National Cyber Security Centre
a part of GCHQ

Cyber Incident Response Technical Standard (Level 2)

Version 1.5

April 2023

Contents

1. Definitions used in this document

Attacker

Malicious actor who seeks to exploit computer systems with the intent to change, destroy, steal or disable their information, and then exploit the outcome.

CIR

Cyber Incident Response. The activities which take place during and immediately after a cyber incident response, such as determining the extent of an incident, managing its impact, restoring systems, and working to increase security across the network.

CIR Provider

The company providing the cyber incident response (CIR) service.

Common Legacy Operating Systems

Any version of Windows, MacOS or Linux for which vendor support ended in the previous 5 years.

Common Supported Mobile Operating Systems

Any version of Android or iOS which is currently supported by the developer.

Common Supported Operating Systems

Any version of Windows, MacOS or Linux which is currently supported by the developer.

Engaged

A Target Organisation is engaged by a CIR Assured Service Provider at the point at which a contract has been signed in support of an initial scope of work.

Endpoint Detection and Response (EDR)

Activities focussed on detecting and investigating suspicious activities and other problems on end-user devices such as workstations, laptops and smartphones.

MITRE ATT&CK

MITRE ATT&CK is a knowledge base of adversary tactics and techniques used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cyber security community.

STiX v2.1

Structured Threat Information Expression (STIX™) is a language and serialisation format used to exchange cyber Threat Intelligence (TI).

Target Organisation

The organisation that is a consumer of the CIR service.

Threat Intelligence (TI)

Threat Intelligence. Information about threats that has been aggregated, analysed and enriched to provide the useful context for decision-making processes.

TTPs

The **Tactics**, **Techniques** and **Procedures** of an attacker. Patterns of activities or methods associated with a specific threat actor or group of threat actors.

Unusual Operating Systems

Any non-mobile operating system not covered by the definitions of:

- common supported operating systems
- common legacy operating systems
- common supported mobile operating systems

2. Scheme Introduction

1. Incident Response takes place during and immediately after a cyber incident. This document sets out the standards which current and prospective **CIR Assured Service Providers** are assessed against, in order to become an NCSC-assured CIR Assured Service Provider for Level 2. It defines the expected range of cyber crisis management assistance of an incident for Target Organisations dealing with category 3, category 4, and category 5 incidents, as defined by the NCSC's cyber attack categorisation system.
2. CIR Assured Service Providers will be expected to perform technical analysis and suggest practical containment/mitigation alongside longer term remediation and eradication guidance (see section 8 for more information on the capabilities an Assured Service Provider is required to demonstrate). The scope of work in any specific engagement will be set by the customer and so the scope of work required may be changed at any point throughout the project (dependent on the contractual agreement and the severity of the incident).
3. The Cyber Incident Response (CIR) Level 2 (L2) scheme has been introduced to complement the original CIR scheme, which will now be re-designated as CIR "Level 1" (L1). The aim of CIR L2 is to assure providers against a different standard, which calls for a more widely attainable level of technical experience in order to widen the supply of assured CIR providers.
4. The NCSC has designed the standards for the two schemes to reflect the following typical use cases:
    - CIR L1: the requirements of the CIR L1 standard are designed to support target organisations which are typically at risk of sophisticated and bespoke cyber attack. Such organisations are likely to include UK central government, organisations forming part of the Critical National Infrastructure or which operate in a regulated sector or more than one country.
    - CIR L2: the requirements of the CIR L2 standard are designed to support target organisations which are at risk of common cyber attack. Such organisations are likely to include most private sector organisations, charities, Local Authorities and smaller public sector organisations and organisations which operate predominantly in the UK.
5. For clarity, providers which have been assured against either the CIR L1 standard or the CIR L2 standard – or both standards – will be able to offer CIR services to any target organisation. Target Organisations will need to do their own due diligence to decide the suitability of the Assured Service Providers to meet their needs.
6. CIR Assured Service Providers must advise clients that they are members of an NCSC Assured Scheme and that they are required to submit limited, non-attributable information about their incident response engagements to the NCSC. The NCSC will use this information for trend analysis purposes, to inform future advice and guidance to the UK and help improve the NCSC's products and services.
7. CIR Assured Service Providers must always act in accordance with the instructions of the Target Organisation. CIR Assured Service Providers are expected to advise the Target Organisation but if the Target Organisation decides not to take the advice (or they do not wish the CIR Assured Service Provider to undertake certain activities) then there will be no negative consequence in the assessment of the CIR Assured Service Provider against this Standard.

