(s) which provide direct support to organisations when they become victims of a cyber incident.
CIR Team	Means the team of individuals at the Company carrying out the CIR Services.
NCSC	Means the National Cyber Security Centre.
Scheme	Means the Cyber Incident Response Scheme – Enhanced Level.

Scheme Standard	Means the standards which must be met to be part of the Scheme as set out in this document.
We/Us/Our	Means the NCSC.
Working Practices Document	Means the document setting out expected working practices in relation to the Scheme titled 'Assured Cyber Incident Response Scheme – Enhanced Level Working Practices'.
You/Your	Means the Company.

About the Cyber Incident Response (CIR) Scheme – Enhanced Level

Scheme Membership Requirements

1. This document defines the standards required for membership of the Cyber Incident Response Scheme at Enhanced Level. It is split into two sections:

    - The Company Standard - Section A
    - The Technical Standard - Section B

2. You must read this Scheme Standard in conjunction with the Working Practices Document and the Agreement. You must always (unless otherwise approved by the NCSC):

    - satisfy all the requirements defined in this Scheme Standard.
    - meet the requirements of the overarching Ecosystem Agreement.
    - work in accordance with the Scheme Working Practices.
    - be regularly delivering Cyber Incident Response Services.

3. All applicants must already be, and must remain, members of the NCSC's CIR scheme at the Standard Level.

Section A – The Company Standard

Overall Mandatory Defining Features

4. The primary defining feature of a Company on the CIR scheme at the Enhanced Level (over and above the standards of the CIR scheme at the Standard Level) is the ability to track, attribute to, and deal with incidents involving an Advanced Persistent Threat (APT). For these purposes, we define an APT as:

> "A sophisticated, ongoing cyber attack which occurs when an intruder covertly infiltrates a network and remains hidden with the intention of stealing confidential information over an extended period of time."

5. You must be able to accurately attribute incidents (potentially including to a specific APT actor) using sound methodology[1], explain your assessment and express your levels of confidence in that assessment and attribution.

6. Your threat intelligence and incident response and management teams must work together to generate reports based on the Company's own information, to show valid attribution to an APT. These reports must contain enough detail that other incident response companies could use them to detect similar incidents.

[1] While there are no set industry standards for Attribution Methodology, the NCSC believes that the UK Government's 'Professional Development Framework for all-source intelligence assessment' (available from this link) provides a good framework and description of the activities which must be present for an attribution methodology to be described as 'sound'. You should include the principles outlined in the Framework's Appendices: 'The Common Analytical Standards' (available from this link) and 'The Probability Yardstick' (available from this link).

Additional Mandatory Features

Types of Incidents

7. In addition, all Companies on the Scheme, must be able to respond to:

   a. major disruptive incidents (such as ransomware attacks) on organisations with a large number of devices. The NCSC considers ‘a large number’ in this context to be around 5000 minimum.

   b. incidents attracting significant media coverage i.e. where the customer must consider public statements.

   c. incidents affecting a large, publicly listed company. The NCSC considers ‘large’ in this context to mean a company with a market capitalisation of around £50 million minimum.

   d. incidents in specifically regulated sectors, including those regulated by the Network and Information Systems (NIS) Regulations 2018, but excluding the Information Commissioner’s Office as a regulator. Examples involving foreign countries with regulation frameworks which are similar to the UK may be acceptable.

   e. high risk incidents resulting in cyber-enabled data breaches.

   f. incidents affecting organisations requiring response activities in multiple jurisdictions. This includes having processes to deal with local laws and understanding how those impact on response activities.

   g. incidents where the customer engaged Outside Counsel in relation to the incident.

   h. incidents where Law Enforcement (“LE”) is engaged, including:

      i. sharing information on an incident with LE on the instructions of the victim.

      ii. co-operating on an incident where LE are running a concurrent investigation.

i. co-operating on an incident where the UK's NCSC was involved. Evidence of engagement with the National CERTs of allied foreign countries may be considered if the NCSC deems it appropriate.

Communication

8. In all the aforementioned scenarios, the team responding to the incident must include members who are able to competently brief Customers, from desk level to board level, advising on what actions the Customer should take both technically and in terms of their wider operation and covering such topics as:

   a. threat intelligence

   b. attribution

   c. possible targets

   d. the attacker's motivations

   e. the attacker's predicted or likely next steps.

