

# VECTR v4.2 Feature Breakdown

## Table of Contents

- Assessment Group/Assessment Cloning ..... 2
- Database Schema Versioning..... 3
- Data Integrity Report ..... 5
- Detection Rule UI Update ..... 6
- HEAT Map Report ..... 7
- Mitre ATT&CK Framework Test Cases ..... 8
- Report Filtering by Outcome/Status..... 9
- Vendor & Tools UI Update ..... 11

# Assessment Group/Assessment Cloning

## What is it?

VECTR can now clone Assessments and Assessment Groups.

## How does it work?

The Assessment Group and Assessment page now show a Clone button:

Assessment Group			
Name	Type	Status	Actions
Test Campaign Assessment	Campaign	Not Performed	      
2015 Q4 Purple Team	Campaign	In Progress	      
2016 Q2 Purple Team	Campaign	In Progress	      
2017 Q1 Purple Team	Campaign	In Progress	      

Clicking the clone button will allow you to duplicate the referenced Assessment or Assessment Group, clearing out the status and outcomes.

## How can this feature help me?

Cloning an Assessment Group can help the process of setting up regularly scheduled Campaigns or parallel Campaigns in different environments.

# Database Schema Versioning

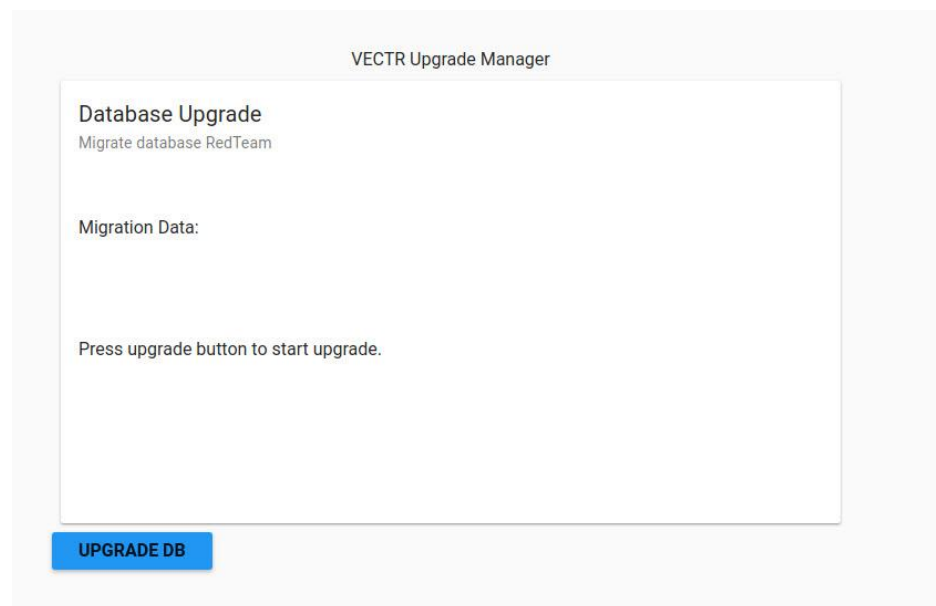
## What is it?

Database Schema Versioning is an enterprise software feature that allows for the migration of existing data from one version of an application to another.

In VECTR, this feature is built using internally developed tools and Mongobee (<https://github.com/mongobee/mongobee>)

## How does it work?

When you login to VECTR, you may be prompted with an upgrade screen that looks like this:



Clicking the "UPGRADE DB" button will launch the migration process, graying out the button on the page and updating the display box with log data from the migrations. This will first create a backup of your database and then begin running a series of scripts that migrate your data to the latest schema. Once this activity is complete, the button will reactivate with the text "DONE." Clicking this will take you to VECTR.

Note: The Gold Standard database often needs to be updated in addition to each of your engagement databases. After installing a new version of VECTR you may be prompted to upgrade two databases.

## **How can this feature help me?**

This feature allows you to upgrade your VECTR instance to match the latest data model and keep existing data without manual data manipulation.

