Using the DfE Continuous Assurance Platform

CISD
Ian Pearl
v 0.0.1
2025-07-21

BACKGROUND

Continuous Assurance

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 system - on a daily basis, DCAP provides an insight into outstanding security vulnerabilities that have been identified for each Digital Service. By systemically incorporating the data coming from DCAP as the basis for planning ongoing work to remediate security vulnerabilities, Digital Services can demonstrate compliance with Policies and good security practice.

DCAP provides a single pain 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. Finally, DCAP gives DfE leadership feedback on how the department's posture is improving over time, and where additional resources might be required.

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. There are 5 Foundational Systems : Azure, Entra Active Directory, DNS, M365 and GitHub. From the perspective of a Digital Service, these Foundational Systems are the platform on which the services run; so while most Digital Services have a dependency on the Foundational Systems being secure, they have no direct control over the platforms themselves.

The compliance of the Foundational Systems is being measured by DCAP against the CIS industry benchmarks, the objective being to ensure that the posture of critical systems is hardened and to give further confidence to Digital Services that the technology platforms on which they rely are themselves secure.

Digital Services

A Digital Service is 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 implicitly has dependency on the reliability and availability of the infrastructure on which it depends, it is not the responsibility of the Service Team to manage that infrastructure. It is, however, their responsibility to manage the architecture and configuration of the assets within their applications that live on that infrastructure, and DCAP seeks to offer a tool to assist the Teams with adhering to DfE Policy and remediating vulnerabilities and security issues within those applications.

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 AKS Kubernetes 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, and takes the data directly from GitHub and ADO to test posture compliance.

- GitHub and 3rd parties also provide tools to check various aspects of the contents of code; an example being scanning for secrets being uploaded into a public repo. 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.

Asset Attribution

DCAP has an inventory database of all Azure assets and GitHub & ADO repositories, with every asset attributed to a single Digital Service. The basis of the taxonomy by which Digital Services are categorised is taken from the Financial Business Partners database, so it is common with how those assets are accounted and cross-charged for. The Taxonomy has 3 levels : There are 9 'Portfolios'; each Portfolio has a number of 'Service Lines'; each Service Line has a number of 'Products'. The database also holds details of Service Owners and other contact information.

Azure assets are matched to the FBP using the 'Product' tag that all DfE Azure assets must have by Policy. Where an asset does not have a product tag, this is derived from the Resource Group in which the asset lives, assuming that has a Product tag. GitHub Repositories are attributed to the Digital Services that own them according to the same taxonomy; the mechanism for GitHub attribution is by implementing a Policy whereby every Repo must be tagged using Custom Tags with the Portfolio, Service Line, and Portfolio of the Digital Service that owns it. These tags must be selected from the approved list of canonical tags, to ensure complete and consistent coverage.

Controls

A 'Control' or 'Use Case' is the manifestation, in Splunk, of a specific Policy against which Compliance is being 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 is individually attributed to the Digital Service that owns it.

Scores

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

Scores will mean different things in different contexts, but throughout SSPHP a score of 100 is perfectly compliant, and a score of 0 is the worst possible where every single test failed. Scores between 0 and 100 are non-compliant, but the closer to 100 the better.

For each Control, the Score is calculated from a 'Numerator' and a 'Denominator'. The denominator is the number of things tested, and the numerator is the number of those tests which failed. There are 2 types of Controls - those which require a single setting or collection of settings to be a certain way for the system or service as a whole, and those which require many users or resources to each have the specified settings. For the former, the denominator is the number of fields that were tested and the numerator is the number of fields that failed the tests. For the latter, each line is either a pass or a fail based on whether it contains 1 or more fields which failed a test, the denominator is the total number of lines that were tested, and the numerator is the number of lines that failed one or more tests.

DfE Mandated Controls

Every Control has been individually assessed and assigned a level of priority within 3 bands - DfE Mandated, Recommended, Desirable. The designation is largely based on the IG categorisation in the Benchmark docs (DfE Mandated being IG1, etc), but some have been moved depending on CISD's interpretation of risk based on DfE's usage.

