Department for Education

DfE Continuous Assurance Platform

Version: 1.2

December 2025

Contents

DCAP Background

DfE Continuous Assurance Platform (DCAP)

DCAP is a system that allows Digital Services to see their Security Posture across a range of technologies, the objective being to drive posture hardening through remediation of vulnerabilities.

DCAP is a Splunk-based platform that provides visibility into outstanding security vulnerabilities identified across Digital Services. By systematically integrating DCAP data into planning and remediation efforts, services can demonstrate alignment with DfE Mandated Policies and broader security best practices.

DCAP provides a single pane of glass through which a Service can see vulnerabilities across the stack. It also offers guidance on which ones represent the highest priority to help the Service decide where to allocate resources first. Additionally, DCAP enables DfE leadership to track improvements in the department's overall security posture and identify areas where further support may be needed.

Foundational Systems

A Foundational System is a technology or system that, were it to be compromised, the workings of the whole DfE would be critically impaired inside a week. DfE has 5 Foundational Systems:

- Azure,
- Entra Active Directory,
- DNS,
- M365,
- GitHub.

Digital Services have a dependency on the foundational systems being secure, they have no direct control over platforms themselves. The compliance of the Foundational Systems is measured in DCAP against the CIS industry benchmarks. Compliance demonstrates that the posture of critical systems is hardened and give further confidence to Digital Services that the technology platforms on which they rely are secure.

Digital Services

For DCAP, a Digital Service is defined as a custom application that is built in the business with business functionality and is hosted within the DfE Azure Cloud environment. While a Digital Service may depend on infrastructure reliability and availability, it is not their responsibility to manage that infrastructure.

Their responsibility is to manage the architecture and configuration of their Digital Service and its assets that live on that infrastructure.

DCAP supports services teams adhere to DfE policy and resolve vulnerabilities or security issues in those applications.

Asset Attribution

DCAP maintains an inventory database that aims to catalogue all Azure assets, GitHub repositories, and Azure DevOps (ADO) repositories, with each asset ideally attributed to a single Digital Service. While this is the target, in practice, some assets may span multiple services or lack clear attribution which may complicate vulnerability resolution and ownership.

The basis of the taxonomy by which Digital Services are categorised is taken from the Financial Business Partners (FBP) database, so it is common with how those assets are accounted and cross-charged for. The Taxonomy has three levels:

- There are 9 'Portfolios'
- Each Portfolio has several 'Service Lines'
- Each Service Line has several 'Products'

The database also holds details of Service Owners and other contact information.

DCAP also keeps data relating to how Service Cost Centre Owners roll up through the DfE management chain to their Directors, and data about how CISD ISOs and SIRAsare allocated to Services.

Azure assets are linked to the FBP database using the Product tag, which is mandated by DfE Policy for all Azure resources. If an asset lacks a Product tag, DCAP attempts to derive it from the Resource Group it belongs to, assuming the Resource Group itself is correctly tagged. It is the responsibility of the Services to ensure that all of their Azure assets are tagged correctly according to the FBP taxonomy.

GitHub repositories are attributed to their respective Digital Services using the same taxonomy. Attribution is enforced through a tagging policy requiring every repository to include Custom Tags for the Portfolio, Service Line, and Product of the owning Digital Service. These tags must be selected from an approved list of canonical tags, ensuring consistent and complete coverage across all assets.

Posture Hardening

Opportunities to improve the security of configuration, operations, and architecture of digital assets come in a number of forms:

- Microsoft has thousands of checks that are constantly running against Azure resources testing for good practice, and DCAP ingests these from the Defender for Cloud stream. These ‘Defender Assessments’ are documented and prioritised by CISD.
- DCAP also uses Microsoft Defender Assessments to identify vulnerabilities relating to Azure Kubernetes Service (AKS) Clusters.
    - DCAP uses the CIS Benchmarks to define good practice in terms of how Digital Services should be setting up their GitHub and ADO Repositories to be secure. To validate and test posture compliance, DCAP takes data directly from GitHub and ADO.
    - GitHub and 3rd parties also provide scanning tools to check various aspects of the contents of code. An example being scanning for secrets being uploaded into a public repository. Every detection by one these tools is ingested by DCAP as an Alert.
- All Virtual Machines in the DfE Azure estate have a Qualys agent enabled, which provides details of known vulnerabilities that have not been patched. This data is consumed as Alerts by DCAP.

Alerts

Security alerts notify the detection of vulnerabilities across digital assets, including misconfigurations, exposed secrets, and unpatched software. An alert is a notification generated by a security tool indicating the detection of a potential threat, vulnerability, or deviation from expected behaviour. DCAP ingests alerts from Qualys, GitHub APIs and third-party repository-related scanners.

