NHS Digital › ••• › Objective C - Detecting cyber security events ›
Principle: C1 Security monitoring

Part of Objective C - Detecting cyber security events

Principle: C1 Security monitoring

← Previous Chapter

Objective C - Detecting cyber security events

Current Chapter

Current chapter – Principle: C1 Security monitoring

View all

Next Chapter →

Principle: C2 Proactive security event discovery

Page contents

C1.a Monitoring coverage

> "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)."

Overview

This outcome relates to the scope of your monitoring activities, and the extent to which your collected logs enable you to detect unusual events, indicators of compromise and security incidents.

Mapping to the 23-24 DSPT framework

Under the previous 23-24 Data Security and Protection Toolkit (DSPT) framework, your organisation was required to perform activities that help meet the expectations of this contributing outcome.

For more detail on what these activities were, see the mapping exercise published by NHS England and the Department of Health and Social Care (DHSC).

Monitoring

Your organisation should have an effective monitoring strategy in place which enables you to identify signs of malicious activity and respond in a way which is timely and effective. Logs should be collected and analysed on an ongoing basis.

See NCSC's 10 steps to cyber security guidance for additional factors to consider when implementing your monitoring strategy.

Monitoring coverage

You should collect logs for an appropriate range of sources across your systems and networks. Examples are:

- host-based logs – for events relating to the file system, running processes and program load events
- service logs – for services such as identity, mail, document storage and back-end services such as databases
- infrastructure logs – for device events such as website connections and domain name system (DNS) requests
- device compliance – for device status and configuration
- device attestation – for device and device software signals and measurements

For expanded explanations of the above, see the logging and protective monitoring section in NCSC's device security guidance.

You should be able to demonstrate that you have prioritised the sources you monitor based on an assessment of the associated risks, and that your coverage is as comprehensive as possible.

Network boundary traffic

As part of your monitoring activities, particular consideration should be paid to boundary devices which monitor inbound and outbound connections.

Boundaries that should be prioritised include those located between your:

- network and the internet
- network and third-party networks
- IT system and connected medical devices

Monitoring user activity

You should establish what typical user activity looks like on your systems and networks for users to fulfil their roles and deliver your organisation's essential functions healthcare services. These users could be internal staff members or external partner organisations.

From this understanding of typical activity, you should be able to agree and document parameters for user behaviour which is suspicious or undesirable. Typical examples of suspicious or undesirable user activity include:

- unusually high instances of failed login attempts
- access attempts at unusual hours and locations
- changes in system configuration or permissions
- addition or removal of applications and system services from operating systems
- transferral of large amounts of data
- changes to important system files and data records

These documented parameters for unusual activity should support your monitoring procedures.

Privileged user activity

Privileged users such as system administrators have more potential to cause disruption given their higher level of access. They should be subject to more stringent logging requirements, and an elevated level of monitoring.

Detecting indicators of compromise

Your monitoring tools and procedures should allow you to understand typical patterns of activity on your networks. Indicators of compromise and unusual system behaviour should stand out as deviations from the norm.

The forms that indicators of compromise take are always changing, but will include known bad internet protocol (IP) addresses, domains, hashes and strings. Your approach to detecting them should be informed by threat intelligence acquired through NHS England’s National Cyber Security Operations Centre (CSOC), including via Microsoft Defender for Endpoint.

Exceeding the ‘Standards met’ expectation for 2024-25

Monitoring user activity

To meet the highest achievement benchmark, you need to demonstrate that you have not only defined parameters for suspicious or undesirable behaviour, but also ensured that these are comprehensively monitored by your organisation in all cases where it is practical to do so.

For systems where precise monitoring is not possible, such as for some connected medical devices, procedural controls should be in place to manage access.

Reliably detecting security incidents

To reliably detect security incidents, your monitoring tools should be able to access data gathered from all critical elements of your networks and systems, allowing you to precisely identify the point of intrusion for an incident.

You should also have justified confidence in your ability to detect security incidents through monitoring. This confidence is gained through robust assurance activities such as simulation exercises.

Supporting evidence

To support your response, you can review and upload (or link to) evidence which best demonstrates your achievement of the contributing outcome. Examples include:

- policy, process, procedure or strategy documents (such as security logs)
- minutes and terms of reference from relevant meetings and groups
- overview of logging activities
- baseline profiles for user activity logs
- assets inventories (such as for boundary devices)
- monitoring technology configurations

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers where appropriate.

Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | C1 Security monitoring
National Cyber Security Centre | Device security guidance – Logging and protective monitoring
National Cyber Security Centre | 10 steps to cyber security – Logging and monitoring

Mapping to other cyber frameworks

NHS England and DHSC have produced a mapping document showing where the requirements of the CAF-aligned DSPT overlap with those of other cyber frameworks. New frameworks will be added to this document over the course of the year.

C1.b Securing logs

> "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."

Overview

To meet this outcome, you need to demonstrate that you have secured your log data through secure design, identity and access management (IAM) and procedural controls.

Mapping to the 23-24 DSPT framework

Under the previous 23-24 Data Security and Protection Toolkit (DSPT) framework, your organisation was required to perform activities that help meet the expectations of this contributing outcome.

For more detail on what these activities were, see the mapping exercise published by NHS England and Department of Health and Social Care (DHSC).

Securing logs

If compromised, internal log files would enable an attacker to conceal their activities, divert attention and manipulate assessments of ongoing incidents.

For this reason, it is important to establish a clearly defined set of protective controls and design your system architecture in a way which keeps logs secure.

Controlling access

You should hold logging data in a secure location, appropriately limiting the ways in which it can be accessed from your network.

Identity and Access Management (IAM) permissions should be employed. Only privileged users with a legitimate business need should be granted access rights, and this should be done on a case-by-case basis and reviewed regularly.

To safeguard the integrity of log files, access should also uniquely be granted in read-only form.

Policy and procedural controls

Your organisation must agree a permitted scope of activities relating to log files and ensure that they are documented in your policies and followed by staff members. No member of staff should view, copy, delete or modify log files unless they have a legitimate reason to.

Monitoring access

You should monitor access to logs. Your monitoring activities should enable you to identify security events such as:

- unauthorised access attempts
- modification or deletion of logging data by users before the agreed retention period has elapsed

Supporting evidence

To support your response, you can review and upload (or link to) evidence which best demonstrates your achievement of the contributing outcome. Examples include:

- policy, process, procedure or strategy documents (such as security logs)
- minutes and terms of reference from relevant meetings and groups
- details of security measures for logging

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers where appropriate.

Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | C1 Security monitoring

NHS England | NHS Secure boundary service

NHS England | Microsoft Defender for Endpoint service

Mapping to other cyber frameworks

NHS England and DHSC have produced a mapping document showing where the requirements of the CAF-aligned DSPT overlap with those of other cyber frameworks. New frameworks will be added to this document over the course of the year.

C1.c Generating alerts

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

Overview

This outcome relates to using security alerts to drive effective remediation activities.

Mapping to the 23-24 DSPT framework

Under the previous 23-24 Data Security and Protection Toolkit (DSPT) framework, your organisation was required to perform activities that help meet the expectations of this contributing outcome.

For more detail on what these activities were, see the mapping exercise published by NHS England and Department of Health and Social Care (DHSC).

Alerts

You should ensure that you investigate and take follow up actions in response to:

- alerts you have configured responding to suspicious user behaviour, unusual events or indicators of compromise
- any threats which you have been contacted about directly by DHSC/NHS England
- threat intelligence and alerts received from NHS England’s National Cyber Security Operations Centre (CSOC), including via Microsoft Defender for Endpoint

Where mitigating actions are needed in response to alerts, these actions should be documented and prioritised, involving other teams as appropriate.

Resolution of alerts

You should monitor alerts on a continuous basis and deal with them promptly. Where multiple alerts are received, you should prioritise them according to risk and follow up the most urgent alerts first.

For systems and platforms where alerts are enabled locally but do not feed through to your security information and event management (SIEM) system, you should schedule monitoring of those specific systems and platforms at the source on a scheduled basis to ensure alerts are picked up without undue delay.

Search tools

You should have a system and procedure that enables you to effectively collect, search for and analyse logs for reporting and investigations. This could be done via a SIEM.

The logs you collect should be prioritised according to the key security outcomes you want to achieve. The more coverage you have of your systems and networks, the better.

Data sources which cannot be integrated into a central system or procedure may be configured locally to enable the capture of security information. Where this is the case, you should enable logging and ensure you are able to search and analyse local data if needed for incident response.

