**VECTR v5.3 Feature Breakdown**

Table of Contents

[Browser Cache Fix 2](#_Toc22627405)

[Context Sensitive Help 3](#_Toc22627406)

[Data Integrity Report Updates 5](#_Toc22627407)

[Historical Trending Redesign 6](#_Toc22627408)

[Import MITRE CTI Data Improvements 9](#_Toc22627409)

[Test Case Evidence File Upload Improvements 11](#_Toc22627410)

[Test Case Icons Additional Support 12](#_Toc22627411)

[Heat Map Technique Duplications Filter 14](#_Toc22627412)

# Browser Cache Fix

What is it?

This is a fix for situations where when using VECTR for long term assessments you encounter issues with the application after a version upgrade. VECTR now builds its client side dependencies in a way that prevents cached data from interfering with new or changed features.

How does it work?

Previously, the workaround for these issues was to use Chrome’s incognito mode. Now, after this fix you can use the application as normal without incognito or private browsing mode. This change is behind-the-scenes.

How can this feature help me?

This fixes an application usability bug.

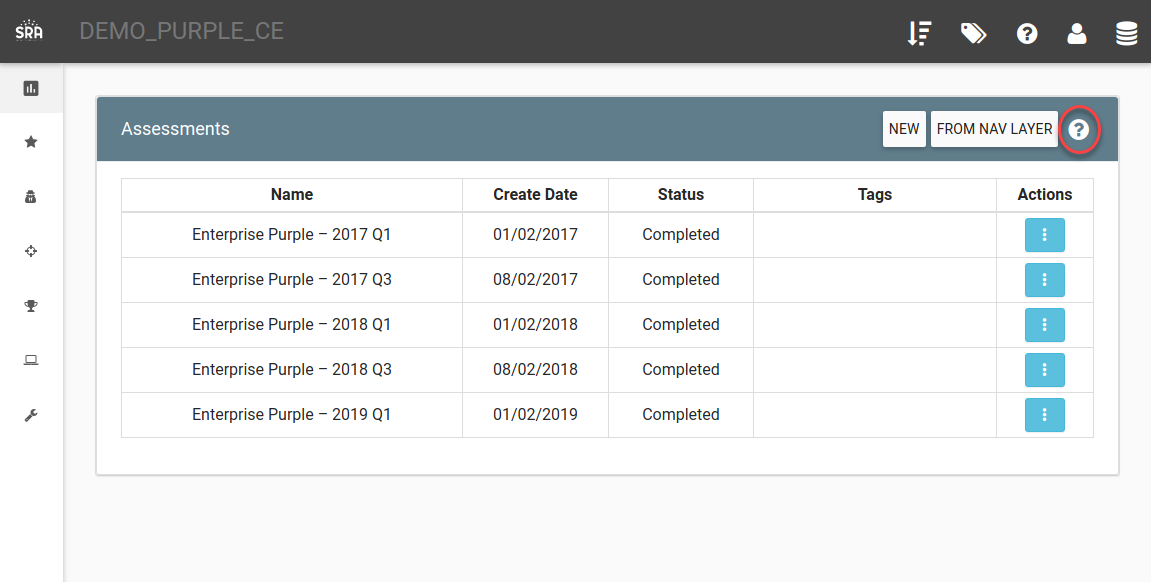
# Context Sensitive Help

What is it?

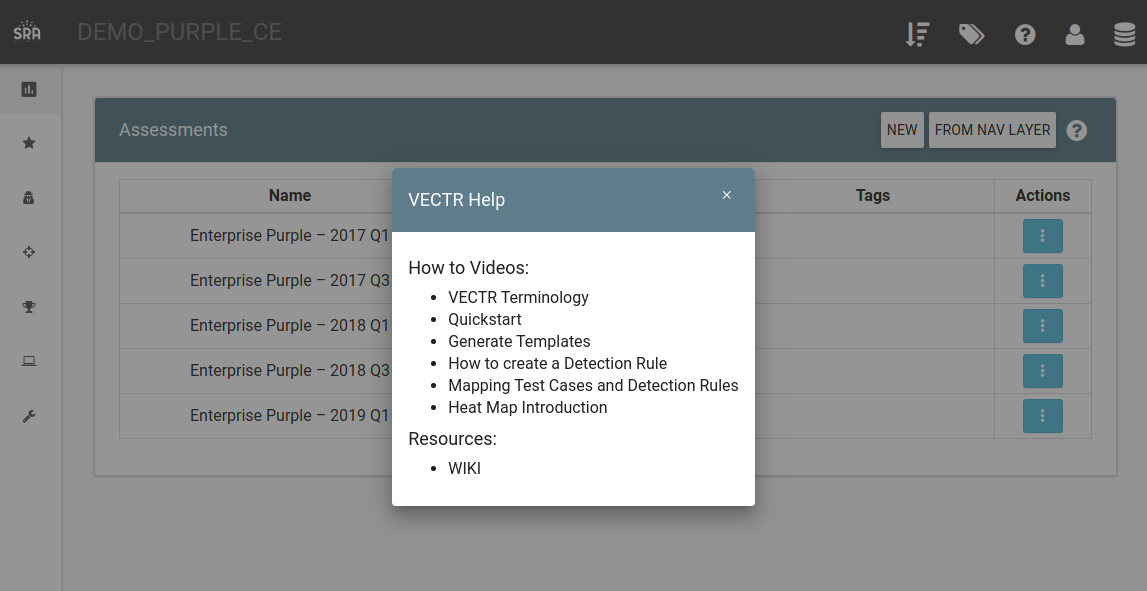
This adds a new Help menu to core functionality screens with links to relevant documentation or user guides. For now these link to relevant VECTR help videos and the GitHub wiki depending on the page.

How does it work?

On some VECTR screens you will see a question mark in a circle signifying help is available.



Clicking the question mark will open help in a modal dialog.



How can this feature help me?

This feature provides easier access to help and guide resources that are pertinent to areas of the application where you are working.

