How to Build a Cyber Threat Intelligence (CTI) Overlay Using MITRE ATT&CK Navigator

Task. Build a CTI overlay using MITRE ATT&CK Navigator.

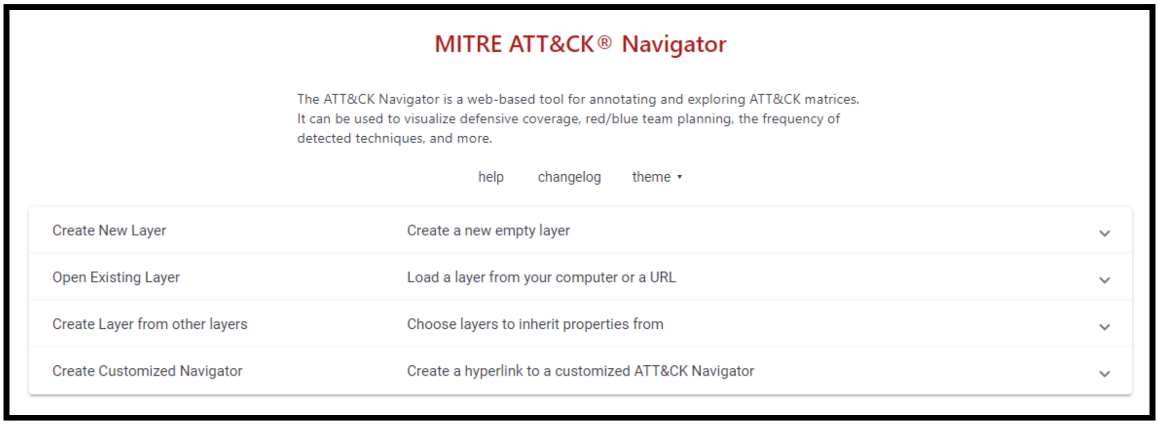
Purpose. The ATT&CK Navigator is designed to provide basic navigation and annotation of MITRE ATT&CK matrices. A "layer" is a custom view of the ATT&CK knowledge base. By compounding layers (i.e., "building an overlay"), an analyst can highlight common techniques used by cyber adversaries and identify detection requirements.

Conditions. You have knowledge of the threat groups most likely to target your organization. You have access to MITRE ATT&CK Navigator.

Standard. You were able to build a CTI overlay using MITRE ATT&CK Navigator.

Step 1. Use a web browser and navigate to MITRE ATT&CK Navigator.