# Data Integrity Report

## What is it?

This report shows Test Cases that may have incorrect data. The two primary examples of this are 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. Both of these scenarios should be resolved so that reporting data is accurate.

## How does it work?

Select the Data Integrity report from the Assessment Group page:

Test Cases						
Phase	Method	Test Case	Status	Outcome	BlueTools	Action
search filter ...						
External Recon	Register possible phishing domain	Domain registration containing brand keyword 3	Completed	Not Detected	<ul style="list-style-type: none"><li>MarkMonitor</li><li>PhishEye</li></ul> <a href="#">REMOVE TOOLS</a>	
Exploitation	Stolen Laptop	Stolen laptop without credentials	Completed	Blocked	<a href="#">ADD TOOLS</a>	
Initial Delivery	Email with malicious attachment	Emailing - MS Office Macro Attack - Cobalt Strike Bitsadmin	Completed	Not Detected	<ul style="list-style-type: none"><li>Symantec Messaging Gateway</li></ul> <a href="#">REMOVE TOOLS</a>	

## How can this feature help me?

In the event data has not been completely entered, this acts as a second set of eyes to get the assessment to be as accurate as possible.

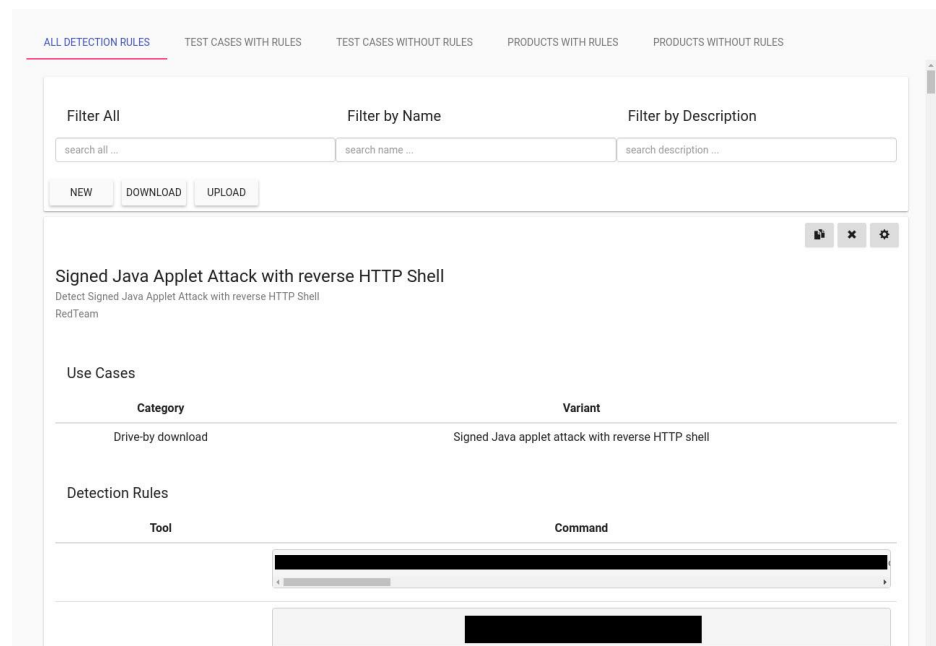
# Detection Rule UI Update

## What is it?

The Detection Rule UI screen has been updated to show more information and allow easier searching.

## How does it work?

Browsing to the Detection Rules page will show this:



Users can filter on various properties, and now the detection rule details are shown in a card view making it easier to copy and paste them out into external systems. Test data is redacted from the screenshot.

## How can this feature help me?

This feature should allow for easier management and traversal of user cultivated detection rule data.

