Part of Objective C - Detecting cyber security events

# Principle: C2 Proactive security event discovery

← Previous Chapter

Principle: C1 Security monitoring

Current Chapter

Current chapter – Principle: C2 Proactive security event discovery

View all

Page contents



## C2.a System abnormalities for attack detection

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

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

This outcome relates to your ability to identify system abnormalities via a range of means and take pre-emptive measures against potential attacks.

## 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).

## System abnormalities

Your activities established under 'C1.a Monitoring coverage' should give you broad visibility of how your data sources are being used across your organisation. This view should enable you to establish a baseline of expected behaviours for system users through analysis of:

- data volumes being accessed
- which users are interacting with which systems
- how systems are being used

After establishing a baseline of expected behaviours, you should be able to identify deviations from the norm, such as:

- logins in from unusual locations, or at unusual times
- sensitive data downloads in large quantities
- systems or data being used in unexpected ways
- spikes in data access or usage

You should establish protocols for identifying system abnormalities and following up with appropriate remediation activities.

## Threat intelligence

Your identification of system abnormalities should be informed by:

- past security events
- 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

- threat intelligence you have received via professional networks, such as the Cyber Associates Network (CAN)

## Considering likely impacts

Using your knowledge of threats which are likely to occur and your understanding of your own network and system architecture, you should be able to conduct risk assessments to understand how these threats are likely to materialise on your networks, and use risk assessment findings to optimise your detection capabilities.

Your detection capabilities should consist not only of monitoring activities outlined in 'C1 Security monitoring', but also technologies (for example, advanced detection technologies employing artificial intelligence), to ensure system abnormalities are identified and followed up on across your IT estate.

## Updating system abnormality descriptions

You should be able to demonstrate how your scope for identifying system abnormalities has been updated over time. Situations which may result in changes include:

- occurrence of incidents, both internal and external
- significant changes to your networks and systems
- significant changes to your operations

## 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 logs and vulnerability management)
- user behaviour profiles and analysis
- risk assessments

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 | C2 Proactive security event discovery
NHS England | NHS Secure boundary 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.

---

# C2.b Proactive attack discovery

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

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 meet this outcome, your processes and technologies should enable you to proactively identify and remediate security events.

## 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).

## Routine searches for system abnormalities

You should routinely search your networks and systems for abnormalities which might be indicative of malicious activity. You can achieve this through a combination of means such as:

- monitoring activities (see 'C1 Security monitoring')
- threat hunting
- detection technologies

Detection technologies can facilitate searching across every asset on a near continuous basis. However, this may not be practical or feasible to implement. You should therefore target specific assets for routine searches, based on your assessment of the underlying risks they pose to the operation of your essential functions.

Your strategies, processes and procedures should rationalise how your activities and tools are effectively utilised to ensure that searches are conducted on a scheduled basis, and establish workflows for cyber security teams to follow.

## Alerts

Alerts should be produced when abnormalities are detected. These should be appropriately configured and promptly acted upon (see 'C1.c Generating alerts').

## Assuring your proactive attack detection capability

You should perform assurance activities, for example breach and attack simulation exercises, to gain justified confidence in the effectiveness of your detection processes and technologies.

You should be satisfied that during business-as-usual operations, you would be able to identify and manage known threats that are likely to affect your networks and systems.

Any weak points which you identify through assurance activities should be documented and used to make improvements to your detection strategy.

## 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 logs and vulnerability management)
- detection technology configurations
- reports from assurance activities

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** | A#1<br>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. |
| **Term** | "routinely" |
| **Interpretation** | On a scheduled basis, with enough frequency to ensure that indicators of compromise that your systems are able to detect |

would reliably be picked up before unacceptable consequences could occur.

## Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | C2 Proactive security event discovery
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.

---

Last edited: 29 August 2024 9:28 am

← Previous Chapter

Principle: C1 Security monitoring

---

## Get in touch

Contact us

Press office

Tell us what you think of our website

RSS feeds

## Follow us on social media

Twitter

Facebook

LinkedIn

YouTube