VECTR v5.3 Feature Breakdown

Table of Contents

Browser Cache Fix....2

Context Sensitive Help....3

Data Integrity Report Updates....5

Historical Trending Redesign....6

Import MITRE CTI Data Improvements....9

Test Case Evidence File Upload Improvements....11

Test Case Icons Additional Support....12

Heat Map Technique Duplications Filter....14

Browser Cache Fix

What is it?

This is a fix for situations where when using VECTR for long term assessments you encounter issues with the application after a version upgrade. VECTR now builds its client side dependencies in a way that prevents cached data from interfering with new or changed features.

How does it work?

Previously, the workaround for these issues was to use Chrome's incognito mode. Now, after this fix you can use the application as normal without incognito or private browsing mode. This change is behind-the-scenes.

How can this feature help me?

This fixes an application usability bug.

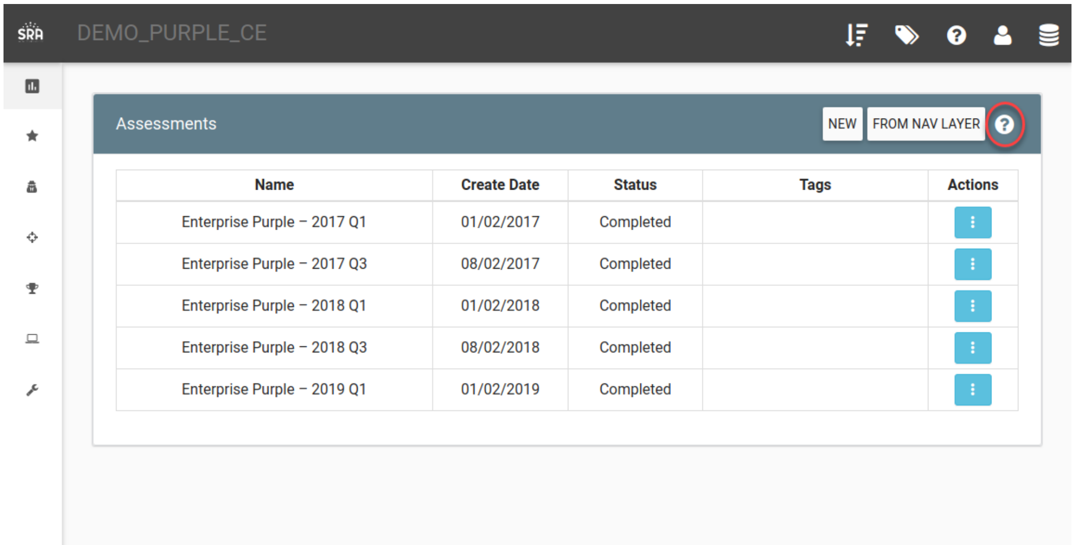
Context Sensitive Help

What is it?

This adds a new Help menu to core functionality screens with links to relevant documentation or user guides. For now these link to relevant VECTR help videos and the GitHub wiki depending on the page.

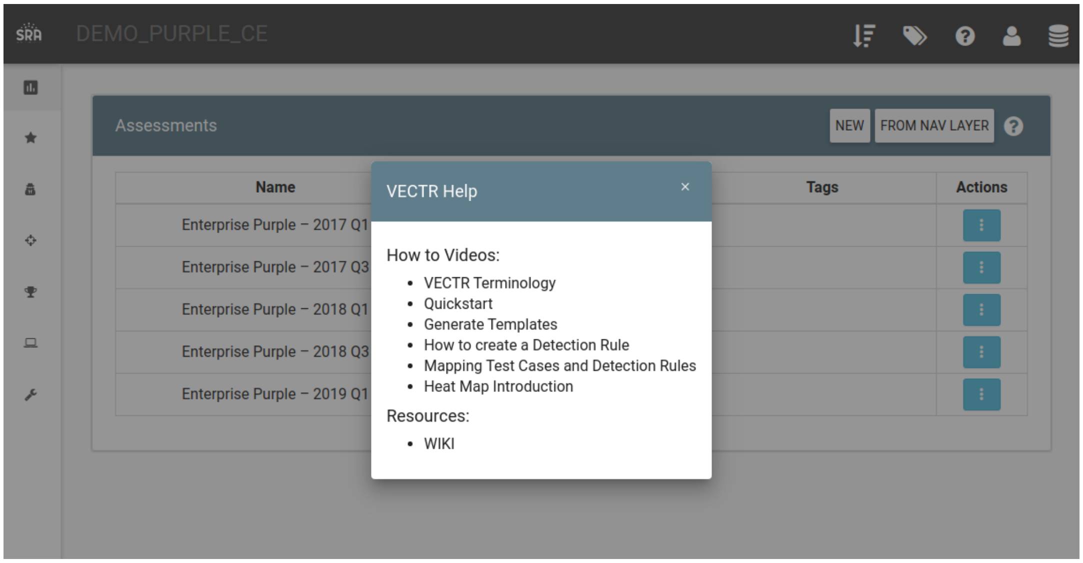
How does it work?

On some VECTR screens you will see a question mark in a circle signifying help is available.



Name	Create Date	Status	Tags	Actions
Enterprise Purple – 2017 Q1	01/02/2017	Completed		⋮
Enterprise Purple – 2017 Q3	08/02/2017	Completed		⋮
Enterprise Purple – 2018 Q1	01/02/2018	Completed		⋮
Enterprise Purple – 2018 Q3	08/02/2018	Completed		⋮
Enterprise Purple – 2019 Q1	01/02/2019	Completed		⋮

Clicking the question mark will open help in a modal dialog.


DEMO_PURPLE_CE
Assessments
NEW
FROM NAV LAYER
Name
Tags
Actions
Enterprise Purple – 2017 Q1
Enterprise Purple – 2017 Q3
Enterprise Purple – 2018 Q1
Enterprise Purple – 2018 Q3
Enterprise Purple – 2019 Q1
VECTR Help
×

How to Videos:

- VECTR Terminology
- Quickstart
- Generate Templates
- How to create a Detection Rule
- Mapping Test Cases and Detection Rules
- Heat Map Introduction

Resources:

- WIKI

How can this feature help me?

This feature provides easier access to help and guide resources that are pertinent to areas of the application where you are working.