Exceeding the 'standards met' expectation for 2024-25

Configuring alerts

To meet the highest achievement benchmark, you need to demonstrate that you have configured alerts in a way which is optimised for your organisation, with detailed consideration of:

- the critical assets you are protecting
- a wide range of signatures and indicators of compromise to help identify and analyse suspicious activity
- threat intelligence from a wide range of sources
- a robust framework of attacker tactics and techniques

Testing alerts

To meet the highest achievement level, you should conduct validation activities to ensure that your alerts are being generated reliably, and that the potential for false positives is reduced.

Validation should be conducted before and after deployment of your alerts systems through simulation exercises and performance testing.

Supporting evidence

To support your response, you can review and upload (or link to) evidence which best demonstrates your achievement of the contributing outcome. Examples include:

- policy, process, procedure or strategy documents (such as data security, vulnerabilities, security logs, assurance)
- minutes and terms of reference from relevant meetings and groups
- risk assessments
- documented actions taken in response to alerts

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers where appropriate.

Interpreting indicators of good practice

Indicator(s) of good practice	PA#3 The resolution of alerts to a network asset or system is performed regularly.
Term	'regularly'
Interpretation	As soon as alerts are brought to your attention, plans should be made for how they will be resolved as soon as feasibly possible.

Indicator(s) of good practice	PA#5 Logs are reviewed at regular intervals.
Term	'at regular intervals'
Interpretation	On a scheduled basis, with enough frequency to ensure that alerts are not left unnoticed or unresolved for an unacceptable length of time.

Indicator(s) of good practice	A#2 A wide range of signatures and indicators of compromise is used for investigations of suspicious activity and alerts.
Term	'A wide range of signatures and indicators of compromise'
Interpretation	There is no specific set of signatures or indicators of compromise to consider when optimising your alerts and investigations. The important thing is that you draw upon a sufficiently wide knowledge base to ensure that the most important threats are detectable by your systems.

Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | C1 Security monitoring
NHS England | NHS Secure boundary service
NHS England | Microsoft Defender for Endpoint service

NHS England | Vulnerability monitoring service

NHS England | Bitsight cyber security ratings service

Mapping to other cyber frameworks

NHS England and DHSC have produced a mapping document showing where the requirements of the CAF-aligned DSPT overlap with those of other cyber frameworks. New frameworks will be added to this document over the course of the year.

C1.d Identifying security incidents

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

Overview

This outcome is about your ability to detect signatures, indicators of compromise and security incidents through your threat intelligence, monitoring and associated technologies.

Mapping to the 23-24 DSPT framework

Under the previous 23-24 Data Security and Protection Toolkit (DSPT) framework, your organisation was required to perform activities that help meet the expectations of this contributing outcome.

For more detail on what these activities were, see the mapping exercise published by NHS England and Department of Health and Social Care (DHSC).

Threat intelligence

Your monitoring activities should be informed by:

- current and emerging threats described in DHSC/NHS England’s Cyber Security Strategy for Health and Care to 2030
- any threats which you have been contacted about directly by DHSC/NHS England
- threat intelligence and alerts received from NHS England’s National Cyber Security Operations Centre (CSOC), including via Microsoft Defender for Endpoint

Updating for new signatures or indicators of compromise

Your antivirus or malware protection technologies should automatically be updated with the latest signatures or indicators of compromise. If you have a large IT estate, these updates can be initialised from a central management source.

Where updates are performed manually, you should have a robust process for ensuring they are applied promptly.

Threat intelligence effectiveness

(This is an increase in requirements for 2024-25 'Standards met')

To determine how effective your threat intelligence is, you need to validate your capability to identify signatures and indicators of compromise through means such as:

- in-house testing and exercising
- breach and attack simulation tools
- independent third-party testing
- conducting root cause analysis following incidents

You should use these approaches to identify blind spots in your detection capabilities and resolve accordingly.

Supporting evidence

To support your response, you can review and upload (or link to) evidence which best demonstrates your achievement of the contributing outcome. Examples include:

- policy, process, procedure or strategy documents (such as anti-virus/malware, security monitoring)
- minutes and terms of reference from relevant meetings and groups
- risk assessments
- documented actions taken in response to alerts, testing, simulation exercises
- board reports or assurance and risk committee reports
- audit reports
- membership of the Cyber Associates Network (CAN)

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers where appropriate.