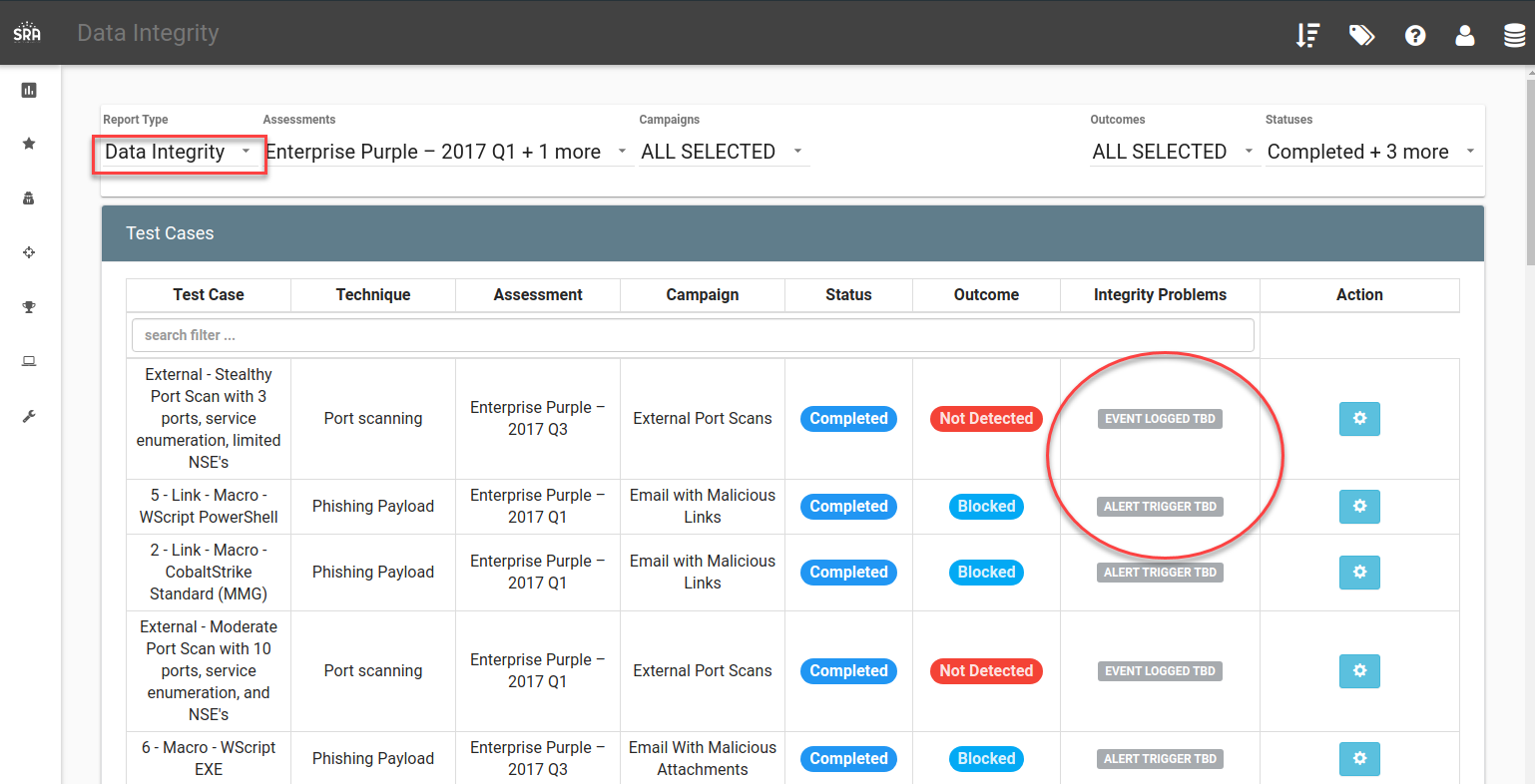
# Data Integrity Report Updates

What is it?

The Data Integrity Report shows Test Cases that may be have incorrect data.  Existing functionality Test Cases with an Outcome of "Not Detected" that have Blue Tools checked and Test Cases with an Outcome of "Blocked" or "Detected" with no Blue Tools checked.  We’ve added reporting for Test Cases where the Outcome is “Not Detected” and Event Logged is “TBD” or Outcome is “Blocked” and Alert Triggered is “TBD.”

How does it work?

Select the Data Integrity report from the Reporting page:



How can this feature help me?

In the event data has not been completely or accurately entered, this report shows inconsistencies or incomplete recording of finished assessment activities.

