NHS England

Cyber Assessment Framework–aligned Data Security and Protection Toolkit

Strengthening Assurance – Independent Assessment and Audit Framework

Creating a culture
of Improvement

Information and Technology
for better health and care

Final

17/12/24

Objective C – Detecting cyber security events

Description

Capabilities exist to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential function(s).

Overview of the underlying Principles

Principle C1: Security monitoring

Principle C2: Proactive security event discovery

Principle C1: Security monitoring

Description

The organisation monitors the security status of the network and information systems supporting the operation of essential functions in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.

Overview of the underlying Contributing outcomes

Contributing outcome C1.a – Monitoring coverage

Contributing outcome C1.b – Securing logs

Contributing outcome C1.c – Generating alerts

Contributing outcome C1.d – Identifying security incidents

Contributing outcome C1.e – Monitoring tools and skills

Contributing outcome C1.a – Monitoring coverage

Description

The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function(s).

The expectation for this contributing outcome is **Partially Achieved.**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	**Partially Achieved** All the following statements are true:	**Achieved** All the following statements are true:
NA#1. Data relating to the security and operation of your essential function(s) is not collected. NA#2. You do not confidently detect the presence or absence of Indicators of Compromise (IoCs) on your essential function(s), such as known malicious command and control signatures (for example, because applying the indicator is difficult or your log data is not sufficiently detailed). NA#3. You are not able to audit the activities of users in relation to your essential function(s). NA#4. You do not capture any traffic crossing your network boundary including as a minimum IP connections.	PA#1. Data relating to the security and operation of some areas of your essential function(s) is collected but coverage is not comprehensive. PA#2. You easily detect the presence or absence of IoCs on your essential function(s), such as known malicious command and control signatures. PA#3. Some user monitoring is done, but not covering a fully agreed list of suspicious or undesirable behaviour. PA#4. You monitor traffic crossing your network boundary (including internet protocol (IP) address connections as a minimum).	A#1. Monitoring is based on an understanding of your networks, common cyber-attack methods and what you need awareness of in order to detect potential security incidents that could affect the operation of your essential function(s) (such as the presence of malware, malicious emails, user policy violations). A#2. Your monitoring data provides enough detail to reliably detect security incidents that could affect the operation of your essential function(s). A#3. You easily detect the presence or absence of IoCs on your essential function(s), such as known malicious command and control signatures. A#4. Extensive monitoring of user activity in relation to the operation of essential function(s) enables you to detect policy violations and an agreed list of suspicious or undesirable behaviour. A#5. You have extensive monitoring coverage that includes host-based monitoring and network gateways.

		A#6. All new systems are considered as potential monitoring data sources to maintain a comprehensive monitoring capability.

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework (CAF).

The approach and documentation list described below provides guidance on how to conduct testing and should be adapted as appropriate in order to assess whether the NHS providers outcomes are effectively achieved.

Suggested approach to testing – Partially Achieved

1. **Monitoring coverage** – Enquire with the organisation which data sources it collects security logs for. Obtain and inspect documentation provided by the organisation showing how it has prioritised these sources based on risks to its essential functions. (PA#1)
2. **Security monitoring activities** – Inspect documents provided by the organisation relating to its security monitoring activities and/or discuss with management, which evidence how it:
    a) Detects the presence or absence of indicators of compromise (IoCs)- the organisation should be able to demonstrate how IoCs would be easily detected. (PA#2, A#3)
    b) Monitors user activity - at least some user activity should be monitored, based on risk or agreed list of suspicious or undesirable behaviours. (PA#3)
    c) Monitors traffic crossing the network boundary- as a minimum, IP address connections should be monitored. (PA#4)