In the first phase, System and Service Owners are expected to be compliant with all of the DfE Mandated Policies/Controls that relate to their particular technology. Where they are not, they are expected to remediate, or to demonstrate to the satisfaction of the CISO that the associated risk has been mitigated in a different way. 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 3 bands.

Cadence

The configuration data from the underlying systems and services is requested every day starting at 3am, and sent to Splunk. The Control algorithms run during a period between 4am and 7am. So the data in the dashboards is updated on a daily basis.

Sources

Microsoft Defender for Cloud is the source of Posture Assessment information in Azure and AKS. Qualys agents on Virtual Machines is the source of the Vulnerability data. DCAP uses GitHub APIs to acquire data relating to the CIS Controls looking at Repo configuration; these controls include checks that other tools are enabled, such as Dependabot and Secret Scanning. DCAP uses the GitHub and 3rd party APIs to acquire repo-related Alert data, including SonarCloud, CodeQL, Dependabot, Secret scanning, and other SAST tools.

DASHBOARDS & MENUS

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.

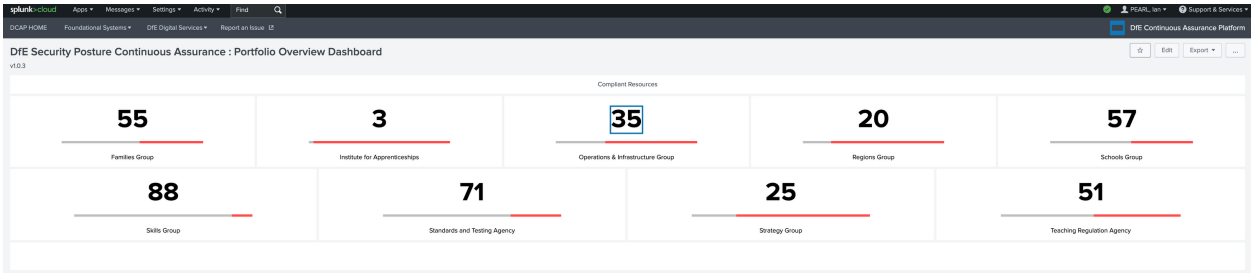
Note that many of the dashboards are contextual; what they show is specific to the Service. So for most dashboards, the only way to navigate is by click through (drilldown) from the previous dashboard in the hierarchy.

DCAP HOME

There is an option to the left of the menu items labelled DCAP HOME. This will always take you back to the dashboard configured to the default for you personally.

Most users will be assigned to a Service, and their default dashboard will open as the Service Posture Dashboard for their Service.

