VECTR v5.2.0 Feature Breakdown

Table of Contents

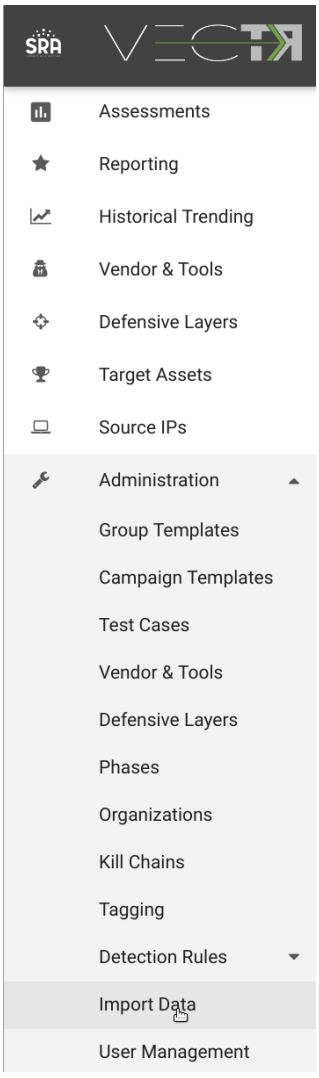
Data Import

What is it?

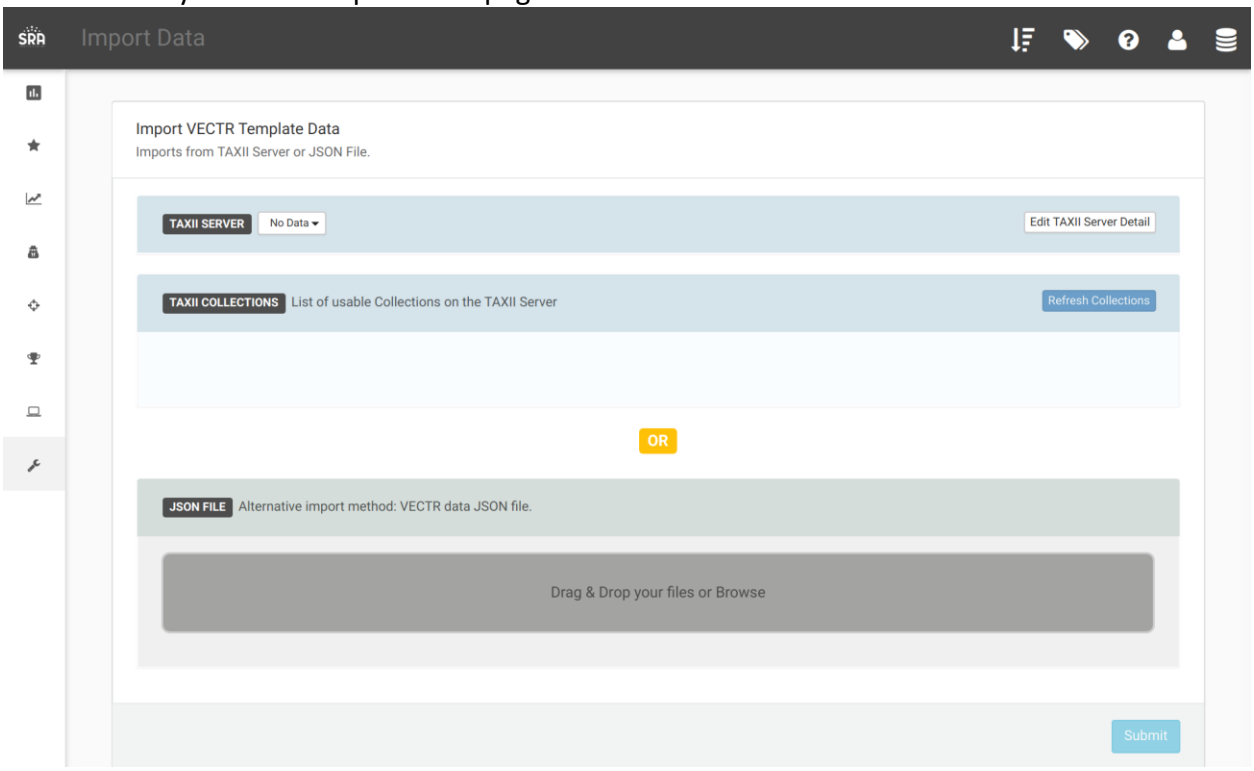
Allows generation of templated Assessments, Campaigns, and Test Cases using STIX 2.0 data format. Data can be imported via flat files or from a TAXII Server, but the TAXII Server is not currently used.

How does it work?

You can access the Data Import screen by selecting the Data Import tab on the Left Nav under Administration:

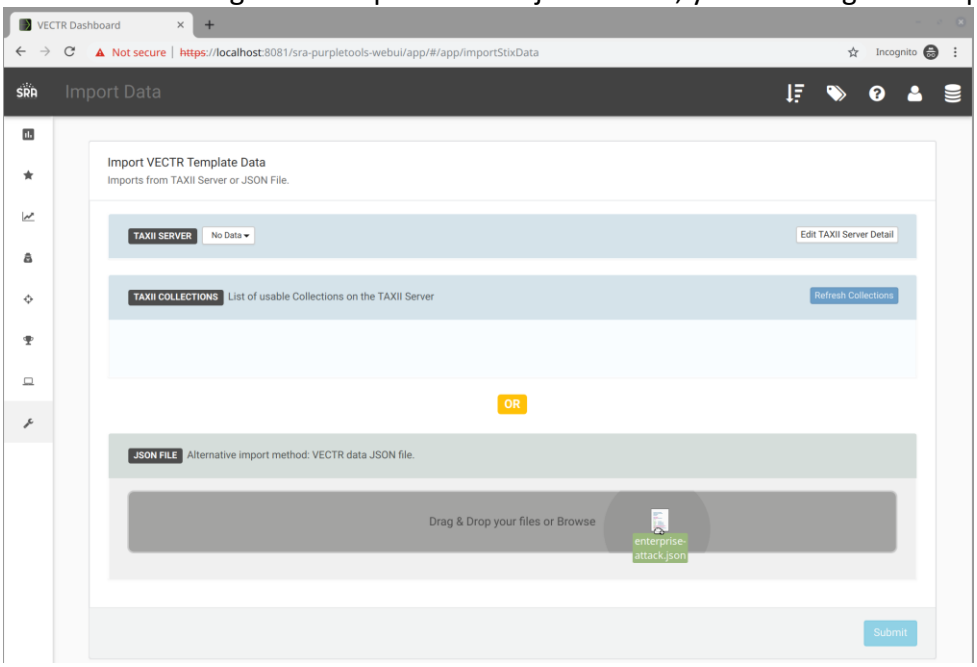


This will take you to the Import Data page:

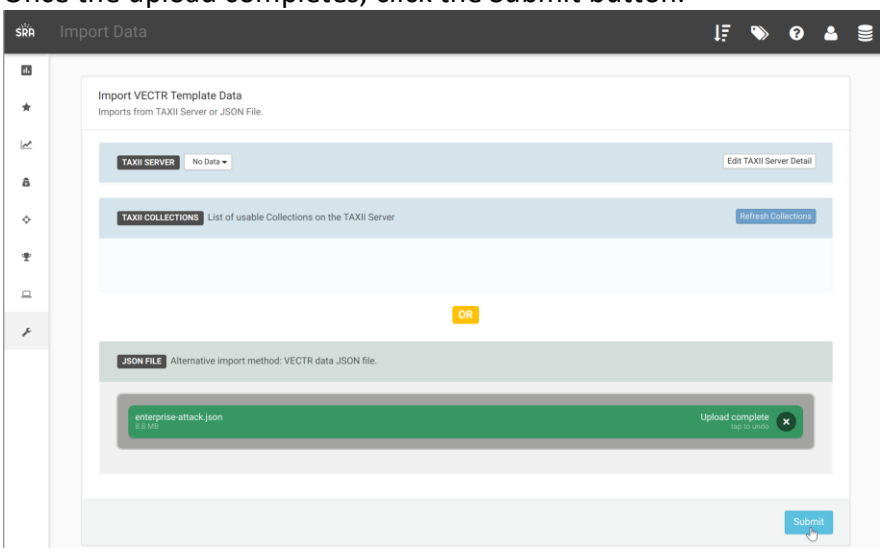


A good place to get started is using the enterprise-attack bundle from MITRE: https://github.com/mitre/cti/blob/master/enterprise-attack/enterprise-attack.json