Additional approach to testing – Achieved

1. **Security monitoring strategy** – Obtain and inspect documents provided by the organisation to demonstrate that it has a comprehensive strategy for security monitoring which has been specifically targeted towards:
    a. The key risks the organisation has identified to its essential functions (A#1)
    b. The organisation's own network architecture (A#1)
    c. The attack techniques to which the organisation is most susceptible, based on its architecture (A#1)
2. **Security event and incident sampling –** Obtain the list of security incidents, checking how frequently incidents are identified and raised based on the organisation's monitoring data. From this list, inspect a sample of incidents to ascertain how much detail was provided through the monitoring logs, and whether this detail was enough to support identification of more sophisticated threats through monitoring and threat hunting. (A#2)
3. **User monitoring** – Obtain and inspect the list of suspicious or undesirable behaviour that is used to monitor user behaviours against. Obtain evidence that this monitoring takes place. (A#4)
4. **Security event monitoring** – Inspect documents provided by the organisation relating to its security monitoring coverage and assess whether:
    a. The organisation collects security logs from a wide enough range of sources to ensure that it is able to detect potential security incidents across all critical networks and systems. (A#5)
    b. Extensive monitoring is performed on network gateways. (A#5)
    c. Host-based monitoring is performed on devices which the organisation has identified as critical. (A#5)

5. **Maintaining comprehensive monitoring** - Verify documents provided by the organisation which demonstrate its process for evaluating new systems being added to its networks and determining whether they should be monitored as data sources. (A#6)

Suggested documentation – Partially Achieved

- Documents showing data sources being monitored and rationale
- Procedures for detecting IoCs
- Procedures for monitoring users
- Procedures for monitoring network boundary traffic

Additional documentation – Achieved

- Security Monitoring Strategy;
- List of security incidents;
- Documents showing extensive monitoring coverage
- Procedures for considering new systems as potential monitoring sources

Contributing outcome C1.b – Securing logs

Description

You hold log data securely and grant appropriate access only to accounts with business need. No system or user should ever need to modify or delete master copies of log data within an agreed retention period, after which it should be deleted.

The expectation for this contributing outcome is **Partially Achieved**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	**Partially Achieved** All the following statements are true:	**Achieved** All the following statements are true:
NA#1. It is possible for log data to be easily edited or deleted by unauthorised users or malicious attackers. NA#2. There is no controlled list of the users and systems that can view and query log data. NA#3. There is no monitoring of the access to log data. NA#4. There is no policy for accessing log data. NA#5. Log data is not synchronised, using an accurate common time source.	PA#1. Only authorised staff can view log data for investigations. PA#2. Authorised users and systems can appropriately access log data. PA#3. There is some monitoring of access to log data, (including copying, deleting or modification, or even viewing)	A#1. The integrity of log data is protected, or any modification is detected and attributed. A#2. The logging architecture has mechanisms, processes and procedures to ensure that it can protect itself from threats comparable to those it is trying to identify. This includes protecting the essential function(s) itself, and the data within it. A#3. Log data analysis and normalisation is only performed on copies of the data keeping the master copy unaltered. A#4. Log data are synchronised, using an accurate common time source, so that separate datasets can be correlated in different ways.

		A#5. Access to log data is limited to those with business need and no others. A#6. All actions involving all log data can be traced back to a unique user (including copying, deleting or modification, or even viewing) A#7. Legitimate reasons for accessing log data are given in use policies.

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework (CAF).

The approach and documentation list described below provides guidance on how to conduct testing and should be adapted as appropriate in order to assess whether the NHS providers outcomes are effectively achieved.

Suggested approach to testing – Partially Achieved

1. **Authorised user access** – Obtain and inspect documents provided by the organisation evidencing that:
    a) Only authorised staff can view log data for investigation. The organisation should have defined who the authorised users are. Obtain a sample of users that have accessed log data and verify that they are authorised; (PA#1)
    b) Authorised users and systems can appropriately access log data. The organisation should have defined the authorised users and systems, and which logs they have access to. Obtain a sample of users and systems that have accessed log data and verify that they are authorised; (PA#2)
2. **Monitoring access** - Access to log data should be monitored, including monitoring of copying, deleting, modifying, and viewing actions. Obtain evidence of this monitoring. (PA#3)