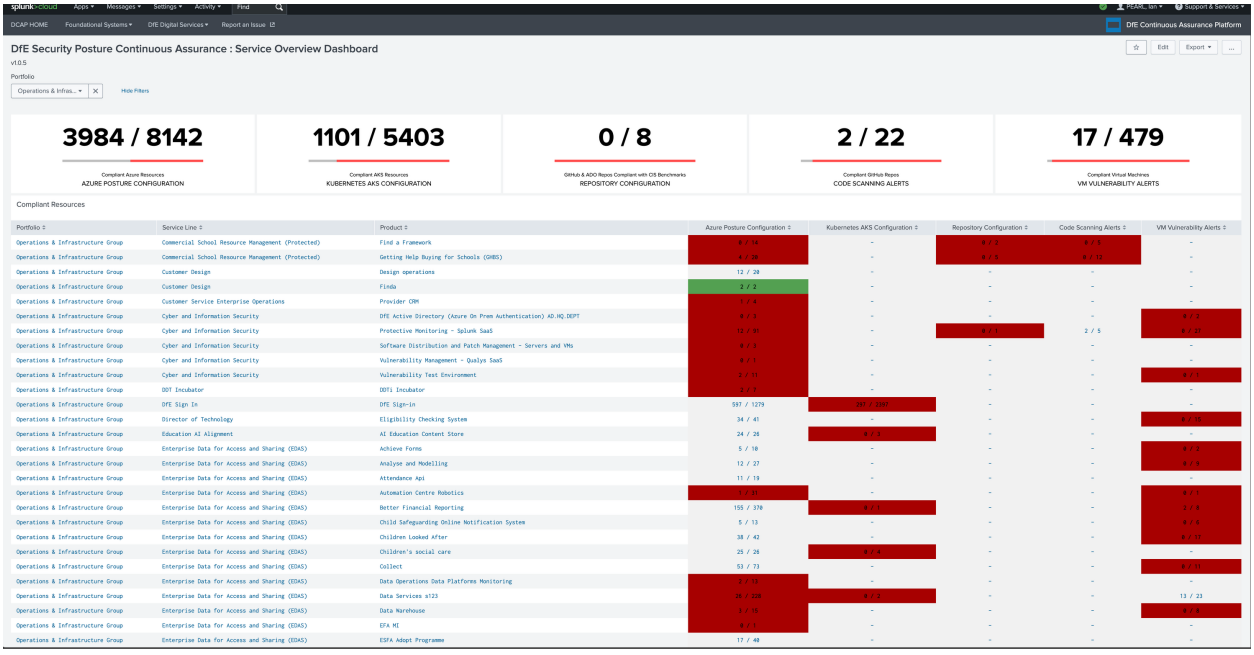
Portfolio Overview Dashboard



This dashboard shows a panel showing the percentage score for each of the Portfolios. The score here is the percentage of all resources owned by the Portfolio that are compliant with DfE Mandated Policies.

Clicking on the panel for a Portfolio will open the Service Overview Dashboard for that Portfolio in a new Tab.

Service Overview Dashboard



This dashboard is for a single Portfolio – the above screenshot is for Operations & Infrastructure.

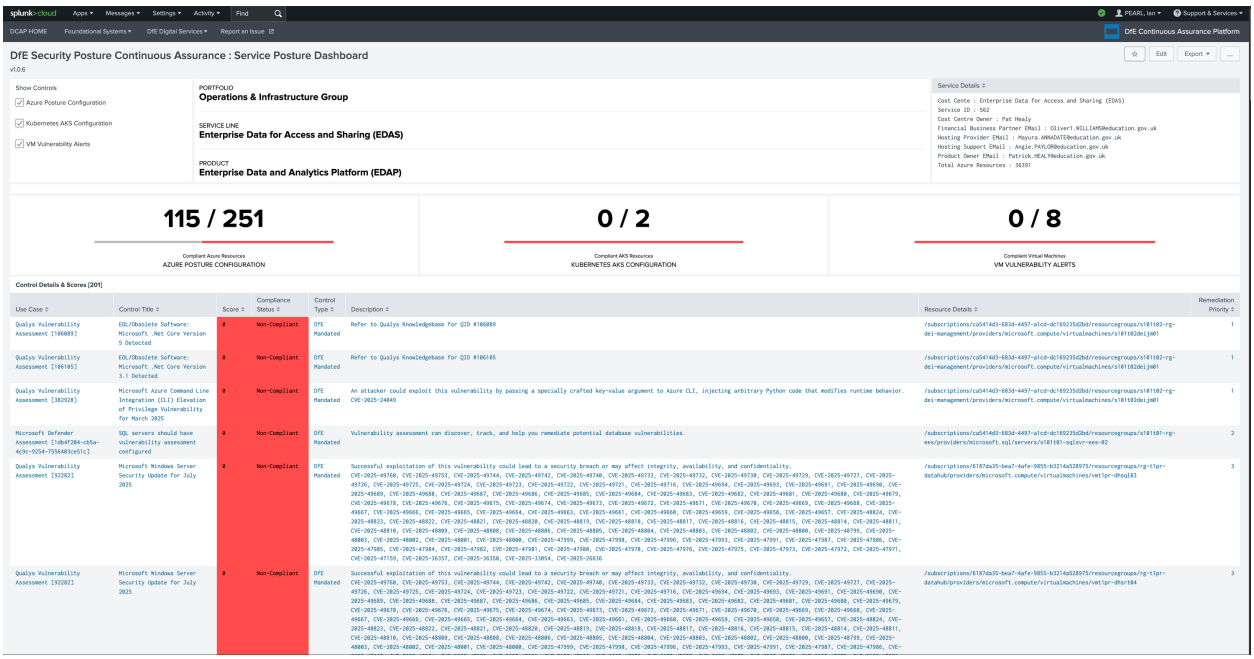
(Note : since May 2025, ESFA assets have become part of Operations & Infrastructure).