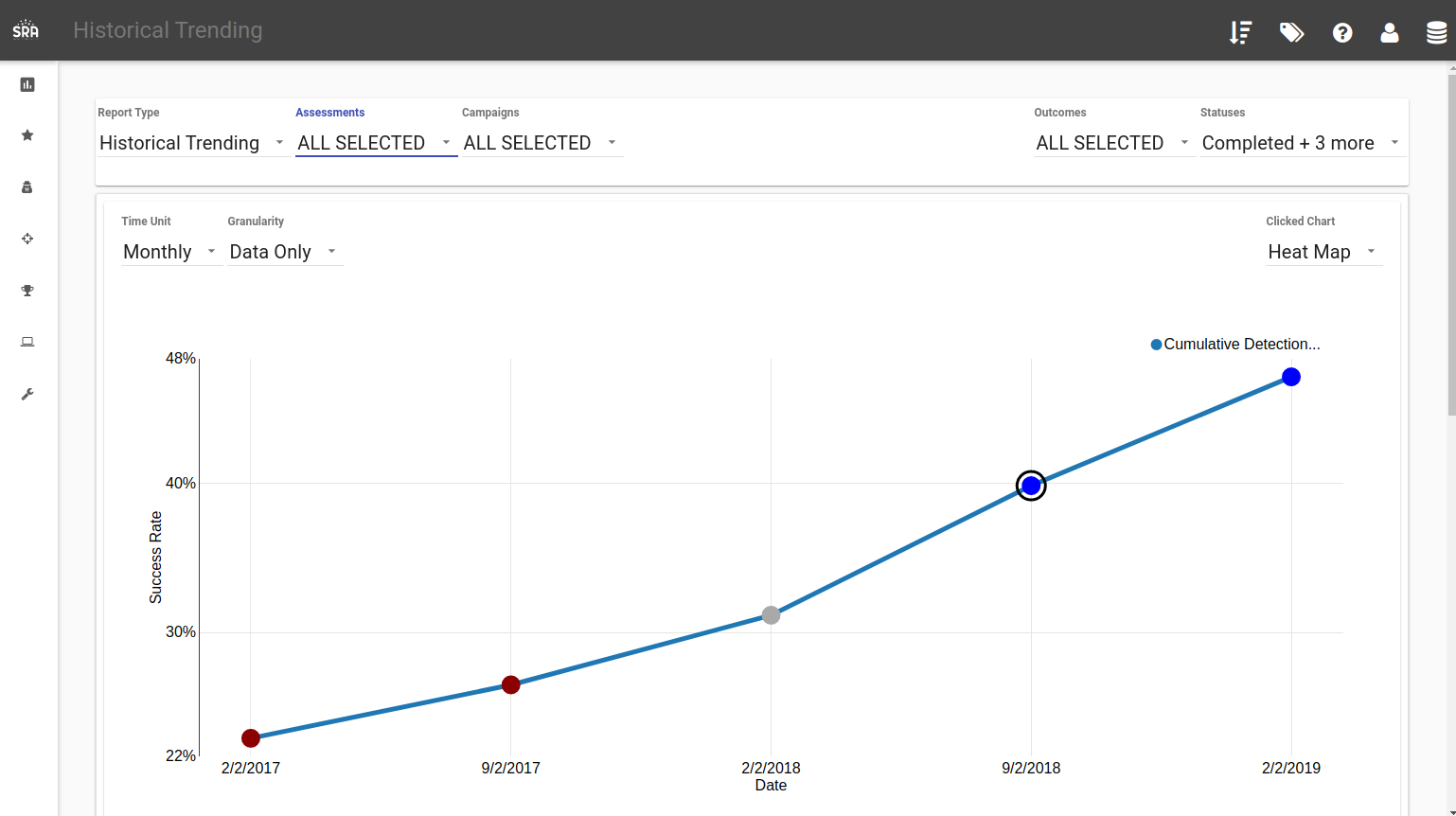
# Historical Trending Redesign

What is it?

The Historical Trending Report has been redesigned to add more flexibility to the report

How does it work?

Browsing to the “Historical Trending” Report Type will show this:

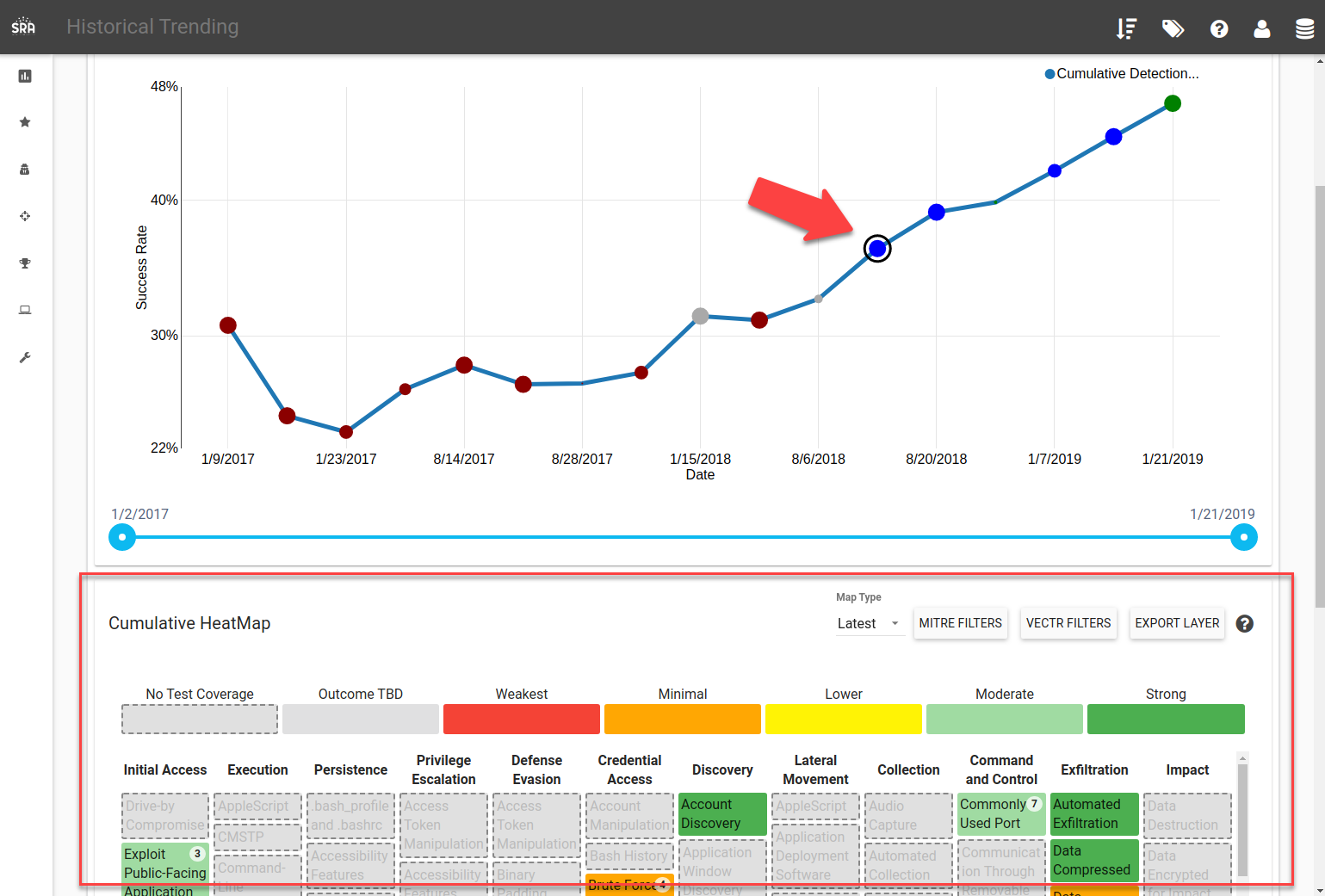


Users can select the number of assessments they want to include in the trendline using the report filters at the top of the page and adjust the Time Unit (Monthly, Quarterly, etc.) and Granularity of the graphed data.



Hovering over a point on the chart will show statistics as of that point. Note that here we’re showing Weekly data and between 8/6/2018 and 8/13/2018 we performed 57 Test Cases according to the Aggregated count. The total count of test cases performed was 546 between 1/9/2017 and 8/13/2018. The data in this hover chart tells you that between 8/6/2018 and 8/13/2018 you detected 68.42% of your Test Cases run and this was significantly better than your prior average detection rate of around 33%. This bumped up your cumulative detection score to 36.45%.

The blue circle on the chart shows you performed well in the preceding time period, and the size of the circle shows how many Test Cases relative to the total were performed in that time. Many Test Cases shows a larger circle.



Clicking on a point in the Historical Trending graph allows you to show different report types below the trending graph driven by the “Clicked Chart” filter. In this case, it is showing the MITRE Heat Map view as of that point.