Additional approach to testing – Achieved

1. **Authorised user access -** Obtain and inspect documents provided by the organisation evidencing:
    a) How it protects the integrity of log data, and ensures that any modification is detected and attributed. (A#1)
    b) How it has configured access controls so that log data can only be accessed by those with business need and no others. Obtain a list of restricted users who are able to access logging data to verify this is limited to those with business need and this is reviewed on a regular basis. (A#5)
    c) How it monitors all actions involving log data including copying, deleting, modifying and viewing, ensuring these can be traced back to individual users. (A#6)
    d) That it has use policies which define legitimate reasons for accessing log data. (A#7)
2. **Protection against threats -** Verify what mechanisms, processes and procedures are in place to protect the logging architecture from cyber threats. The organisation should be able to justify how their measures ensure log data remain protected in likely threat scenarios. (A#2)
3. **Maintenance of log data -** Obtain and inspect documents provided by the organisation evidencing:
    a) How it ensures that log data analysis and normalisation is only performed on copies of the data keeping the master copy unaltered; (A#3)
    b) That it has synchronised log data, using an accurate common time source, so that separate datasets can be correlated in different ways. (A#4)

Suggested documentation – Partially Achieved

- Documents evidencing log access controls
- Lists of authorised users and systems
- Procedures for monitoring access and actions to log data

Additional documentation – Achieved

- Documents evidencing log data access controls
- Procedures for monitoring access and actions to log data
- Lists of authorised users and systems
- Log data use policies
- Procedures for protecting log data against threats
- Procedures for maintaining log data master copies
- Evidence of time synchronisation of log data

Contributing outcome C1.c – Generating alerts

Description

Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts.

The expectation for this contributing outcome is **Partially Achieved**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	**Partially Achieved** All the following statements are true:	**Achieved** All the following statements are true:
NA#1. Alerts from third party security software is not investigated for example anti-virus (AV) providers. NA#2. Logs are distributed across devices with no easy way to access them other than manual login or physical action. NA#3. The resolution of alerts to a network asset or system is not performed. NA#4. Security alerts relating to essential function(s) are not prioritised. NA#5. Logs are reviewed infrequently.	PA#1. Alerts from third party security software are investigated, and action taken. PA#2. Some, but not all, log data can be easily queried with search tools to aid investigations. PA#3. The resolution of alerts to a network asset or system is performed regularly. PA#4. Security alerts relating to some essential function(s) are prioritised. PA#5. Logs are reviewed at regular intervals.	A#1. Log data is enriched with other network knowledge and data when investigating certain suspicious activity or alerts. A#2. A wide range of signatures and indicators of compromise is used for investigations of suspicious activity and alerts. A#3. Alerts can be easily resolved to network assets using knowledge of networks and systems. The resolution of these alerts is performed in almost real time. A#4. Security alerts relating to all essential function(s) are prioritised and this information is used to support incident management. A#5. Logs are reviewed almost continuously, in real time. A#6. Alerts are tested to ensure that they are generated reliably and that it is possible to distinguish genuine security incidents from false alarms.

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework (CAF). The approach and documentation list described below provides guidance on how to conduct testing and should be adapted as appropriate in order to assess whether the NHS providers outcomes are effectively achieved.

Suggested approach to testing – Partially Achieved

1. **Resolving alerts -** Obtain and inspect documents provided by the organisation evidencing that it has procedures in place to:
    a) Act on alerts from third-party security software, including investigation of the alert and subsequent actions being taken. (PA#1)
    b) Identify and resolve alerts as part of its business as usual activities. (PA#3)
    c) Identify alerts related to essential functions and prioritise them (PA#4, A#4)
2. **Sample testing -** Obtain samples of alerts to verify that procedures outlined in 1) have been successfully implemented and followed by the organisation. (PA#1, PA#3, PA#4, A#4)
3. **Using log data -** Verify that the organisation has:
    a) Technical capabilities to query log data with search tools to aid investigations. Not all the organisation's log data needs to be searchable. (PA#2)
    b) A defined schedule for the review of logs which the organisation can justify in the context of the threats it faces. Evidence should be provided that logs have been reviewed at the correct intervals. (PA#5)