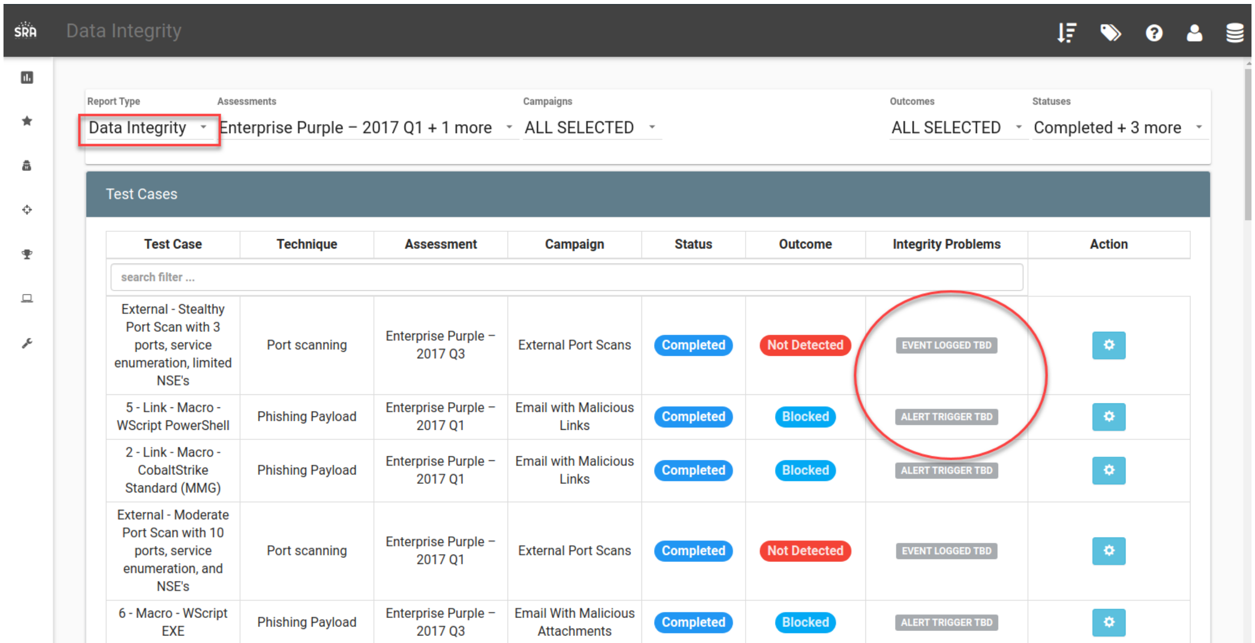
Data Integrity Report Updates

What is it?

The Data Integrity Report shows Test Cases that may be have incorrect data. Existing functionality 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. We've added reporting for Test Cases where the Outcome is "Not Detected" and Event Logged is "TBD" or Outcome is "Blocked" and Alert Triggered is "TBD."

How does it work?

Select the Data Integrity report from the Reporting page:



Report Type: Data Integrity
Assessments: Enterprise Purple – 2017 Q1 + 1 more
Campaigns: ALL SELECTED
Outcomes: ALL SELECTED
Statuses: Completed + 3 more

Test Cases

Test Case	Technique	Assessment	Campaign	Status	Outcome	Integrity Problems	Action
External - Stealthy Port Scan with 3 ports, service enumeration, limited NSE's	Port scanning	Enterprise Purple – 2017 Q3	External Port Scans	Completed	Not Detected	EVENT LOGGED TBD	⚙
5 - Link - Macro - WScript PowerShell	Phishing Payload	Enterprise Purple – 2017 Q1	Email with Malicious Links	Completed	Blocked	ALERT TRIGGER TBD	⚙
2 - Link - Macro - CobaltStrike Standard (MMG)	Phishing Payload	Enterprise Purple – 2017 Q1	Email with Malicious Links	Completed	Blocked	ALERT TRIGGER TBD	⚙
External - Moderate Port Scan with 10 ports, service enumeration, and NSE's	Port scanning	Enterprise Purple – 2017 Q1	External Port Scans	Completed	Not Detected	EVENT LOGGED TBD	⚙
6 - Macro - WScript EXE	Phishing Payload	Enterprise Purple – 2017 Q3	Email With Malicious Attachments	Completed	Blocked	ALERT TRIGGER TBD	⚙

How can this feature help me?

In the event data has not been completely or accurately entered, this report shows inconsistencies or incomplete recording of finished assessment activities.

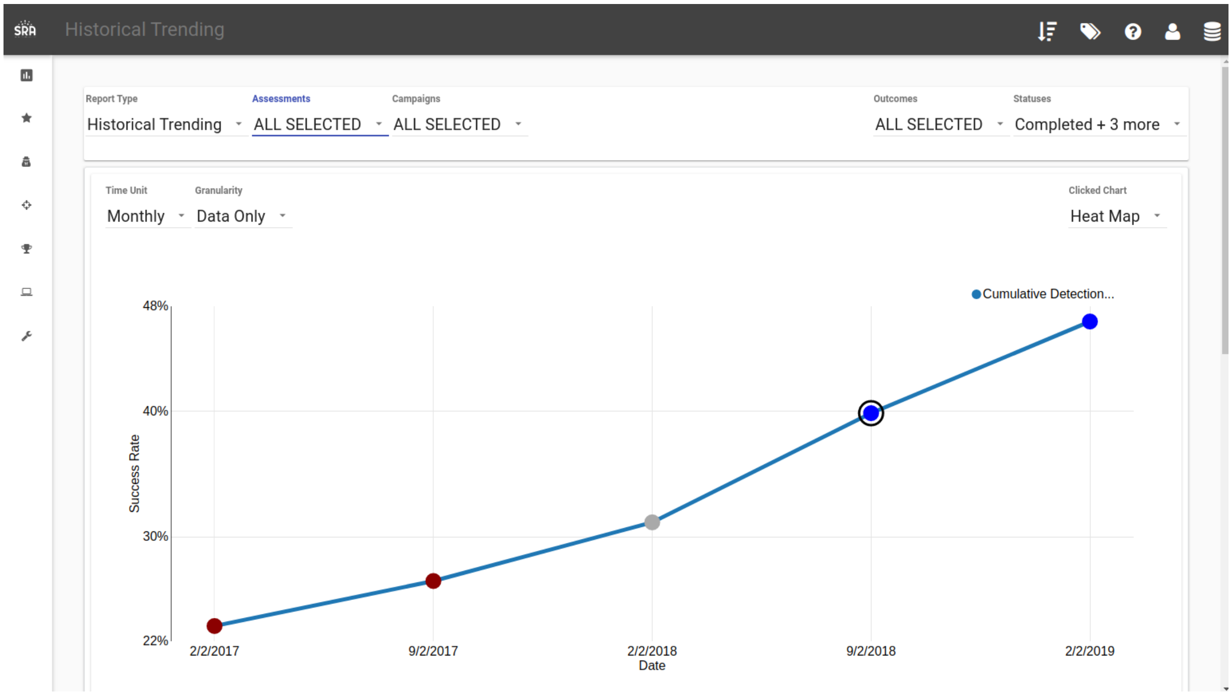
Historical Trending Redesign

What is it?