The scores for each technology type show the number of compliant resources / the total number of resources, for the Portfolio as a whole.

Each line is a Service (or Product) within the Portfolio. The scores are for each technology type for the Service.

Clicking on a row will open the Service Posture Dashboard for that Service in a new Tab.

Service Posture Dashboard



This dashboard is for the technical owners responsible for remediation. It shows the list of all the Controls, their Scores, and their compliance statuses.

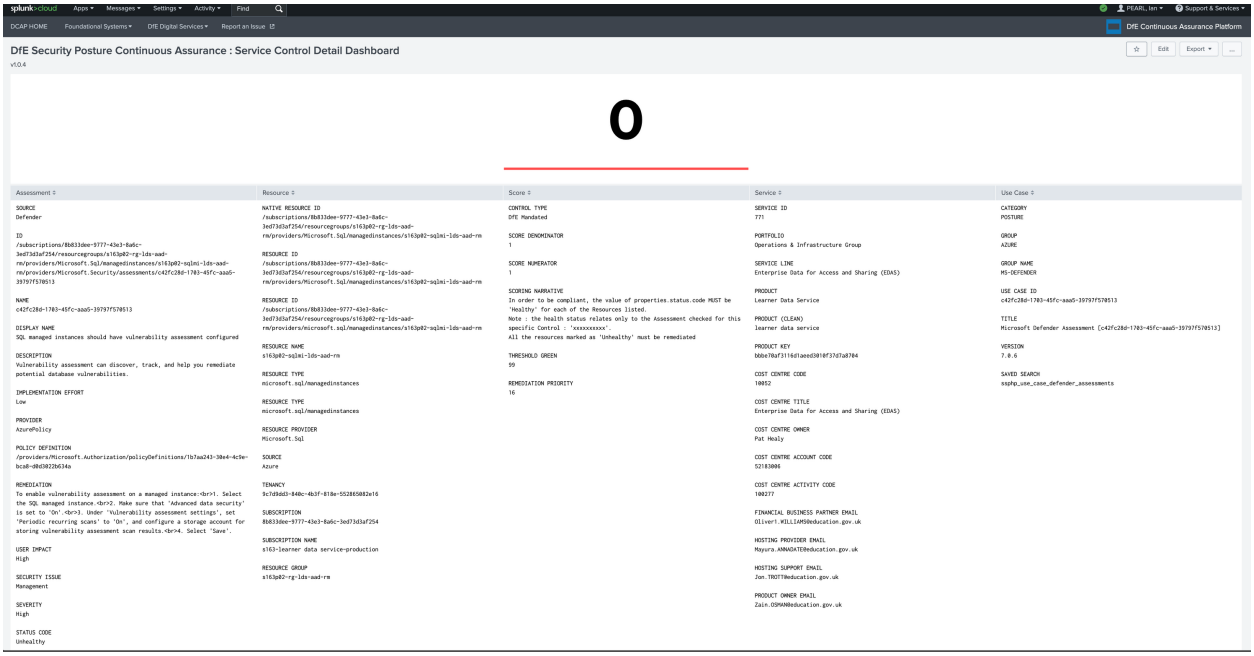
The overall scores show the number of compliant resources for each technology type. The panels will only show for technology types that are relevant for the individual Service.