Additional approach to testing - Achieved

1. **Alert investigation** – Inspect the process for investigating alerts and suspicious activity. Assess whether the organisation has the technical capability to correlate log data from multiple different sources (such as servers, firewalls, devices and other sources) and does so to identify information relevant to a particular potential incident. (A#1)
2. **Signatures and indicators of compromise** - Review the signatures and indicators of compromise used by the organisation for investigation of suspicious activity and alerts. Verify how the organisation detects these on its systems and networks. The organisation should be able to justify how the range of signatures and IoCs it uses is wide enough to be alerted to most or all of its key threats. (A#2)
3. **Mapping to assets** - Verify that the organisation can trace alerts back to individual assets on its network almost in real time to aid investigations. The organisation should be able to produce documentation showing how it has designed, implemented and tested alerting systems to enable resolution to individual impacted assets. (A#3)
4. **Log review tool** - Inspect the tool used for reviewing logs, and assess whether this tool allows for real-time automated monitoring, sending alerts when a suspicious activity is identified. (A#5)
5. **Testing of alerts** - Inspect whether a defined process has been documented for testing the reliability of alerts created by the log review tool. This process should include inspection of the alert and the corresponding asset, and a discussion involving relevant staff when the alert is found to be false, with actions taken to improve the log analysis process. Obtain a sample of alerts generated by the log review tool, and enquire how the organisation would assess the veracity of the alert. For false alerts, obtain evidence that actions were discussed and implemented following the test. (A#6)

Suggested documentation – Partially Achieved

- Procedures for acting on alerts from third-party security software
- Procedures for identifying and resolving alerts
- Sample of alerts demonstrating effective implementation of procedures
- Evidence of tools for querying log data
- Evidence of scheduled log reviews

Additional documentation – Achieved

- Evidence of tools for correlating log data from different sources
- Evidence of signatures and indicators of compromise used for investigations
- Documents showing how alerting system resolves alerts to individual assets
- Evidence of tools for real-time automated log monitoring
- Procedures for testing alerts

Contributing outcome C1.d – Identifying security incidents

Description

You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response.

The expectation for this contributing outcome is **Partially Achieved**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	**Partially Achieved** All the following statements are true:	**Achieved** All the following statements are true:
NA#1. Your organisation has no sources of threat intelligence. NA#2. You do not apply updates in a timely way, after receiving them. (For example, antivirus signature updates, other threat signatures or Indicators of Compromise (IoCs)). NA#3. You do not receive signature updates for all protective technologies such as antivirus and intrusion detection systems or other software in use. NA#4. You do not evaluate the usefulness of your threat intelligence or share feedback with providers or other users.	PA#1. Your organisation uses some threat intelligence services, but you don't necessarily choose sources or providers specifically because of your business needs, or specific threats in your sector (example include sector-based info share, ICS software vendors, anti-virus providers, specialist threat intel firms, special interest groups). PA#2. You receive updates for all your signature based protective technologies (such as antivirus, intrusion detection system). PA#3. You apply some updates, signatures and IoCs in a timely way. PA#4. You know how effective your threat intelligence is (for example by tracking how threat intelligence helps you identify security problems).	A#1. You have selected threat intelligence feeds using risk-based and threat-informed decisions based on your business needs and sector (examples include, vendor reporting and patching, strong anti-virus providers, sector and community-based info share, special interest groups. A#2. You apply all new signatures and IoCs within a reasonable (risk-based) time of receiving them. A#3. You receive signature updates for all your protective technologies (such as antivirus, intrusion detection system). A#4. You track the effectiveness of your intelligence feeds and actively share feedback on the usefulness of IoCs and any other indicators with the threat community, (such as partners, threat intelligence providers, government agencies).

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework (CAF).

The approach and documentation list described below provides guidance on how to conduct testing and should be adapted as appropriate in order to assess whether the NHS providers outcomes are effectively achieved.

Suggested approach to testing – Mandatory policy requirement

1. **Acknowledging receipt of high severity alerts** – Verify that:
   b) The organisation maintains up-to-date contact details with the NHS England 'Respond to an NHS cyber alert' service
   b) Receipt of each high severity alert is acknowledged on the service within 48 hours of issue

2. **Sample testing** - Review a sample of high severity alerts received by the organisation from over the past 12 months. Confirm that for each one, the organisation has acknowledged the alert within 48 hours.