The Historical Trending Report has been redesigned to add more flexibility to the report

How does it work?

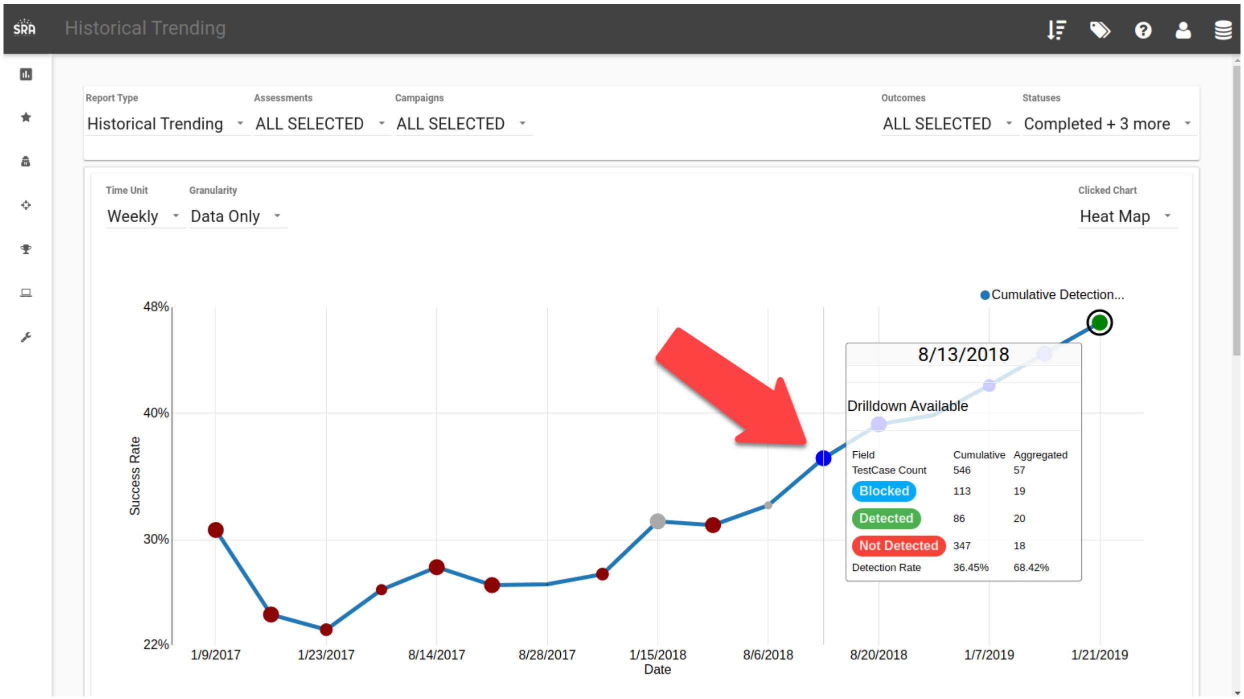
Browsing to the “Historical Trending” Report Type will show this:



Report Type: Historical Trending
Assessments: ALL SELECTED
Campaigns: ALL SELECTED
Outcomes: ALL SELECTED
Statuses: Completed + 3 more

Time Unit: Monthly
Granularity: Data Only
Clicked Chart: Heat Map

Users can select the number of assessments they want to include in the trendline using the report filters at the top of the page and adjust the Time Unit (Monthly, Quarterly, etc.) and Granularity of the graphed data.



Report Type: Historical Trending
Assessments: ALL SELECTED
Campaigns: ALL SELECTED
Outcomes: ALL SELECTED
Statuses: Completed + 3 more

Time Unit: Weekly
Granularity: Data Only
Clicked Chart: Heat Map

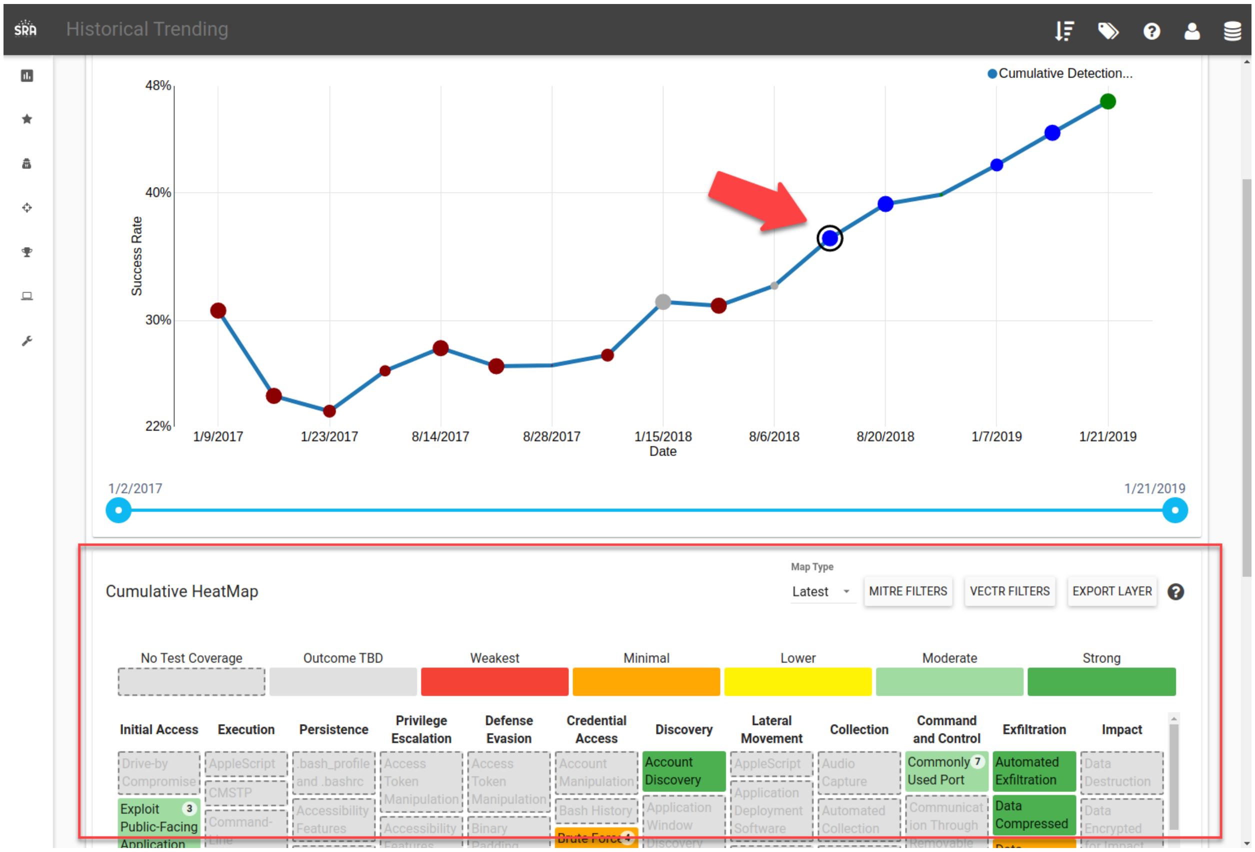
8/13/2018

Drilldown Available

Field	Cumulative	Aggregated
TestCase Count	546	57
Blocked	113	19
Detected	86	20
Not Detected	347	18
Detection Rate	36.45%	68.42%