How can this feature help me?

These new Historical Trending views are helpful for showing high-level detection improvements over time and analyzing strengths and weaknesses in tested data.

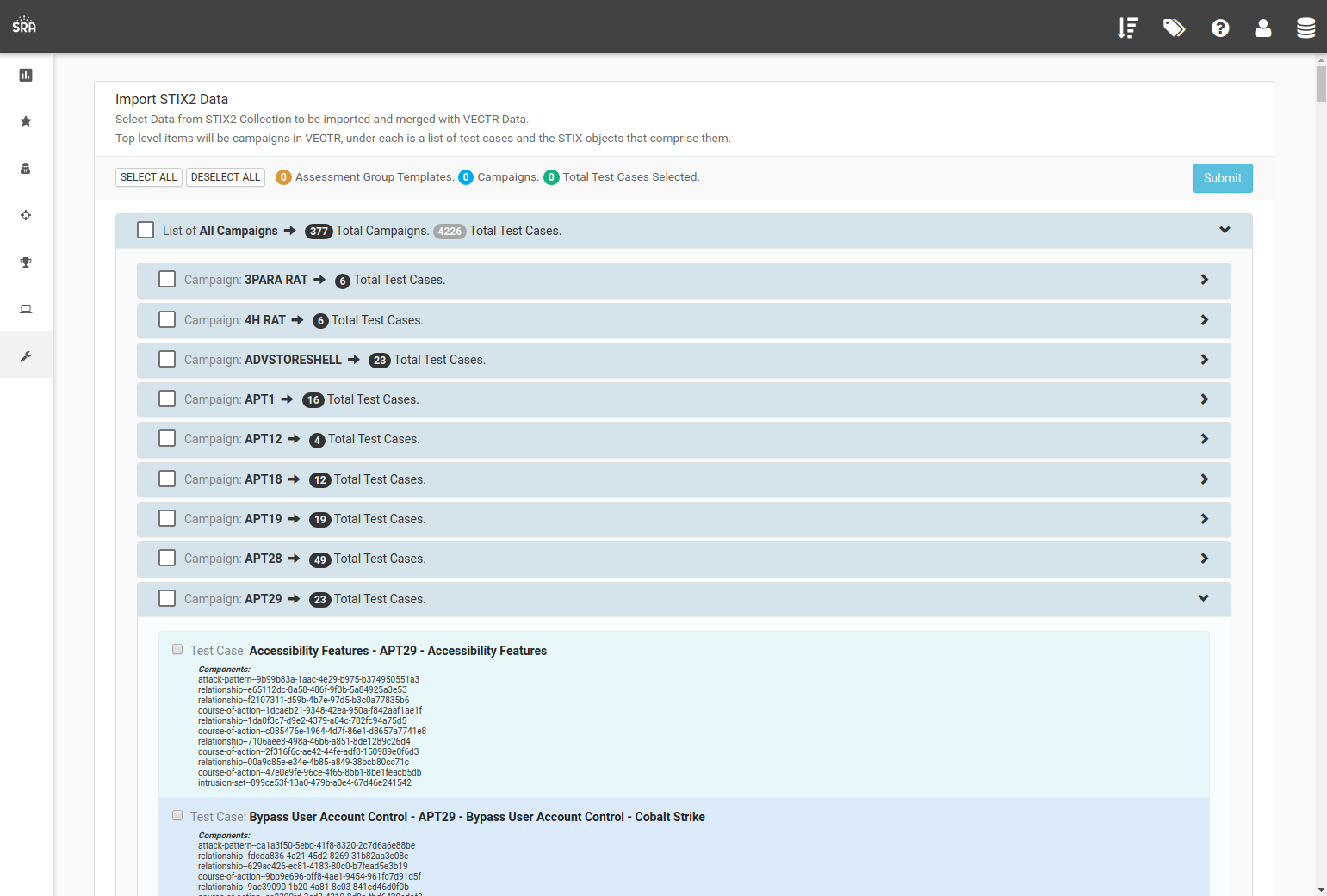
# Import MITRE CTI Data Improvements

What is it?

VECTR can import MITRE CTI STIX data to create Test Cases and Campaigns for common threat actors. Recent improvements make it so that as of this latest version of VECTR, importing new data will update existing imported data in the system UNLESS you have made changes to that data. In the scenario where you have modified imported data, any future imports will try to preserve your modifications and enrichments.

How does it work?

Download the enterprise-attack.json file from MITRE <https://github.com/mitre/cti/blob/master/enterprise-attack/enterprise-attack.json> and import it using the Administration -> Import Data user interface for importing JSON data.



Note: Do NOT import all MITRE CTI data, only select campaigns you plan on manually enriching and emulating for threat actors or malware that pertain to your environment. Pulling too much data into the system will be overwhelming and unlikely to lead to good testing outcomes.

MITRE updates their enterprise-attack.json CTI data on a regular basis. After importing data, wait some time for MITRE updates and try to import new data, selecting previously imported campaigns for an update. The system should now update your previously imported data for any Test Cases you haven’t modified rather than creating duplicates.

How can this feature help me?

This feature allows you to keep up to date with MITRE CTI Threat Actor and Malware data without manually adding and deleting older imported Test Cases.