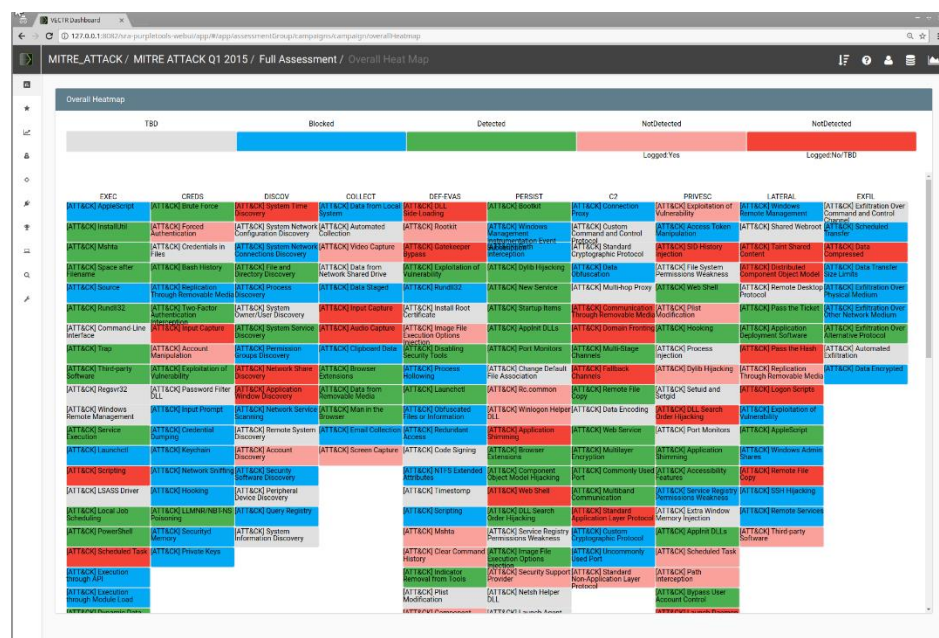
# HEAT Map Report

## What is it?

The HEAT Map is a common MITRE ATT&CK framework common reporting deliverable. This shows at a glance where gaps and competencies exist when evaluating blue team detection and blocking against the MITRE ATT&CK framework.

## How does it work?

Select the HEAT Map Report from the report attribute selection dialog and you will be presented with this report:



Note: HEAT Map reporting is generally ATT&CK-specific. While the report will function for other assessments, it won't be as visually useful and may present oddly.

## How can this feature help me?

This feature allows you to view MITRE ATT&CK Framework assessment results in an easy to digest HEAT Map.

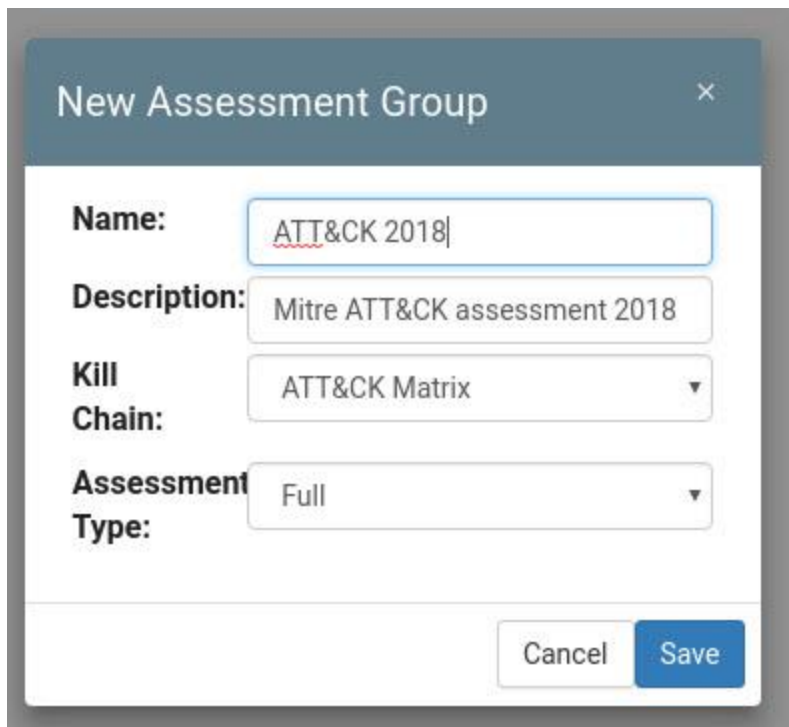
# Mitre ATT&CK Framework Test Cases

## What is it?

Mitre ATT&CK Framework ([https://attack.mitre.org/wiki/Main\\_Page](https://attack.mitre.org/wiki/Main_Page)) Test Cases are now included in the Gold Standard database. These can be used to perform purple team activities according to this industry standard attack set.

