**VECTR v5.0.0 Feature Breakdown**

Table of Contents

[Generic Detection Rules 2](#_Toc935459)

[Analysis Engine Detection Rules 5](#_Toc935460)

[Detection Behaviors 8](#_Toc935461)

[Organizations 11](#_Toc935462)

[MITRE ATT&CK Heatmap Coverage 13](#_Toc935463)

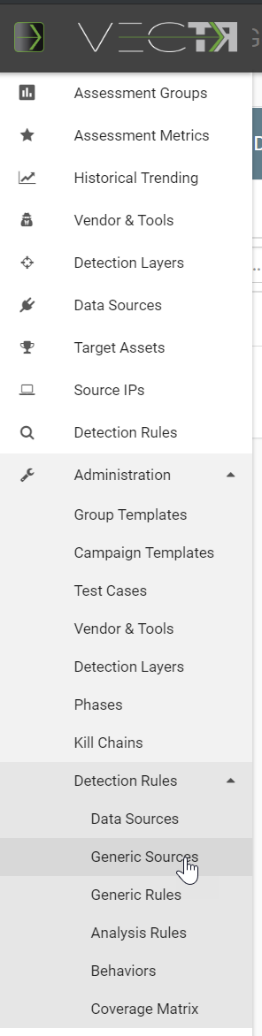
# Generic Detection Rules

What is it?

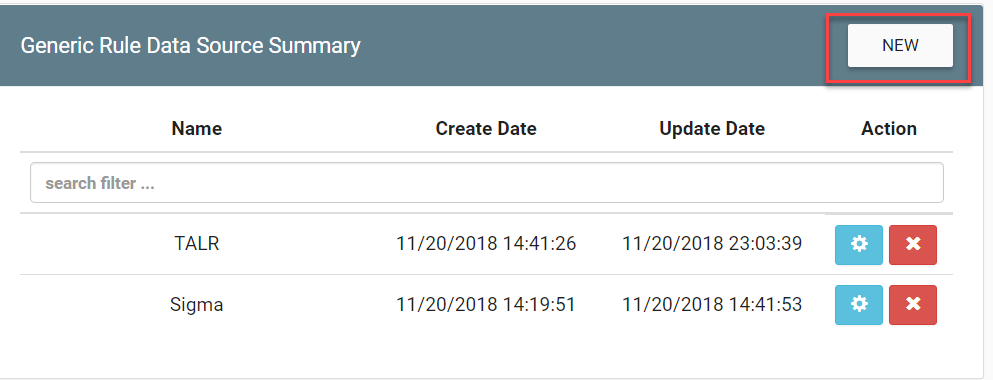
VECTR provides out of the box generic detection rules to assist in the detection of some of the test cases throughout the campaigns.

How does it work?

First, you must define a “Generic Source” for your detection rules. That can be done through the Administration -> Detection Rules -> Generic Sources page:

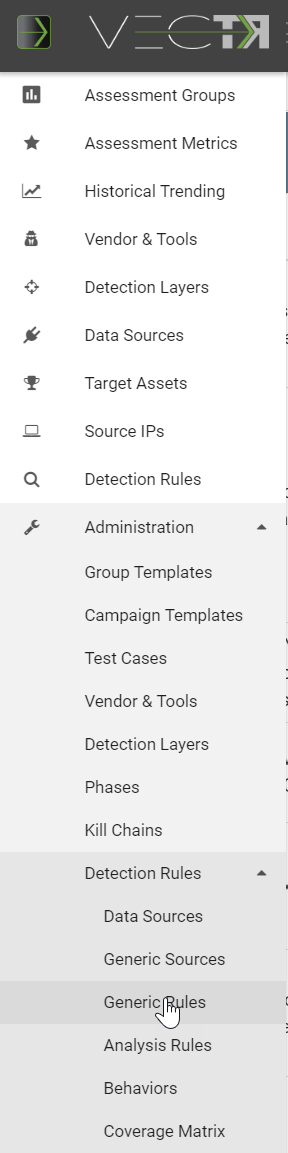


This will take you to the Data Sources page. From here you can define a new Generic Data Source:

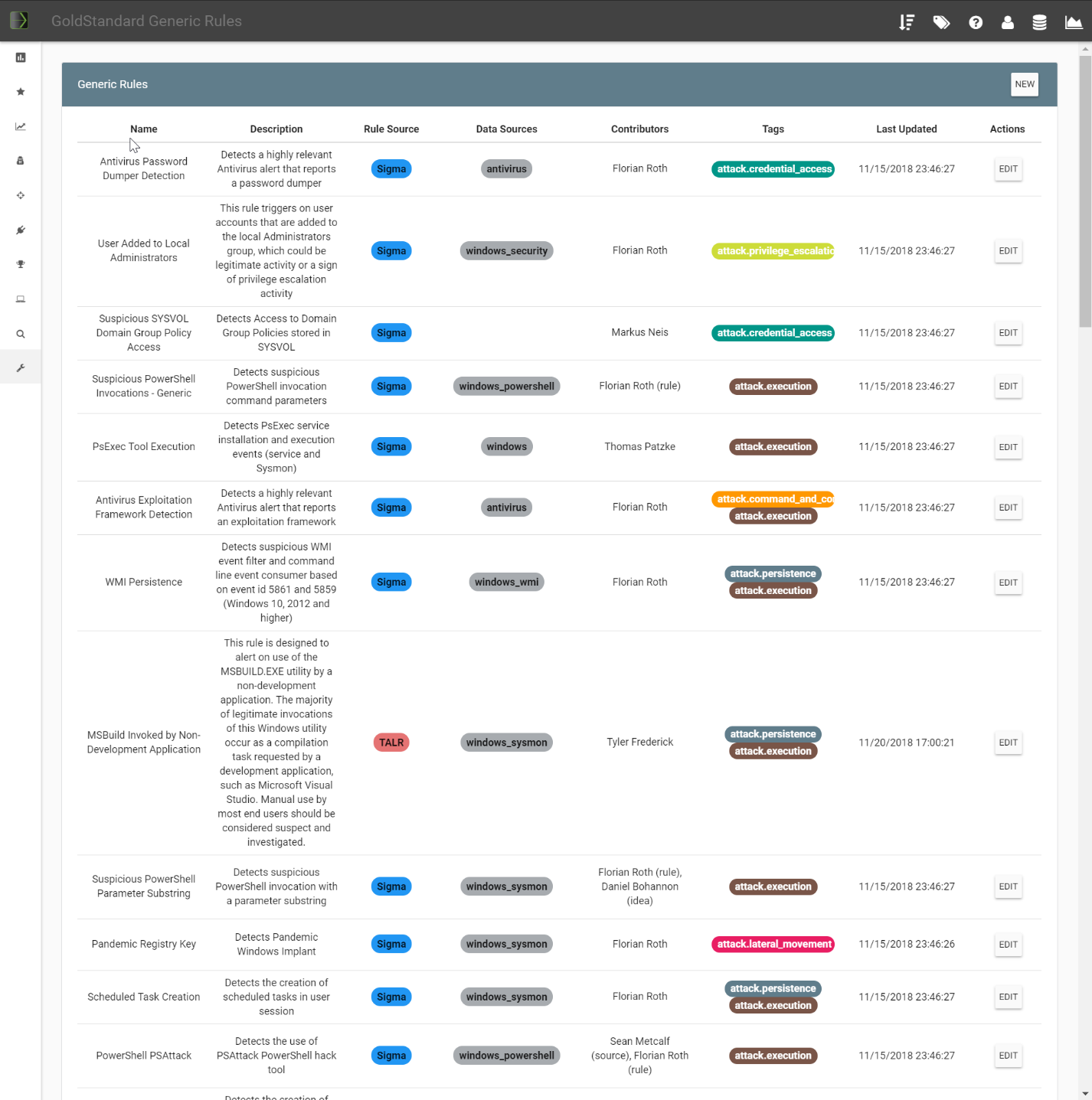


After you fill in the popup, your Generic Source will show up in the list (TALR and Sigma are shown above).