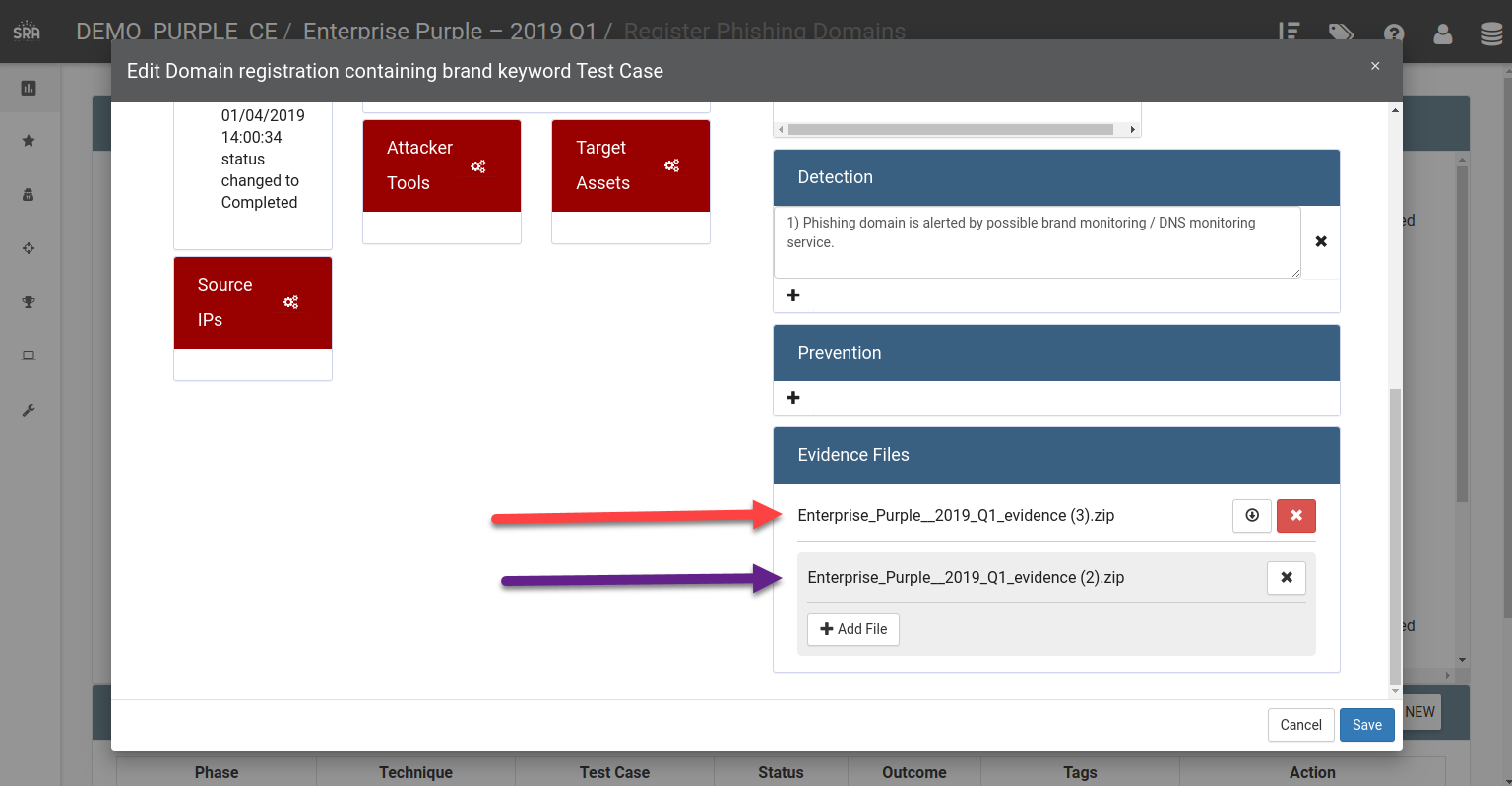
# Test Case Evidence File Upload Improvements

What is it?

The VECTR Test Case Evidence File upload interface has been modified for better usability.

How does it work?

In the screenshot below, an existing Evidence File is shown next to the red arrow. A file to be uploaded is shown next to the purple arrow. Clicking save will upload the file in the Add File box and a progress bar will be shown.



How can this feature help me?

This improvement makes it easier to interact with Evidence Files in the Test Case view.