Hovering over a point on the chart will show statistics as of that point. Note that here we're showing Weekly data and between 8/6/2018 and 8/13/2018 we performed 57 Test Cases according to the Aggregated count. The total count of test cases performed was 546 between 1/9/2017 and 8/13/2018. The data in this hover chart tells you that between 8/6/2018 and 8/13/2018 you detected 68.42% of your Test Cases run and this was significantly better than your prior average detection rate of around 33%. This bumped up your cumulative detection score to 36.45%.

The blue circle on the chart shows you performed well in the preceding time period, and the size of the circle shows how many Test Cases relative to the total were performed in that time. Many Test Cases shows a larger circle.



Cumulative HeatMap

No Test Coverage	Outcome TBD	Weakest	Minimal	Lower	Moderate	Strong

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise Exploit Public-Facing Application 3	AppleScript CMSTP Command-Line	.bash_profile and .bashrc Accessibility Features	Access Token Manipulation Accessibility Features	Access Token Manipulation Binary Padding	Account Manipulation Bash History Brute Force 4	Account Discovery Application Window Discovery	AppleScript Application Deployment Software	Audio Capture Automated Collection	Commonly Used Port 7 Communication Through Removable	Automated Exfiltration Data Compressed Data	Data Destruction Data Encrypted for Impact

Clicking on a point in the Historical Trending graph allows you to show different report types below the trending graph driven by the “Clicked Chart” filter. In this case, it is showing the MITRE Heat Map view as of that point.

How can this feature help me?

These new Historical Trending views are helpful for showing high-level detection improvements over time and analyzing strengths and weaknesses in tested data.

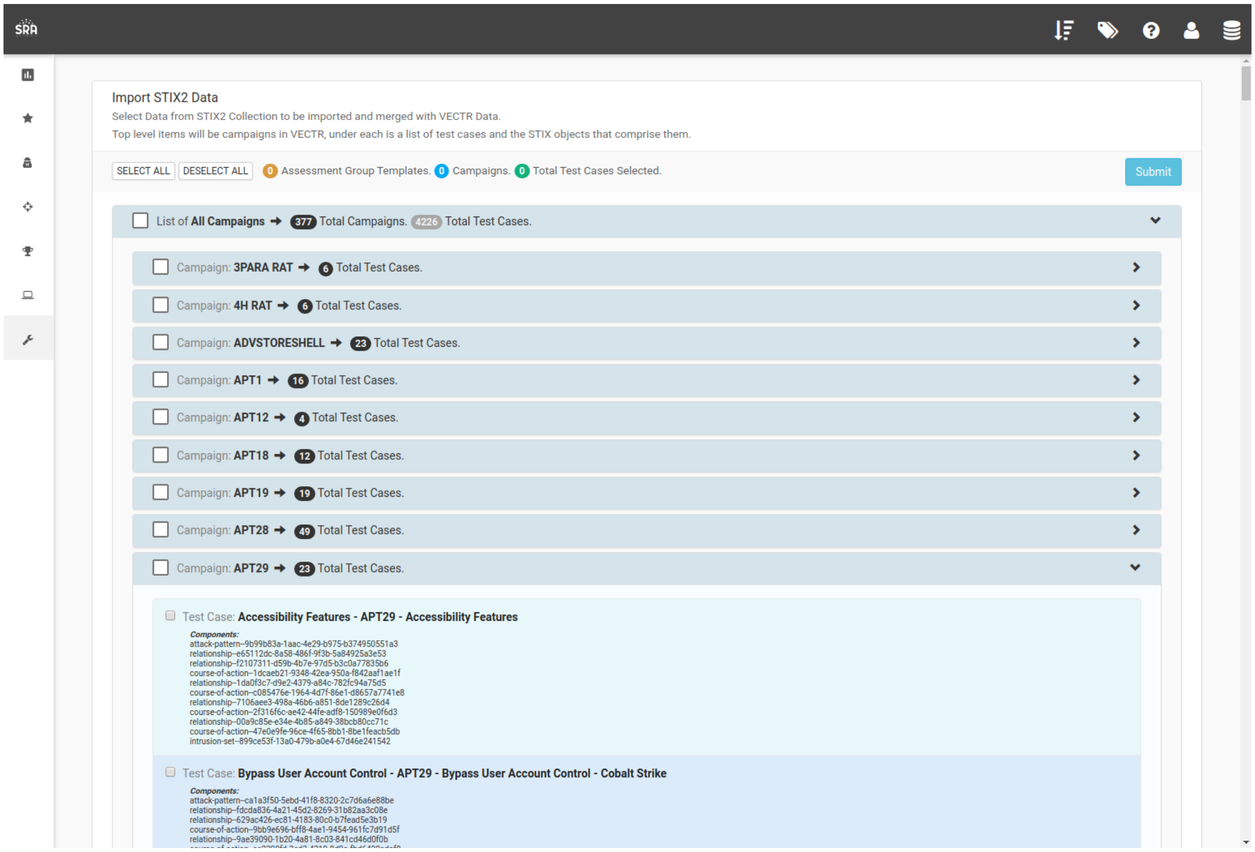
Import MITRE CTI Data Improvements

What is it?

VECTR can import MITRE CTI STIX data to create Test Cases and Campaigns for common threat actors. Recent improvements make it so that as of this latest version of VECTR, importing new data will update existing imported data in the system UNLESS you have made changes to that data. In the scenario where you have modified imported data, any future imports will try to preserve your modifications and enrichments.

How does it work?

Download the enterprise-attack.json file from MITRE https://github.com/mitre/cti/blob/master/enterprise-attack/enterprise-attack.json and import it using the Administration -> Import Data user interface for importing JSON data.



Import STIX2 Data

Select Data from STIX2 Collection to be imported and merged with VECTR Data.

Top level items will be campaigns in VECTR, under each is a list of test cases and the STIX objects that comprise them.