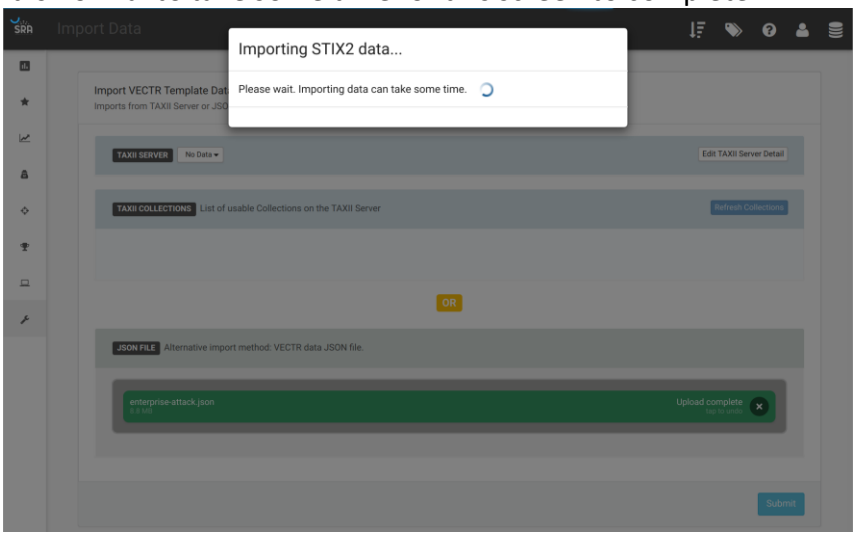
After downloading the enterprise-attack.json above, you can drag and drop to the gray area:



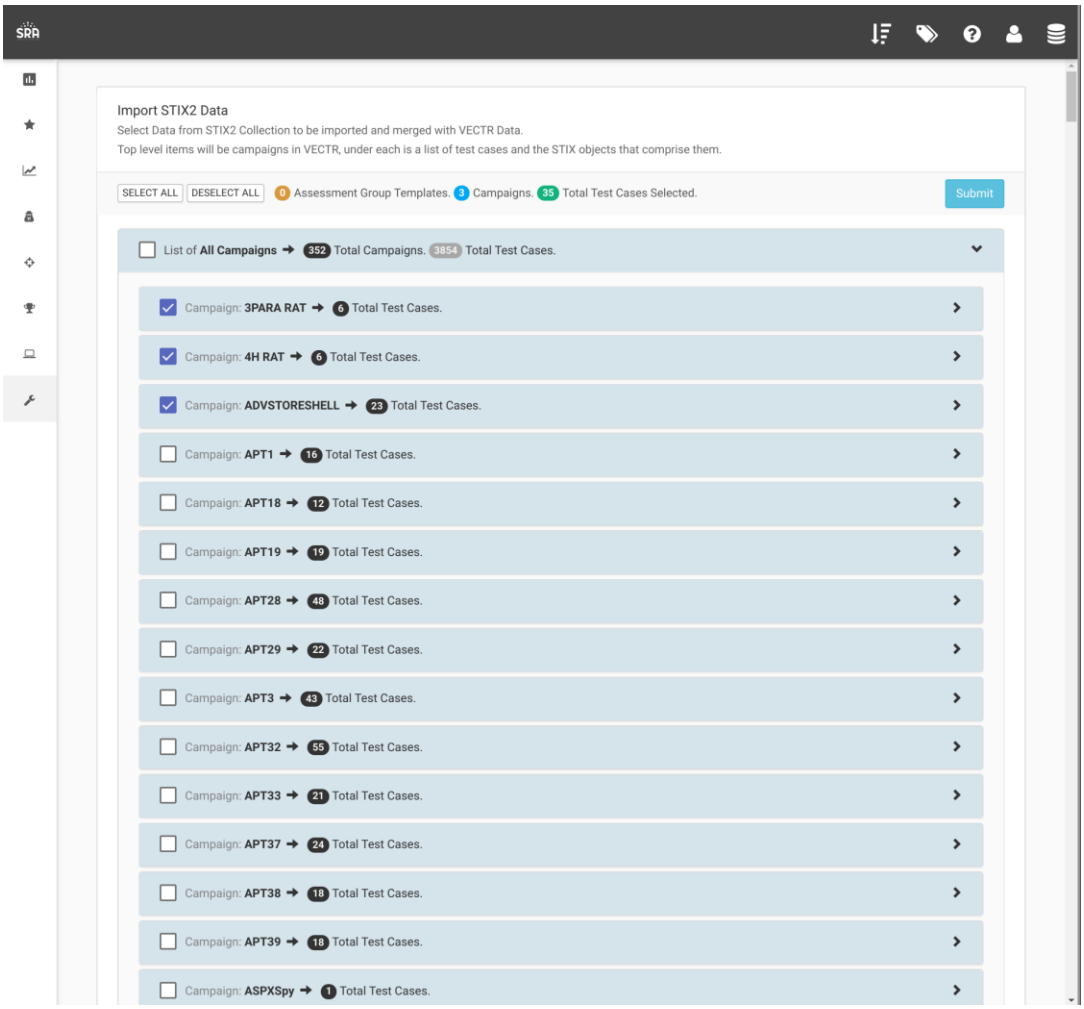
Once the upload completes, click the Submit button:



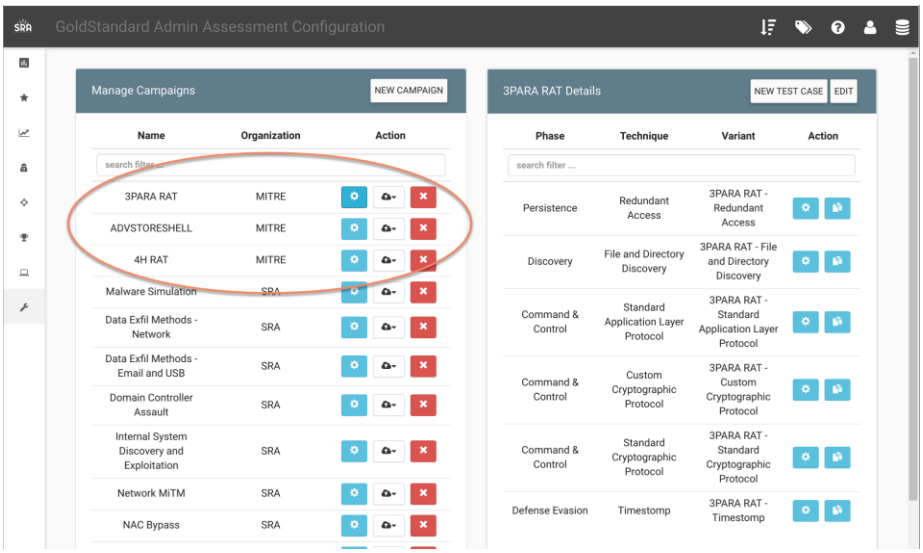
It is normal to take some time for this screen to complete:



The next screen will show you all the content that can be generated within VECTR from the STIX 2.0 bundle. It is recommended to select on the content you will use, as selecting everything could result in thousands of Test Cases.