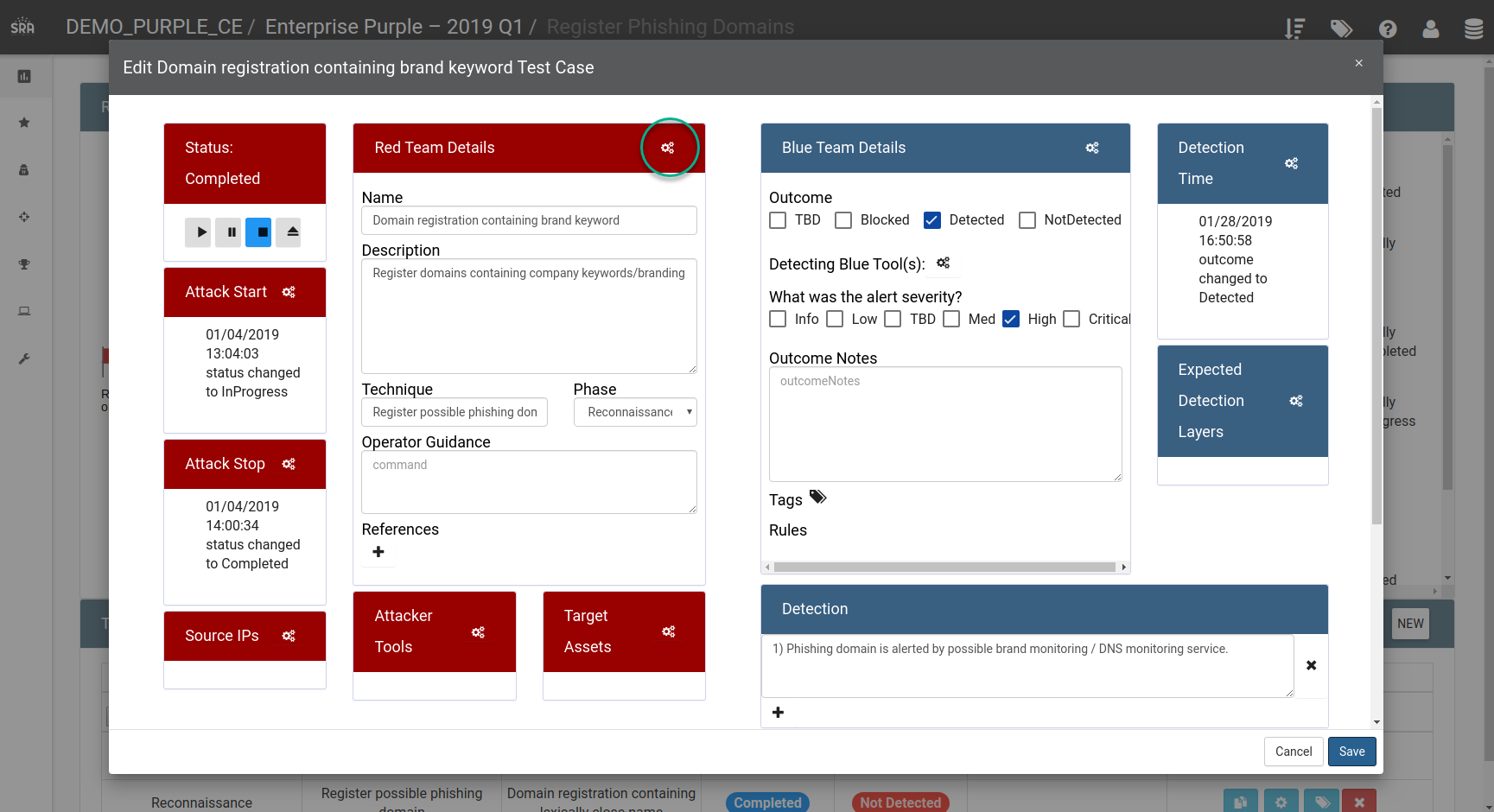
# Test Case Icons Additional Support

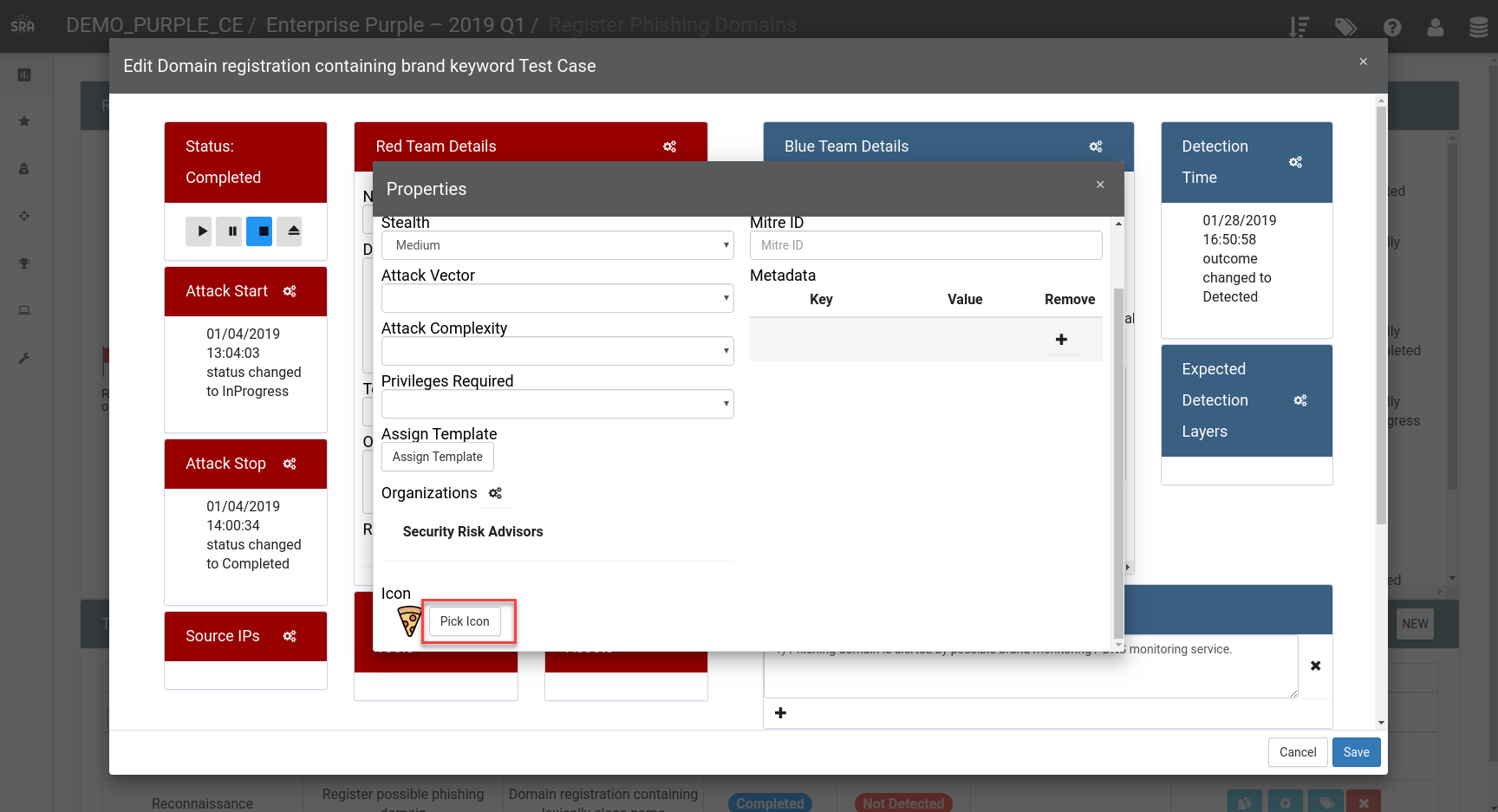
What is it?