Response Times

9. You must provide round-the-clock contact options and guaranteed response times for both new customers and existing customers with live incidents. The NCSC considers one hour to be the maximum reasonable response time.

10. You must be able to deploy team members to identified locations globally within one working day of being formally engaged. 'Deploy' means the team members must have begun to travel, subject to sanctions, visas, legal and safety constraints.

Network Security

11. Subject to paragraph 18 of the Working Practices Document, you must maintain an in-date Cyber Essentials Plus certification for all the systems on which information relating to Customers' engagements is stored and processed.

Personnel

12. You must carry out all the following activities: We have divided them into two categories and given a role title to each. These role titles may not exist in your company, but we do expect there to be a defined person who is accountable to the NCSC for ensuring they are carried out.

    - Business requirements – "CIR Service Owner"
    - Technical Oversight and Health of the Company's CIR Service – "CIR Head Consultant"

CIR Service Owner

13. While we do not expect one person to personally deliver all aspects of the incident response service, the named CIR Service Owner must be directly accountable for delivery of the service as a whole. Under the Scheme, the following tasks are all mandatory:

    a. Acting as the NCSC's primary contact for all Scheme communications and all onward action.

    b. Positively contributing to the wider Scheme community. This includes:

        i. contributing to Scheme improvements.

        ii. taking an active part in community meetings.

iii. meeting with the NCSC from time to time, as requested.

c. Actively ensuring that the Company meets all its obligations under this Scheme and the associated Agreement.

d. Submitting, on time, an annual Management Information Report to the NCSC.

e. Documenting and maintaining Company Quality Management processes as they apply to the delivery of their CIR Service.

f. Reviewing and updating Company processes in accordance with the Scheme Standard.

g. Ensuring that everyone involved in the CIR Service adheres to the Company's own documented processes.

h. Providing the company's Cyber Essentials Plus certificate number to the NCSC on an annual basis.

i. Actively monitoring and managing Customer relationships and seeking Customer feedback to provide evidence of Customer satisfaction with the Company's work.

CIR Head Consultant

14. The CIR Head Consultant must have achieved a UK Cyber Security Council 'Incident Response' Title at the 'Chartered' level.

15. The CIR Head Consultant must be a permanent employee and not employed by any other CIR company.

16. The CIR Head Consultant must be directly accountable for the technical quality and

health of the CIR Service. The following are all mandatory:

a. Acting as the NCSC's primary contact for all technical feedback and questions regarding the technical aspects of the CIR Service, and any onward action required.

b. Accountability for the technical quality and standard of delivery of the CIR Service and each engagement, ensuring they meet both the CIR and company's own standards. We do not expect the CIR Head Consultant to personally lead and quality control every engagement, but we do expect the company to have and adhere to a quality control process, for which the CIR Head Consultant is accountable.

c. Maintaining the overall technical health of the CIR Team. This includes ensuring all CIR Team members have appropriate professional training and development plans. This may include, by way of example only:

   i. Identifying mentors for inexperienced staff.
   ii. Ensuring there is a training lead for CIR Team staff.

17. For every engagement the CIR Head Consultant:

   a. is accountable for the engagement and ensuring the response team members have an appropriate mix of expertise and experience to meet the Customer's needs.
   b. must ensure that a senior consultant is contactable by all members of the response team and by the customer for the duration of the engagement.
   c. is accountable for the behaviours, actions and advice given by their team.
   d. is accountable for conducting the engagement in accordance with the Company's methodology, which they must have previously shared with the Customer.

Threat Intelligence Team

18. The Company must have staff who routinely produce threat intelligence. This includes:

    a. tracking APT actors as well as cyber-criminal groups.

    b. tracking all public reporting on attackers, and compiling Indicators of Compromise (IOC), Tactics, Techniques and Procedures (TTP), and malware information for use by the incident response and management teams.

    c. synthesising the Company's own raw data, as well as third party reporting and raw data to create independent findings. (Note that it is not sufficient to rely wholly on third party analysed threat intelligence.)

    d. create reports similar to NCSC Advisories to be shared with external stakeholders. Click here to see an example of an NCSC Advisory.

Section B - Required Technical Capabilities

Endpoint Agent

19. The NCSC defines an Endpoint Agent as:

    "Software installed on a computing device with the ability to detect and record details of process and file creation, and network connections. The Endpoint Agent must be able to collect files and memory regions from systems either based on specific locations or on metadata or on YARA search criteria (or equivalent search criteria). The Endpoint Agent may have other capabilities including being able to make changes to endpoint systems for remediation purposes."