## How does it work?

A new Assessment Group can be created with ATT&CK Test Cases by selecting the Kill Chain "ATT&CK Matrix" and the Assessment Type "Full". From there, the Full Assessment Campaign will be populated with Mitre ATT&CK Framework data.



The screenshot shows a "New Assessment Group" dialog box. It has a title bar with a close button (X). The dialog contains the following fields:

- Name:** A text input field containing "ATT&CK 2018".
- Description:** A text input field containing "Mitre ATT&CK assessment 2018".
- Kill Chain:** A dropdown menu with "ATT&CK Matrix" selected.
- Assessment Type:** A dropdown menu with "Full" selected.

At the bottom right of the dialog are two buttons: "Cancel" and "Save".

**Note:** ATT&CK Framework reports and UI screens may differ in data and functionality from typical VECTR campaigns.

## How can this feature help me?

This feature allows you to track assessment data based on the Mitre ATT&CK Framework industry standard.



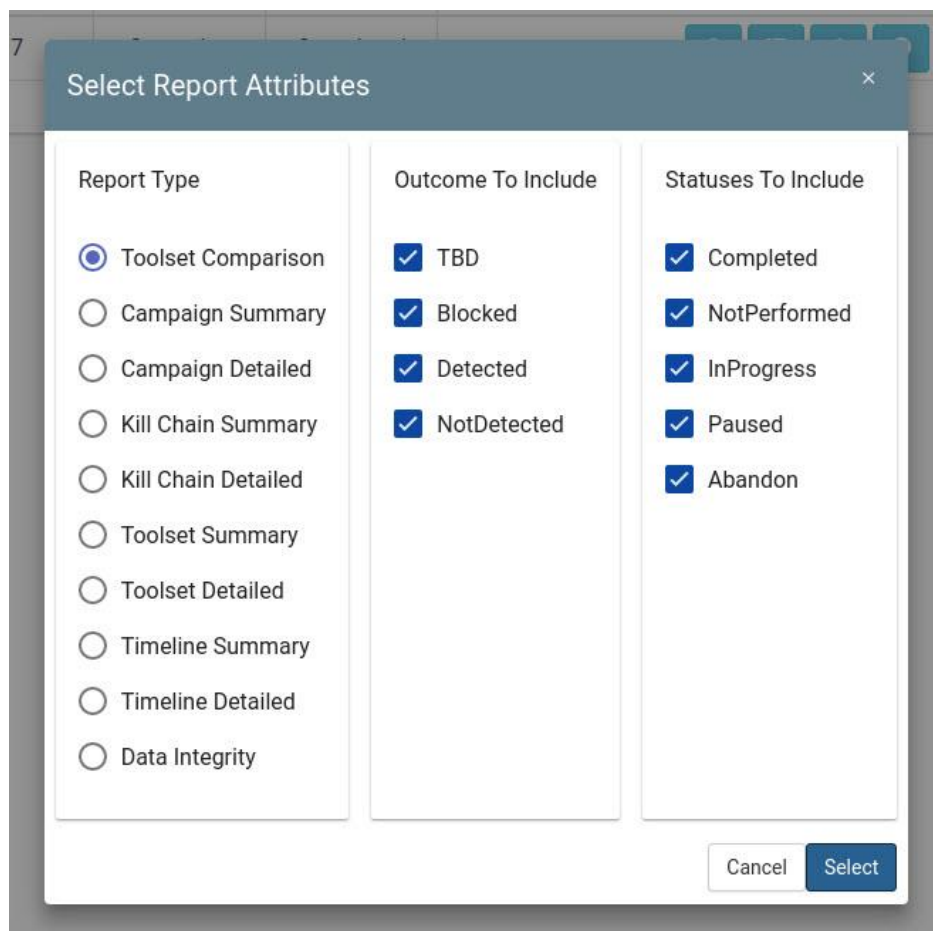
# Report Filtering by Outcome/Status

## What is it?

This is a new report attributes selection screen that allows for more granular data filtering.