In the top left there are checkboxes which allow you to either include or exclude the Control output for a technology type in the remediation list.

Each line of the Remediation List is a separate non-compliant assessment where the requirements of the Control have not been met, and that will need to be addressed. The remediation list only shows the output of Controls which are DfE Mandated and Non-Compliant.

On the right side of the line for each Control is a number indicating the ‘Remediation Priority’. DCAP has attempted to prioritise the Controls based on which order it determines they should be addressed. Clearly it is for the Service to decide how much resource can be applied to Security, the Priority really is only a recommendation and no more.

Service Control Detail Dashboard



This dashboard is intended for the individual responsible for understanding and remediating individual non-compliance issues; it shows the field level technical details about the tests that were run for a single Control, the Resources that it ran against, the expected results, and what needs to be changed in order to comply.

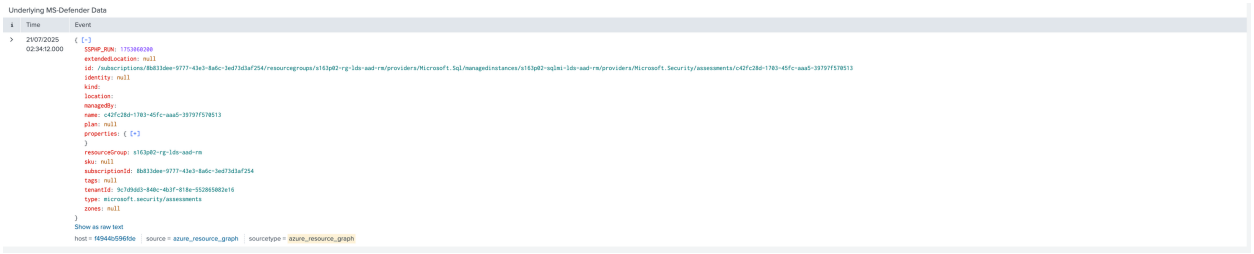
The dashboard has 3 rows of data panels :

(1) the Score; the Score is calculated from the 'numerator' (Tests Failed in this Control) / 'denominator' (Number of Tests in this Control), expressed as a percentage. Depending on the context of the Control, numerator and denominator have different meanings…(a) for a Control where there is only a single setting to be investigated (ie 1 line), numerator and denominator means the number of fields that were investigated in the algorithm. (b) for a Control which has meany lines (for example, where the Control requires us to look at every user to see whether they each have the correct settings), then each use is

deemed to be either Compliant or Non-Compliant and the denominator and numerator would be the number of events (in the example, users) and the number that failed the tests.

(2) details of the Control Assessment, the Resource, the Service, and the Use Case;

(3) the Underlying Data; this is original data that was returned from the source by the API, and is displayed in a format appropriate to that source. For underlying data that originates from a CIS Use Case, the data will be a table with non-compliant fields displayed in red. For other sources of underlying data, the display will be JSON.



On-Boarding to DCAP

There are a small number of requirements that a Service must fulfill in order to use DCAP :

- Create User Accounts - each end user must have an account created for them in Splunk, so a complete list of Users for the Service is a necessary pre-requisite;
- Check data ingestion – the Azure, Qualys, and K8S data will already be in DCAP; but we like to run a check to ensure that all of your resources are recognized in our asset inventory;
- Check Azure tagging – it is a requirement that the Service runs checks to ensure that the Azure resources are correctly tagged for their Service;
- Tag GitHub repos – if the Service keeps its source code in GitHub, then some custom tags will need to be added to each repo so that it can be attributed to the Service. The taxonomy of the tags exactly matches to that of the FBP.
- ADO repos – provide a list of ADO repos. It may also be necessary to provide assistance to DCAP engineering to get access to the subscription in order to collect the required data.

Once all of these are in place, then the dashboards should all light up automatically, and remediation work can commence.

Issue Reporting

DCAP has it's own Slack channel. Please report an issues or requests in the Slack Channel.