Now that you have a Generic Source, you can use this as the ‘parent’ of Generic Rules. From the Navigation menu, go to Administration -> Detection Rules -> Generic Rules



This will take you to the Generic Rules page:



Here you can create new rules by clicking the New button in the top right or Edit existing rules by clicking EDIT.

How can this feature help me?

Having Generic Rules can help users of the platform to have remediation recommendations for Test Cases.

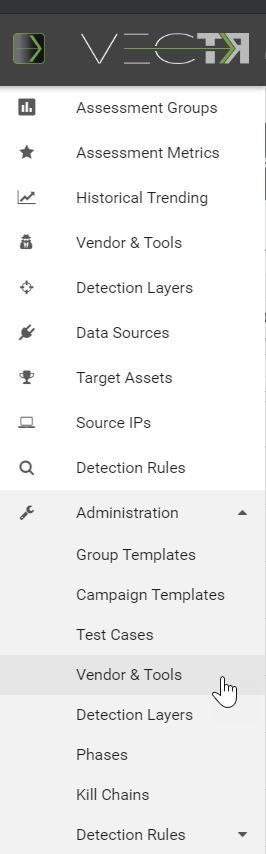
# Analysis Engine Detection Rules

What is it?

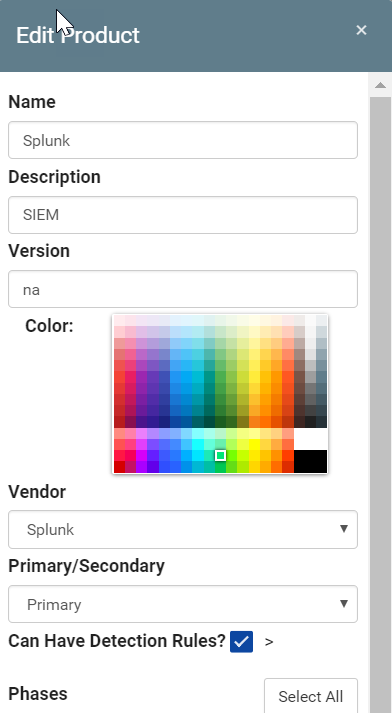
VECTR provides the ability to define product specific detection rules to assist in the detection of some of the test cases throughout the campaigns.

How does it work?

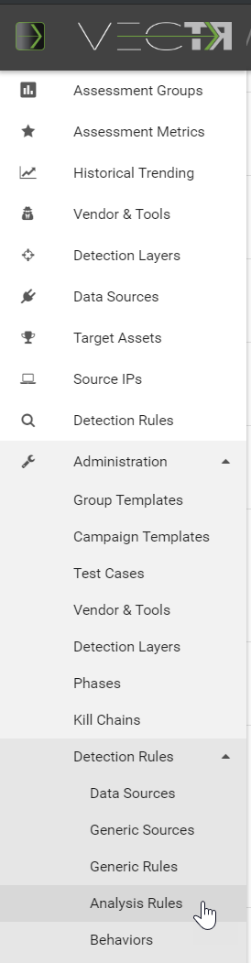
First, you must enable one of your blue team Products to be capable of using Detection Rules. That can be done through the Administration -> Vendors & Tools page:



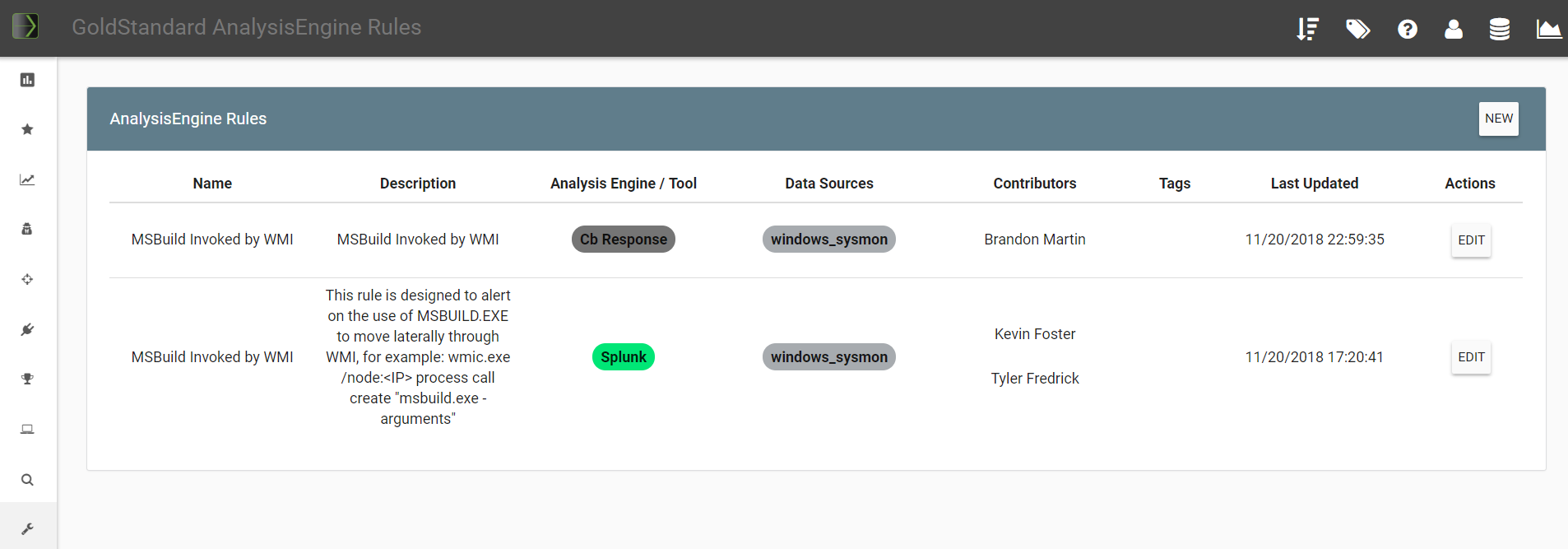
This will take you to the Vendors/Tools page. From here you can edit one of your Products by clicking the cog on the right. In the popup, click the “Can Have Detection Rules” checkbox:



Now that a Product has been identified as an Analysis Engine, you can use this as the ‘parent’ of Analysis Engine Rules. From the Navigation menu, go to Administration -> Detection Rules -> Analysis Rules:



This will take you to the Analysis Engine Rules page:



Here you can create new rules by clicking the New button in the top right or Edit existing rules by clicking EDIT.

How can this feature help me?

Having Analysis Engine Rules can help users of the platform to have remediation recommendations for Test Cases.