Suggested approach to testing – Partially Achieved

1. **Threat intelligence feeds** – Obtain and inspect evidence related to threat intelligence feeds to determine which services are being used, and how they were chosen. (PA#1)
2. **Applying updates**– Obtain evidence that demonstrates:
   a) Updates are received for all signature-based protective technologies; (PA#2)
   b) Updates, signatures and IoCs are applied in a timely way; (PA#3)
3. **Testing effectiveness** – Verify that the organisation has an informed understanding of what potential incidents it can and cannot be alerted to using its range of signatures and indicators of compromise. Obtain evidence that the organisation has conducted testing to inform its judgment. (PA#4)

Additional approach to testing – Achieved

1. **Threat intelligence feeds** – Obtain and inspect evidence related to threat intelligence feeds to determine if they have been selected using risk-based and threat-informed decisions based on their business needs and sector. (A#1)
2. **Applying updates** – Obtain evidence that demonstrates:
   a) The allowed timeframe between receiving and applying an update is documented, and is based on the risk presented by the update. Verify that all new signatures and IoCs are applied within the documented timeframe; (A#2)
   b) Signature updates are received for all protective technologies such as antivirus, intrusion detection system; (A#3)
3. **Ongoing testing and development** – Verify that the organisation has an informed understanding of what potential incidents it can and cannot be alerted to using its range of signatures and indicators of compromise. Obtain evidence that the organisation:
   a) Conducts ongoing scheduled testing to ensure threat intelligence used is in line with industry best practice (A#4)

b) Actively engages with sector partners and technical authorities to share feedback on threat intelligence received and develop cross-sector understanding of threats (A#4)

Suggested documentation – Mandatory policy requirement

- Contact details registered on the NHS England 'Respond to an NHS cyber alert' service
- Sample of high severity alert acknowledgements to NHS England from past 12 months

Suggested documentation – Partially Achieved

- Threat intelligence feeds information
- Evidence of updates received
- Procedures for applying updates
- Evidence of testing threat intelligence received

Additional documentation – Achieved

- Threat intelligence feeds information
- Selection criteria for threat intelligence feeds referencing risks and business need
- Procedures for applying updates
- Evidence of ongoing testing of threat intelligence feeds and content
- Evidence of cross-sector engagement

Contributing outcome C1.e – Monitoring tools and skills

Description

Monitoring staff skills, tools and roles, including any that are outsourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have knowledge of the essential function(s) they need to protect.

The expectation for this contributing outcome is **Not Achieved**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	**Partially Achieved** All the following statements are true:	**Achieved** All the following statements are true:
NA#1. There are no staff who perform a monitoring function. NA#2. Monitoring staff do not have the correct specialist skills. NA#3. Monitoring staff are not capable of reporting against governance requirements. NA#4. Monitoring staff lack the skills to successfully perform some significant parts of the defined workflow. NA#5. Monitoring tools are only able to make use of a fraction of logging data being collected. NA#6. Monitoring tools cannot be configured to make use of new logging streams, as they come online. NA#7. Monitoring staff have a lack of awareness of the essential function(s) the organisation provides, what assets relate to those functions and hence the importance of the log data and security events.	PA#1. Monitoring staff have some investigative skills and a basic understanding of the data they need to work with. PA#2. Monitoring staff can report to other parts of the organisation (such as security directors, resilience managers). PA#3. Monitoring staff are capable of following most of the required workflows. PA#4. Your monitoring tools can make use of logging that would capture most unsophisticated and untargeted attack types. PA#5. Your monitoring tools work with most log data, with some configuration. PA#6. Monitoring staff are aware of some essential function(s) and can manage alerts relating to them.	A#1. You have monitoring staff, who are responsible for the analysis, investigation and reporting of monitoring alerts covering both security and performance. A#2. Monitoring staff have defined roles and skills that cover all parts of the monitoring and investigation process. A#3. Monitoring staff follow process and procedures that address all governance reporting requirements, internal and external. A#4. Monitoring staff are empowered to look beyond the fixed process to investigate and understand non-standard threats, by developing their own investigative techniques and making new use of data. A#5. Your monitoring tools make use of all log data collected to pinpoint activity within an incident. A#6. Monitoring staff and tools drive and shape new log data collection and can make wide use of it.