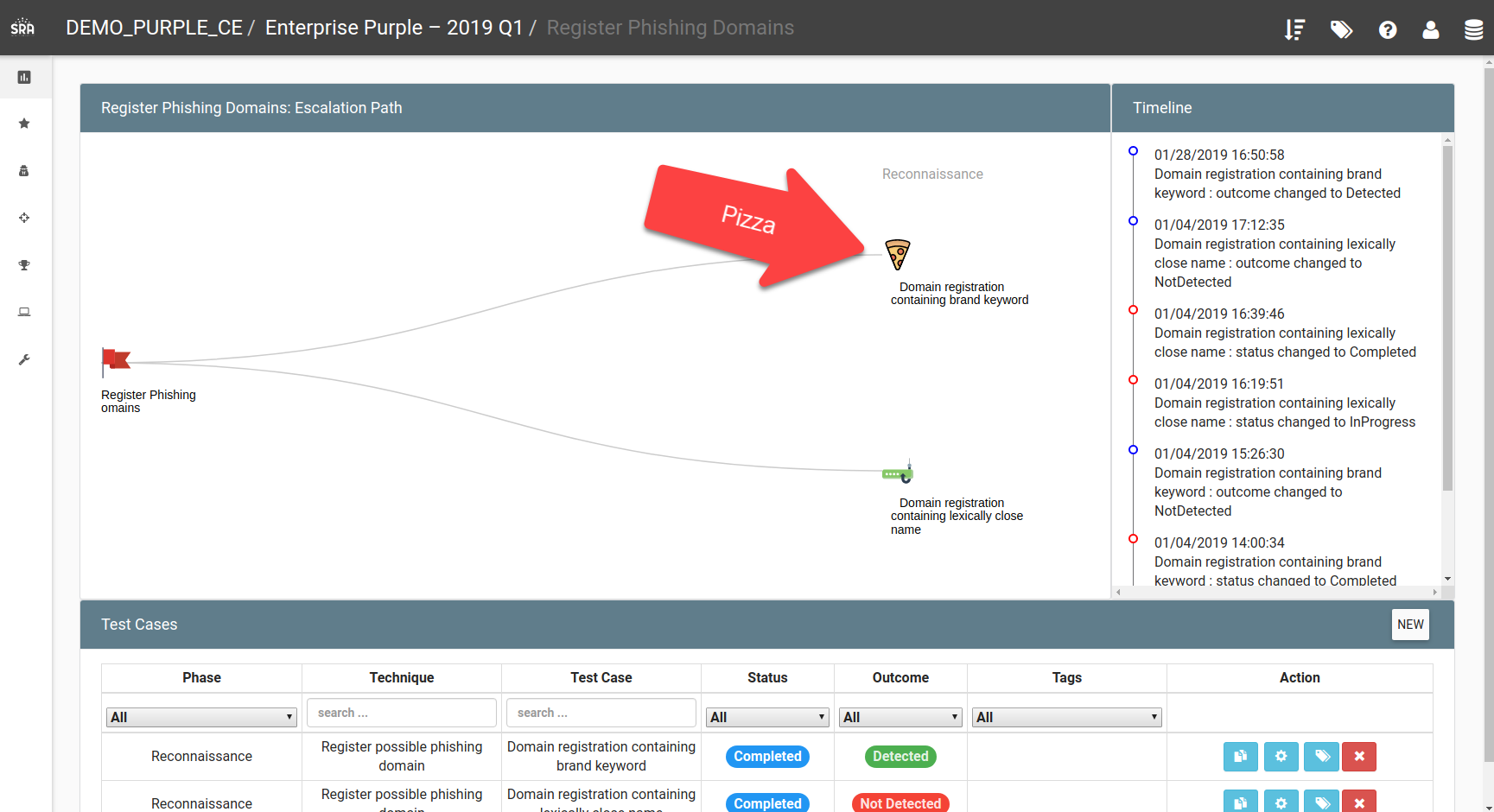
VECTR now supports adding additional or custom icons for Test Cases to display in the Escalation Path on the Campaign view.

How does it work?

For now, you will need access to the VECTR deployment environment to use this feature. You can put new icons in VECTR deployment directory path under app/static/icons. Icons should be in SVG format. You may place new icons in this directory. We highly recommend keeping the existing icons in the folder. Many existing Test Cases rely on bundled icons.







How can this feature help me?

This feature allows you to customize escalation path icons in more detail which may be desirable when testing web applications in depth, industrial control systems, physical hardware, or other company-specific assets.

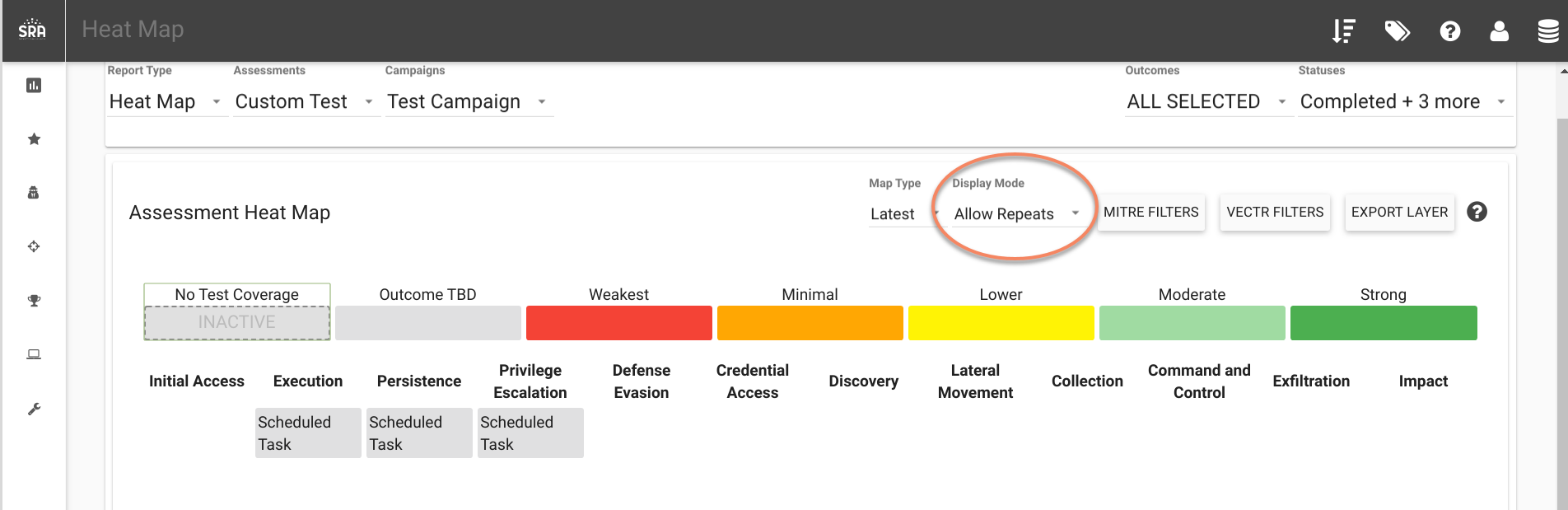
# Heat Map Technique Duplications Filter

What is it?