## How does it work?

The new report attributes screen looks like this with check boxes to allow filtering by Outcome and/or Status of Test Cases. You can get there by viewing an Assessment Group and clicking the View Reports action button.



The screenshot shows a dialog box titled "Select Report Attributes" with a close button (X) in the top right corner. The dialog is divided into three columns: "Report Type", "Outcome To Include", and "Statuses To Include".

Report Type	Outcome To Include	Statuses To Include
<input checked="" type="radio"/> Toolset Comparison	<input checked="" type="checkbox"/> TBD	<input checked="" type="checkbox"/> Completed
<input type="radio"/> Campaign Summary	<input checked="" type="checkbox"/> Blocked	<input checked="" type="checkbox"/> NotPerformed
<input type="radio"/> Campaign Detailed	<input checked="" type="checkbox"/> Detected	<input checked="" type="checkbox"/> InProgress
<input type="radio"/> Kill Chain Summary	<input checked="" type="checkbox"/> NotDetected	<input checked="" type="checkbox"/> Paused
<input type="radio"/> Kill Chain Detailed		<input checked="" type="checkbox"/> Abandon
<input type="radio"/> Toolset Summary		
<input type="radio"/> Toolset Detailed		
<input type="radio"/> Timeline Summary		
<input type="radio"/> Timeline Detailed		
<input type="radio"/> Data Integrity		

At the bottom right of the dialog, there are two buttons: "Cancel" and "Select".

## How can this feature help me?

This feature allows you to filter reports to get more usable views of your Test Cases and Assessments. A common use case is to filter out Abandoned, NotPerformed, InProgress, and Paused Test Cases so that you can get a view of Completed Test Cases during an

engagement. This allows you to report on an ongoing purple team exercise without operational noise.

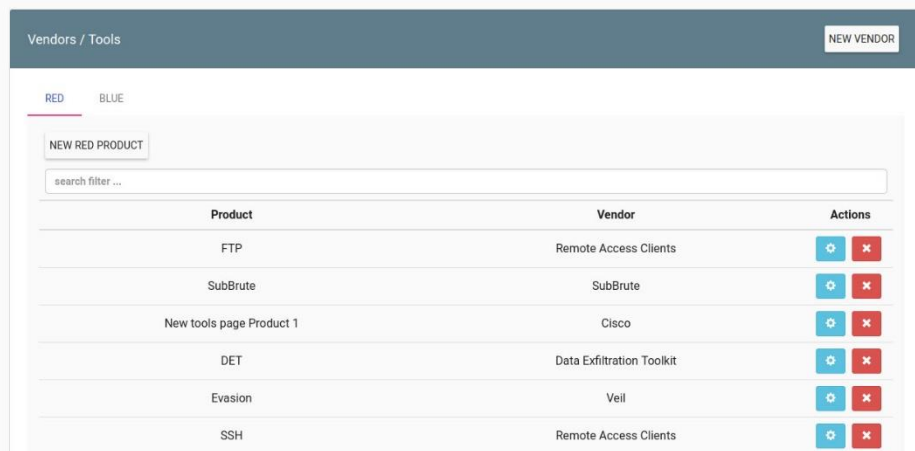
# Vendor & Tools UI Update

## What is it?

The Vendor & Tools User Interface has been updated to make it easier to add and edit Vendors and Products.

## How does it work?

Browsing to the Vendor & Tools page will show this:



Users can filter on products and vendors. It's now quicker to create or edit a new product or vendor.

## How can this feature help me?

This feature should allow for easier management and traversal of user cultivated vendor and tool data.