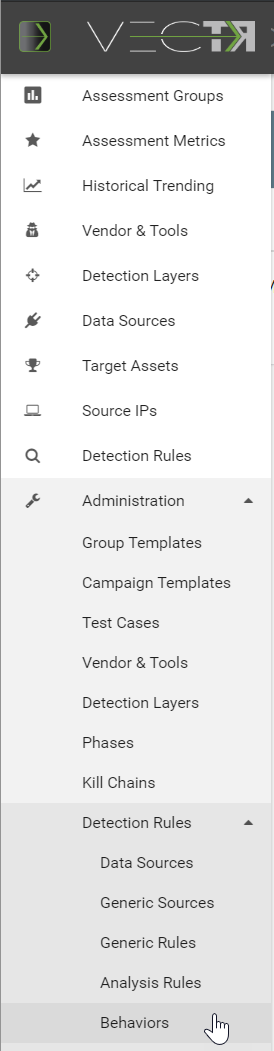
# Detection Behaviors

What is it?

VECTR provides the ability to define Detection Behaviors that map Test Cases to Generic Rules and Analysis Engine Rules.

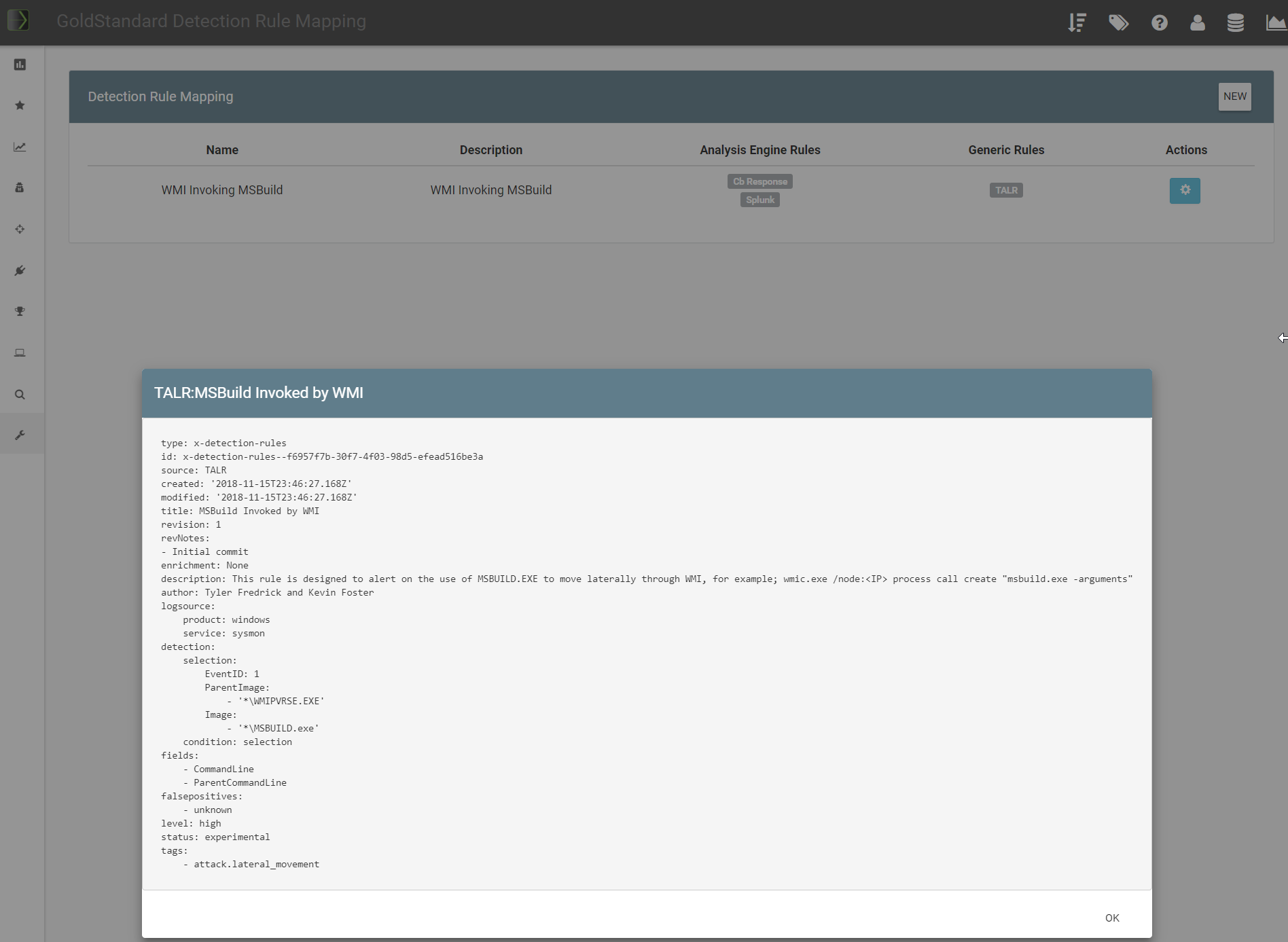
How does it work?

Navigate to the Administration -> Detection Rules -> Behaviors page:

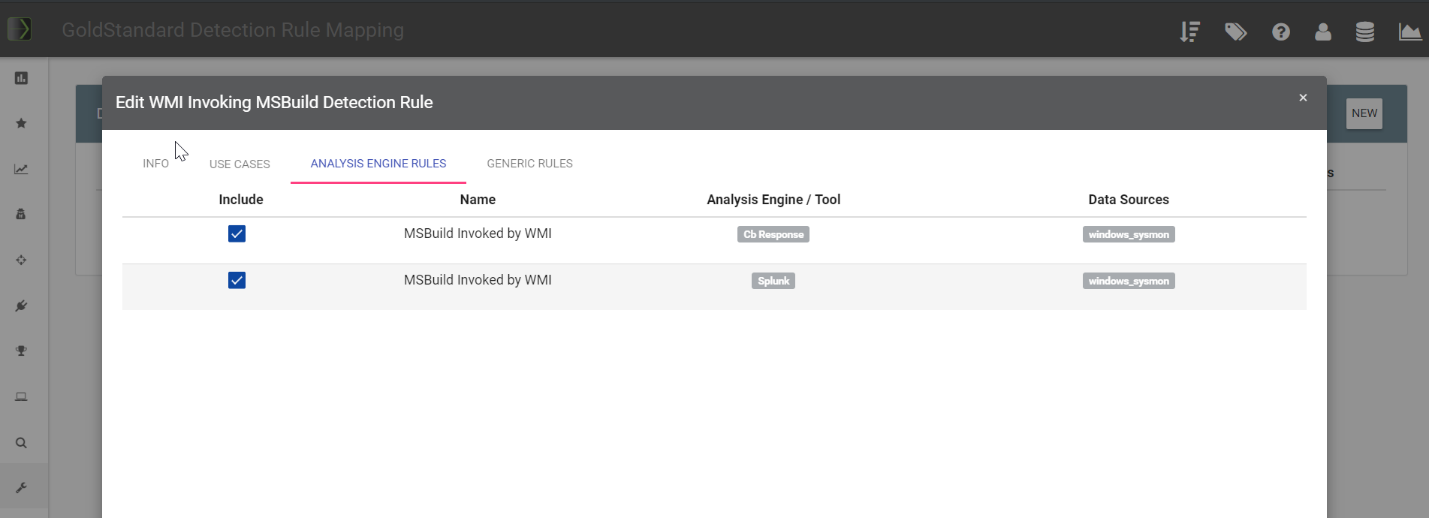


This will take you to the Detection Rule Mapping page.