		A#7. Monitoring staff are aware of the operation of essential function(s) and related assets and can identify and prioritise alerts or investigations that relate to them.

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework (CAF). The approach and documentation list described below provides guidance on how to conduct testing and should be adapted as appropriate in order to assess whether the NHS providers outcomes are effectively achieved.

Suggested approach to testing – Partially Achieved

1. **Staff responsibilities** - Obtain evidence that the following requirements have been met:
   a) There are staff who perform monitoring activities as part of their BAU role. The organisation understands what its in-house team are capable of investigating. (PA#1)
   b) There are procedures enabling staff who perform monitoring to report issues across the organisation. (PA#2)
   c) The organisation has developed use cases to support its monitoring processes. Staff who perform monitoring are familiar with these. (PA#3)
   d) Staff who perform monitoring are familiar with the organisation's essential functions and which alerts are related to them. (PA#6)
2. **Monitoring tools** - Verify that:
   a) The organisation's monitoring tools are capable of detecting most unsophisticated and untargeted attack types. (PA#4)
   b) Most of the organisation's security logs can be monitored via their monitoring tools. (PA#5)

Additional approach to testing – Achieved

1. **Network and system** Establish whether the network and system monitoring is carried out in-house or outsourced to a supplier. If the activities are done in-house, follow the approach from step 2 to 3. If the activities are done via a supplier, follow the approach from step 4 to 8.
2. **Staff responsibilities** - Obtain evidence from the organisation to demonstrate that the following requirements have been met:
   a) Monitoring staff are responsible, as established through a contract, procedure, or otherwise, for the analysis, investigation and reporting of monitoring alerts covering both security and performance; (A#1)
   b) The investigation process has been documented, and staff have been given defined roles for each step of the process and are adequately qualified through training, experience or otherwise to perform their roles; (A#2)
   c) Monitoring staff follow documented procedures, and take action to ensure alerts which are indicative of incidents are escalated and reported where impact thresholds are met; (A#3)
   d) Monitoring staff recognise the documented procedures as a minimum baseline of activities and have demonstrably gone beyond them during investigations to understand non-standard threats. (A#4)
   e) Monitoring staff drive and shape new log data collection and can make wide use of it; (A#6)
   f) Monitoring staff are aware of the operation of essential function(s) and related assets and can identify and prioritise alerts or investigations that relate to them. (A#7)

3. **Security monitoring tools** – Obtain evidence that security monitoring tools used by the organisation can make use of all log data collected to pinpoint activity within an incident and the tools can help to drive and shape new log data collection to enhance this ability for the future. (A#5, A#6)
4. **Supplier responsibilities** – Obtain the contract or equivalent documentation agreed with the supplier and verify whether there is an agreed process for analysing, investigating and reporting monitoring alerts covering both security and performance. There should also be assurances from the supplier that monitoring staff roles have been defined and designated to appropriately skilled staff members. (A#1, A#2)
5. **Governance reporting** - Assess whether there is an agreement for the supplier to follow all the governance reporting requirements of the organisation. (A#3)
6. **Monitoring tools** - Verify whether the organisation understands the monitoring tools used by the supplier, and have agreed a sufficiently comprehensive scope of log data to be used for monitoring. Also verify whether the collection of log data is discussed and reviewed on a regular basis and new logs included where appropriate. (A#5, A#6)
7. **Essential functions** - Verify that essential functions have been clearly identified, with a requirement for the supplier to prioritise alerts and investigations related to them. (A#7)

Suggested documentation list – Partially achieved

- Descriptions of roles and monitoring-related activities
- Evidence of in-house monitoring skills and understanding
- Reporting procedures
- Monitoring use cases
- Evidence of monitoring tool coverage and capabilities

Additional documentation list – Achieved

- Roles and responsibilities for monitoring activities
- Monitoring staff procedures for analysis, investigations, reporting
- Evidence of monitoring staff skills and experience
- Evidence of monitoring tool coverage and capabilities
- Supplier assurance relating to monitoring activities conducted by supplier

Principle C2: Proactive security event discovery

Description

The organisation detects, within networks and information systems, malicious activity affecting, or with the potential to affect, the operation of essential functions even when the activity evades standard signature based security prevent/detect solutions (or when standard solutions are not deployable).