SELECT ALL | DESELECT ALL | 0 Assessment Group Templates. 0 Campaigns. 0 Total Test Cases Selected. | Submit

□ List of **All Campaigns** → 377 Total Campaigns. 4226 Total Test Cases.

□ Campaign: **3PARA RAT** → 6 Total Test Cases.

□ Campaign: **4H RAT** → 6 Total Test Cases.

□ Campaign: **ADVSTORESHELL** → 23 Total Test Cases.

□ Campaign: **APT1** → 16 Total Test Cases.

□ Campaign: **APT12** → 4 Total Test Cases.

□ Campaign: **APT18** → 12 Total Test Cases.

□ Campaign: **APT19** → 19 Total Test Cases.

□ Campaign: **APT28** → 49 Total Test Cases.

□ Campaign: **APT29** → 23 Total Test Cases.

□ Test Case: **Accessibility Features - APT29 - Accessibility Features**

Components:
```
attack-pattern--9b99b83a-1aac-4e29-b975-b374950551a3
relationship--e65112dc-8a58-486f-9f3b-5a84925a3e53
relationship--f2107311-d59b-4b7e-97d5-b3c0a77835b6
course-of-action--1dcaeb21-9348-42ea-950a-f842aaf1ae1f
relationship--1da0f3c7-d9e2-4379-a84c-782fc94a75d5
course-of-action--c085476e-1964-4d7f-86e1-d8657a7741e8
relationship--7106aee3-498a-46b6-a851-8de1289c26d4
course-of-action--2f316f6c-ae42-44fe-adf8-150989e0f6d3
relationship--00a9c85e-e34e-4b85-a849-38bcb80cc71c
course-of-action--47e0e9fe-96ce-4f65-8bb1-8be1feacb5db
intrusion-set--899ce53f-13a0-479b-a0e4-67d46e241542
```

□ Test Case: **Bypass User Account Control - APT29 - Bypass User Account Control - Cobalt Strike**

Components:
```
attack-pattern--ca1a3f50-5ebd-41f8-8320-2c7d6a6e88be
relationship--fdcda836-4a21-45d2-8269-31b82aa3c08e
relationship--629ac426-ec81-4183-80c0-b7fead5e3b19
course-of-action--9bb9e696-bff8-4ae1-9454-961fc7d91d5f
relationship--9ae39090-1b20-4a81-8c03-841cd46d0f0b
```

Note: Do NOT import all MITRE CTI data, only select campaigns you plan on manually enriching and emulating for threat actors or malware that pertain to your environment. Pulling too much data into the system will be overwhelming and unlikely to lead to good testing outcomes.

MITRE updates their enterprise-attack.json CTI data on a regular basis. After importing data, wait some time for MITRE updates and try to import new data, selecting previously imported campaigns for an update. The system should now update your previously imported data for any Test Cases you haven't modified rather than creating duplicates.

How can this feature help me?

This feature allows you to keep up to date with MITRE CTI Threat Actor and Malware data without manually adding and deleting older imported Test Cases.

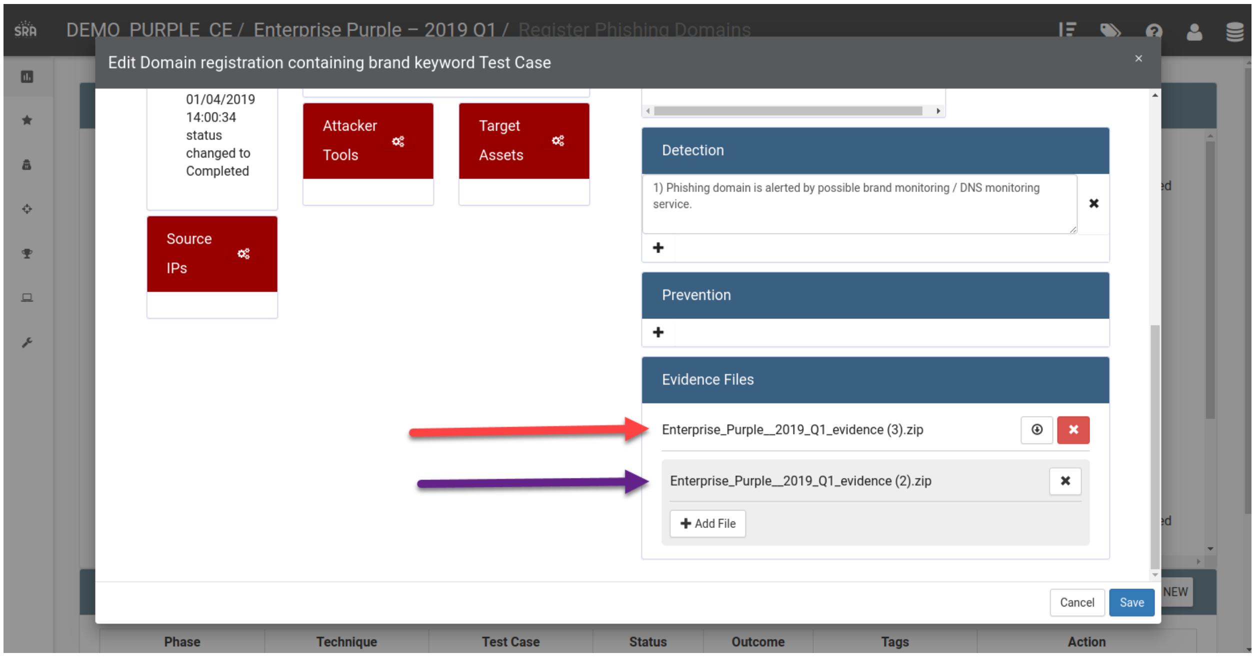
Test Case Evidence File Upload Improvements

What is it?

The VECTR Test Case Evidence File upload interface has been modified for better usability.

How does it work?

In the screenshot below, an existing Evidence File is shown next to the red arrow. A file to be uploaded is shown next to the purple arrow. Clicking save will upload the file in the Add File box and a progress bar will be shown.



DEMO_PURPLE_CE / Enterprise Purple – 2019 Q1 / Register Phishing Domains

Edit Domain registration containing brand keyword Test Case

01/04/2019 14:00:34 status changed to Completed

Detection

1) Phishing domain is alerted by possible brand monitoring / DNS monitoring service.

Evidence Files

Enterprise_Purple__2019_Q1_evidence (3).zip

Enterprise_Purple__2019_Q1_evidence (2).zip

How can this feature help me?

This improvement makes it easier to interact with Evidence Files in the Test Case view.