3. Scheme Principles

8. Incident response and management must be a core business function of CIR Assured Service Providers. CIR Assured Service Providers should be capable of supporting a Target Organisation (where requested) to eradicate an attacker and secure their environment.
9. In practice this means providing evidence of how responses to incidents can be performed across the UK and ensure that the Target Organisation is assisted to recover as effectively as possible. This could be either as a direct part of the CIR team, or through working with other organisations with relevant expertise, or other CIR Assured Service Providers.
10. CIR Assured Service Providers **must** provide evidence that they:
    - provide technical support to targets of cyber incidents between 9am and 5pm, 7 days a week
    - have 24/7 telephone service for initial Target Organisation engagement
11. CIR Assured Service Providers must evidence their **methodology** and **processes.** Simply having access to skilled analysts is not sufficient; they must operate within a mature structure around a repeatable methodology.
12. In addition, CIR Assured Service Providers must:
    - clearly demonstrate the use of appropriate analysis methods and selection of appropriate tools to provide an effective response to common attacker methodologies.
    - clearly demonstrate their ability to give detailed advice and guidance on eradicating an attacker and securing affected environments.

4. Use of applied Threat Intelligence

13. CIR Assured Service Providers must make use of Threat Intelligence that they gather as part of their day-to-day operations (ie outside of incidents), during incident response in order to enhance the management of the incident.
14. CIR Assured Service Providers may acquire Threat Intelligence from various sources, including publicly accessible intelligence, internal tools and techniques or licensed Threat Intelligence platforms.
15. CIR Assured Service Providers must demonstrate how Threat Intelligence is applied to the benefit of the Target Organisation, including sharing this information with the Target Organisation where appropriate.
16. CIR Assured Service Providers must understand and make use of the MITRE ATT&CK framework and YARA rules.

5. Communication requirements

17. CIR Assured Service Providers must demonstrate how they communicate effectively across technical and managerial staff.
18. CIR Assured Service Providers must have a repeatable methodology for capturing and recording every substantive step of the incident including actions, findings and recommendations.
19. CIR Assured Service Providers reports must be written so that they can be widely understood across the Target Organisation. Where it is impossible to remove jargon, technical wording or company-specific words, clear explanations must be given.

Stakeholder communications

20. CIR Assured Service Providers must obtain a contact list for all relevant internal stakeholders in the following areas:
    - technical lead/recovery manager
    - crisis management, business continuity, disaster recovery
    - investigators and analysts, cyber security specialists
    - IT and infrastructure
21. The list should be updated, if necessary, over the course of the incident.
22. CIR Assured Service Providers do not need to be responsible for all elements of the response plan, but they must ensure that lines of responsibility are clear and recorded.

6. Staff requirements

23. CIR Assured Service Providers must offer a diverse technical skill set at all managerial and operational levels, CIR Assured Service Provider staff must have the relevant experience with appropriate qualifications.

24. Where requested by the Target Organisation, CIR Assured Service Providers must be able to deploy team members to identified locations in the UK to support the Target Organisation. If required by the Target Organisation, deployment must start on the next working day after the commencement of the engagement.

Team Lead responsibilities

25. CIR Assured Service Providers must designate an individual as the Team Lead. The Team Lead must be appropriately qualified and experienced and is accountable for the technical execution of the incident response.

26. Whilst the Team Lead is unlikely to personally deliver all aspects of the service, they are accountable for ensuring that it is delivered to a high standard, and for the overall quality of the technical output of the incident response.

27. The Team Lead is accountable for:

- identifying and fulfilling Target Organisation requirements with regard to the incident response
- ensuring that individuals assigned to a task have the appropriate technical competence
- maintaining effective communication channels with the Target Organisation, and all other interested parties
- reporting to the Target Organisation at regular intervals on progress or, as necessary, applying for further instructions or approval to proceed
- escalating any risks or issues to the Board as appropriate
- knowledge transfer to other individuals within the Target Organisation

7. Scope of work

28. As the scope of work is liable to change during an engagement, all versions of the scope of work must be retained. This will allow both CIR Assured Service Providers and Target Organisations to see what work was agreed, and to assess the standard of the completed work.
29. As part of the audit process, any complaints made against a CIR Assured Service Provider may be investigated. The scope of work is a critical piece of evidence in such cases.
30. Throughout the incident, the scope may be altered if both parties have agreed, and the amendment has been logged.
31. CIR Assured Service Providers must fully understand all applicable laws relevant to the service provided.
32. CIR Assured Service Providers must ensure that there is a clear closedown of the engagement and that the Target Organisation understands and accepts responsibility for any outstanding activities.

8. Technical capabilities for incident investigation

34. CIR Assured Service Providers must have the capability to mitigate common incidents. CIR Assured Service Providers may not necessarily have the level of staffing required to actually make changes to a Target Organisation's IT estate but must demonstrate the capability to advise on containing or eradicating an incident.

Endpoint Detection and Response (EDR)

35. CIR Assured Service Providers must demonstrate the capability to deploy EDR capability rapidly to gain visibility of hosts running current supported versions of the Microsoft Windows Operating System and at least one major version earlier.