You can also click the rules in the table to have them display in a popup:

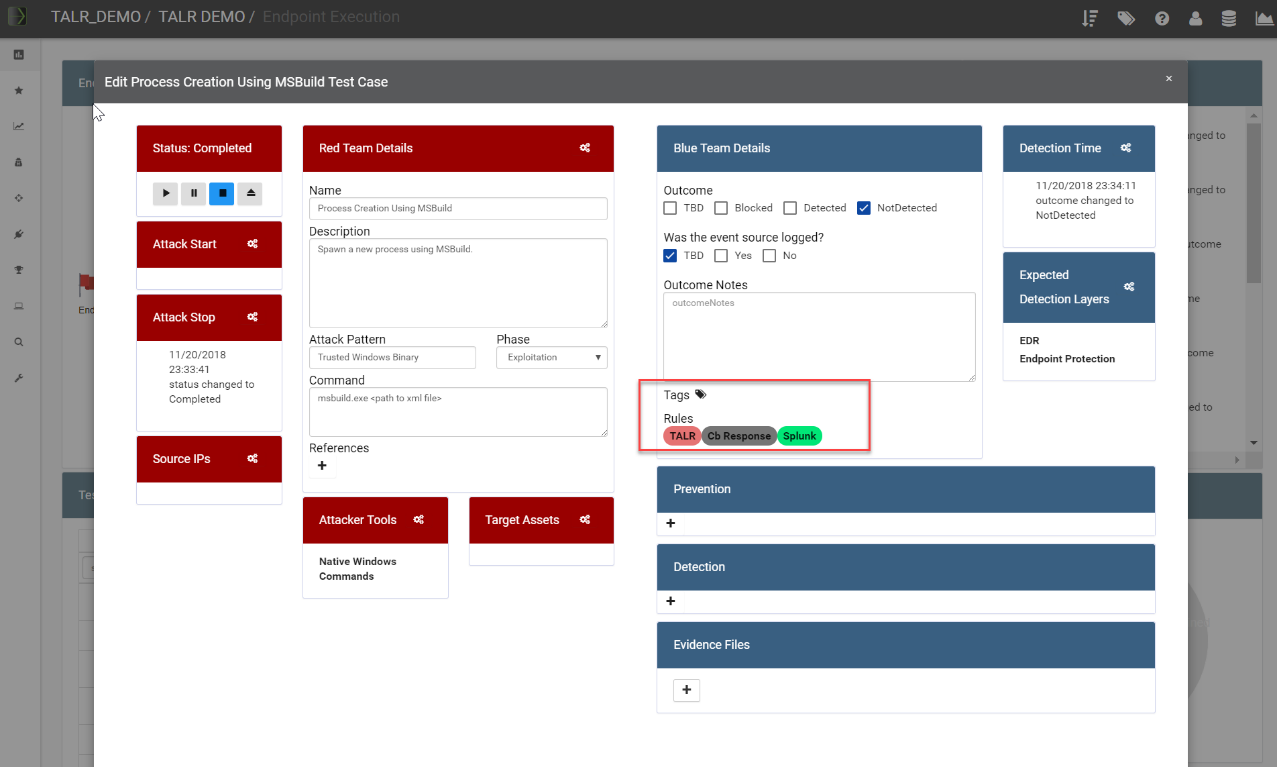


You can also edit one of your Behaviors by clicking the cog on the right. There are 4 tabs. Info, which is metadata, Use Cases which are the Test Case templates the rules will be applied to, Analysis Engine Rules / Generic Rules to associate to the Use Cases:

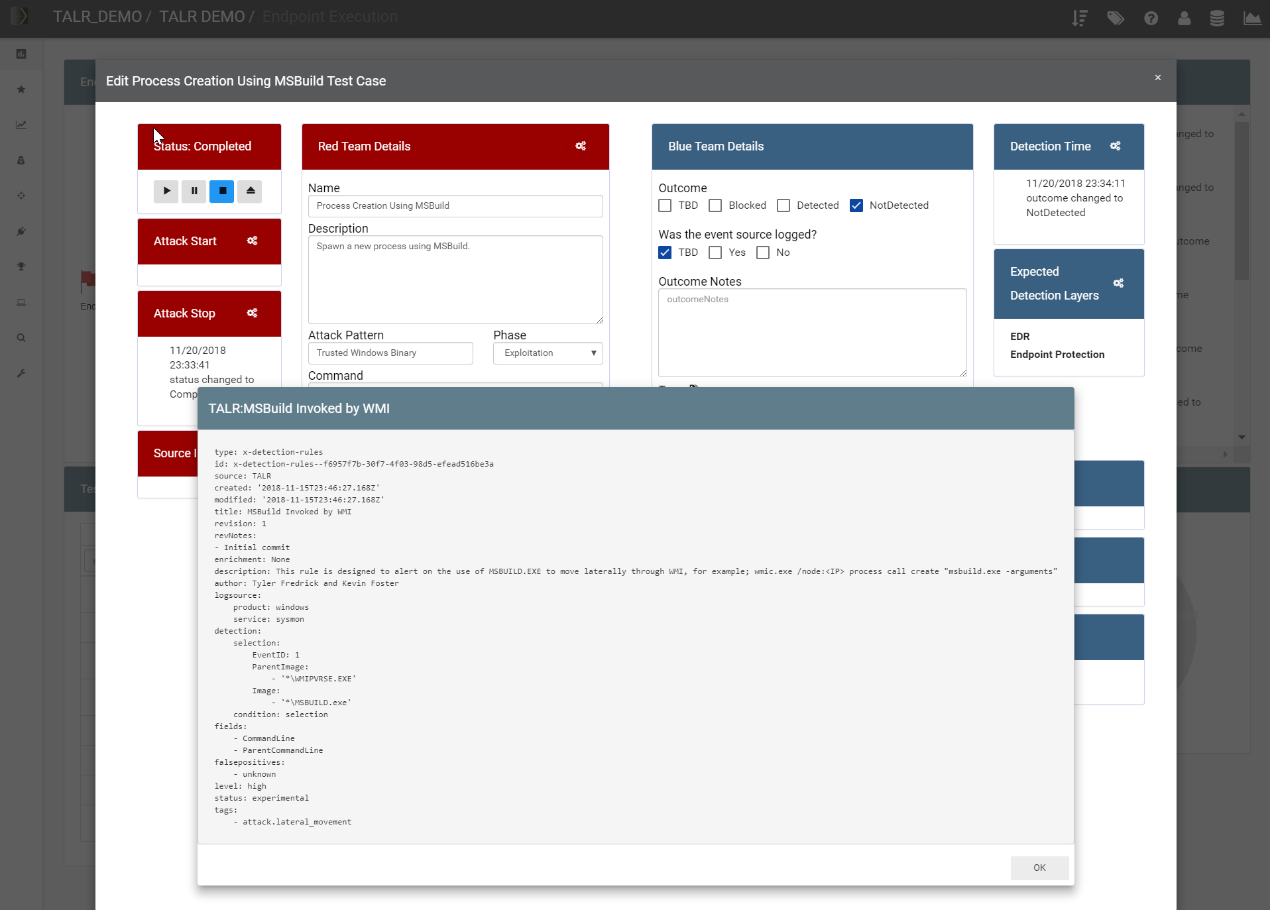


How can this feature help me?