Interpreting indicators of good practice

Indicator(s) of good practice	PA#3 You apply some updates, signatures and indicators of compromise (IoCs) in a timely way. A#2

	You apply all new signatures and IoCs within a reasonable (risk-based) time of receiving them.
Term	'in a timely way' 'within a reasonable (risk-based) time'
Interpretation	There is no set time frame in which updates should be applied. Instead, your focus should be the level of risk your organisation is prepared to accept, which may increase the longer that updates are left unactioned.

Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | C1 Security monitoring
NHS England | Microsoft Defender for Endpoint service
NHS England | Vulnerability monitoring service
NHS England | Bitsight cyber security ratings service
NHS England | Cyber incident response exercise service

Mapping to other cyber frameworks

NHS England and DHSC have produced a mapping document showing where the requirements of the CAF-aligned DSPT overlap with those of other cyber frameworks. New frameworks will be added to this document over the course of the year.

C1.e Monitoring tools and skills

> “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.”

For this contributing outcome, there is no minimum expected level of achievement for ‘Standards met’. You are still required to assess your achievement level and provide a response, showing you have considered the implications of the contributing outcome for your organisation’s cyber security and information governance (IG) activities. The DSPT ‘Standards met’ expectation should be regarded as a minimum compliance level, not the end goal of your organisation’s cyber security and IG activities.

Overview

To achieve this outcome, you need to have considered your monitoring team's skills, tools and overall structure to ensure they can competently identify, analyse, investigate and report security threats.

Mapping to the 23-24 DSPT framework

Under the previous 23-24 Data Security and Protection Toolkit (DSPT) framework, your organisation was required to perform activities that help meet the expectations of this contributing outcome.

For more detail on what these activities were, see the mapping exercise published by NHS England and Department of Health and Social Care (DHSC).

Monitoring skills

Your training needs analysis (TNA) (see 'B6.b Training') should identify the competency requirements for staff members who are conducting your organisation's security monitoring activities, and plan how training is to be delivered where it is needed.

The training should be informed by relevant professional competency frameworks to ensure that appropriate standards are being met. The result of your organisation's training and resources should be that monitoring staff:

- have an awareness of the relative importance of your organisation's assets, functions and systems
- can prioritise actions based on the probable impact to your essential functions
- make risk informed response decisions
- are supported in effectively identifying and investigating alerts

If your monitoring activities are carried out by partner organisations or suppliers, you should seek assurances regarding the competencies of their personnel relating to the areas outlined above.

Monitoring tools

You should choose your monitoring technologies based on a clearly defined criteria of the threats your organisation faces, the assets you hold and your security objectives.

You should be assured that common indicators of compromise are reliably detected by your chosen technologies.

Monitoring policies, processes and procedures

Your policies, processes and procedures should establish workflows for monitoring teams to adhere to when:

- analysing logs and relevant data
- investigating sources
- reporting findings and suggested follow up actions to relevant decision makers

Your documentation should clearly define:

- lines of reporting
- communication channels
- processes for escalation and resolution

Comprehensive monitoring team considerations

To meet the highest achievement benchmark, you need to demonstrate that you have considered in detail and established:

- a monitoring team composition that is carefully matched to the threats your organisation faces – (such as via the team's personnel, structure and size)
- defined roles and responsibilities within the monitoring team – (such as for analysis, investigation and reporting)
- a detailed and broad knowledge base amongst monitoring team members – (such as your networks and information systems, how your system architecture is designed, how data is used across your estate)
- a proactive monitoring team culture, for example by empowering monitoring personnel to employ their initiative relating to techniques and monitoring coverage (see 'C1.a Monitoring coverage') for optimal identification, analysis and resolution of security threats

Supporting evidence

To support your response, you can review and upload (or link to) evidence which best demonstrates your achievement of the contributing outcome. Examples include:

- policy, process, procedure or strategy documents (including security monitoring and events management)
- training needs analysis (TNA)
- training records
- job specifications for specialised roles
- supplier assurance documentation

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers where appropriate.

Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | C1 Security monitoring

NHS England | Vulnerability monitoring service

NHS England | Bitsight cyber security ratings service

NHS England | Cyber incident response exercise service

Mapping to other cyber frameworks

NHS England and DHSC have produced a mapping document showing where the requirements of the CAF-aligned DSPT overlap with those of other cyber frameworks. New frameworks will be added to this document over the course of the year.

Last edited: 19 September 2024 3:28 pm

← **Previous Chapter**

Objective C - Detecting cyber security events

Next Chapter →

Principle: C2 Proactive security event discovery

Chapters

Twitter

Facebook

LinkedIn

YouTube