You will then be taken to the Administration Campaign Configuration screen which shows the results of your import:



Create Assessment from MITRE ATT&CK™ Navigator Layer

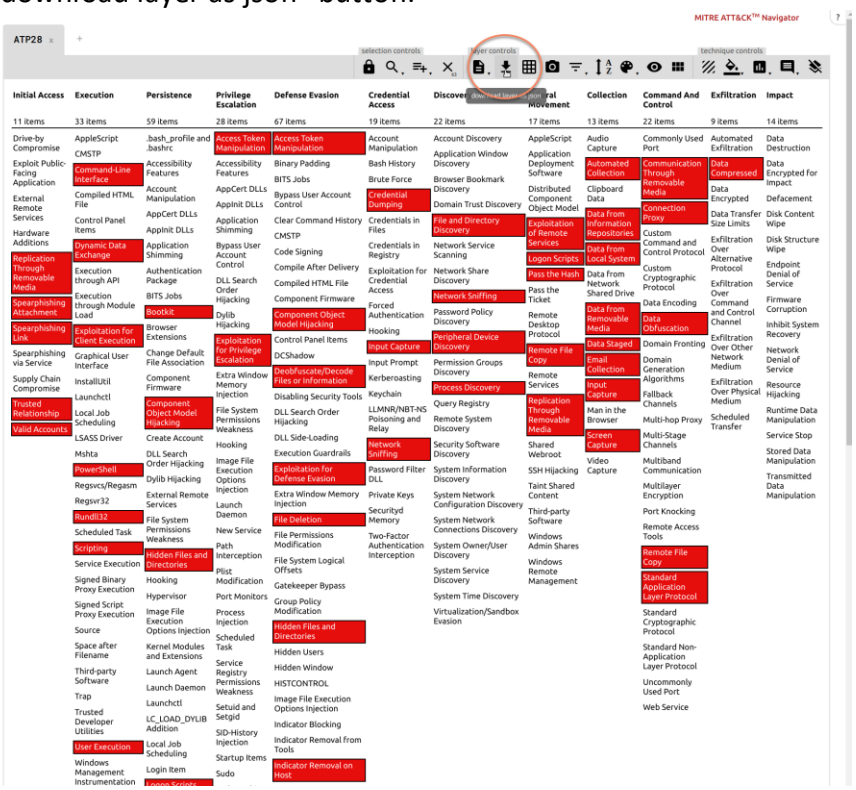
What is it?

Allows a user to create an Assessment and Campaigns to run through all Test Cases that VECTR has a Template defined matching the Technique ID from a Layer generated from MITRE ATT&CK™ Navigator.

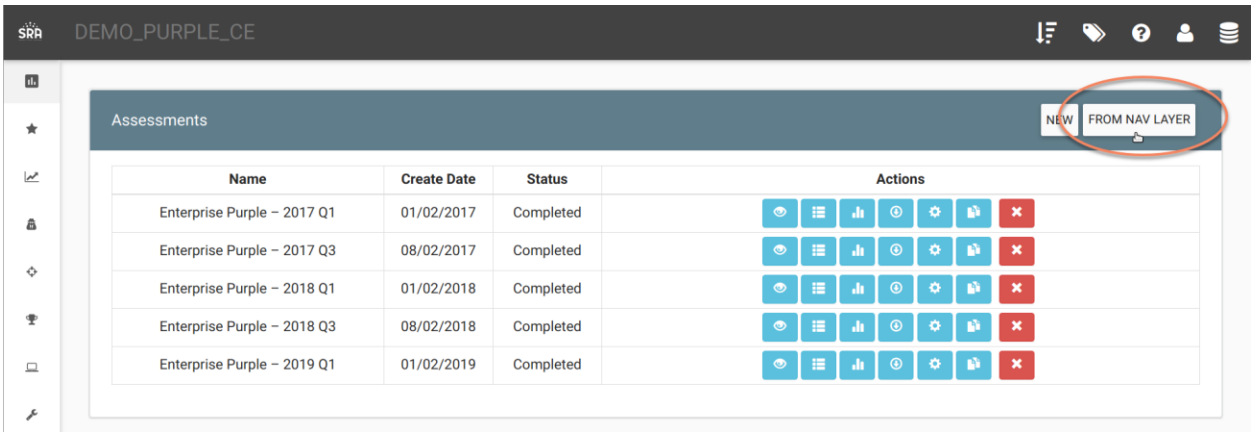
How does it work?

Define a Layer using the MITRE ATT&CK™ Navigator: (https://mitre-attack.github.io/attack-navigator/enterprise)

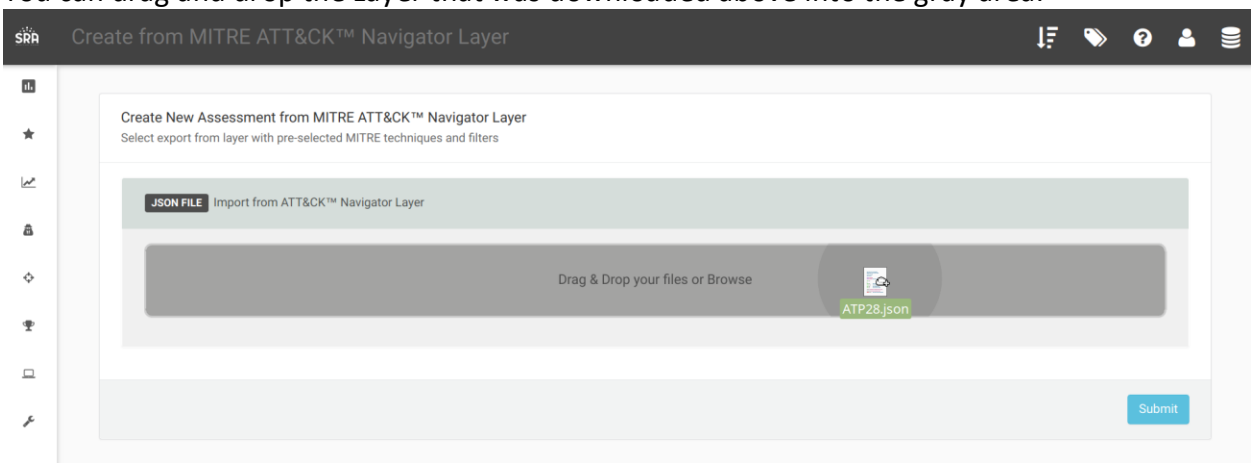
For the sake of this document, we selected the APT28 from the multi-select widget, then colored the selected techniques red. This is just for demonstration. All “Selected” cells will be applied to the import. Once you select all the techniques you’re interested in, click the “download layer as json” button:



From the Assessments dashboard, click the “From Nav Layer” in the top right:

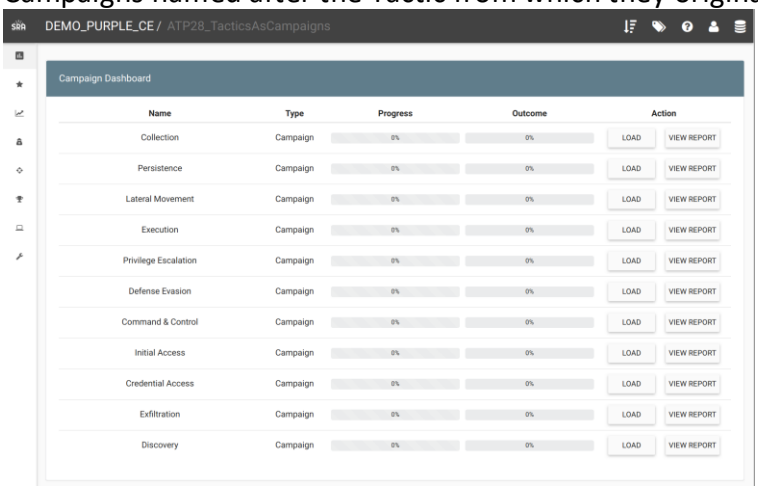


This will take you to the Create New Assessment from MITRE ATT&CK™ Navigator Layer screen. You can drag and drop the Layer that was downloaded above into the gray area:

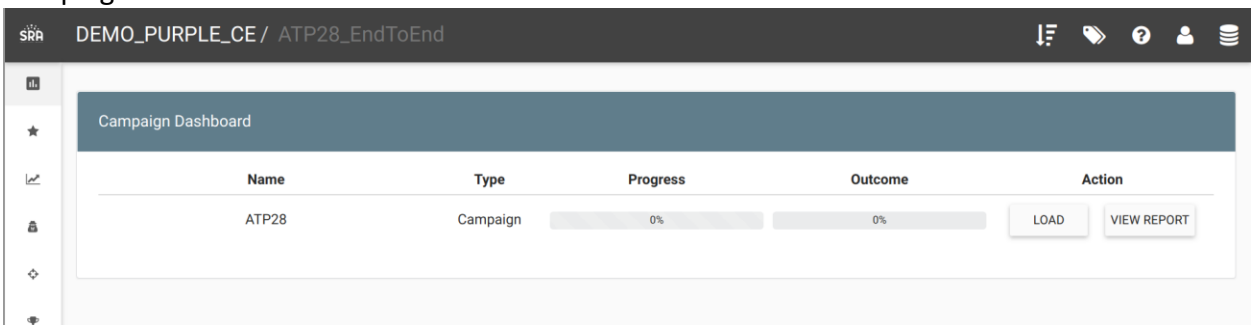


After you click submit, a popup will ask you if you want to create “Tactics As Campaigns” or “End to End”.

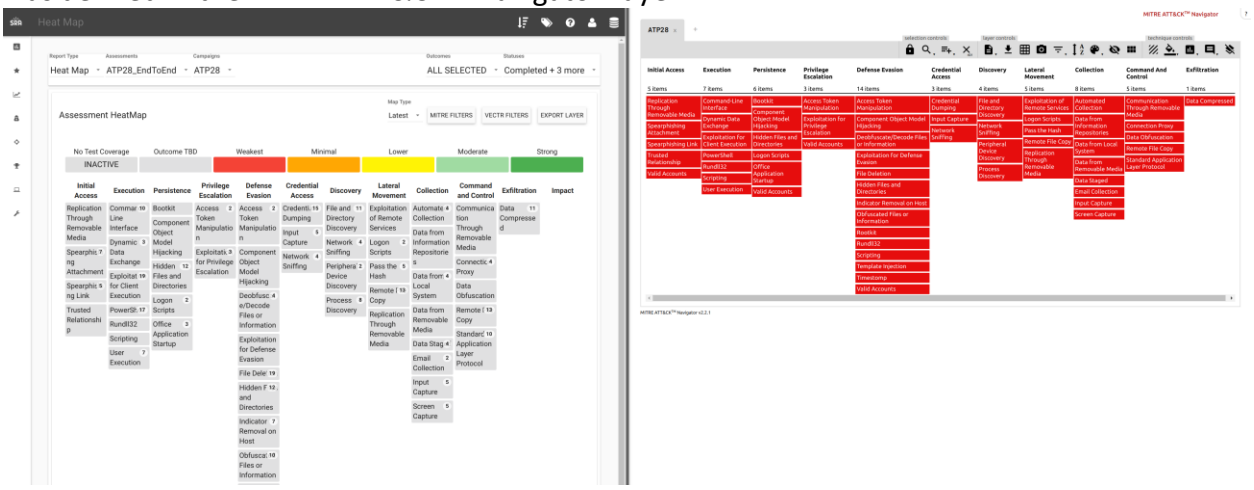
Tactics As Campaigns will separate all the Test Cases that match all selected Techniques into Campaigns named after the Tactic from which they originated:



End To End will group all the Test Cases that match all selected Techniques into a single Campaign:



This is an example of the coverage generated from the Assessment in VECTR vs the Layer that was defined in the MITRE ATT&CK™ Navigator Layer:



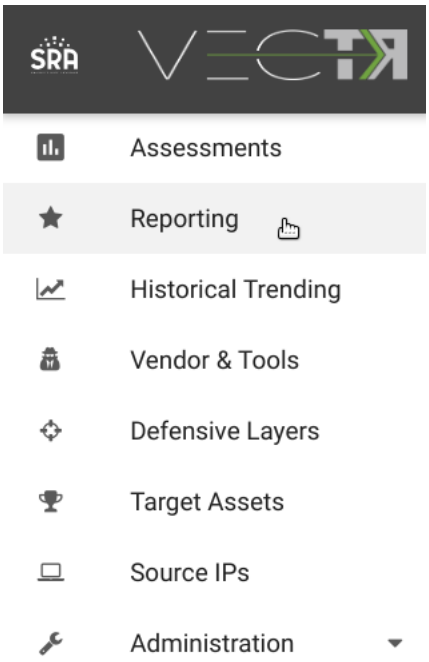
Heat Map: MITRE Filters

What is it?

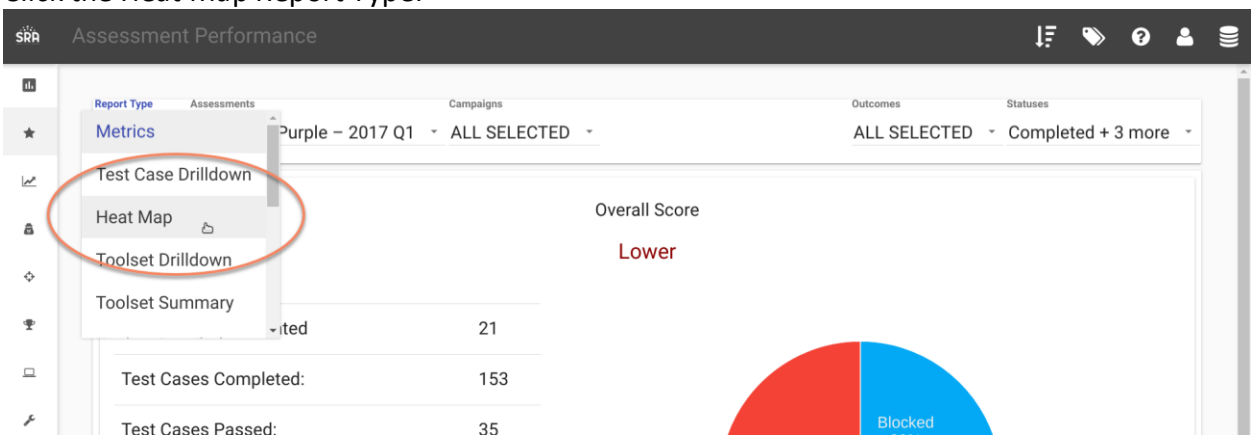
Allows user to compare coverage relative to a specific Threat Group or Malware.

How does it work?

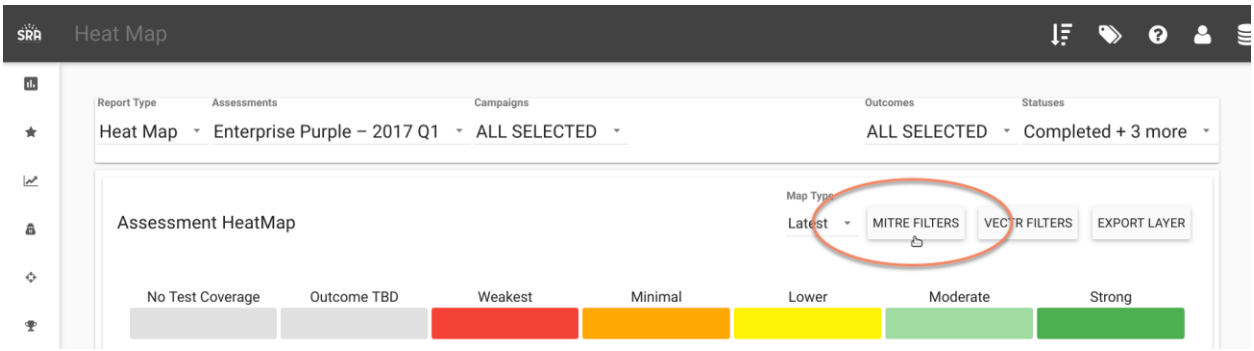
Navigate to the Reporting section:



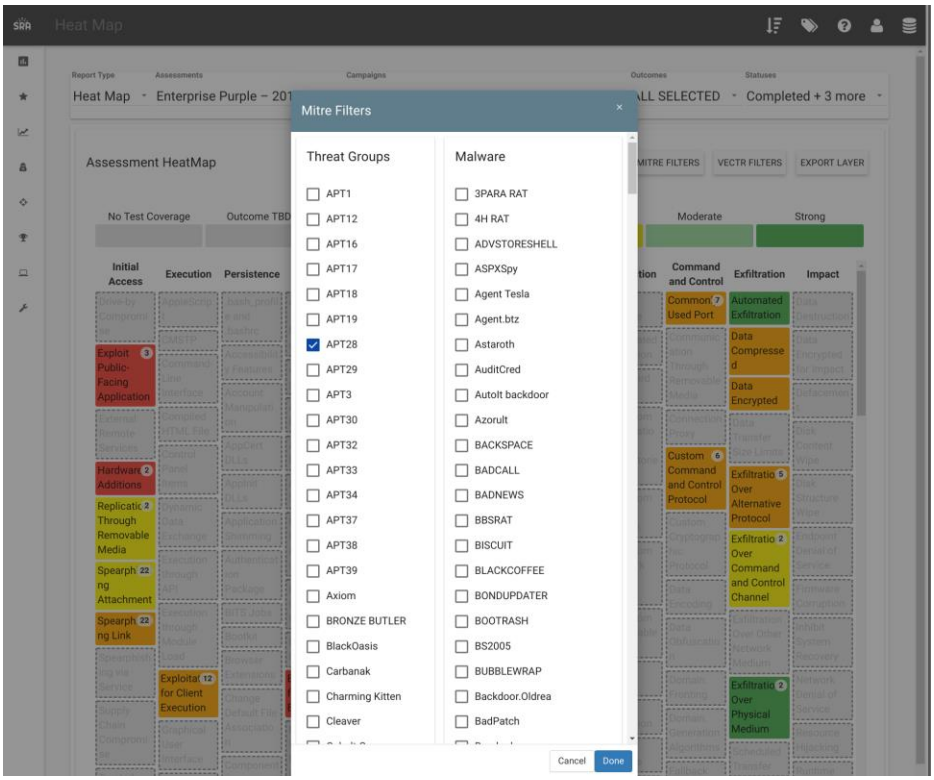
Click the Heat Map Report Type:



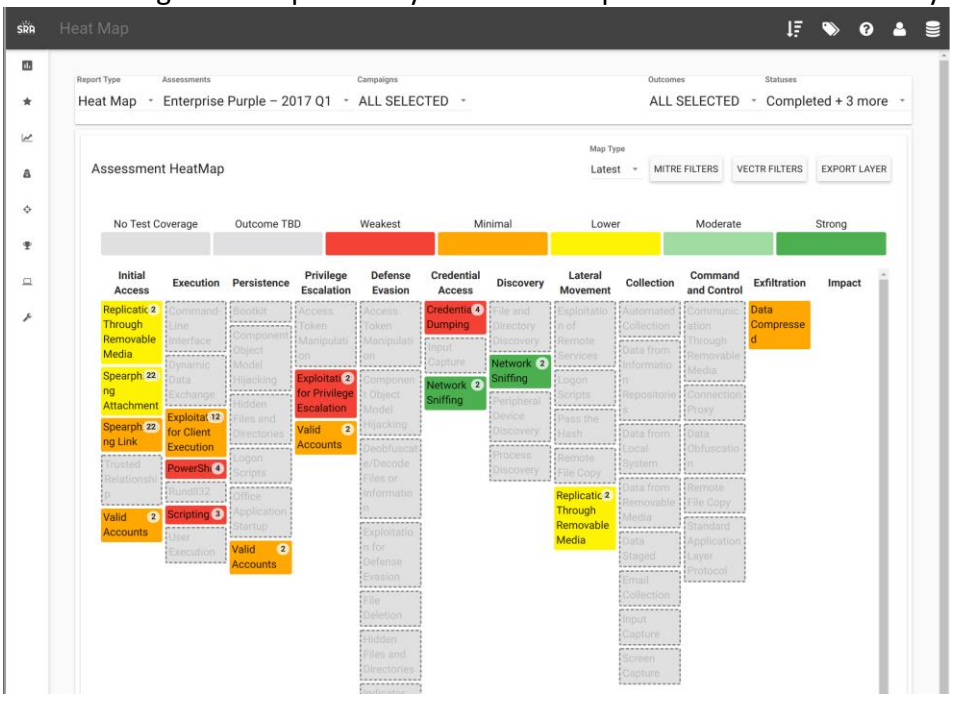
Click the MITRE FILTERS Button:



You can select one or many Threat Groups or Malwares to compare against:



The resulting Heat Map will only show Techniques related to whatever you had selected:



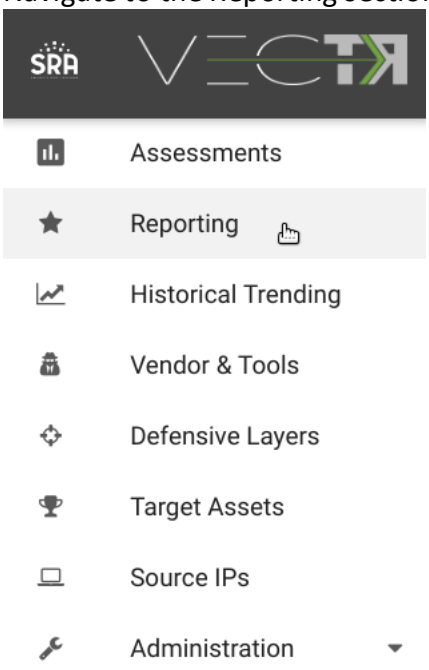
Heat Map: Export Layer

What is it?

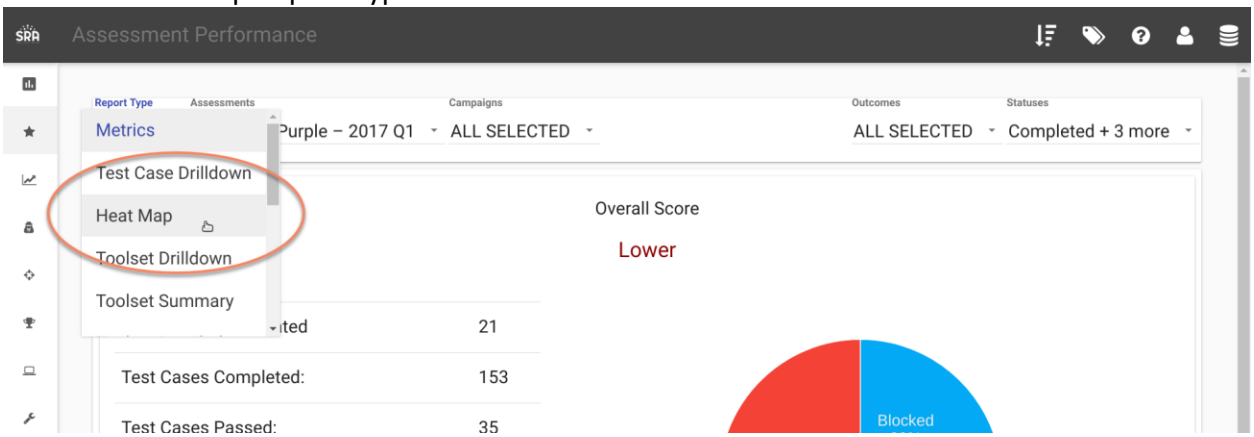
Allows exporting the Heat Map view into a Layer that can be imported into the MITRE ATT&CK™ Navigator as a Layer.

How does it work?

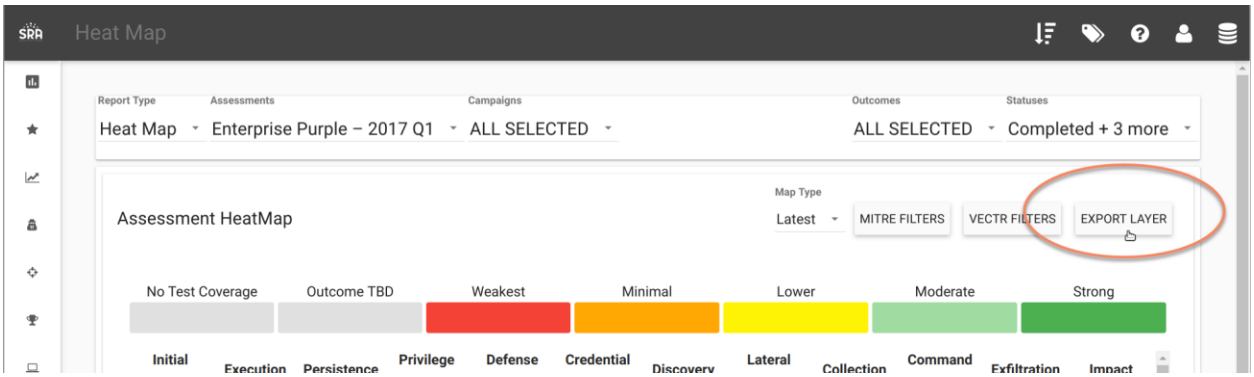
Navigate to the Reporting section:



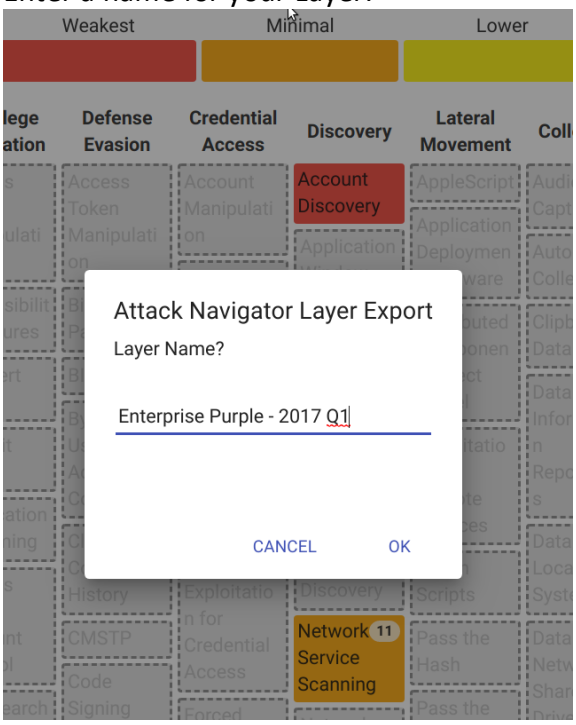
Click the Heat Map Report Type:



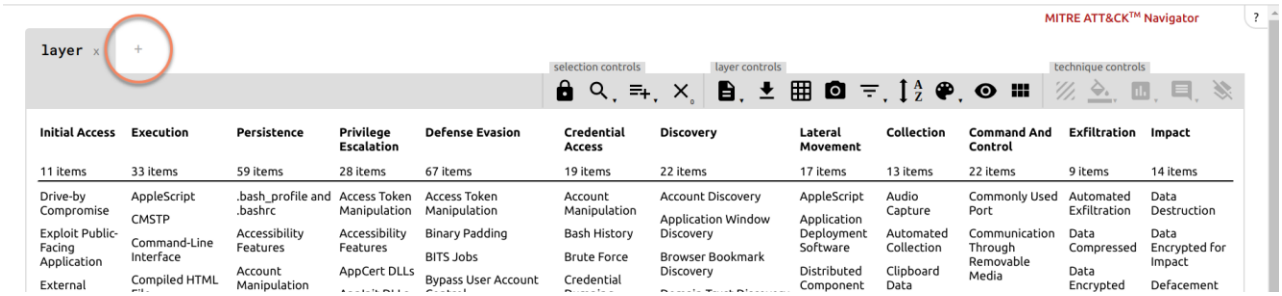
Click Export Layer:



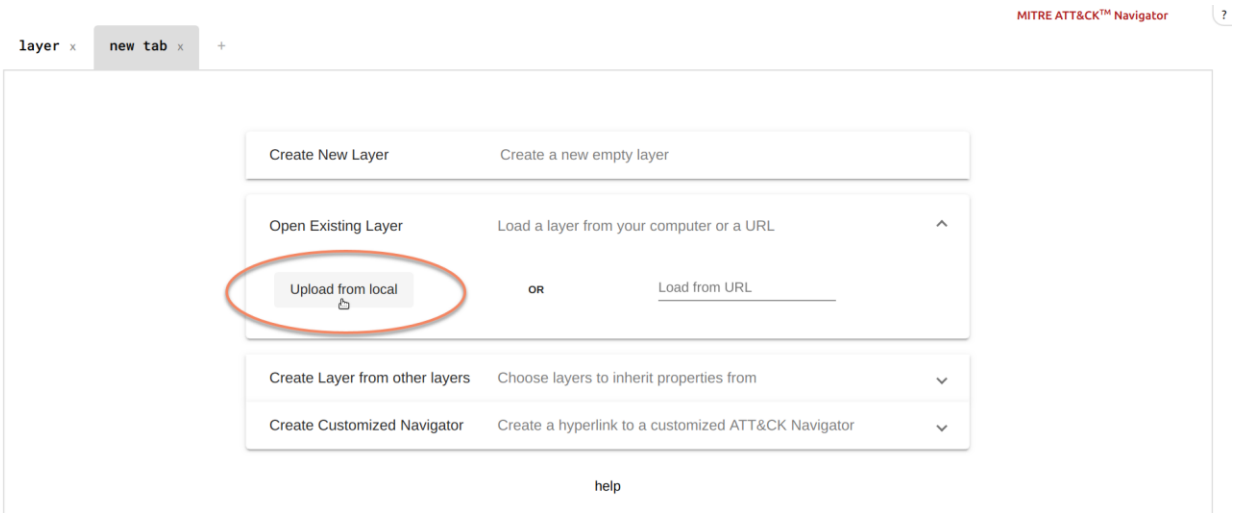
Enter a name for your Layer:



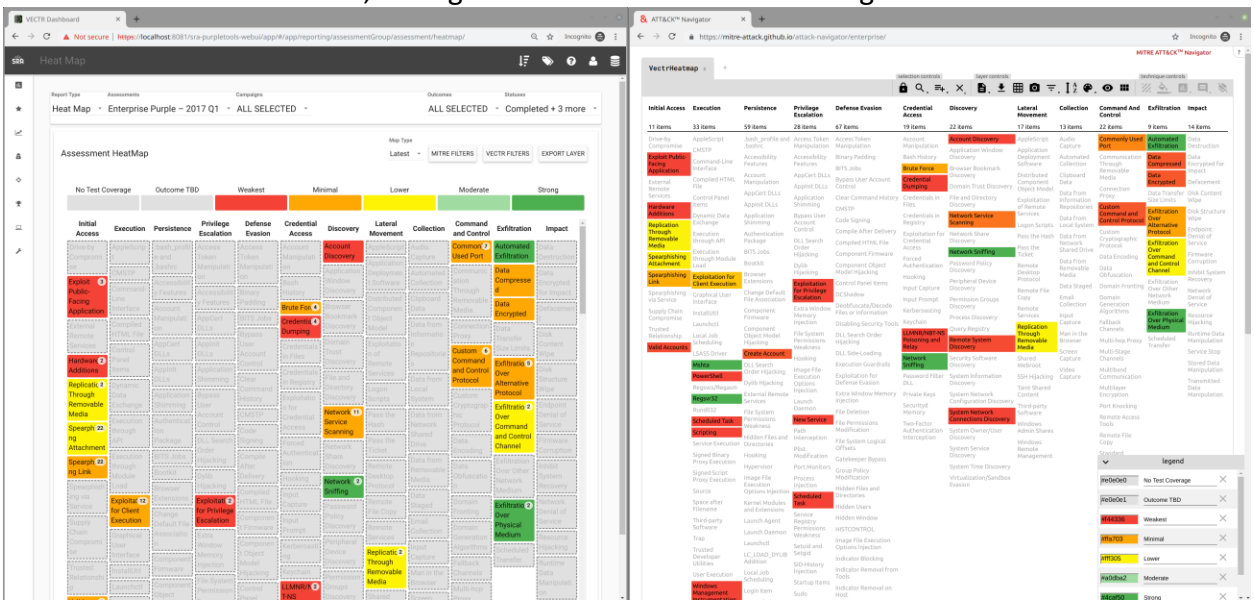
From the MITRE ATT&CK™ Navigator, click the “+” button in the tab section:



Click Open Existing Layer / Upload from local:



The left is the VECTR screen, the right is the MITRE ATT&CK™ Navigator:



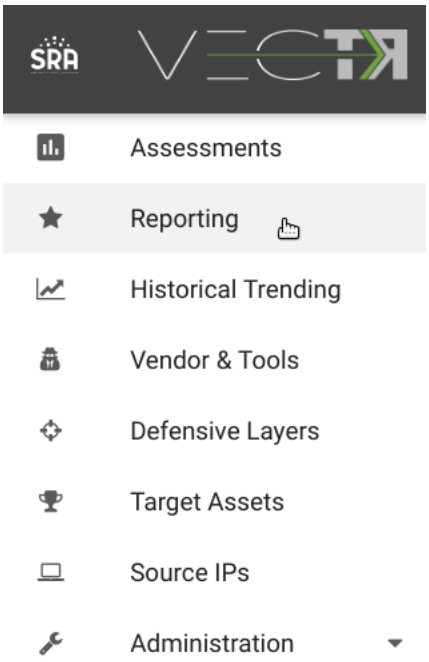
Heat Map: Editing Test Cases

What is it?