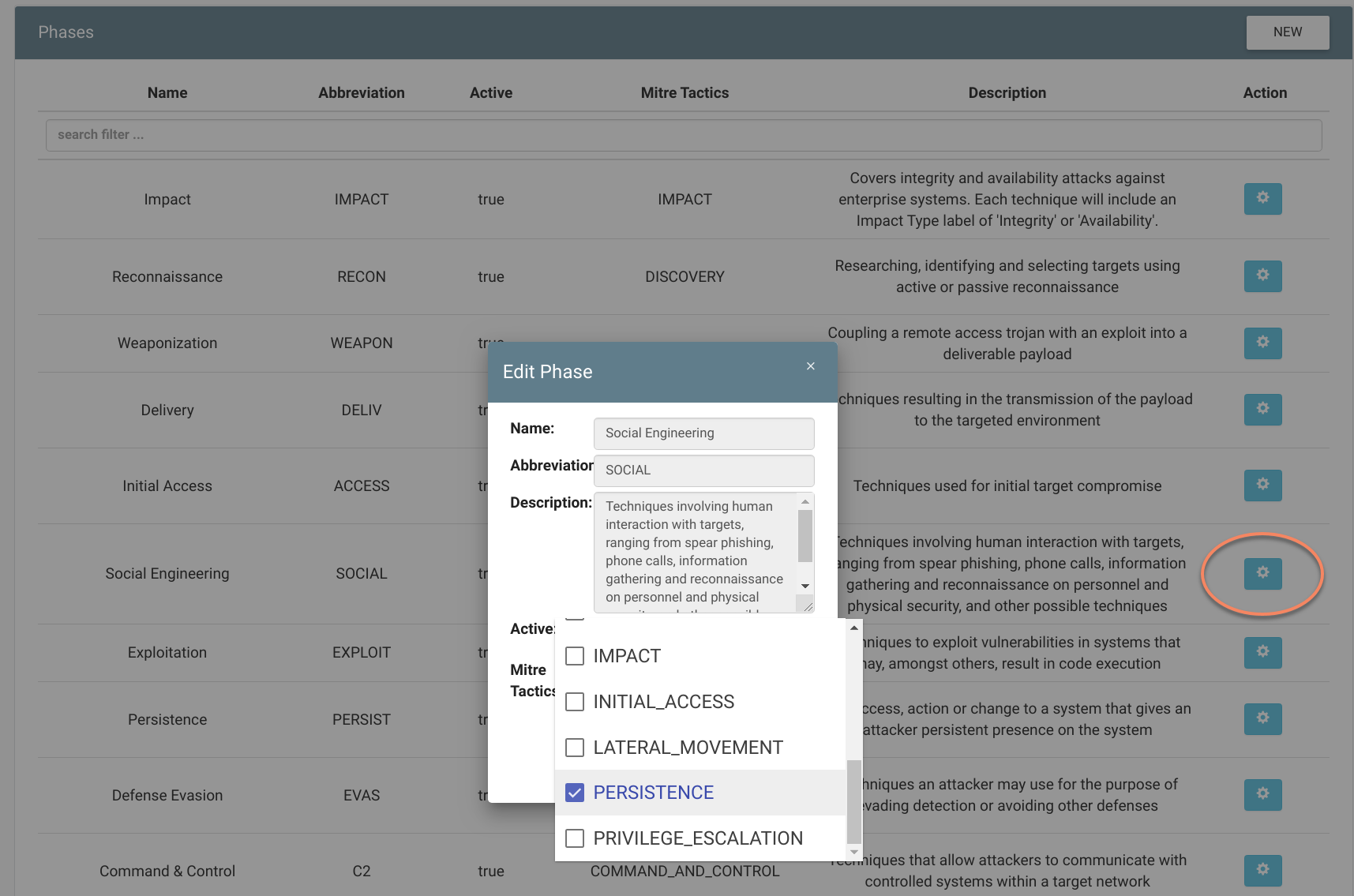
VECTR now supports the ability to align your custom Phases to MITRE Tactics. There is a filter in the Heat Map that will align not only the Technique, but the Tactic as well to eliminate duplicate entries.

How does it work?

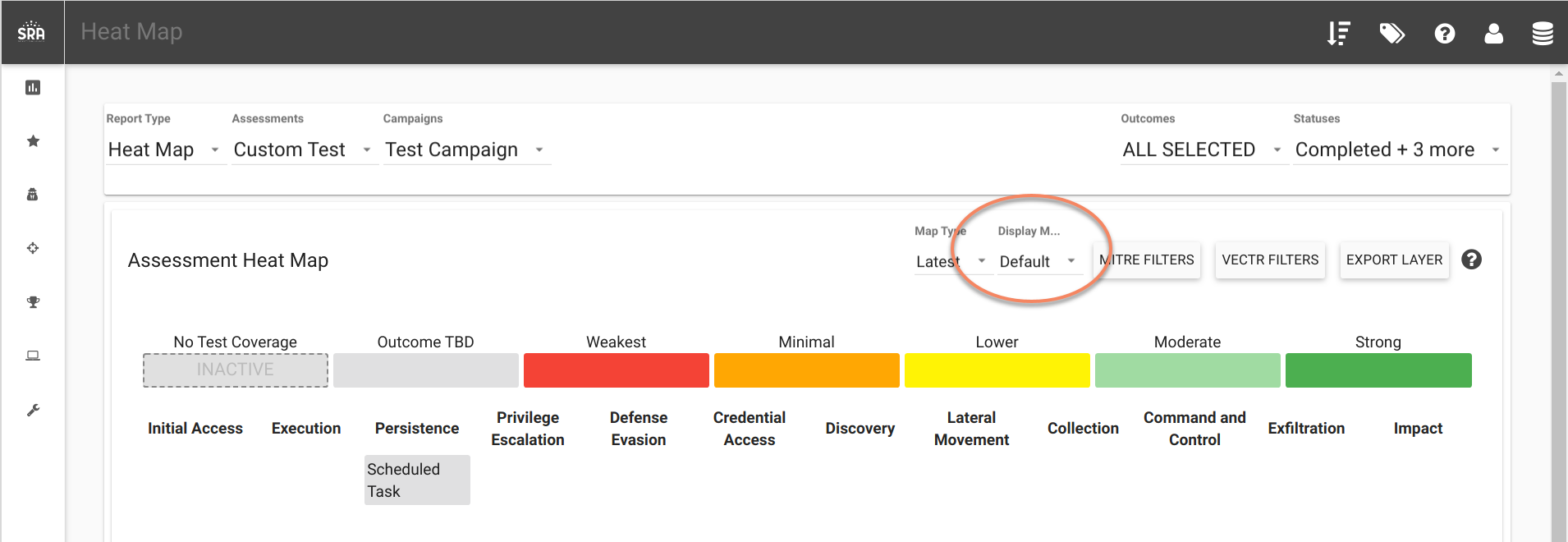
Assume you have a TestCase that is of a Phase (Social Engineering) that is not a MITRE Tactic. You set the MitreID field to T1053. If you set the Allow Repeats Display Mode, the Test Case will show up in all Techniques = T1053:



If you want all Phases of Social Engineering to show up only under Persistence, then you can go to the Admin -> Phases screen, then edit the Social Engineering Phase by clicking the cog. You can then set the Mitre Tactics to PERSISTENCE.



Going back to the Heat Map, you can set the Display Mode to “Default” to eliminate the duplicates.



How can this feature help me?

This feature allows you to more granularly align Test Cases to the Heat Map and eliminate duplicates.