Controls

A 'Control' or 'Use Case' is the manifestation, in Splunk, of a specific Policy against which Compliance is measured. Controls, Use Cases, and Policies are synonyms for the same thing.

For every Control, the output from running the control is either 'Compliant' or 'Non-Compliant'. Each Assessment coming from MS-Defender for a specific asset is a single Control (Posture), as is a vulnerability report coming from Qualys (Alert), or a finding from Dependabot or CodeQL (Alerts). Each alert or control is individually attributed to the Digital Service that owns it.

Scores

To be more useful, the output from a Control is a 'Score'; a score being more granular than simply reporting 'Compliant' or ‘Non-Compliant', since it can hint at the degree of non-compliance.

In DCAP, a score of 100 indicates full compliance, 0 is the worst with all tests failed. Scores between 0 and 99 are non-compliant but the higher, the better.

The score for each Control is calculated using:

- Numerator: the number of tests that failed
- Denominator: the total number of tests conducted for that Control

Controls fall into two types: those requiring a single setting for the entire system and those needing specific settings for individual users or resources.

DfE Mandated Controls

Every Control has been assigned a level of priority within three bands:

- DfE Mandated
- Recommended
- Desirable

The designation is largely based on the Implementation Group (IG) categorisation (DfE Mandated being IG1). Some controls have been reclassified following CISD's assessment of risk, informed by DfE's specific usage.

In the first phase, System and Service Owners are expected to be compliant with all the DfE Mandated Policies/Controls that relate to their technology. Services not compliant must rectify or demonstrate effective risk mitigation to CISO's satisfaction. It is very much the intent of CISD to work with Service Owners to ensure that risk is mitigated and their service status is Compliant.

In later phases and over time, all services will be expected to become compliant with the Controls in all three bands.

For example, a finding coming from Qualys relating to a VM would only become Mandated if it has a severity of 4 or 5 and has been outstanding for more than 90 days.

Cadence

The configuration data from the underlying systems and services is requested and sent to Splunk every day, starting at around 3am.

The control algorithms run between 4:00 AM and 7:00 AM, updating the dashboards with the latest compliance and vulnerability data daily. If you have implemented changes to your service configuration to address vulnerabilities flagged by DCAP, you should not expect these to be visible in the tool until the next ingestion cycle has completed.

Sources

DCAP aggregates posture and vulnerability data from a diverse range of sources to provide comprehensive visibility into the security state of Digital Services. The automated scanning, assessments and alerting is based on best practice benchmarks and tool-specific reporting.

Sources of Posture and Vulnerability Data:

- Microsoft Defender for Cloud provides posture assessment data for both Azure and Azure Kubernetes Service (AKS).
- Qualys agents deployed on Virtual Machines are the source of vulnerability data.
- DCAP uses GitHub APIs to assess compliance with CIS Controls, focusing on repository configuration. These controls include checks that other tools are enabled, such as Dependabot and Secret Scanning.
- DCAP also integrates with GitHub APIs and third-party APIs to collect repository-related alert data from tools including SonarCloud, CodeQL, Dependabot, Secret Scanning, and other SAST (Static Application Security Testing) solutions.

Dashboards & Menus

There is a default Menu for users of the DCAP Splunk App in the top left of the browser tab. Each of the Dashboards described can be accessed via the menu.

Note that many of the dashboards are contextual; what they show is specific to the Service. For most dashboards, the only way to navigate is to click through (drilldown) from the previous dashboard in the hierarchy.

- **DCAP Home**: Quick access to your personal default dashboard, typically the Service Posture Dashboard for your assigned service. If you an ISO or SIRA, then you will automatically be navigated to a dashboard which lists the Services to which you are allocated.
- **Portfolio Overview Dashboard**: Displays compliance scores across portfolios; clicking a portfolio opens its Service Overview Dashboard.
- **ISO Dashboard**: Shows technology-specific compliance scores for each service/product in Services to which the logged in User is allocated; drilldown opens the Service Posture Dashboard.
- **Service Overview Dashboard**: Shows technology-specific compliance scores for each service/product in a portfolio; drilldown opens the Service Posture Dashboard.
- **Service Posture Dashboard**: Lists non-compliant controls and remediation priorities for a specific service; tailored for technical owners.
- **Service Control Detail Dashboard**: Provides in-depth technical data on a single control, including test results, affected resources, and raw data.

DCAP Home

Located to the left of the main menu, the *DCAP Home* option provides a quick way to return to your personal default dashboard. For most users, this will be the *Service Posture Dashboard* associated with their assigned service. This ensures easy navigation back to a familiar starting point, regardless of where you are in the app.