Overview of the underlying Contributing outcomes

Outcome C2.a – System abnormalities for attack detection

Outcome C2.b – Proactive attack discovery

Outcome C2.a – System abnormalities for attack detection

Description

You define examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is otherwise hard to identify.

The expectation for this contributing outcome is **Not Achieved**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	**Partially Achieved**	**Achieved** All the following statements are true:
NA#1. Normal system behaviour is insufficiently understood to be able to use system abnormalities to detect malicious activity. NA#2. You have no established understanding of what abnormalities to look for that might signify malicious activities.	*Partial achievement is not possible for this contributing outcome*	A#1. Normal system behaviour is fully understood to such an extent that searching for system abnormalities is a potentially effective way of detecting malicious activity (for example you fully understand which systems should and should not communicate and when). A#2. System abnormality descriptions from past attacks and threat intelligence, on yours and other networks, are used to signify malicious activity. A#3. The system abnormalities you search for consider the nature of attacks likely to impact on the networks and information systems supporting the operation of your essential function(s). A#4. The system abnormality descriptions you use are updated to reflect changes in your networks and information systems and current threat intelligence.

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework (CAF).

The approach and documentation list described below provides guidance on how to conduct testing and should be adapted as appropriate in order to assess whether the NHS providers outcomes are effectively achieved.

Suggested approach to testing

1. **Understanding of normal system behaviour** - Obtain and inspect organisation's documentation establishing baselines for normal system behaviour. Verify that it is comprehensive, and interrogate how the organisation would use this to search for system abnormalities. (A#1)
2. **Threat intelligence** - Obtain and inspect documentation showing the organisation collects system abnormality descriptions from threat intelligence and past attacks. Verify that it uses them to identify and investigate malicious activity. (A#2)
3. **Searching according to risk** - Obtain and inspect evidence that the organisation has rationalised which attacks are likely to impact its essential functions. Verify that it searches for indicators of these attacks when performing searches for system abnormalities. (A#3)
4. **Updating system abnormality descriptions** - Assess the organisation has a process for updating system abnormality descriptions to reflect changes in the organisation's networks and information systems and current threat intelligence. Obtain samples of updates and verify that the process is followed. (A#4)

Suggested documentation list

- System behaviour baselines
- System abnormality descriptions from threat intelligence and past incidents
- Evidence of risk assessments being used for system abnormality searches
- Review process for system abnormality descriptions

Outcome C2.b – Proactive security event discovery

Description

You use an informed understanding of more sophisticated attack methods and of normal system behaviour to monitor proactively for malicious activity.

The expectation for this contributing outcome is **Not Achieved**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	**Partially Achieved**	**Achieved** All the following statements are true:
NA#1. You do not routinely search for system abnormalities indicative of malicious activity.	*Partial achievement is not possible for this contributing outcome*	A#1. You routinely search for system abnormalities indicative of malicious activity on the networks and information systems supporting the operation of your essential function(s), generating alerts based on the results of such searches. A#2. You have justified confidence in the effectiveness of your searches for system abnormalities indicative of malicious activity.

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework (CAF).

The approach and documentation list described below provides guidance on how to conduct testing and should be adapted as appropriate in order to assess whether the NHS providers outcomes are effectively achieved.

Suggested approach to testing

1. **Proactive security event discovery management** – Obtain and inspect evidence to assess whether:
    a) System abnormalities are routinely searched for to indicate any malicious activity on the networks and information systems; (A#1)
    b) Alerts are generated based on system abnormalities detected; (A#1)
    c) The organisation has carried out testing to gain confidence that its searches are effective in detecting system abnormalities indicative of suspicious activity. (A#2)

Suggested documentation list

- Evidence of system abnormality searches being routinely performed
- Configuration of alerts for system abnormality detection
- Assurance activities relating to system abnormality searches