20. The Company must:

    a. supply Endpoint Agent capability to the Customer (such as installation binaries) within 24 hours of formal engagement.

    b. deploy their Endpoint Agent solution to a large number of devices in a single engagement. The NCSC considers 'a large number' in this context to be around 5000 or more.

    c. provide the Customer with:

       i. documentation to allow a customer to deploy the Endpoint Agent on their estate.

       ii. a written technical overview of the Endpoint Agent capability so that they are fully aware of the implications and course of action from release to clean up.

       iii. documentation to explain the impact of deploying the Endpoint Agent, including any known compatibility issues and load on devices or network bandwidth etc.

21. The Endpoint Agent solution must:

    a. be usable on both Common Supported Operating Systems, and Common Legacy Operating Systems.

    b. support:

        i. near real-time collection of process creation, network activity and system changes.

        ii. collection of artefacts such as files and system memory.

        iii. searching for files that match known signatures.

        iv. isolation of devices.

        v. termination of processes.

22. There must be round-the-clock support during the Endpoint Agent deployment. The Company is responsible for the performance of all support personnel, whether direct employees or not.

Log Collection and Analysis

23. The Company must be able to:

    a. assist the customer in log collection at scale.

    b. assist the customer to rapidly set up and configure centralised logging for on-premises devices where no solution (or an unusable solution) has previously existed.

    c. use standard in-situ operating system tools to do basic log triage.

    d. collect logs from M365 and AWS Cloud providers as a minimum.

e. analyse logs at scale. This includes cleaning, transforming, processing, and ingesting logs to appropriate investigation environments. The NCSC considers ‘at scale’ as around 100Gb minimum.

f. build statistics and insight from large data sets using a basic understanding of statistical analysis techniques and methods.

Network Traffic Inspection

24. The Company must:

a. be able to deploy network traffic interception capability to gain visibility of network activity.

b. be able to start deployment of network capture equipment to a customer site within 24 hours of formal engagement.

c. be able to collect raw network traffic in PCAP format or a format which can be converted to PCAP. The collection must be configurable to filter traffic, as a minimum based on standard BPF filters, although more complex filtering is permitted.

d. have equipment available to allow the deployment of networks taps to intercept traffic and not be wholly reliant on span ports to intercept traffic.

e. have equipment available to intercept high-speed (at least 10Gb) copper or fibre TCP/IP networks.

f. be able to identify anomalies or unusual flows in network traffic.

g. work with customers to identify where to deploy network inspection tooling.

h. be able to collect network traffic from within any wholly virtualised environment.

Digital Investigation/Analysis

25. The Company must be able to:

    a. conduct host forensics on Common Supported Operating Systems and Common Legacy Operating systems. This includes:

        i. full disk imaging and analysis

        ii. memory capture and analysis

        iii. device log collection and analysis.

    b. collect and analyse Infrastructure as a Service (IaaS) host images from Azure and AWS.

    c. conduct systematic forensic analysis, complying with best practice with respect to the collection of digital forensic evidence such that any information obtained may, if necessary, be relied upon in a civil court of law.

    d. access a suitably controlled area for storage of evidence items.

Malware Reverse Engineering

26. The Company must be able to:

    a. perform both static and dynamic malware reverse engineering.

    b. reverse engineer any software found on Common Supported Operating Systems to the degree needed to identify:

        i. capabilities of malware.

        ii. indicators of compromise (IOC) to use for detection of activity.

iii. relationships between malware samples and other known samples to identify the likely actor behind the attack.

c. understand and handle malware samples safely, ensuring that they do not accidentally infect any systems.

d. create Malware write-ups based on your own analysis, which are equivalent to those produced by national agencies or Computer Emergency Response Teams (CERTs). (An example of such a write-up is the Cybersecurity and Infrastructure Security Agency's write-up of ICONICSTEALER, available here.)

Processes

27. You must have a process for obtaining fully informed consent from the Customer to make changes to their systems.

28. You must not mandate usage of your own tooling. If a Customer already has tooling in place, and it is sufficient for the job, you must be able to supply services to that Customer. If the tooling is not sufficient, you must explain the situation to the Customer and gain their agreement to replace it with your tooling.