Assuming a Behavior has a Test Case and Rule mapped, you will be able to view the rules applicable to detecting the command in the Test Case:



You can click on the rule for easy viewing:



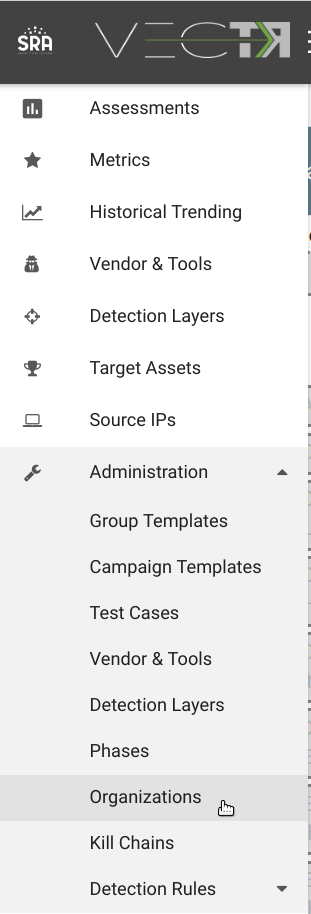
# Organizations

What is it?

VECTR provides the ability to define Organizations that will allow content creation to be credited and organized to an Organization.

How does it work?

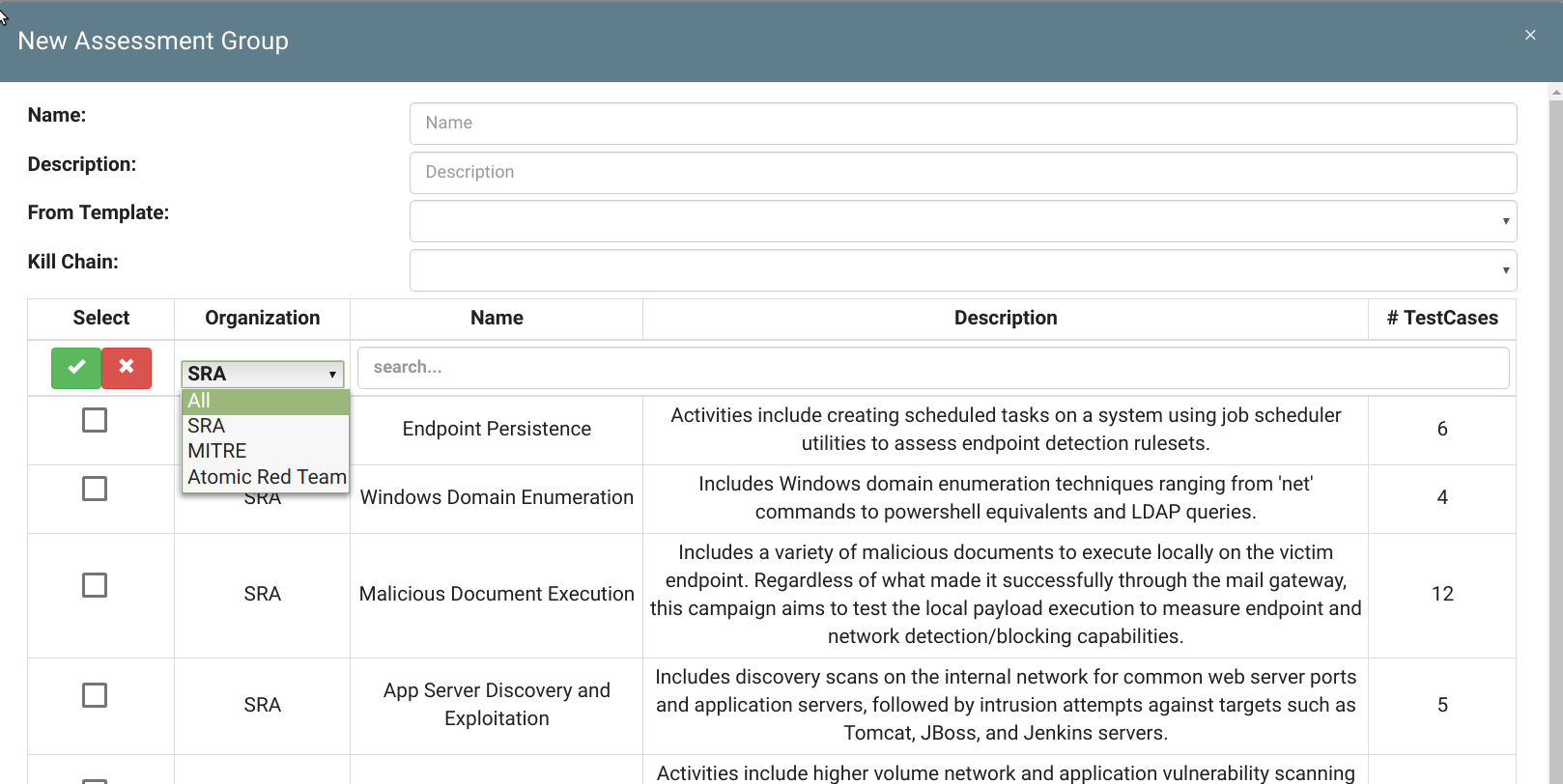
Navigate to the Administration -> Organizations page:



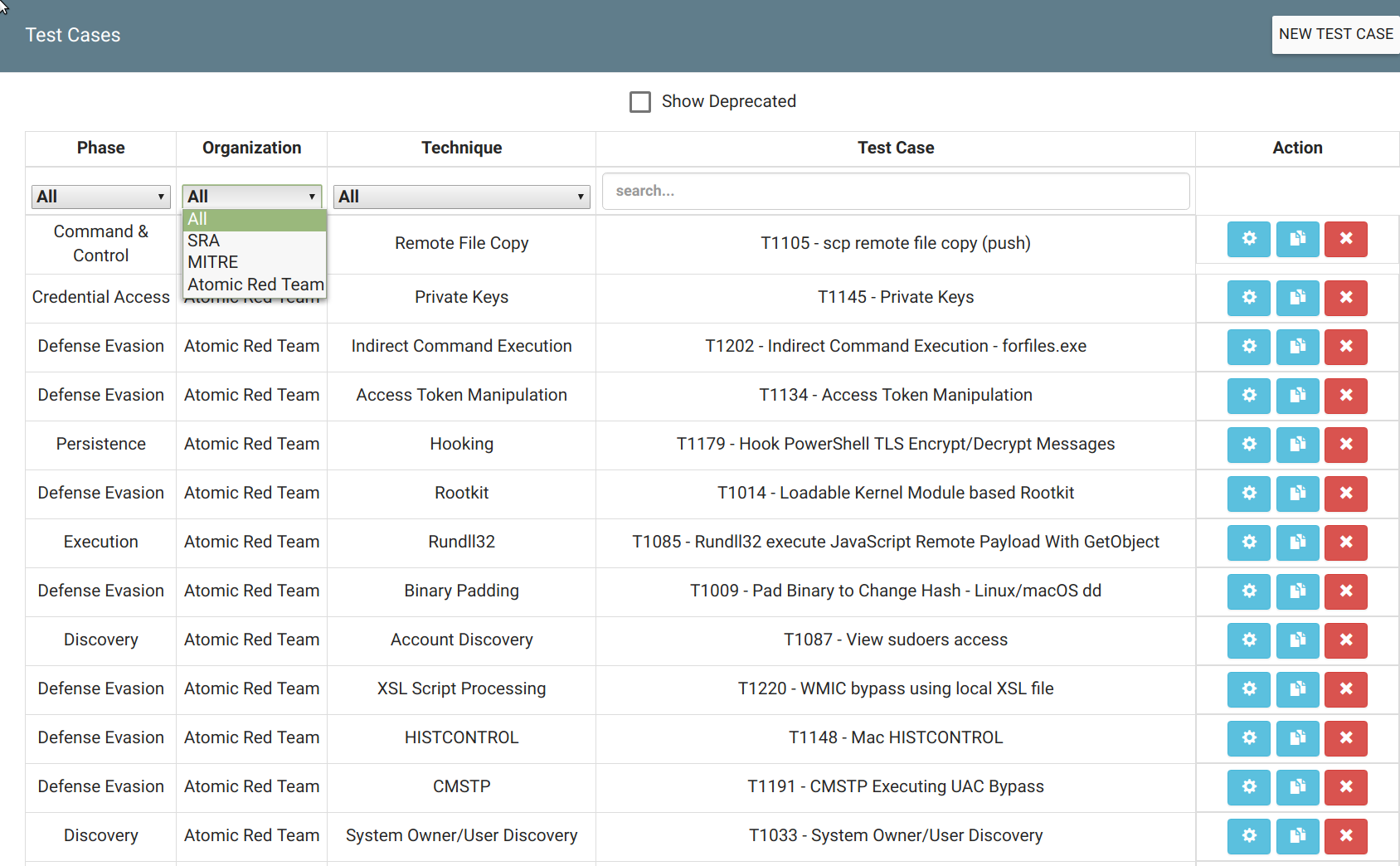
How can this feature help me?

There are various screens that will let you sort and filter data by Organization. Two examples are from the:

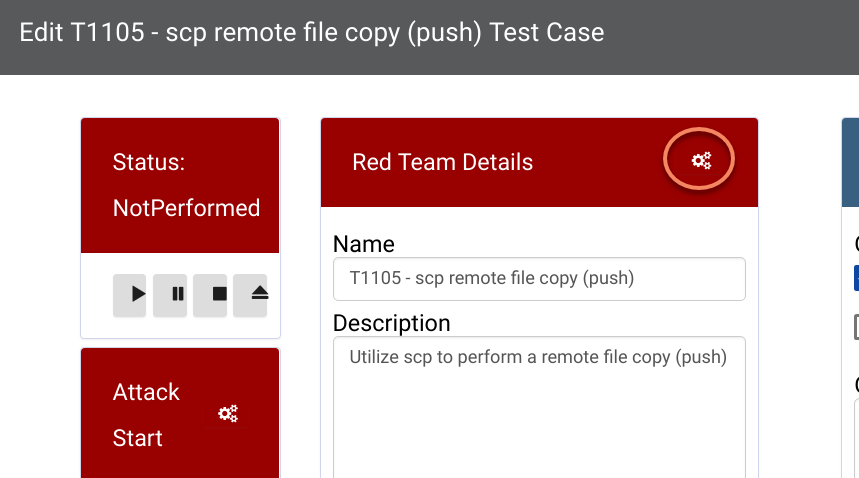
Assessment Group creation screen:



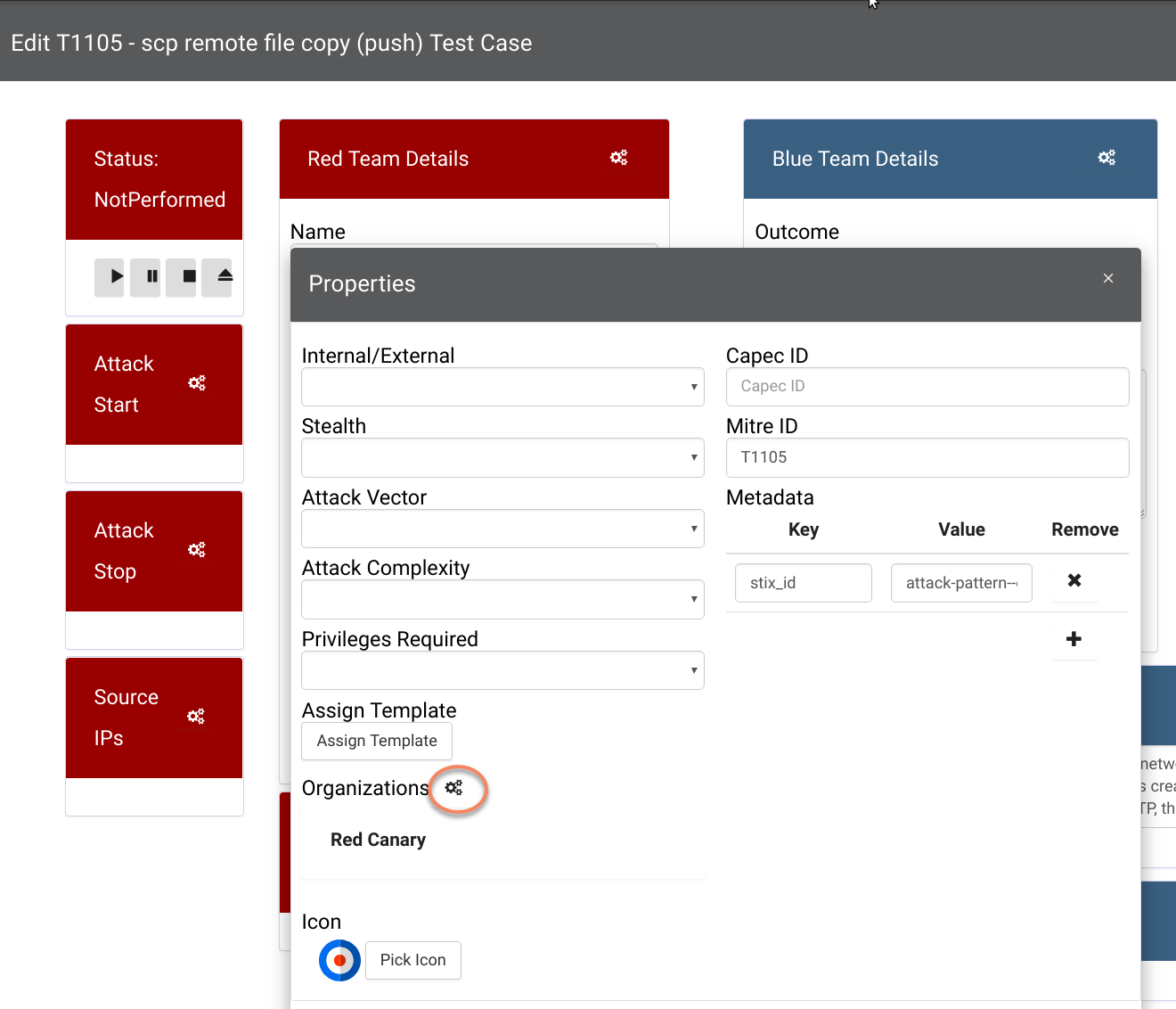
Test Case Administration screen:



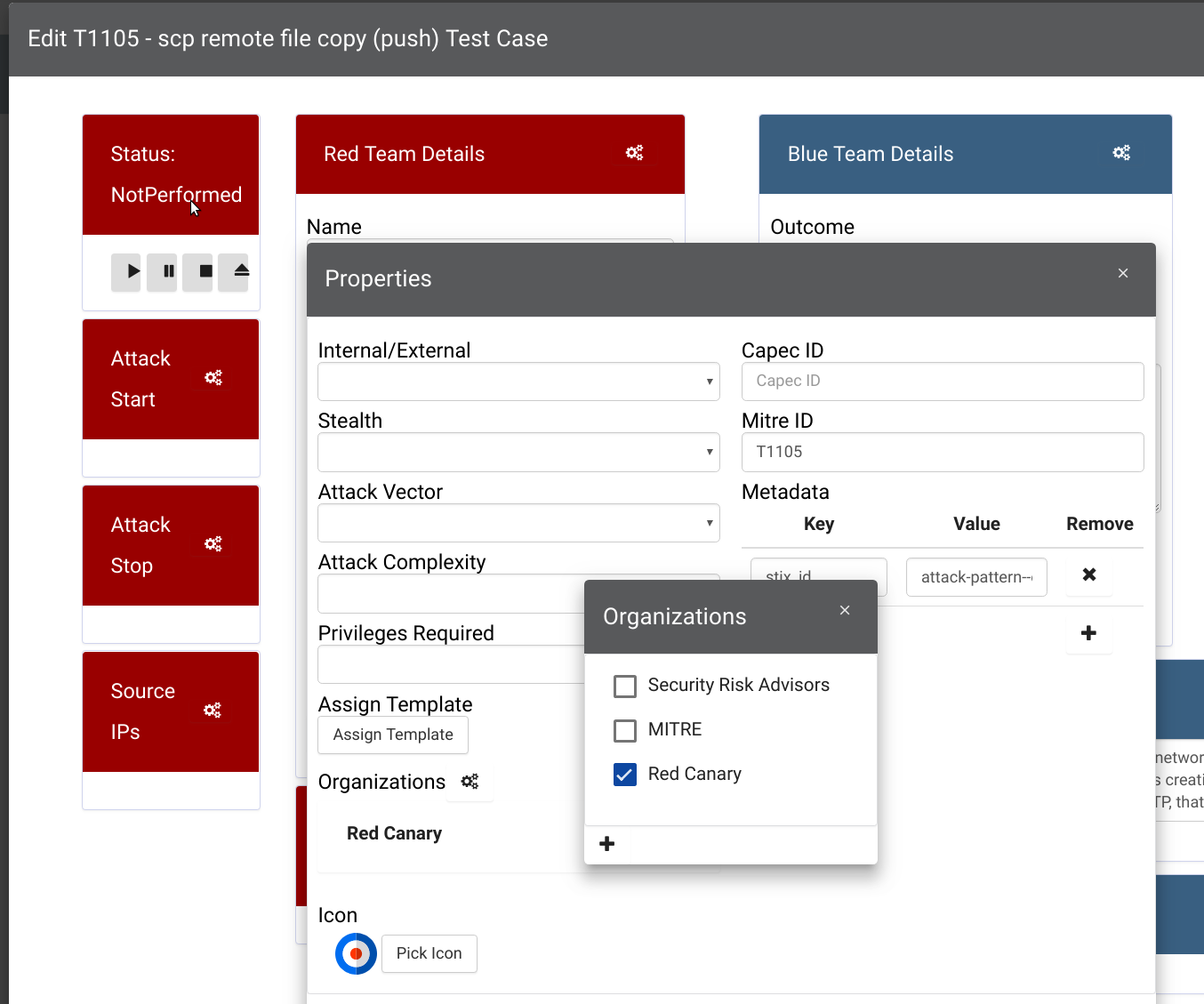
You can add your organization to previously created content. In the Test Case edit screen, click the gears in the Red Team Details:



In the properties popup, click the gears next to the Organizations:



Select the Organizations that you want to credit with the content:



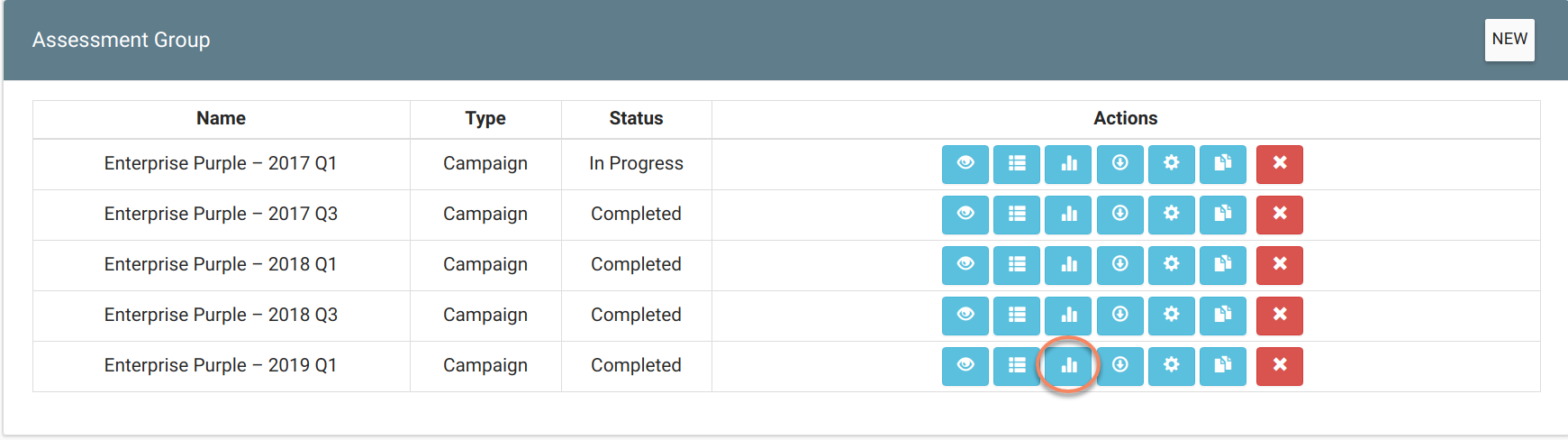
# MITRE ATT&CK Heatmap Coverage

What is it?