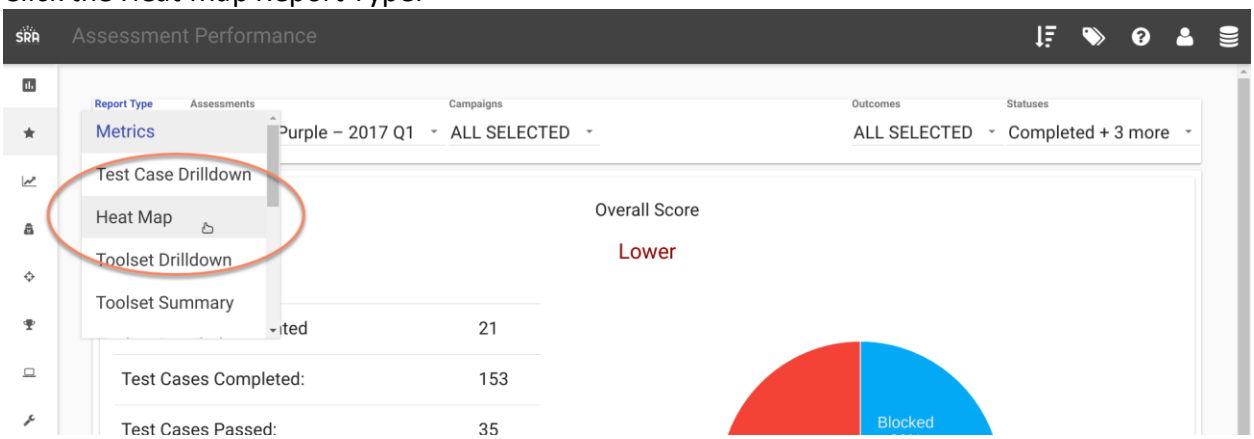
Allows editing of Test Cases from the Heat Map Report Type view.

How does it work?

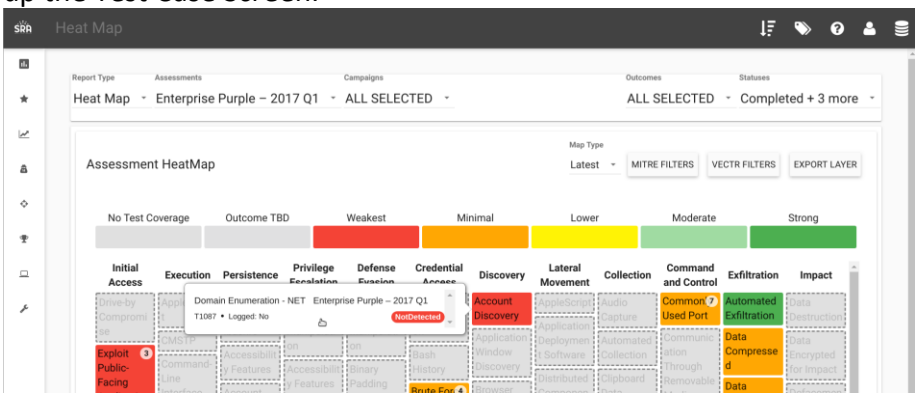
Navigate to the Reporting section:



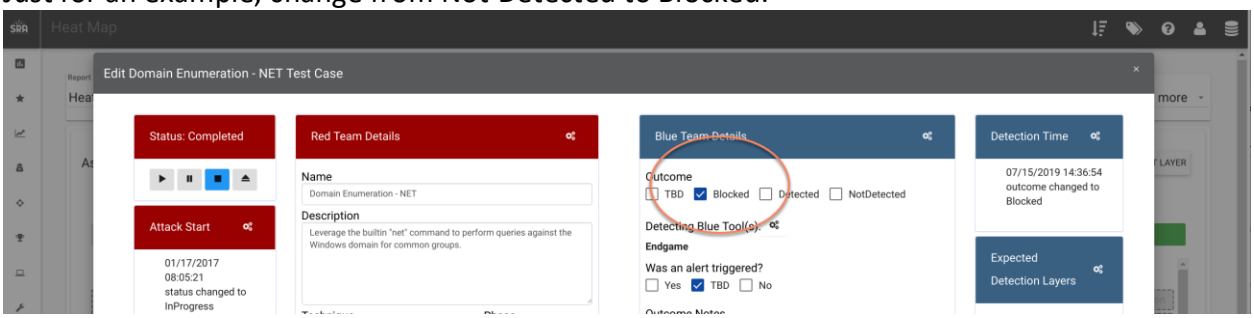
Click the Heat Map Report Type:



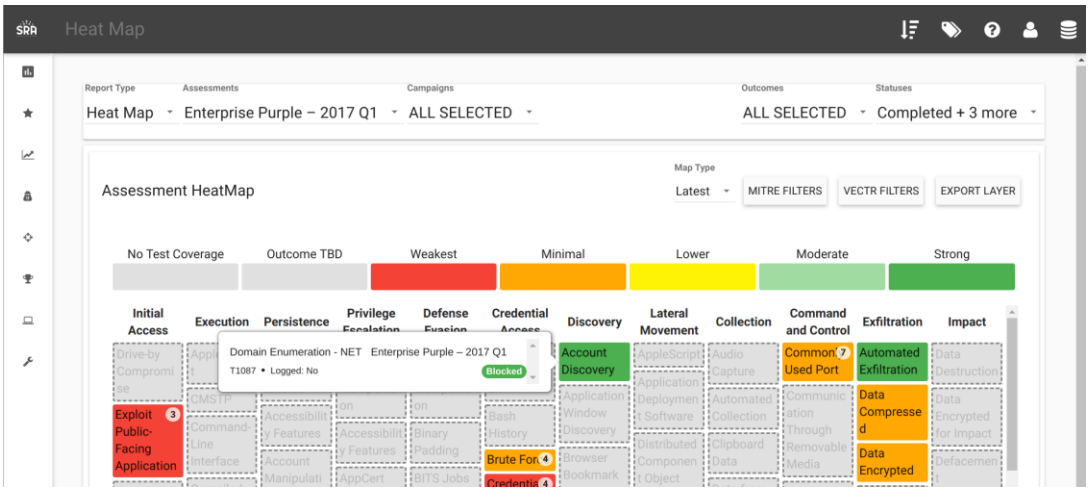
Clicking a cell will bring up the cell summary tooltip. Clicking on a row in the tooltip will bring up the Test Case Screen:



Just for an example, change from Not Detected to Blocked:



The cell is now Green:



User Management: Roles

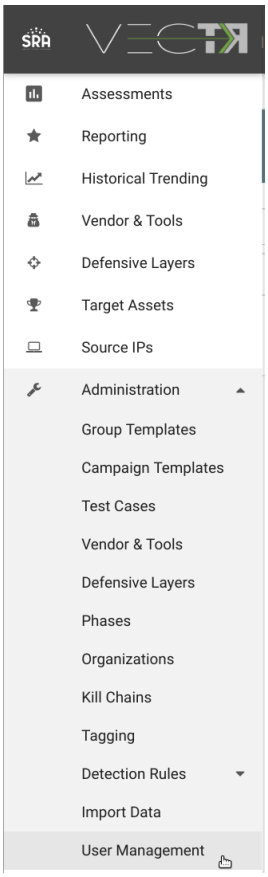
What is it?

Allows for setting Read/Write/Admin permissions to a User.

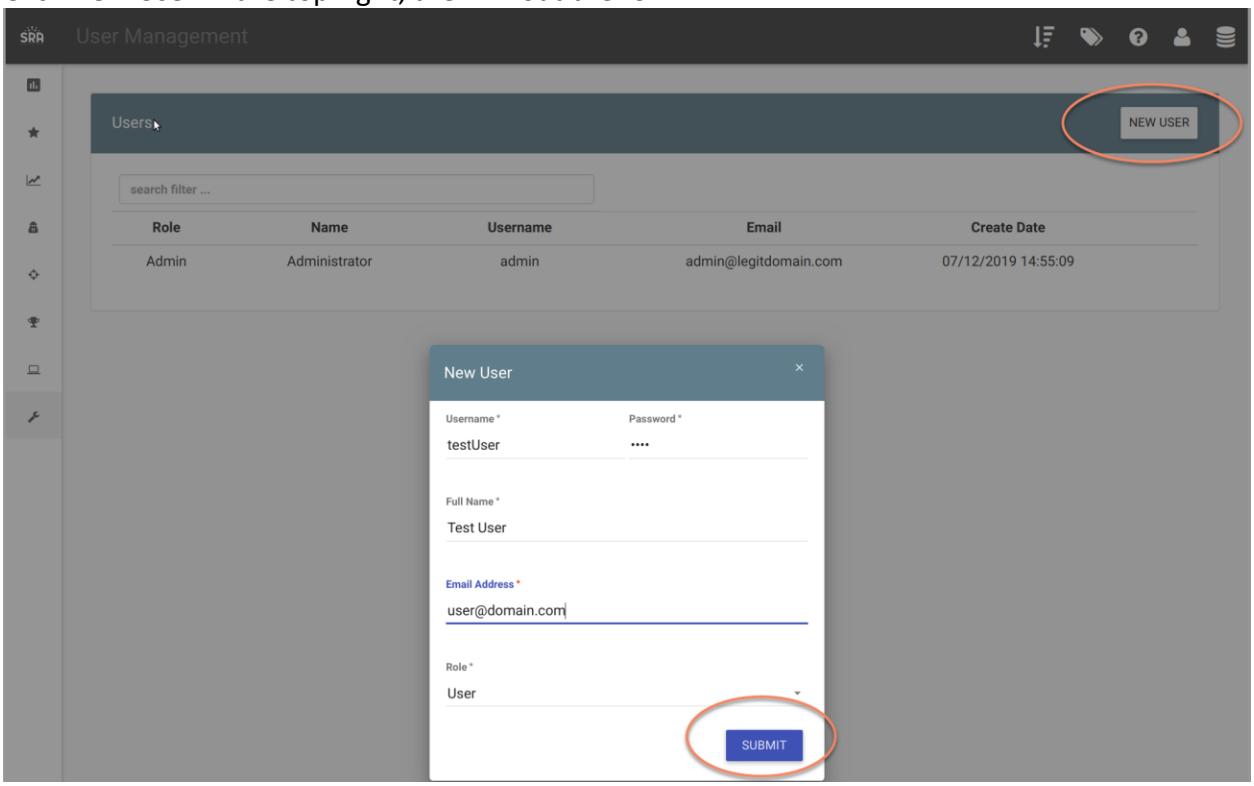
How does it work?

Admin: can create new Users and assign Roles, full Read / Write access.
User: Read / Write access, cannot create Users
Viewer: Read only access, cannot create Users

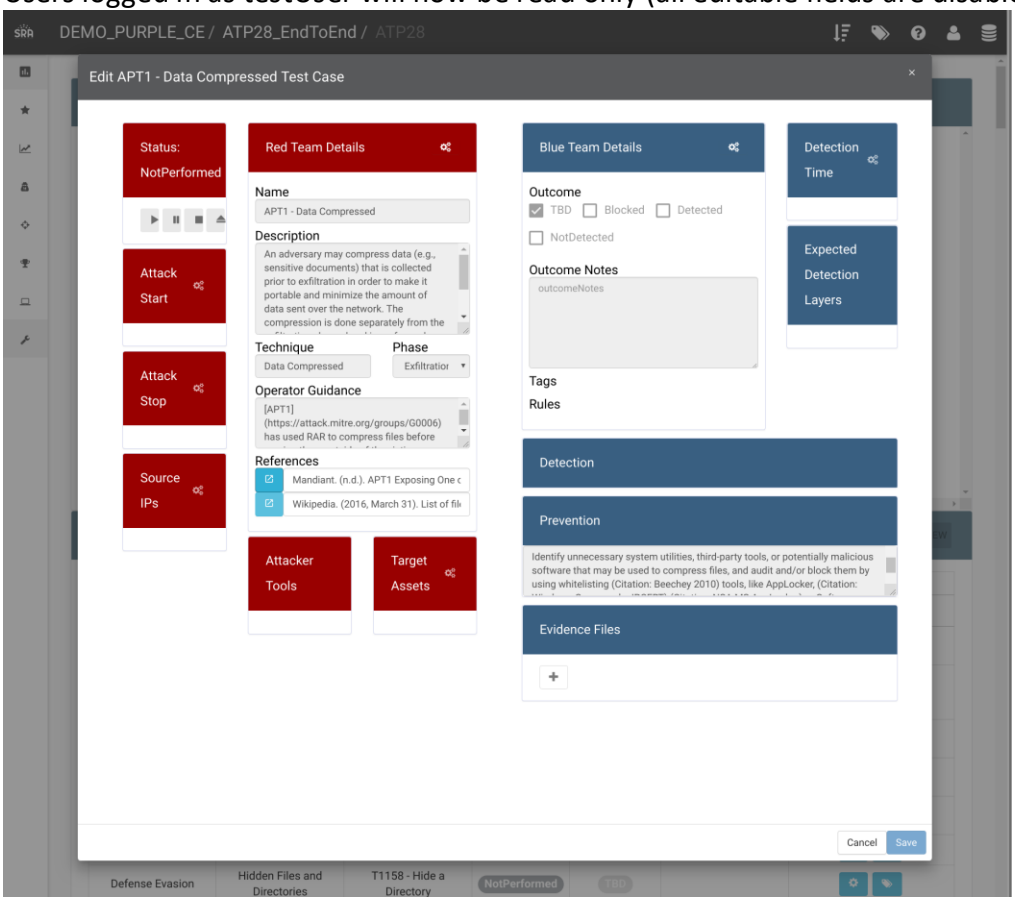
Go to the User Management view:



Click New User in the top right, then fill out the form.



Users logged in as testUser will now be read only (all editable fields are disabled):



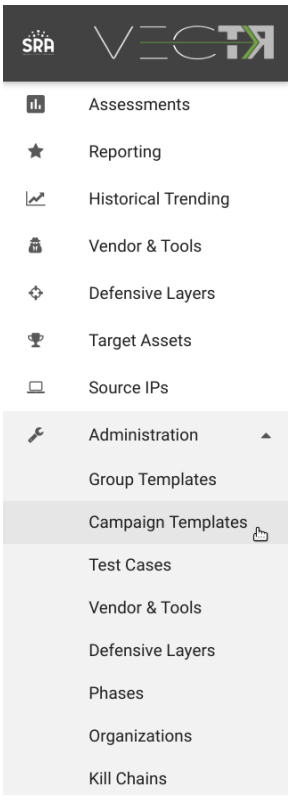
Share Data

What is it?

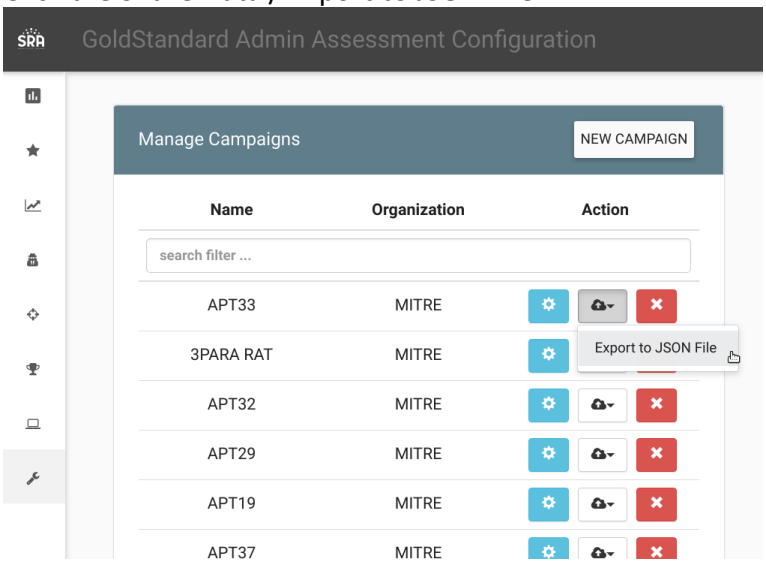
Allows for exporting template content to a valid STIX 2.0 format, which can then be imported into a separate VECTR instance. Note, this is only for templated data, not data with actual results status / outcomes.

How does it work?

Navigate to the Campaign Templates or Group Templates:



Click the Share Data / Export to JSON File:



This will download a STIX 2.0 bundle. You can import the bundle into a separate VECTR instance using the “Data Import” section above.