Portfolio Overview Dashboard

The *Portfolio Overview Dashboard* displays a panel for each portfolio, showing the percentage of resources that are compliant with DfE Mandated Policies. The score represents the proportion of compliant resources out of the total owned by the portfolio. Selecting a portfolio panel opens its corresponding Service Overview Dashboard in a new tab.

Service Overview Dashboard

The *Service Overview Dashboard* displays data for a single portfolio. The dashboard shows compliance scores for each technology type, calculated as the number of compliant resources out of the total resources in the portfolio. Each row represents a service or product within the portfolio, with its own technology-specific scores. Selecting a row opens the Service Posture Dashboard for that service in a new tab.

ISO Dashboard

The *ISO Dashboard* displays data for a single ISO or SIRA. The dashboard shows compliance scores for each technology type, calculated as the number of compliant resources out of the total resources across all their Services. Each row represents a Service within their remit, with its own technology-specific scores. Selecting a row opens the Service Posture Dashboard for that service in a new tab.

Service Posture Dashboard

The *Service Posture Dashboard* is designed for technical owners responsible for remediation. It lists all relevant controls, their compliance scores, and statuses. Overall scores show the number of compliant resources for each technology type, and panels are only displayed for technologies used by the service.

In the top-left corner, checkboxes allow users to include or exclude specific technology types from the remediation list. Each item in the list represents a non-compliant control assessment, where the requirements have not been met and action is needed. Only DfE Mandated and Non-Compliant controls are shown.

On the right of each control, a ‘Remediation Priority’ score is displayed. This priority is suggested by DCAP to guide the order of remediation, but it remains advisory, each service decides how to allocate resources to remedy security issues.

Service Control Detail Dashboard

The *Service Control Detail Dashboard* is intended for individuals responsible for understanding and remediating specific non-compliance issues. It provides detailed technical information about a single control, including the tests performed, the resources assessed, the expected outcomes, and the changes required to achieve compliance.

The dashboard is organised into three rows of data panels:

- **Score Panel:** Displays the compliance score for the control, calculated as the percentage of failed tests (numerator) over total tests (denominator).

    a. For controls with a single setting, the score reflects the number of fields checked.
    b. For controls applied across multiple items (e.g. users), each item is assessed individually, and the score reflects the number of non-compliant items.
- **Assessment Details:** Shows metadata including the control name, affected resource, associated service, and use case.
- **Underlying Data:** Presents raw data returned from the source API.
    a. For CIS-based controls, data is shown in a table format with non-compliant fields highlighted in red.
    b. For other sources, data is displayed in JSON format.

Onboarding to DCAP

There are a number of prerequisites that a Service must fulfil to use DCAP :

- **Service understanding:** Provide a description of the technologies you use, so the DCAP team can offer on-boarding support.

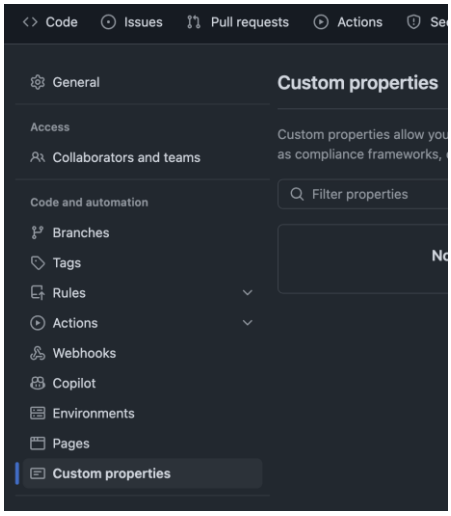
- Splunk Account : in order to access DCAP every user must have a Splunk account enabled. Requests should be made using the DCAP Public Teams channel.

- **Clean up the Tagging on your Azure resources:** Tag your resources with the designated value that corresponds to the FBP (Financial Business Partners) database. The canonical FBP list is available as a link in the DCAP Public Teams channel. At the very least, every resource must have a ‘Product’ tag.

- **Tag GitHub Repositories:** If the Service stores its source code in public GitHub repos, then custom tags will need to be added so that it can be attributed to the Service. **You can add Custom Properties and set values for those properties for repositories by following these steps :**

  - **Under the repository settings page, select custom properties listed under the "Code and automation" section.**

  - **Filter for the custom property you are going to set using the search bar.**



  - **Choose your tags from the custom properties table which can be found in a spreadsheet on** the DCAP Public Teams channel. Note that the 3 required properties – Portfolio, Service Line, and Product – must be selected as a canonical triplet in order for them to be valid.

- **ADO repositories**: Provide a list of your repositories if you use ADO to store your source code.

Once all of these are in place, the dashboards will automatically light up.

Issue Reporting

DCAP has its own Public Teams channel for reporting any on-boarding, support issues or requests.