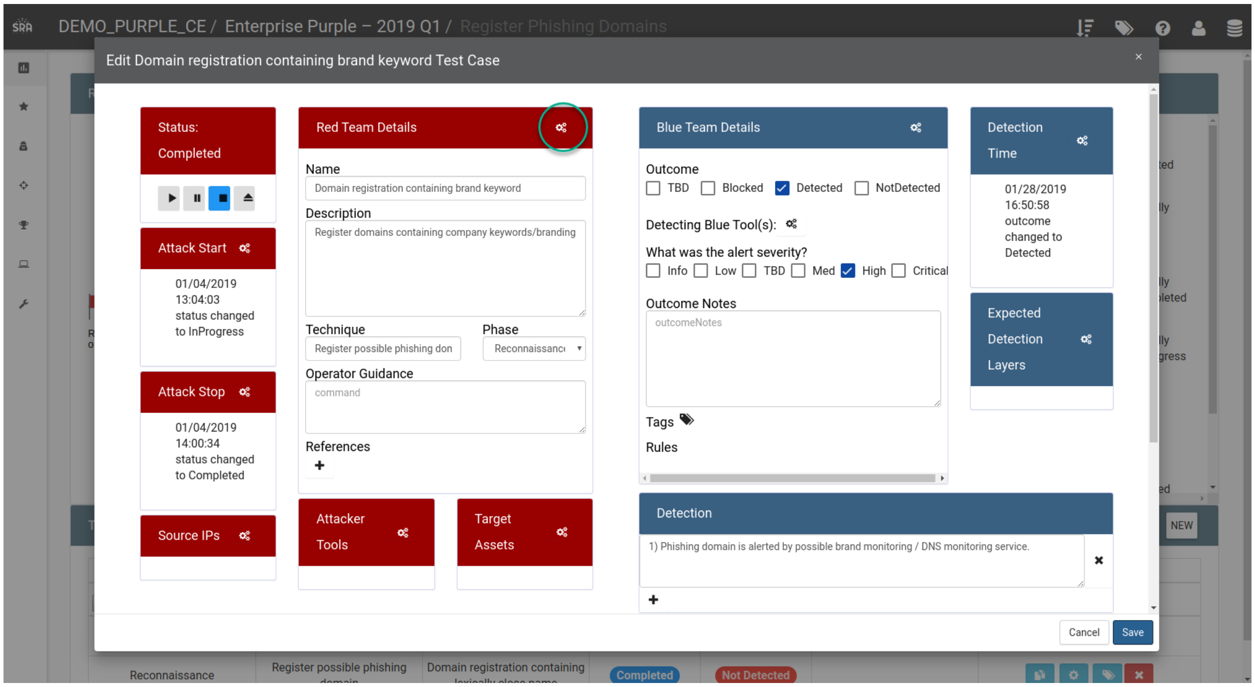
Test Case Icons Additional Support

What is it?

VECTR now supports adding additional or custom icons for Test Cases to display in the Escalation Path on the Campaign view.

How does it work?

For now, you will need access to the VECTR deployment environment to use this feature. You can put new icons in VECTR deployment directory path under app/static/icons. Icons should be in SVG format. You may place new icons in this directory. We highly recommend keeping the existing icons in the folder. Many existing Test Cases rely on bundled icons.



DEMO_PURPLE_CE / Enterprise Purple – 2019 Q1 / Register Phishing Domains

Edit Domain registration containing brand keyword Test Case

Status: Completed

Red Team Details

Name: Domain registration containing brand keyword

Description: Register domains containing company keywords/branding

Technique: Register possible phishing don

Phase: Reconnaissance

Operator Guidance: command

References

Attack Start

01/04/2019 13:04:03 status changed to InProgress

Attack Stop

01/04/2019 14:00:34 status changed to Completed

Source IPs

Attacker Tools

Target Assets

Blue Team Details

Outcome

□ TBD □ Blocked ☑ Detected □ NotDetected

Detecting Blue Tool(s):

What was the alert severity?

□ Info □ Low □ TBD □ Med ☑ High □ Critical

Outcome Notes: outcomeNotes

Tags

Rules

Detection Time

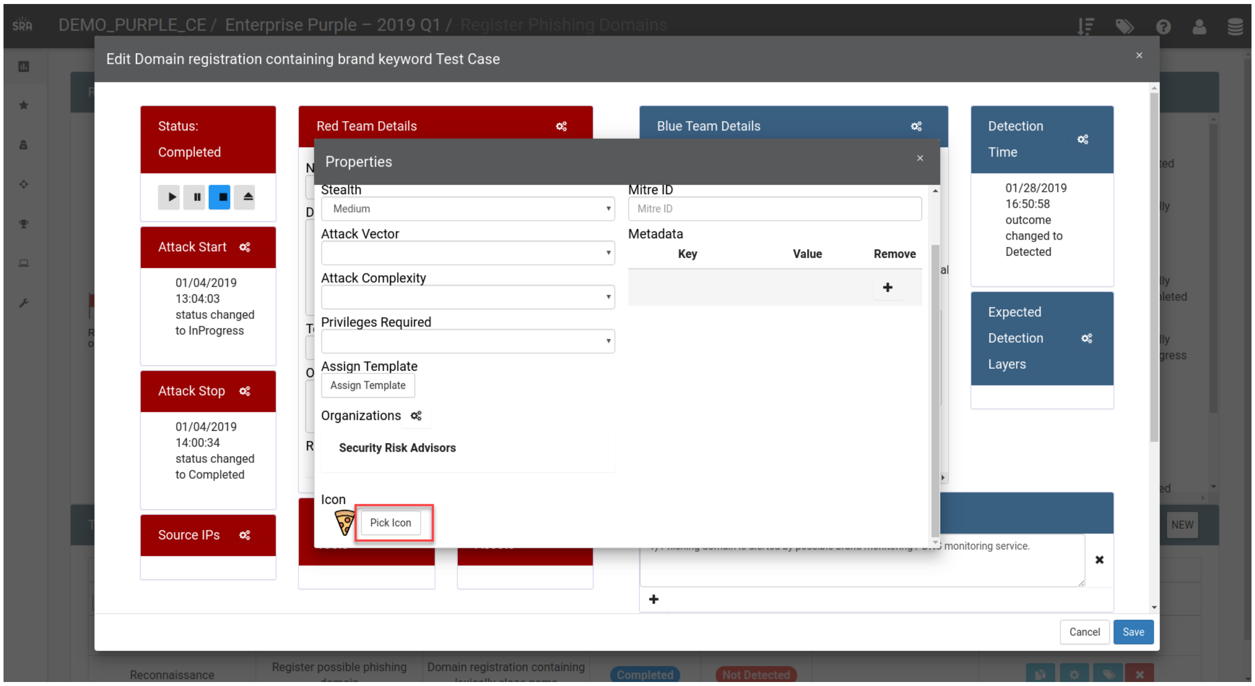
01/28/2019 16:50:58 outcome changed to Detected

Expected Detection Layers

Detection

1) Phishing domain is alerted by possible brand monitoring / DNS monitoring service.

Cancel
Save
Reconnaissance
Register possible phishing domain
Domain registration containing lexically close name
Completed
Not Detected
NEW



DEMO_PURPLE_CE / Enterprise Purple – 2019 Q1 / Register Phishing Domains

Edit Domain registration containing brand keyword Test Case

Status: Completed

Attack Start

01/04/2019 13:04:03 status changed to InProgress

Attack Stop

01/04/2019 14:00:34 status changed to Completed

Source IPs

Red Team Details

Blue Team Details

Detection Time

01/28/2019 16:50:58 outcome changed to Detected

Expected Detection Layers

Properties

Stealth: Medium

Mitre ID: Mitre ID

Attack Vector

Metadata

Key	Value	Remove

Attack Complexity

Privileges Required

Assign Template: Assign Template

Organizations

Security Risk Advisors

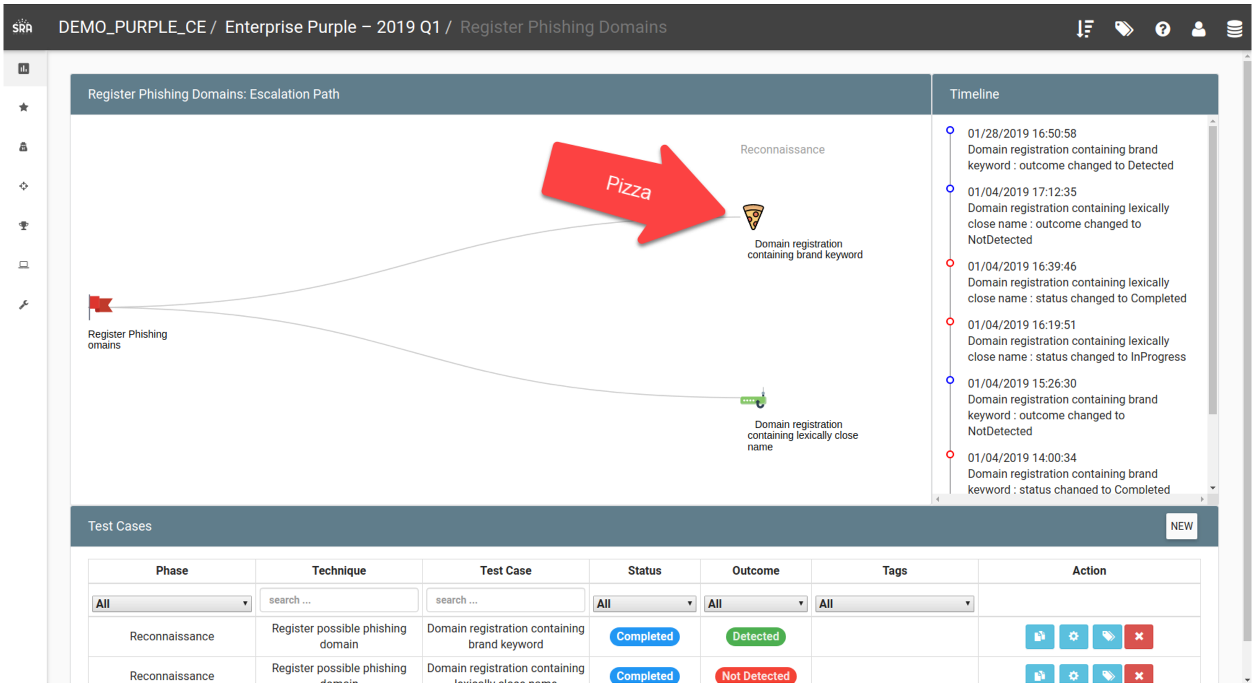
Icon

Pick Icon

monitoring service.

Cancel Save

Reconnaissance	Register possible phishing domain	Domain registration containing lexically close name	Completed	Not Detected



DEMO_PURPLE_CE / Enterprise Purple – 2019 Q1 / Register Phishing Domains

Register Phishing Domains: Escalation Path

Pizza
Reconnaissance
Domain registration containing brand keyword
Register Phishing omains
Domain registration containing lexically close name

Timeline

01/28/2019 16:50:58 Domain registration containing brand keyword : outcome changed to Detected

01/04/2019 17:12:35 Domain registration containing lexically close name : outcome changed to NotDetected

01/04/2019 16:39:46 Domain registration containing lexically close name : status changed to Completed

01/04/2019 16:19:51 Domain registration containing lexically close name : status changed to InProgress

01/04/2019 15:26:30 Domain registration containing brand keyword : outcome changed to NotDetected

01/04/2019 14:00:34 Domain registration containing brand keyword : status changed to Completed

Test Cases NEW

Phase	Technique	Test Case	Status	Outcome	Tags	Action
All	search ...	search ...	All	All	All	
Reconnaissance	Register possible phishing domain	Domain registration containing brand keyword	Completed	Detected		
Reconnaissance	Register possible phishing domain	Domain registration containing lexically close name	Completed	Not Detected		

How can this feature help me?

This feature allows you to customize escalation path icons in more detail which may be desirable when testing web applications in depth, industrial control systems, physical hardware, or other company-specific assets.

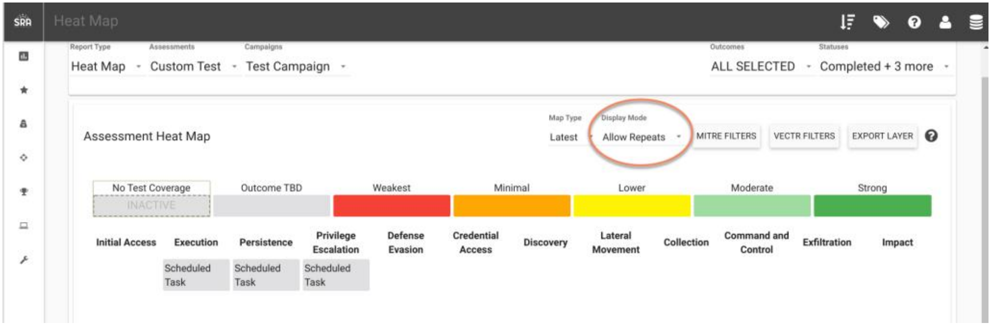
Heat Map Technique Duplications Filter

What is it?

VECTR now supports the ability to align your custom Phases to MITRE Tactics. There is a filter in the Heat Map that will align not only the Technique, but the Tactic as well to eliminate duplicate entries.

How does it work?

Assume you have a TestCase that is of a Phase (Social Engineering) that is not a MITRE Tactic. You set the MitreID field to T1053. If you set the Allow Repeats Display Mode, the Test Case will show up in all Techniques = T1053:



Report Type: Heat Map
Assessments: Custom Test
Campaigns: Test Campaign
Outcomes: ALL SELECTED
Statuses: Completed + 3 more

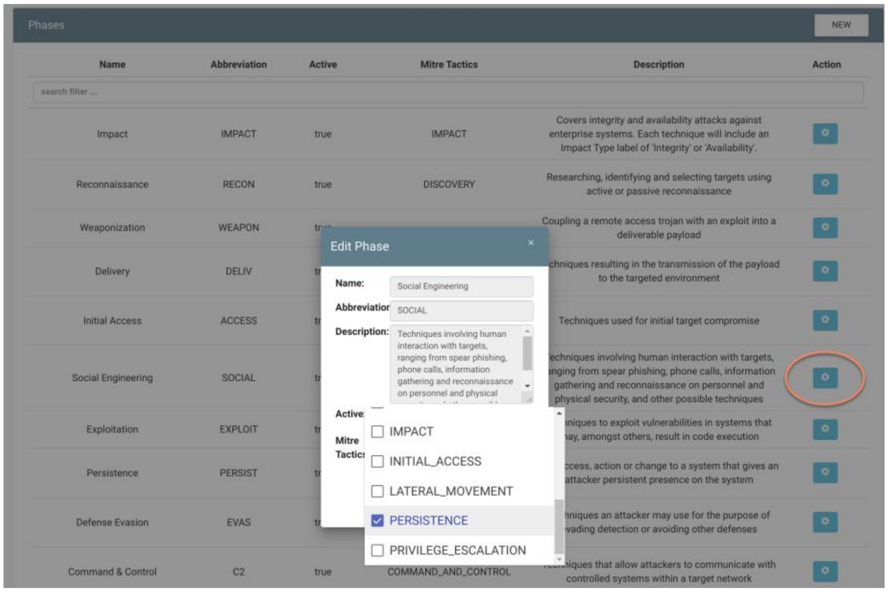
Assessment Heat Map

Map Type: Latest
Display Mode: Allow Repeats

No Test Coverage	Outcome TBD	Weakest	Minimal	Lower	Moderate	Strong
INACTIVE	⬜	🟥	🟧	🟨	🟩	🟩

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	Scheduled Task	Scheduled Task	Scheduled Task								

If you want all Phases of Social Engineering to show up only under Persistence, then you can go to the Admin -> Phases screen, then edit the Social Engineering Phase by clicking the cog. You can then set the Mitre Tactics to PERSISTENCE.



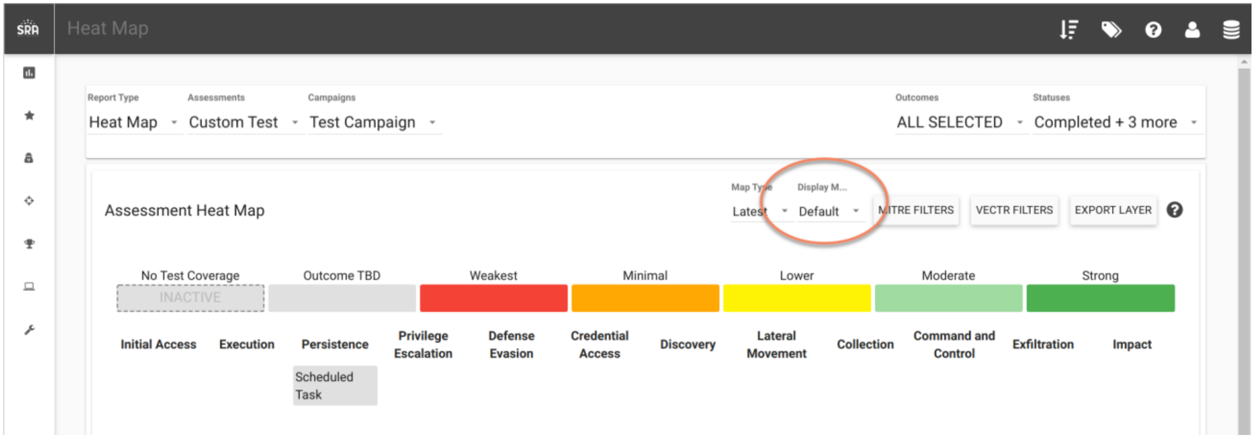
Name	Abbreviation	Active	Mitre Tactics	Description	Action
Impact	IMPACT	true	IMPACT	Covers integrity and availability attacks against enterprise systems. Each technique will include an Impact Type label of 'Integrity' or 'Availability'.	⚙
Reconnaissance	RECON	true	DISCOVERY	Researching, identifying and selecting targets using active or passive reconnaissance	⚙
Weaponization	WEAPON	tr		Coupling a remote access trojan with an exploit into a deliverable payload	⚙
Delivery	DELIV	tr		chniques resulting in the transmission of the payload to the targeted environment	⚙
Initial Access	ACCESS	tr		Techniques used for initial target compromise	⚙
Social Engineering	SOCIAL	tr		echniques involving human interaction with targets, nging from spear phishing, phone calls, information gathering and reconnaissance on personnel and physical security, and other possible techniques	⚙
Exploitation	EXPLOIT	tr		niques to exploit vulnerabilities in systems that ay, amongst others, result in code execution	⚙
Persistence	PERSIST	tr		ccess, action or change to a system that gives an attacker persistent presence on the system	⚙
Defense Evasion	EVAS	tr		niques an attacker may use for the purpose of vading detection or avoiding other defenses	⚙
Command & Control	C2	true	COMMAND_AND_CONTROL	iques that allow attackers to communicate with controlled systems within a target network	⚙

Edit Phase ×

Name: Social Engineering
Abbreviatior SOCIAL
Description: Techniques involving human interaction with targets, ranging from spear phishing, phone calls, information gathering and reconnaissance on personnel and physical
Active
Mitre Tactics

- ☐ IMPACT
- ☐ INITIAL_ACCESS
- ☐ LATERAL_MOVEMENT
- ☑ PERSISTENCE
- ☐ PRIVILEGE_ESCALATION

Going back to the Heat Map, you can set the Display Mode to “Default” to eliminate the duplicates.



Heat Map

Report Type: Heat Map
Assessments: Custom Test
Campaigns: Test Campaign
Outcomes: ALL SELECTED
Statuses: Completed + 3 more

Assessment Heat Map

Map Type: Latest
Display M...: Default

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		Scheduled Task									

How can this feature help me?

This feature allows you to more granularly align Test Cases to the Heat Map and eliminate duplicates.