- https://mitre-attack.github.io/attack-navigator/

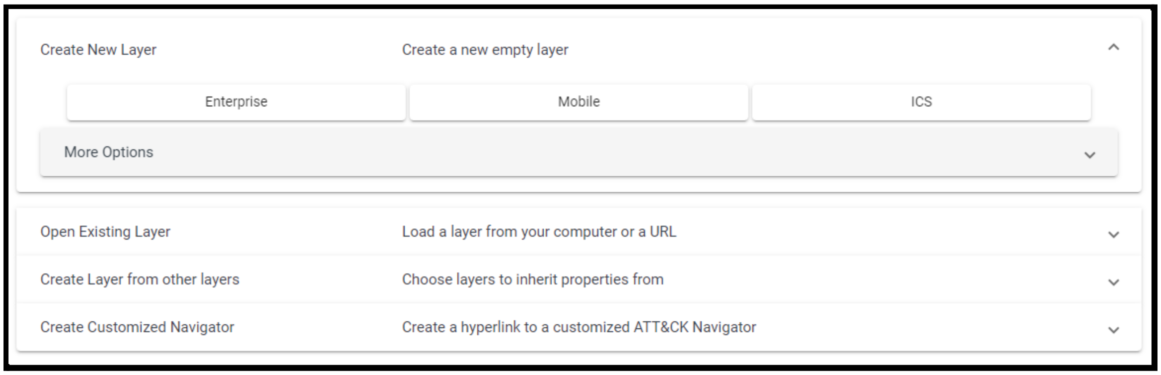


MITRE ATT&CK® Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

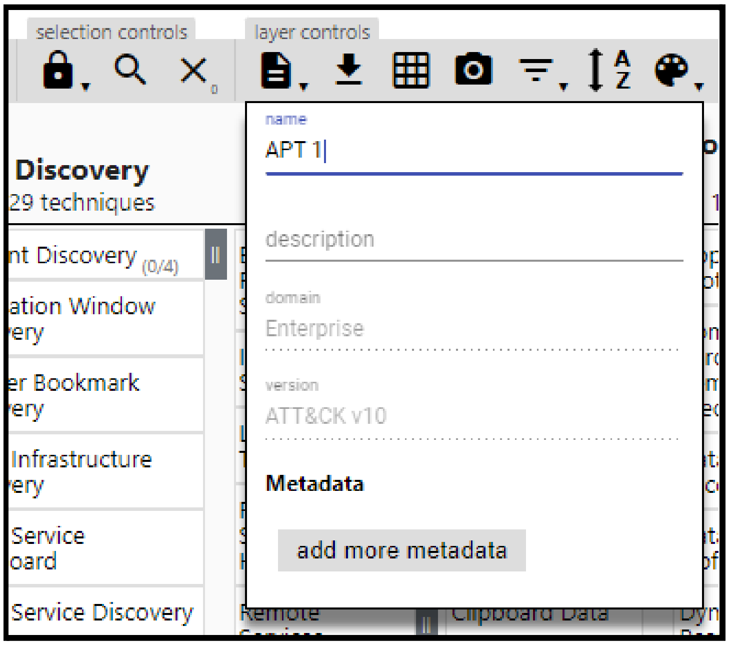
help
changelog
theme ▾
Create New Layer
Create a new empty layer
Open Existing Layer
Load a layer from your computer or a URL
Create Layer from other layers
Choose layers to inherit properties from
Create Customized Navigator
Create a hyperlink to a customized ATT&CK Navigator

Step 2. Click-on "Create New Layer" and select "Enterprise."



Create New Layer
Create a new empty layer
Enterprise
Mobile
ICS
More Options
Open Existing Layer
Load a layer from your computer or a URL
Create Layer from other layers
Choose layers to inherit properties from
Create Customized Navigator
Create a hyperlink to a customized ATT&CK Navigator

Step 3. Click-on the document icon inside the “Layer Controls” toolbar to edit this layer’s “Metadata.” Specify one of the threat groups you are interested in using the “Name” field. Close the “Metadata” pop-up window by clicking-on the document icon again.



name: APT 1

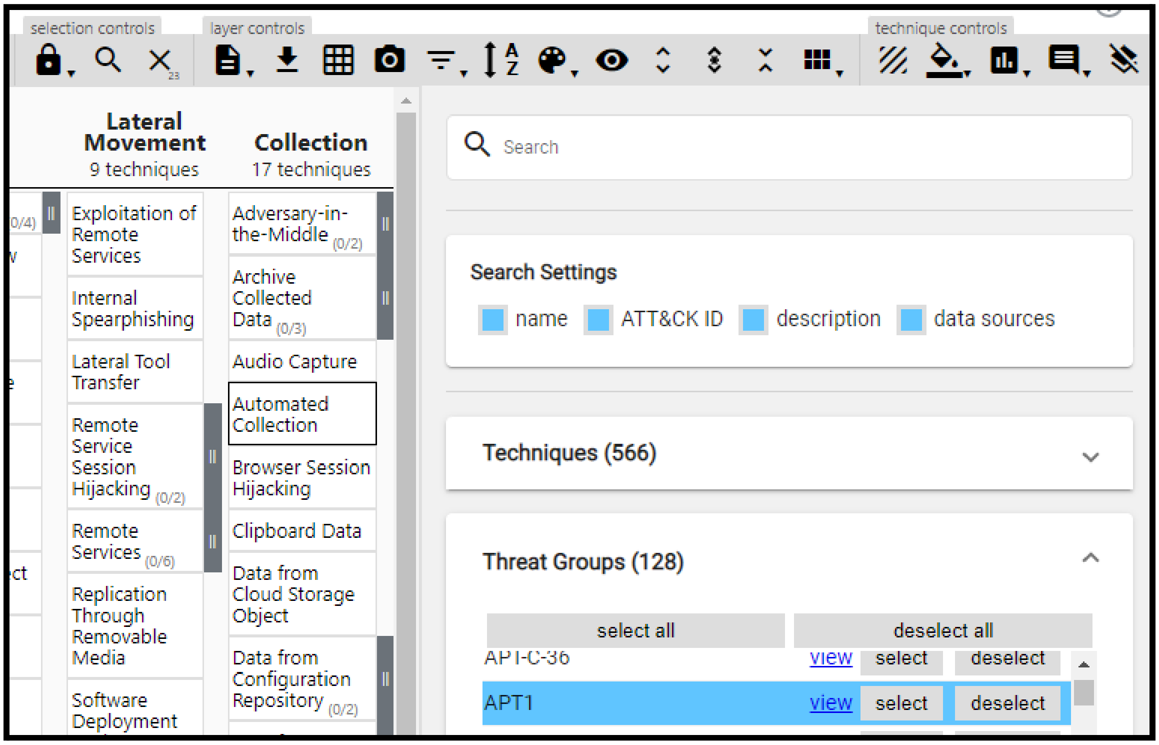
description:

domain: Enterprise

version: ATT&CK v10

Metadata

Step 4. Click-on the magnifying glass inside the “Selection Controls” toolbar to open the “Select & Multiselect” menu. Click-on the “Threat Groups” drop-down menu, find the threat group you are interested in, and click-on “Select” to highlight the group’s techniques. Close the “Select & Multiselect” pop-up window by clicking-on the magnifying glass again.



Search Settings

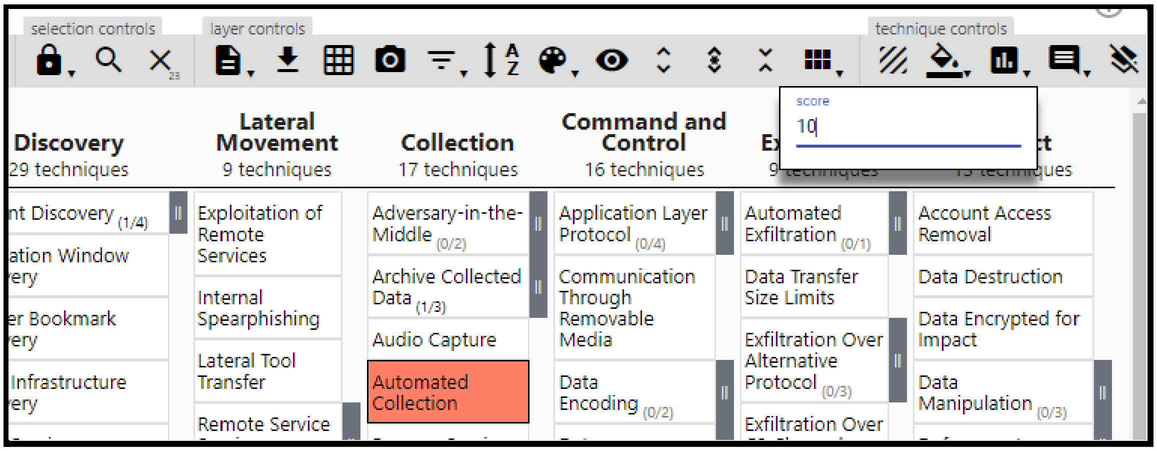
☑ name ☑ ATT&CK ID ☑ description ☑ data sources

Techniques (566)

Threat Groups (128)

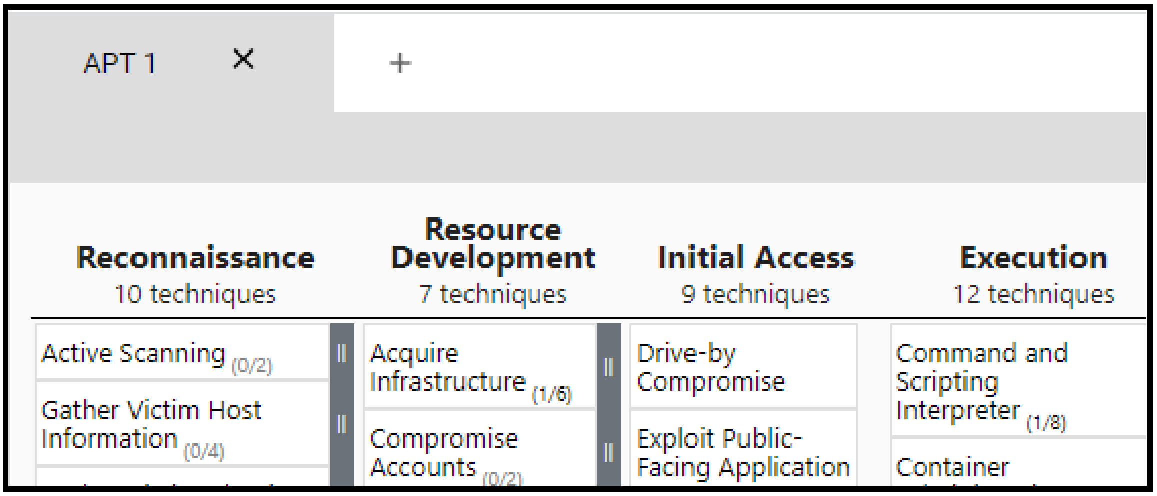
APT-C-36	view	select	deselect
APT1	view	select	deselect

Step 5. Click-on the graph icon inside the “Technique Controls” toolbar to open the “Scoring” menu. Type “10” in the “Score” field. Close the “Scoring” pop-up window by clicking-on the graph icon again.

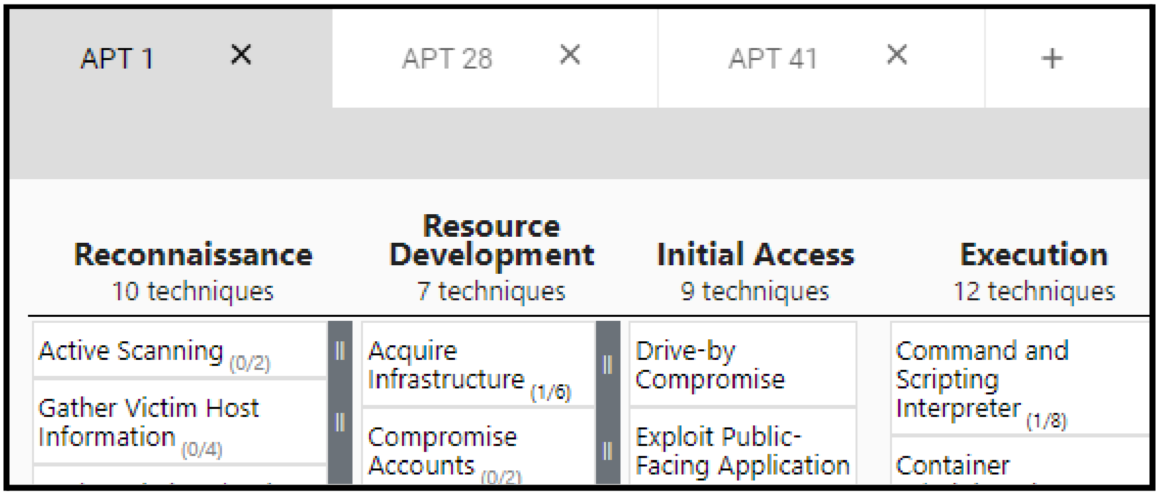


score
10

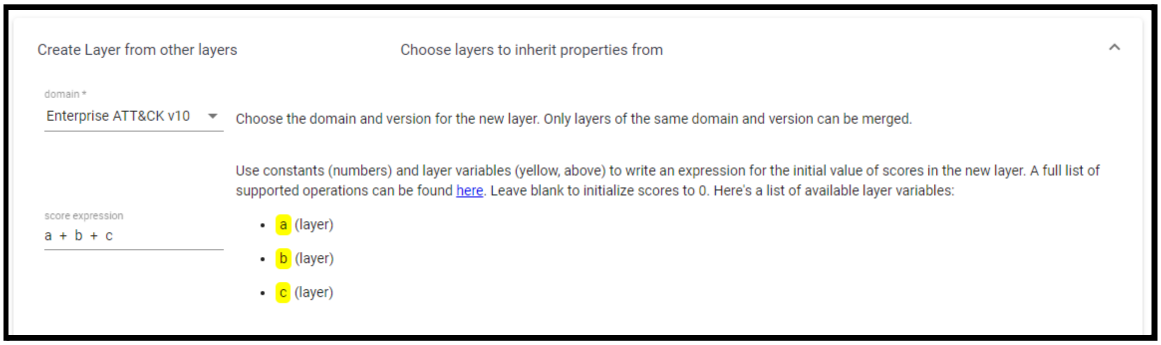
Step 6. Click-on the plus symbol in the top-left corner to open another tab. Repeat Steps 2 through 5 for each of the threat groups you are interested in.



Once complete, your point-of-view should look similar to the screenshot below.