36. Provided Target Organisations can meet the necessary requirements to enable the deployment, CIR Assured Service Providers must demonstrate the capability to provide EDR deployment resources (such as installation software) within 24 hours of engagement. A CIR Assured Service Provider will not be adversely assessed against the standard if the speed of deployment is affected by issues outside of its control.

37. EDR deployment must be supported 24/7. Where the support personnel are not direct employees of the CIR Assured Service Provider, CIR Assured Service Providers remain responsible for their performance and must ensure that there is a proper agreement with external personnel to cover 24/7 support of the EDR while deployed.

38. A full technical overview of the EDR capability service must be offered to the Target Organisation, so that they are fully aware of the implications and course of action from release to clean up. The Target Organisation must decide whether or not to use the tool.

39. CIR Assured Service Providers must demonstrate the capability to effectively gain visibility on the Target Organisation systems and so EDR suites deployed must support:

    - near real-time collection of process creation, network activity and system changes
    - collection of artefacts such as files and system memory
    - searching for files that match known signatures

40. EDR products can support other functionality, such as response actions on end points to block or remove attacker activity.

Log collection and analysis

41. CIR Assured Service Providers must demonstrate the capability to assist in log collection at reasonable scale.

42. CIR Assured Service Providers must demonstrate the capability to perform log analysis for, as a minimum, on-premise Microsoft Windows, Microsoft 365 and Google Workspace.

43. Target Organisations are expected to supply logs to CIR Assured Service Providers for analysis. CIR Assured Service Providers must demonstrate the capability to support Target Organisation staff to obtain these logs.

44. CIR Assured Service Providers must demonstrate maturity in log analysis approach; that is, the ability to clean, transform, process, and ingest log sources to appropriate investigation environments.

Digital investigation/analysis

45. CIR Assured Service Providers must demonstrate the capability to undertake host forensics, encompassing artefact analysis, on-host historic log analysis and full disk forensics, on currently supported versions of the Microsoft Windows Operating Systems. They must also support at least one major earlier version.
46. Host forensic tools can be developed in-house, be acquired from a licensed vendor or open source. CIR Assured Service Providers must justify the methodology or techniques and provide supporting evidence which demonstrates due diligence and real-world experience.
47. Under all circumstances, CIR Assured Service Providers must conduct forensic analysis in a structured way which, if necessary, could be presented in a court of law in any relevant jurisdiction (for example, following the spirit of the ACPO Good Practice Guide [PDF], noting that the actual guide is slightly outdated).
48. CIR Assured Service Provider staff must be trained to handle, capture and document evidence according to appropriate industry guidelines. CIR Assured Service Providers should also have a suitable access-controlled storage area for evidence items.

Malware analysis

49. CIR Assured Service Providers must demonstrate the capability to perform dynamic malware analysis.
50. CIR Assured Service Providers must demonstrate the capability to perform this for any software found on Microsoft Windows Operating Systems.
51. CIR Assured Service Providers must be able to identify:
    - indicators of Compromise (IOC) to use for detection of activity
    - likely function of malware samples (keylogger/remote access trojan/adware etc)

Ad hoc tooling

52. CIR Assured Service Providers must have a recorded process for internal and external sign-off on ad hoc tools developed by the incident response team for dealing with specific incident-related issues. The internal process must ensure that the CIR Assured Service Provider is aware of any risks of deploying the capability and have accepted them. As part of the external sign-off process, the Target Organisation must understand and accept those risks.

Actions to resolve incidents

53. CIR Assured Service Providers must demonstrate the ability to support Target Organisations to perform actions to contain, mitigate, remediate, eradicate and recover from incidents affecting their systems (as detailed in the NCSC's Incident Management guidance on technical response capabilities).
54. CIR Assured Service Providers must demonstrate the ability to:

- offer tailored, specific guidance regarding the technical steps required for incident resolution for Microsoft Windows systems
- understand the risks of mitigation activities they recommend
- explain the possible downsides so that the Target Organisation can take an informed decision on whether to go ahead

55. For example, they must be able to describe how to carry out a full password reset of all Windows Active Directory credentials across a domain, explain the possible risks involved in doing so, and guide someone through those steps.

56. CIR Assured Service Providers must be able to offer general guidance on technical steps required for incident resolution involving other IT components (such as routers, firewalls, Network Attached Storage (NAS) devices). They are not expected to give precise step by step guidance for every possible product or platform. For example, they must be able to describe setting up a firewall rule to block traffic egress but would not be expected to know exactly how to do it on every single firewall platform on the market.

Commitment to team capability development and R&D

57. As tools, techniques and procedures within cyber incidents are constantly evolving, CIR Assured Service Providers must demonstrate how they develop both their personnel and their technical capabilities.

58. CIR Assured Service Providers must demonstrate both training pathways used to train up new staff, and dedication to continuous professional development.

59. CIR Assured Service Providers must demonstrate regular due diligence reviews of their tools and capabilities as outlined in the sections above to ensure they remain fit for purpose.