

VECTR v5.5.8 Feature Breakdown

Table of Contents

- Ability to set Campaign order in Assessment template 2
- Added support for importing atomic-red-team indexes 3
- Allow for non-alphanumeric mongodb username and passwords 5
- Allow users to define an external port for a reverse proxy 6
- Ability to collapse timeline in campaign view 7
- Added ability to download PNGs from certain views 8
- Added icons to match techniques 9

Ability to set Campaign order in Assessment template

What is it?

Added the ability to set and persist the order campaigns appear in an Assessment.

How does it work?

Navigate to the Administration / Group Templates page. Click the gear next to the Assessment you want to change the campaign order on. There is an icon that you can drag and drop in the first column.

The screenshot shows the GoldStandard Admin Assessment Group Configuration interface. The top navigation bar includes the SRA logo and the text 'GoldStandard / Admin Assessment Group Configuration'. The left sidebar contains various icons for navigation. The main content area is divided into two panels.

The left panel, titled 'Manage Assessment Groups', has a 'NEW ASSESSMENT GROUP' button and a table with columns 'Name', 'Type', and 'Action'. The table lists four campaigns, all of type 'Campaign':

Name	Type	Action
Atomic Red Team (MITRE ATT&CK)	Campaign	[Settings] [Share] [Move] [Delete]
SRA Enterprise Assessment (October 2019)	Campaign	[Settings] [Share] [Move] [Delete]
SRA Enterprise Assessment (July 2019)	Campaign	[Settings] [Share] [Move] [Delete]
enterprise-attack-october-2019	Campaign	[Settings] [Share] [Move] [Delete]

The right panel, titled 'enterprise-attack-october-2019 Details', has an 'EDIT' button and a table with columns 'Name' and 'Type'. The table lists five campaigns, all of type 'Campaign':

Name	Type
APT1	Campaign
APT12	Campaign
APT18	Campaign
ADVSTORESHELL	Campaign
3PARA RAT	Campaign
4H RAT	Campaign

A red box highlights the first column of the right panel, which contains drag-and-drop icons (three horizontal lines) for each campaign row.

How can this feature help me?

You can pre-set your campaign order

Added support for importing atomic-red-team indexes

What is it?

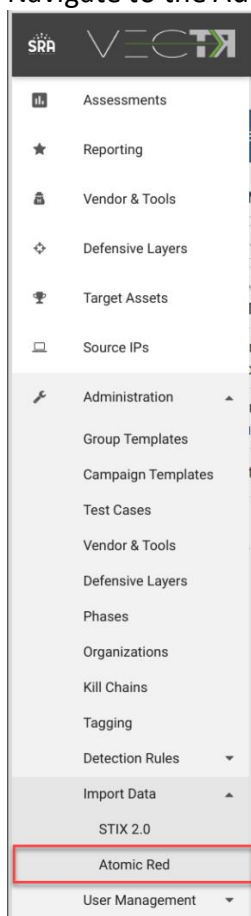
This will allow users to generate Assessment / Campaign / Test Case template content from indexes generated from the Red Canary's Atomic Red project

<https://github.com/redcanaryco/atomic-red-team>.

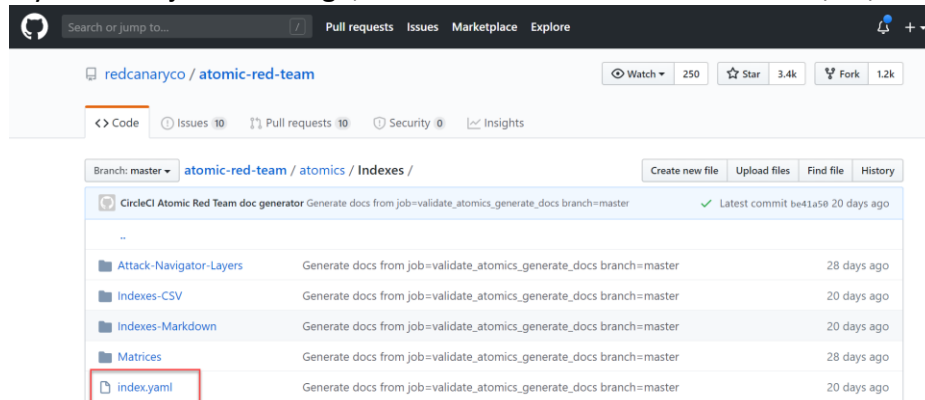
Note: If you already have Atomic Red content in your Administration -> Group Templates , Administration -> Campaign Templates (you will have them if you already have a VECTR installation prior to 5.5.8), this will update them with the latest content provided in the index.yaml. If this is the first time installing VECTR, we no longer ship Atomic Red templates by default, and this will generate brand new content.

How does it work?

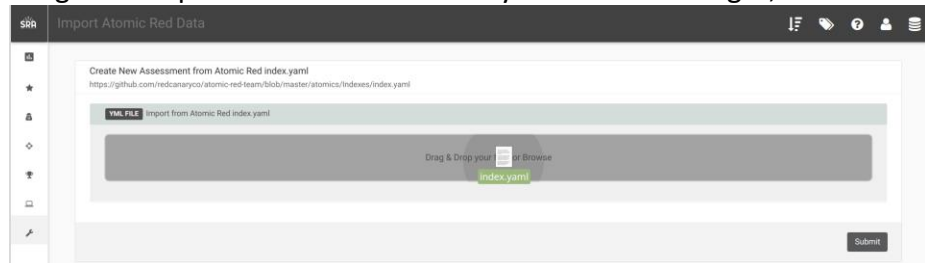
Navigate to the Administration / Import Data / Atomic Red section of the left navigation pane:



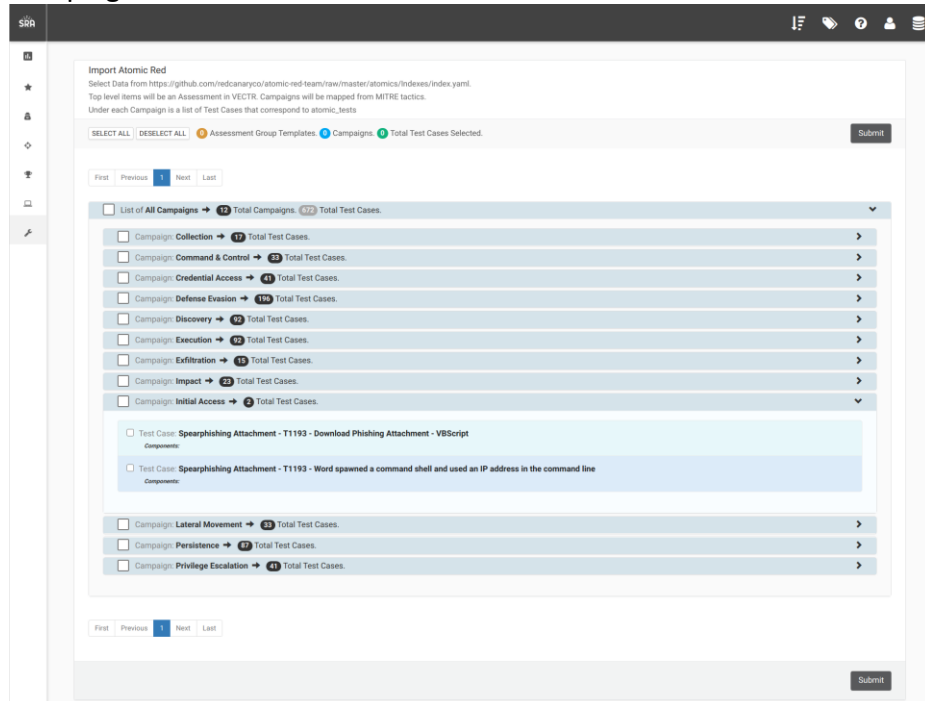
Download the index.yaml file from redcanaryco/atomic-red-team GitHub page. The page layout is subject to change, and this screenshot was taken on 6/10/2020.



Drag and drop the downloaded index.yaml into the widget, then click submit:



This will bring you to a selection screen where you can generate templates from generated Campaigns and Test Cases:



How can this feature help me?

This will allow your team to run through test cases based on the atomic-red project.

Allow for non-alphanumeric mongodb username and passwords

What is it?

When starting up VECTR for the first time, the mongodb is initialized with a root password obtained from the .env file. Allowing non-alphanumeric passwords will allow for additional security.

How does it work?

In the .env file, there is a MONGO_INITDB_ROOT_PASSWORD variable that sets the password:

```
# .env file

VECTR_HOSTNAME=sravectr.internal
VECTR_PORT=8081

# defaults to warn, debug useful for development
VECTR_CONTAINER_LOG_LEVEL=WARN


MONGO_INITDB_ROOT_USERNAME=admin

# PLEASE change this and store it in a safe place. Encrypted data like passwords
# to integrate with external systems (like TAXII) use this key
VECTR_DATA_KEY=CHANGEMENOW

# AND this too
CAS_ENCRYPT_MONGO_KEY=CHANGEMENOW

# ALSO change and store in a safe place
MONGO_INITDB_ROOT_PASSWORD=Test!@#%^&*()_+1234

# This is the FQDN of the VECTR service URL specified in the CAS service registration configuration.
# Only set this if you are running VECTR and CAS behind a load balancer or proxy and VECTR's external
# facing hostname is not the same as VECTR_HOSTNAME.
#VECTR_EXTERNAL_HOSTNAME=
```



How can this feature help me?

This will allow additional security by accepting more complex passwords.

Allow users to define an external port for a reverse proxy

What is it?

If running VECTR behind a reverse proxy, there used to be an error in the redirect URL used in authentication if the listener port of the proxy was anything other than 80 or 443.

How does it work?

There is a new value (VECTR_EXTERNAL_PORT) in the .env file you can use to set the port of the listener of your proxy:

```
# .env file

VECTR_HOSTNAME=sravectr.internal
VECTR_PORT=8081

# defaults to warn, debug useful for development
VECTR_CONTAINER_LOG_LEVEL=WARN

MONGO_INITDB_ROOT_USERNAME=admin

# PLEASE change this and store it in a safe place. Encrypted data like passwords
# to integrate with external systems (like TAXII) use this key
VECTR_DATA_KEY=CHANGEMENOW

# AND this too
CAS_ENCRYPT_MONGO_KEY=CHANGEMENOW

# ALSO change and store in a safe place
MONGO_INITDB_ROOT_PASSWORD=Test1234

# This is the FQDN of the VECTR service URL specified in the CAS service registration configuration.
# Only set this if you are running VECTR and CAS behind a load balancer or proxy and VECTR's external
# facing hostname is not the same as VECTR_HOSTNAME.
#VECTR_EXTERNAL_HOSTNAME=

# This is the port of the VECTR service URL specified in the CAS service registration configuration.
# Only set this if you are running VECTR and CAS behind a load balancer or proxy and VECTR's external
# facing port is not the same as VECTR_PORT.
#VECTR_EXTERNAL_PORT=

#This sets the name of your project. Will show up in the name of your containers.
COMPOSE_PROJECT_NAME=sandbox1

#This is where the mongodb mounts.
VECTR_DATA_DIR=/var/data/
```

How can this feature help me?

This will get rid of the workarounds required when running behind a load balancer or reverse proxy that is not listening on port 80 or 443.

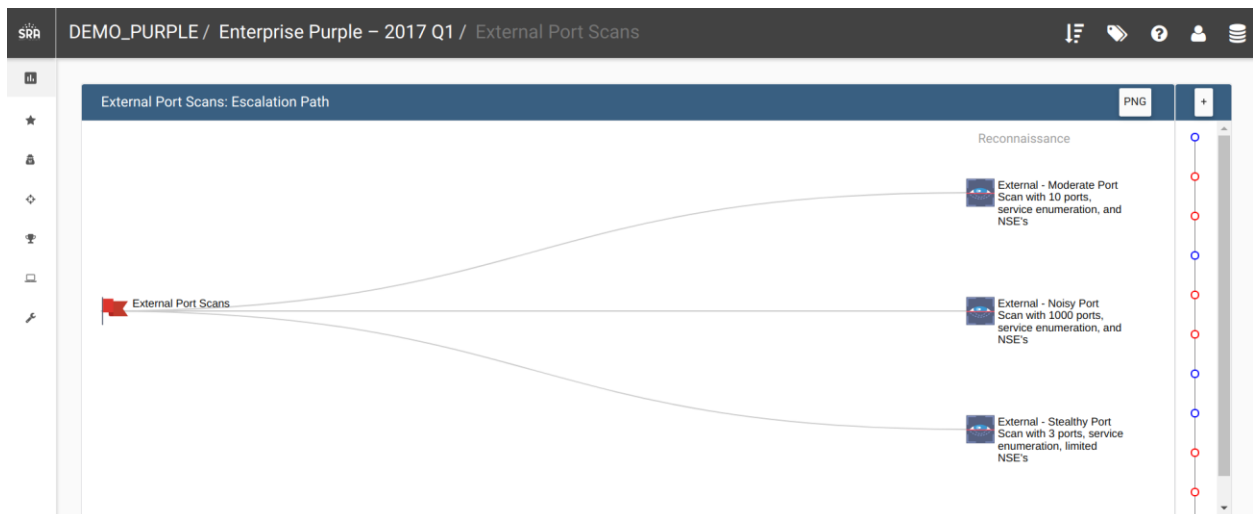
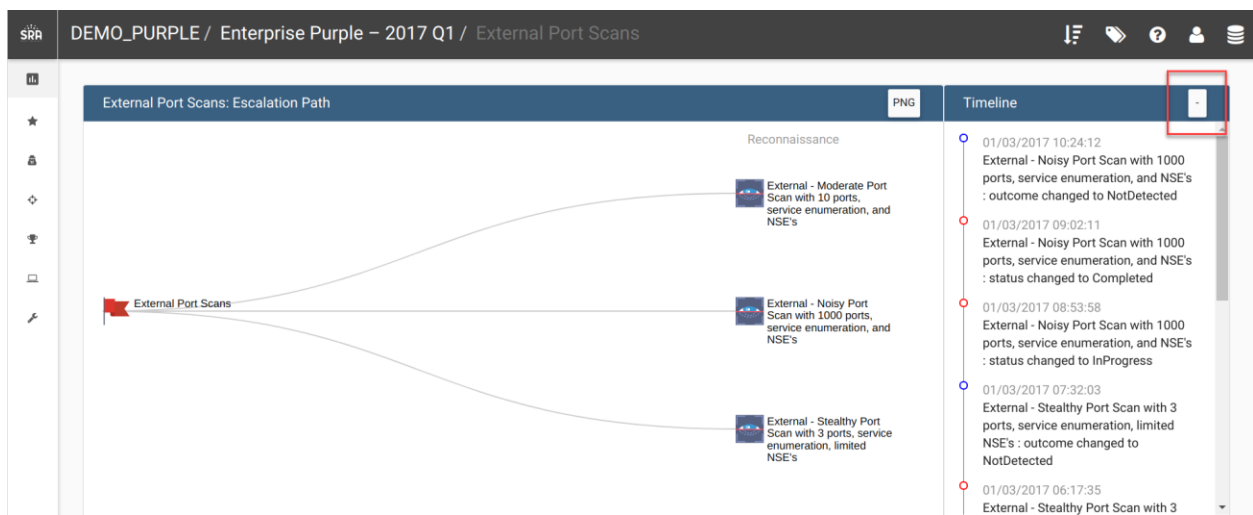
Ability to collapse timeline in campaign view

What is it?

Give users the ability to collapse the timeline area of the campaign view to make the escalation diagram larger.

How does it work?

Click the button in the top right of the timeline:



How can this feature help me?

Allows for more real estate for the escalation diagram.

Added ability to download PNGs from certain views

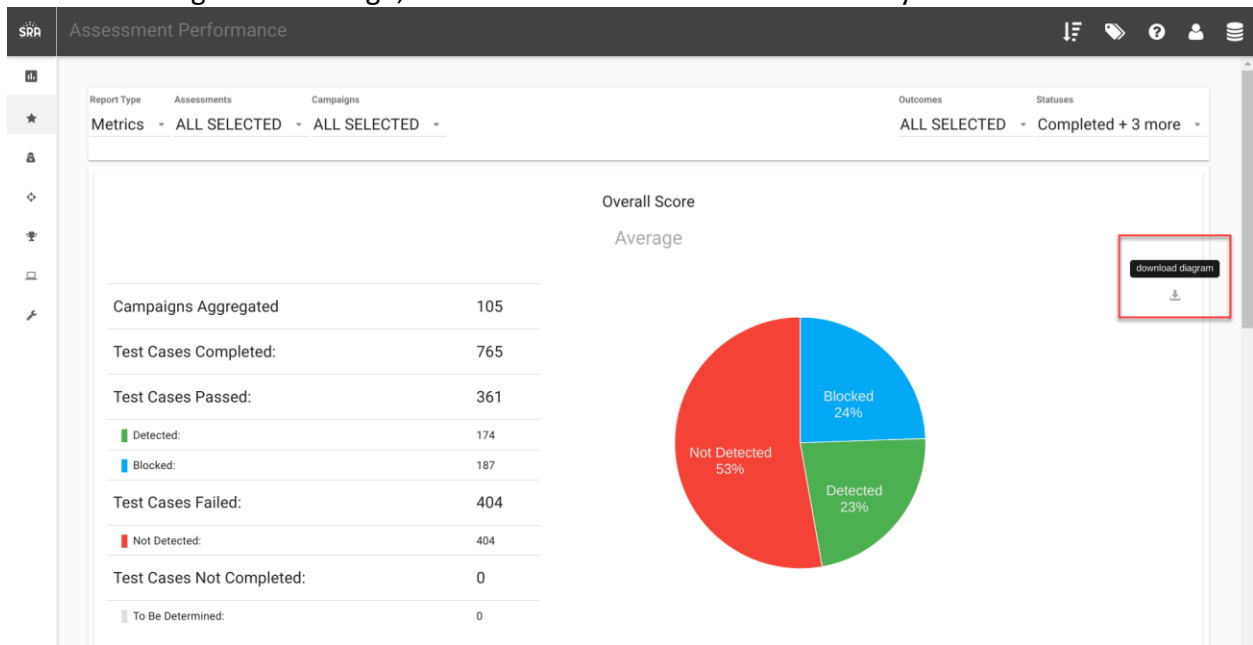
What is it?

Some of the reporting screens and escalation diagram have buttons that will allow you to download PNGs.

NOTE: Microsoft Windows 10's default image viewer does not show the images well. We have tried many other image viewers and they all seem to render properly.

How does it work?

When hovering over an image, there will be a download button that you can click:



How can this feature help me?

This will allow for easier importing of images in reports and presentations.

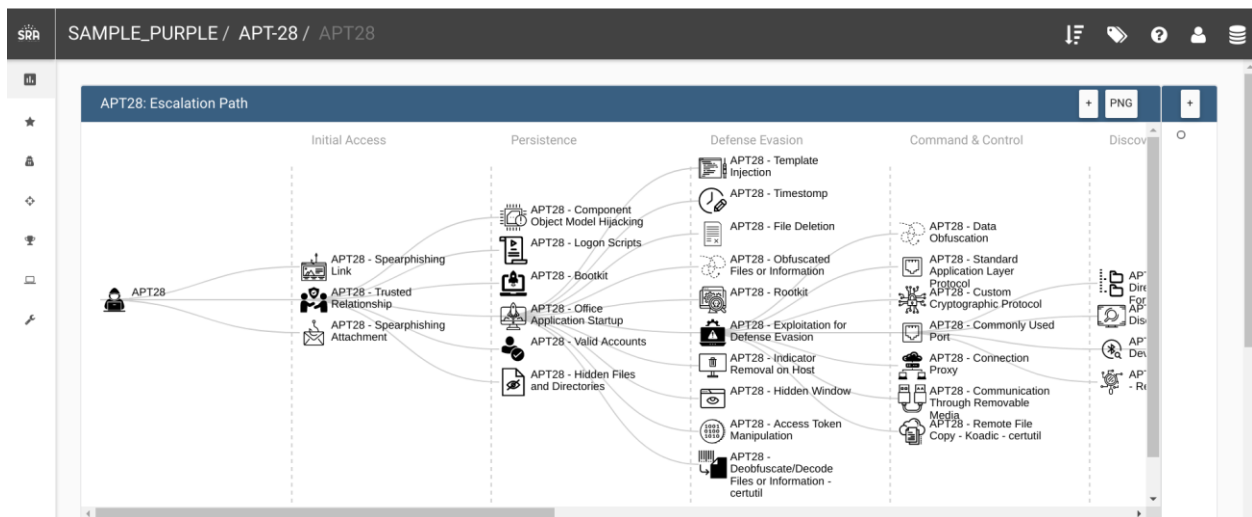
Added icons to match techniques

What is it?

Added default icons to align to the mitre technique ids for test cases.

How does it work?

Whenever creating new test cases, if the mitreID is supplied, it will default to the icon mapping to the mitreID. If no mitreID is supplied, it will use a default icon. The icon can always be overridden by selecting a specific one.



How can this feature help me?

Allows for more contextual awareness when visualizing the escalation diagram.