Step 7. Click-on the plus symbol in the top-left corner to open one more tab. Click-on the “Create Layer From Other Layers” drop-down menu. For the “Domain” field, select “Enterprise ATT&CK v10.” For the “Score Expression,” type “a + b + c” (i.e., your expression should include one letter for each layer you created). Click-on “Create” at the bottom of the “Create Layer From Other Layers” drop-down menu.



Create Layer from other layers

Choose layers to inherit properties from

domain *
Enterprise ATT&CK v10

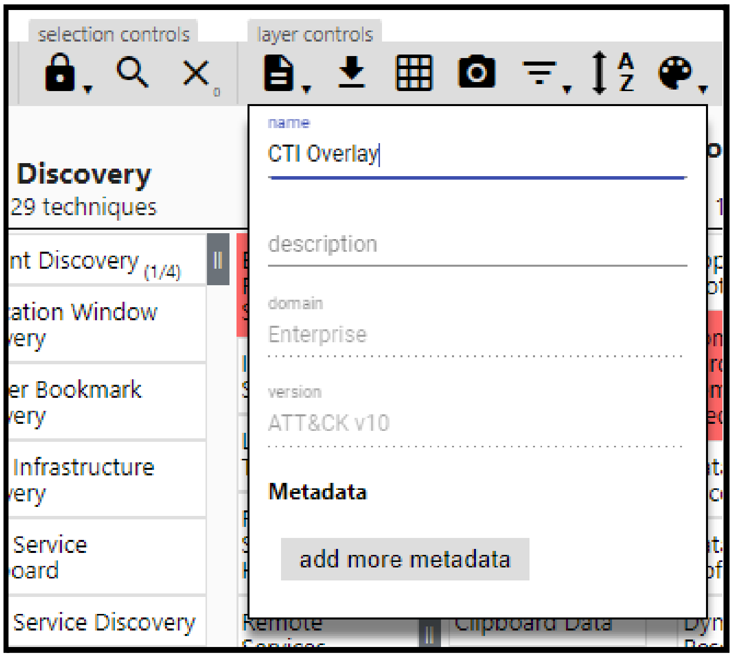
Choose the domain and version for the new layer. Only layers of the same domain and version can be merged.

Use constants (numbers) and layer variables (yellow, above) to write an expression for the initial value of scores in the new layer. A full list of supported operations can be found here. Leave blank to initialize scores to 0. Here's a list of available layer variables:

score expression
a + b + c

- a (layer)
- b (layer)
- c (layer)

Step 8. Click-on the document icon inside the “Layer Controls” toolbar to edit this layer’s “Metadata.” Type “CTI Overlay” in the “Name” field. Close the “Metadata” pop-up window by clicking-on the document icon again.



name: CTI Overlay

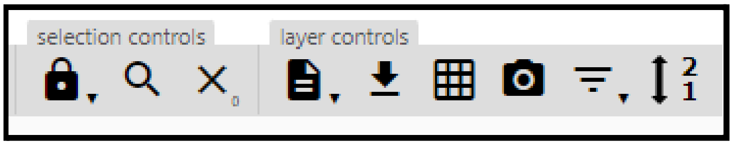
description

domain: Enterprise

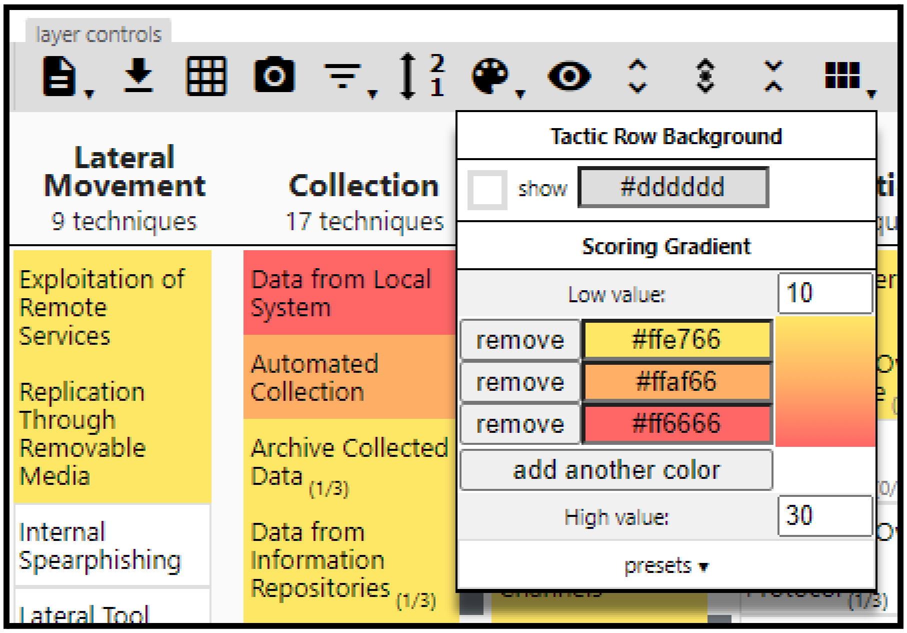
version: ATT&CK v10

Metadata

Step 9. Click-on the bi-directional arrow in the “Layer Controls” toolbar until all techniques are sorted by descending score (if you did this correctly there should be a 2 over a 1 next to the bi-directional arrow like in the screenshot below).



Step 10. Click-on the color palette symbol in the “Layer Controls” toolbar and configure the “Scoring Gradient” to be yellow, orange, and red like shown in the screenshot below. Close the “Color Setup” pop-up window by clicking on the color palette symbol again.



Tactic Row Background

□ show #dddddd

Scoring Gradient

Low value: 10

remove #ffe766

remove #ffaf66

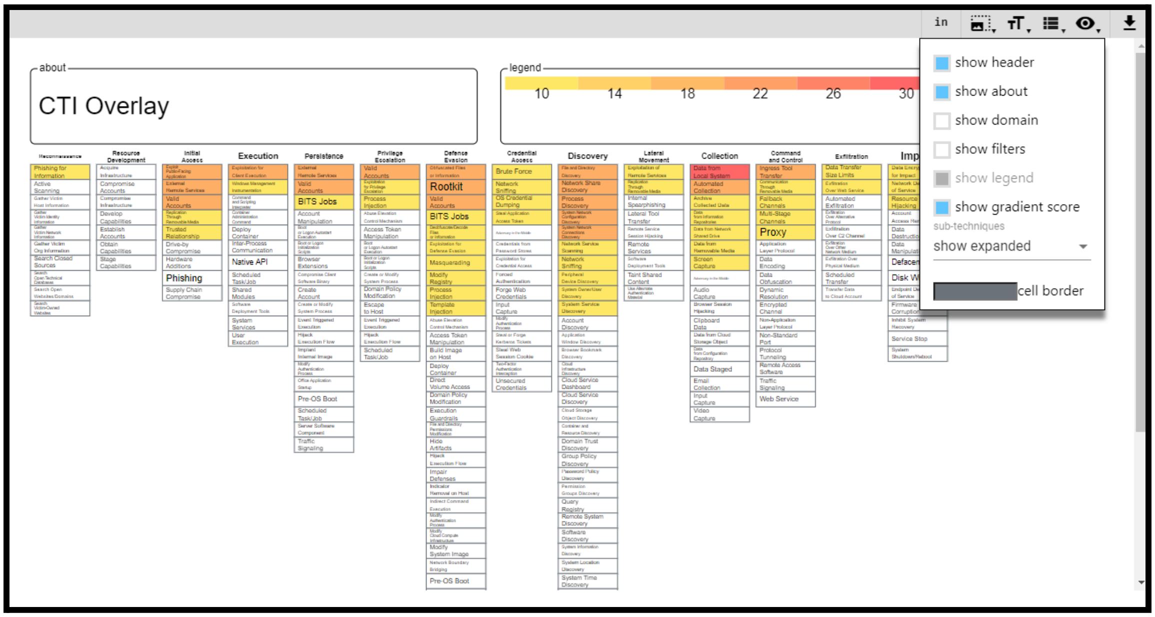
remove #ff6666

add another color

High value: 30

presets ▾

Step 11. Click-on the camera symbol in the “Layer Controls” toolbar to render the current layer (i.e., your overlay) as a SVG file. Once the subsequent pop-up window is displayed, click-on the eyeball symbol and deselect “Show Domain” and “Show Filters.” Close the “Display Settings” pop-up window by clicking on the eyeball symbol again. Finally, click-on the arrow to download your CTI overlay as a SVG file.



☑ show header

☑ show about

□ show domain

□ show filters

☑ show legend

☑ show gradient score

sub-techniques

show expanded ▾

cell border