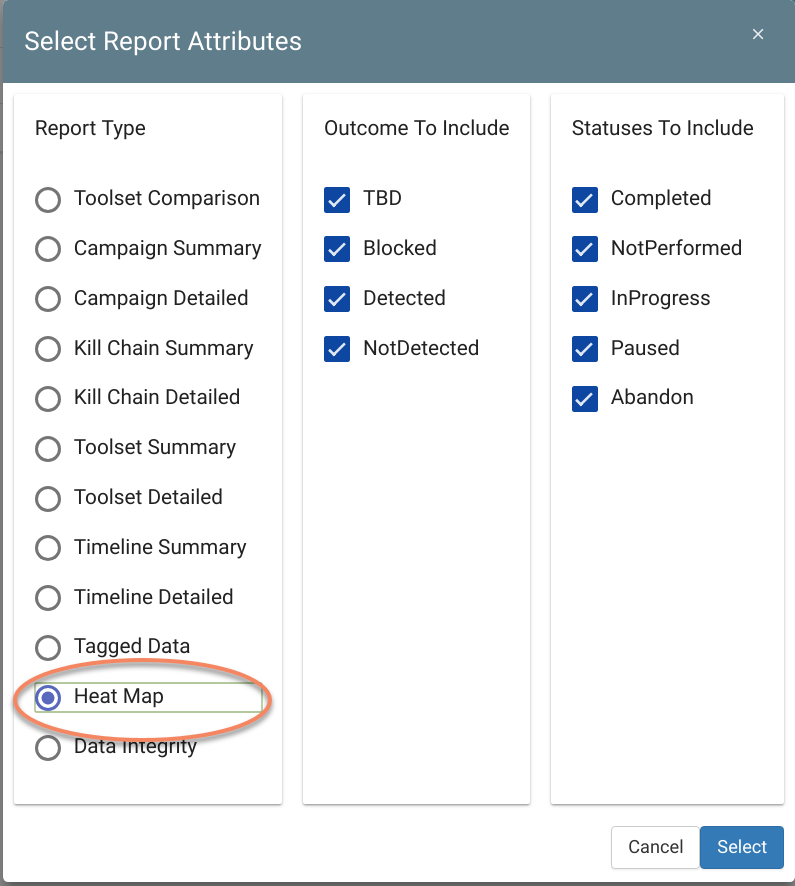
VECTR provides the ability to associate Test Cases with a Mitre Technique. You can view coverage of your Assessments and Assessment Groups on the MITRE ATT&CK Matrix.

How does it work?

From the Assessment Group selection screen, click the graph icon next to an Assessment Group:

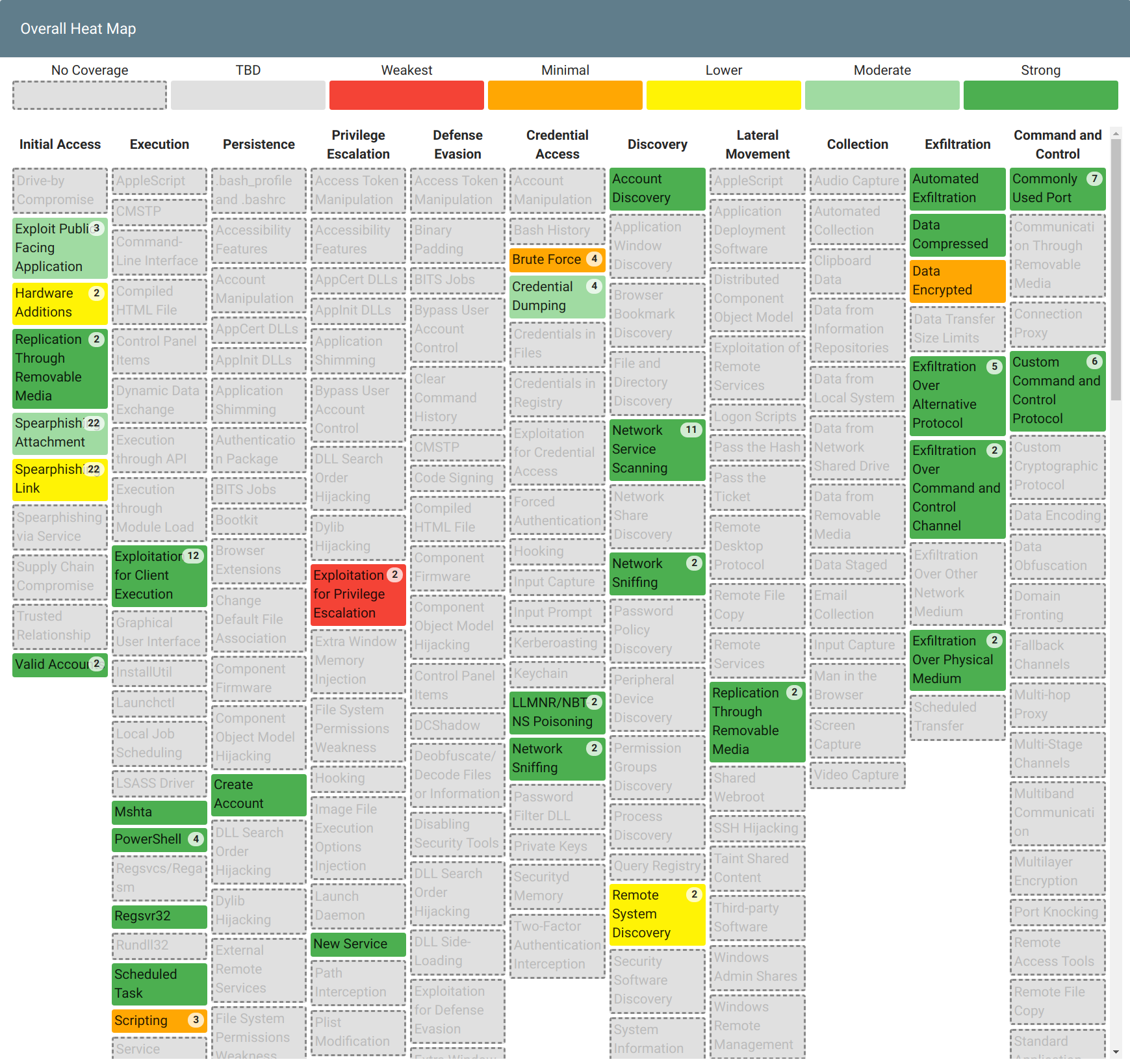


Select Heat Map from the Report selection screen:

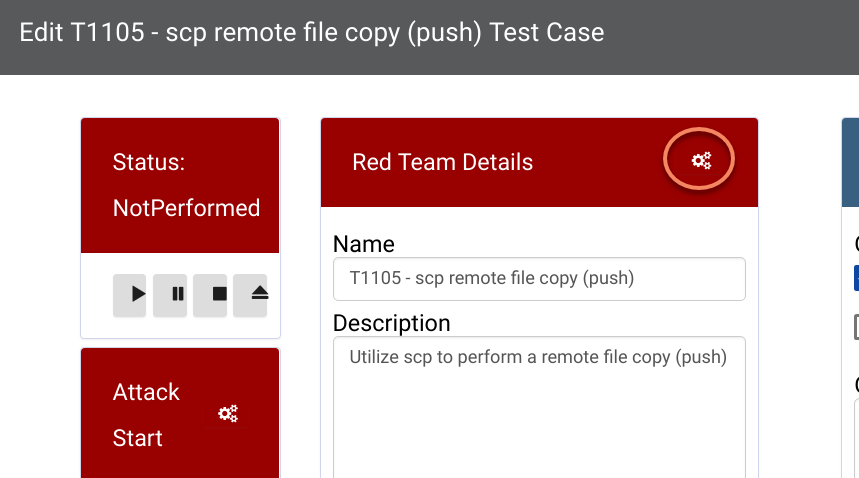


How can this feature help me?

This will allow you to see the Outcomes of all your Test Cases that have associated Technique IDs on the MITRE ATT&CK Matrix:



You can set a Technique ID to a Test Case by bringing up the Test Case edit screen, then clicking the gears in the Red Team Details:



Fill out the Mitre ID field in the Properties Popup:

