

VECTR v5.5 Feature Breakdown

Table of Contents

- Assessments and Campaigns - Add Permalinks..... 2
- Campaign Dashboard - New Campaign Button 3
- Cloning Data - Test Cases - Automatically order cloned item below original 4
- Dependency Updates, Installation Improvements & Security Updates 5
- Filter Options - Usability - Checkbox improvements and Select All 6
- Source IPs and Target Assets - Select all Phases by Default 8
- Tags - Stale tag cleanup 9
- Test Case Panel - Multi-user support 11
- Vendors, Tools, and Defensive Layers - Import from Templates/Administration to Local DBs 13

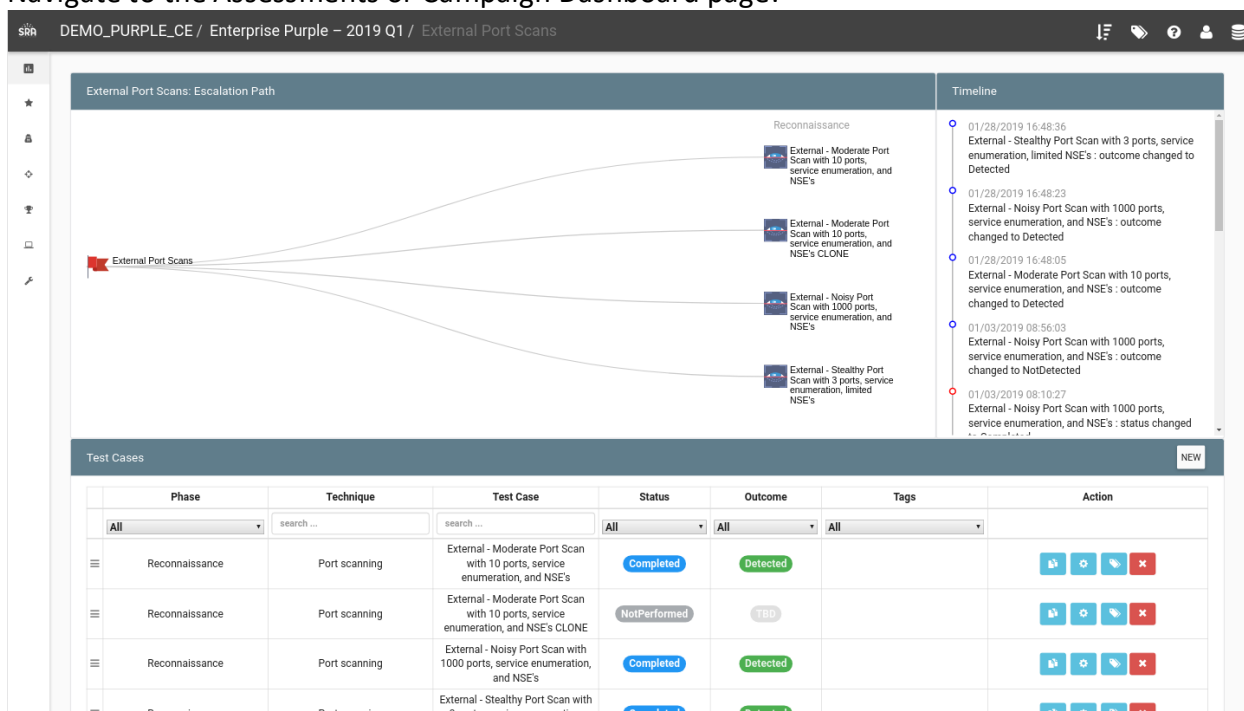
Assessments and Campaigns - Add Permalinks

What is it?

Permalinks have been added to VECTR's Assessment view and Campaign Dashboard to make it easier to share locations in VECTR.

How does it work?

Navigate to the Assessments or Campaign Dashboard page:



Note a URL like the following:

https://sravectr.internal:8081/sra-purpletools-webui/app/#/app/DEMO_PURPLE_CE/f7d28cb1-dd8c-4e73-bf7f-f405e94c8c0c/7704e34e-bb4b-44e2-8b17-4a847039a2c4

How can this feature help me?

It is now easier to share locations in your VECTR instance with other users.

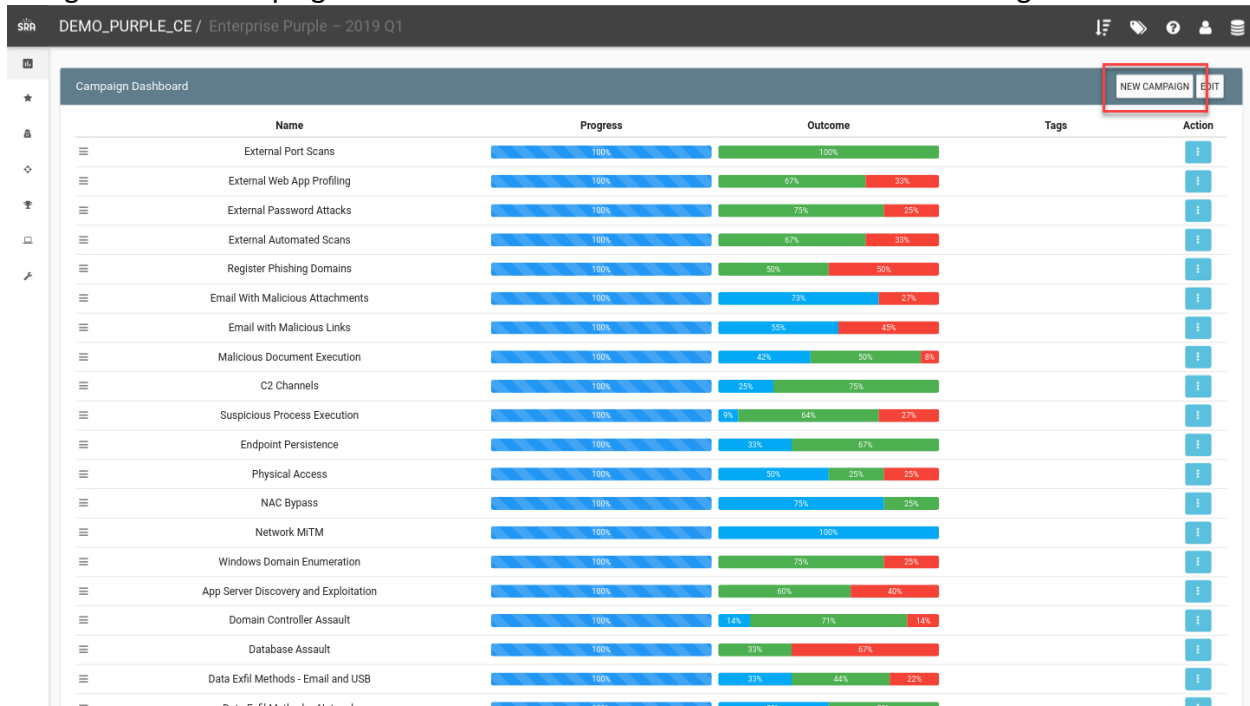
Campaign Dashboard - New Campaign Button

What is it?

A “New Campaign” button was added to the Campaign Dashboard since it was previously impossible to add new campaigns from this screen.

How does it work?

Navigate to the Campaign Dashboard screen and note the user interface change:



How can this feature help me?

Users can add new Campaigns from the Campaign Dashboard, improving the workflow of Purple Team operators.

Cloning Data - Test Cases - Automatically order cloned item below original













What is it?

When cloning Test Cases in VECTR versions prior to 5.5, newly cloned Test Cases would be placed at the very bottom of the list. Now, cloned Test Cases are ordered beneath the original data from which they're cloned.

How does it work?

Cloning a Test Case now places the clone directly beneath the original:

The screenshot displays the VECTR interface. At the top, a breadcrumb trail reads: DEMO_PURPLE_CE / Enterprise Purple – 2019 Q1 / External Port Scans. A notification bar states: Successfully set TestCases order. Below this, a diagram titled 'External Port Scans: Escalation Path' shows a red flag icon labeled 'External Port Scans' with four lines connecting to four separate test case entries. These entries are: 'External - Moderate Port Scan with 10 ports, service enumeration, and NSE's', 'External - Moderate Port Scan with 10 ports, service enumeration, and NSE's CLONE', 'External - Noisy Port Scan with 1000 ports, service enumeration, and NSE's', and 'External - Stealthy Port Scan with 3 ports, service enumeration, limited NSE's'. To the right of the diagram is a 'Timeline' section with five entries, each with a date and time, and a description of the test case outcome. Below the diagram is a 'Test Cases' table. The table has columns: Phase, Technique, Test Case, Status, Outcome, Tags, and Action. The first row is highlighted with a red box, showing a 'Reconnaissance' phase, 'Port scanning' technique, and a 'Completed' status. The second row is also highlighted with a red box, showing a 'Reconnaissance' phase, 'Port scanning' technique, and a 'NotPerformed' status. The third row shows a 'Reconnaissance' phase, 'Port scanning' technique, and a 'Completed' status. The fourth row shows a 'Reconnaissance' phase, 'Port scanning' technique, and a 'Completed' status. The 'Action' column contains icons for cloning, editing, deleting, and other actions.

Phase	Technique	Test Case	Status	Outcome	Tags	Action
Reconnaissance	Port scanning	External - Moderate Port Scan with 10 ports, service enumeration, and NSE's	Completed	Detected		  
Reconnaissance	Port scanning	External - Moderate Port Scan with 10 ports, service enumeration, and NSE's CLONE	NotPerformed	TBD		  
Reconnaissance	Port scanning	External - Noisy Port Scan with 1000 ports, service enumeration, and NSE's	Completed	Detected		  
Reconnaissance	Port scanning	External - Stealthy Port Scan with 3 ports, service enumeration, limited NSE's	Completed	Detected		  

How can this feature help me?

This usability improvement makes it easier to find newly cloned data.

Dependency Updates, Installation Improvements & Security Updates

What is it?

VECTR application dependencies and source code have been updated to improve security and ease the installation process.

How does it work?

The following and more items have been updated in this release:

- MongoDB 3.4 to 4.2
- MongoDB password protection
- VECTR application now available on DockerHub
- Dockerization aligned with industry standards
- CAS 5.x to 6.1.3
- VECTR Application Security Updates

How can this feature help me?

These updates improve application security, performance, ease of installation & maintenance, and prepare the application for enterprise feature upgrades in the future.

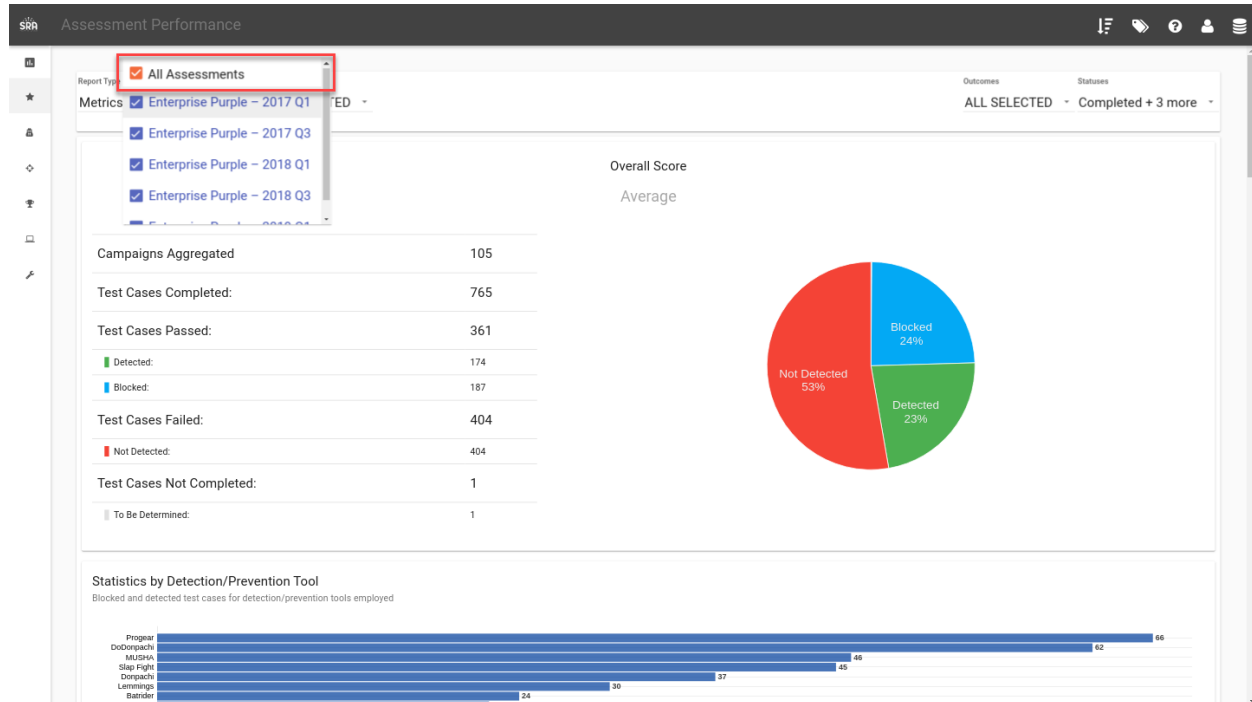
Filter Options - Usability - Checkbox improvements and Select All

What is it?

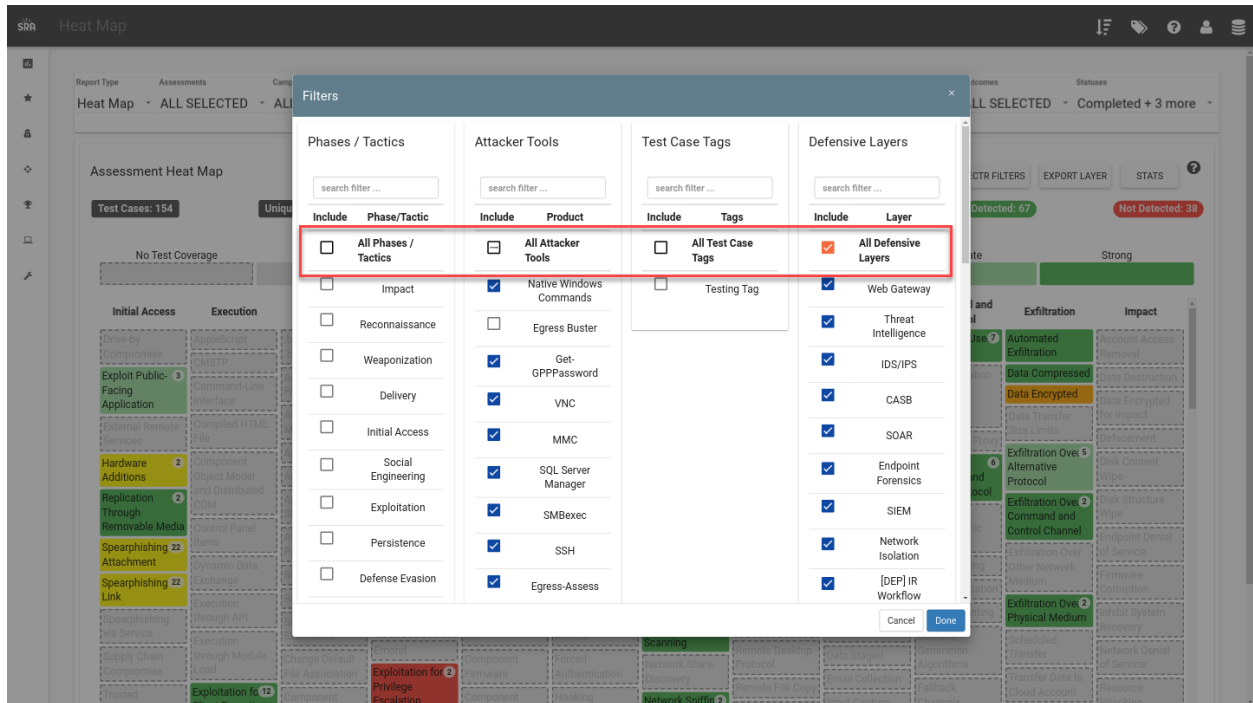
Selection controls on various filters were improved to include a “Select All” option. Additionally, it is now possible to sort long checklists by checked/unchecked to determine which items a user has selected.

How does it work?

Note “All Assessments” and other “Select All” type buttons on the Reporting view.



VECTR filters on the heatmap now shows a “Select All” type button for each filter type.



How can this feature help me?

Filter option data is now easier to use.

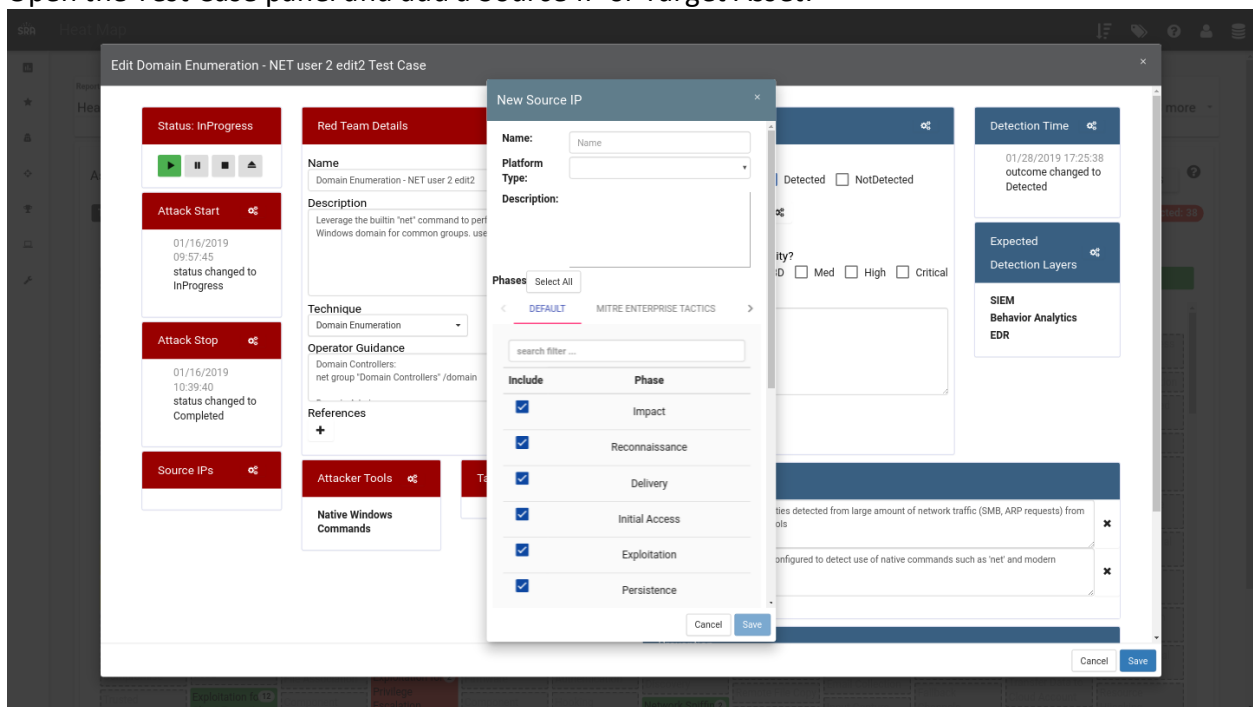
Source IPs and Target Assets - Select all Phases by Default

What is it?

When adding a Source IP or Target Asset to a Test Case, all Phases are now selected by default.

How does it work?

Open the Test Case panel and add a Source IP or Target Asset:



How can this feature help me?

Prior to version 5.5, if you did not select additional Phases for a Source IP or Target Asset, it may not have been visible in other Test Cases except for those in the same Kill Chain Phase. This now defaults to including all Phases.

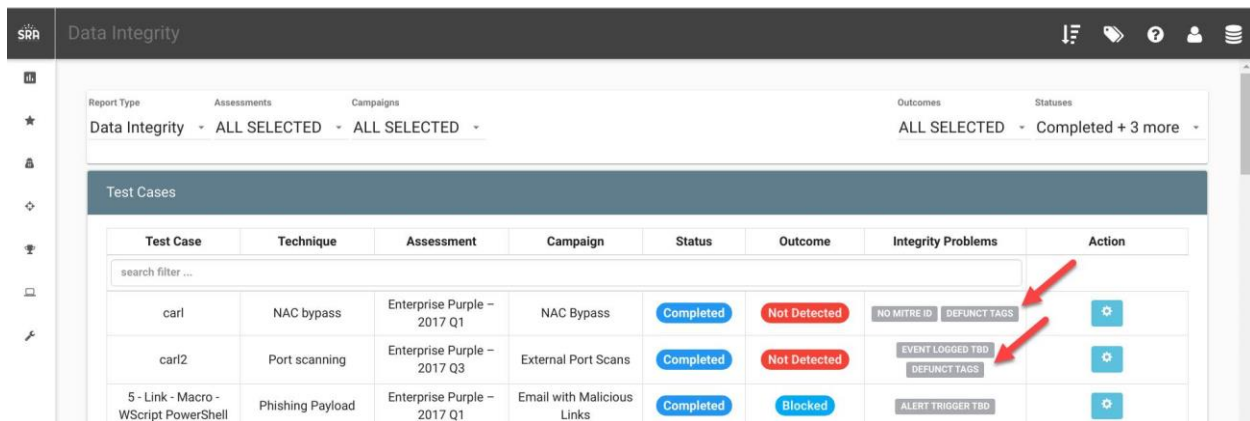
Tags - Stale tag cleanup

What is it?

Tags that are removed from the Administration section but may still be referenced in local database Test Cases can be cleaned up through the UI.

How does it work?

View the Data Integrity report to see if any tags are missing or orphaned (Note “DEFUNCT TAGS” label):



The screenshot shows the 'Data Integrity' report interface. At the top, there are filters for Report Type (Data Integrity), Assessments (ALL SELECTED), Campaigns (ALL SELECTED), Outcomes (ALL SELECTED), and Statuses (Completed + 3 more). Below the filters is a 'Test Cases' section with a table. The table has columns: Test Case, Technique, Assessment, Campaign, Status, Outcome, Integrity Problems, and Action. The table contains three rows of test cases. The first row, 'carl', has a status of 'Completed' and an outcome of 'Not Detected'. The 'Integrity Problems' column for this row shows 'NO MITRE ID' and 'DEFUNCT TAGS'. The second row, 'carl2', has a status of 'Completed' and an outcome of 'Not Detected'. The 'Integrity Problems' column for this row shows 'EVENT LOGGED TBD' and 'DEFUNCT TAGS'. The third row, '5 - Link - Macro - WScript PowerShell', has a status of 'Completed' and an outcome of 'Blocked'. The 'Integrity Problems' column for this row shows 'ALERT TRIGGER TBD'. Red arrows point to the 'DEFUNCT TAGS' labels in the first two rows.

Test Case	Technique	Assessment	Campaign	Status	Outcome	Integrity Problems	Action
carl	NAC bypass	Enterprise Purple – 2017 Q1	NAC Bypass	Completed	Not Detected	NO MITRE ID DEFUNCT TAGS	
carl2	Port scanning	Enterprise Purple – 2017 Q3	External Port Scans	Completed	Not Detected	EVENT LOGGED TBD DEFUNCT TAGS	
5 - Link - Macro - WScript PowerShell	Phishing Payload	Enterprise Purple – 2017 Q1	Email with Malicious Links	Completed	Blocked	ALERT TRIGGER TBD	

From the Administration -> Tagging screen you can click “Run Defunct Report”

Tagging Management			
	Name	Collection	Action
	test1	TestCases	+ x
	test2	TestCases	+ x
	test3	TestCases	+ x
	attack.execution	GenericRules	+ x
	attack.credential_access	GenericRules	+ x
	attack.persistence	GenericRules	+ x
	attack.lateral_movement	GenericRules	+ x
	attack.discovery	GenericRules	+ x
	attack.privilege_escalation	GenericRules	+ x
	attack.command_and_control	GenericRules	+ x
	attack.defense_evasion	GenericRules	+ x
<div> <div>Run Defunct Report</div> </div>			
ID		Collection	Action
bad-tag-3		TestCases	x
bad-tag-2		TestCases	x
bad-tag-1		TestCases	x
<div> <div>Clean All Defunct</div> </div>			

Clicking the red X or clearing all defunct tags will remove bad references from VECTR data.

How can this feature help me?

If a VECTR instance has missing or orphaned tags, data can now be corrected in the UI to prevent reporting or user interface errors.

Test Case Panel - Multi-user support

What is it?

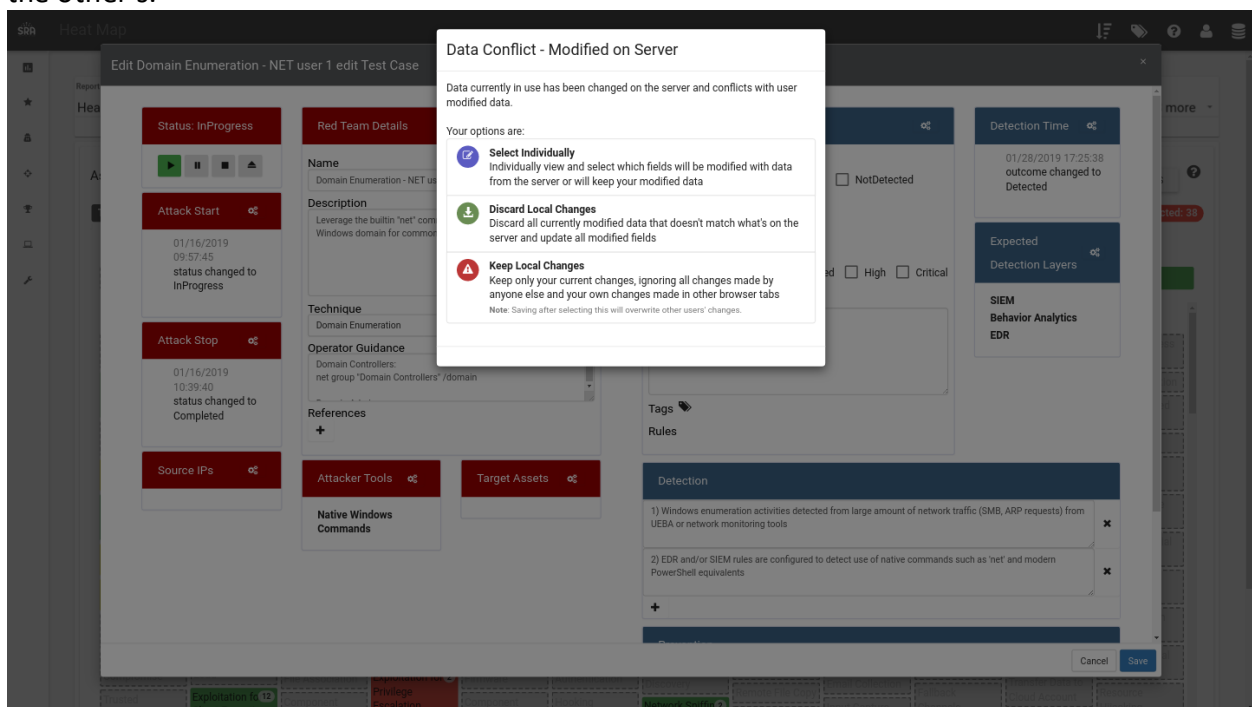
Functionality has been added to make it easier for multiple users to work at the same time in a single Test Case and prevent overwriting the other's data.

How does it work?

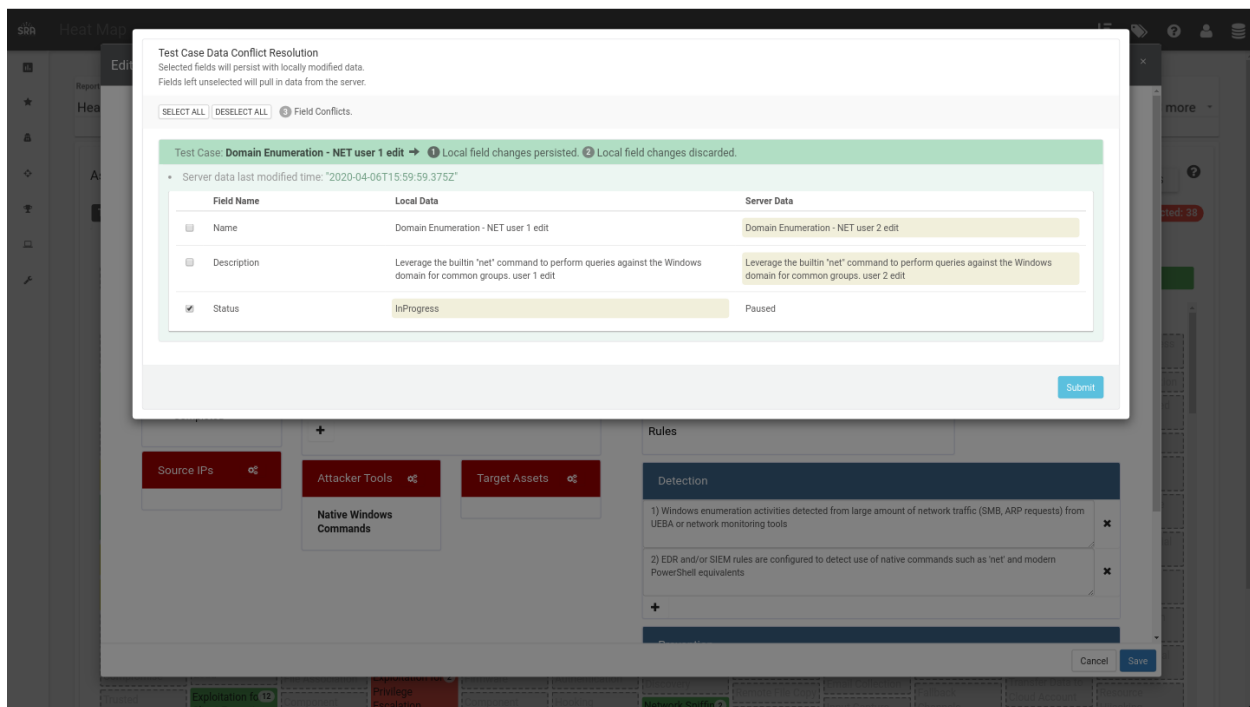
The Test Case panel polls every 20 second to get updates from the server.

If User 1 saves changes to the Test Case while User 2 has open the same Test Case panel but has not modified any data that User 1 has changed, the Test Case panel will automatically update and show an animation for the changed data.

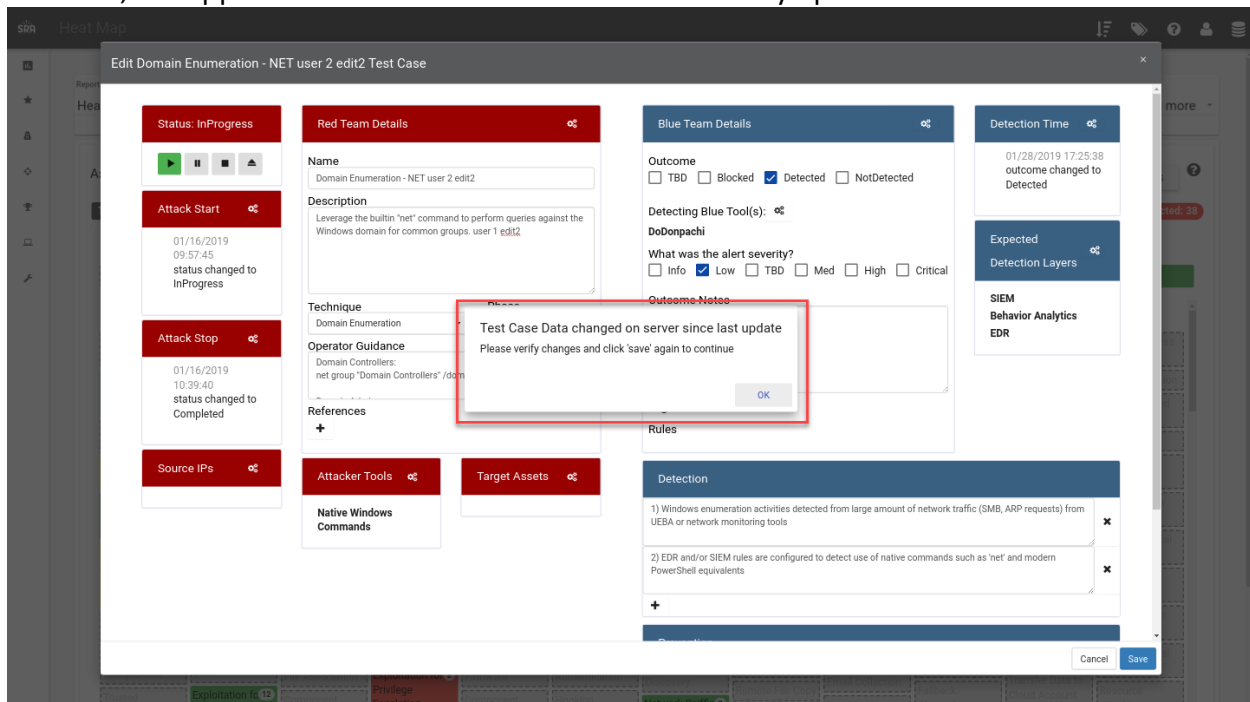
If User 1 saves changes to the Test Case while User 2 is editing the same data, the UI will display a dialog to resolve this data conflict manually or discard all of one user's changes and persist the other's.



The conflict resolution dialog allows you to view which changes are in conflict and select which you want to persist.



Additionally, if there are changes made on the server prior to saving and a user tries to save a test case, the application will warn the user and retrieve any updates.



How can this feature help me?

It is now possible for multiple users to concurrently work in the same Test Case without destroying the other's changes

Vendors, Tools, and Defensive Layers - Import from Templates/Administration to Local DBs

What is it?

This allows users to add data from the Administration section into local databases. This is important because on database creation, Administrative data is copied into a local database. After that event if a user adds data to the Administrative data it is not automatically copied into a local database. Now, users can manually import new data from Administrative data to a local database via the UI.

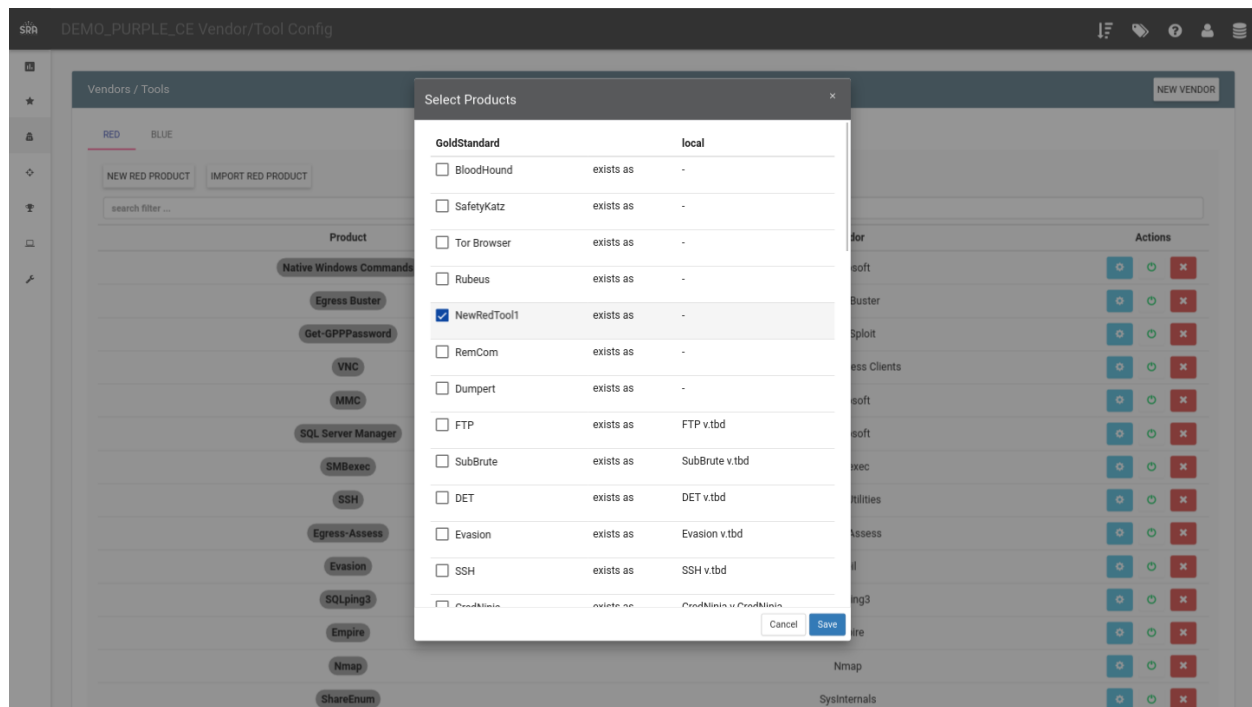
How does it work?

If Administration data is present in VECTR that does not exist in the current local database, there will be an import button on the corresponding data management page.

The screenshot shows the VECTR interface for managing Vendors and Tools. The page title is 'Vendors / Tools' and there is a 'NEW VENDOR' button in the top right. Below the title bar, there are tabs for 'RED' and 'BLUE'. Under the 'RED' tab, there are two buttons: 'NEW RED PRODUCT' and 'IMPORT RED PRODUCT'. The 'IMPORT RED PRODUCT' button is highlighted with a red rectangle. Below these buttons is a search filter input. The main content area is a table with columns: Product, Vendor, and Actions. The table lists various products and their corresponding vendors, with action buttons (add, refresh, delete) for each row.

Product	Vendor	Actions
Native Windows Commands	Microsoft	[Add] [Refresh] [Delete]
Egress Buster	Egress Buster	[Add] [Refresh] [Delete]
Get-GPPPassword	PowerSploit	[Add] [Refresh] [Delete]
VNC	Remote Access Clients	[Add] [Refresh] [Delete]
MMC	Microsoft	[Add] [Refresh] [Delete]
SQL Server Manager	Microsoft	[Add] [Refresh] [Delete]
SMBExec	SMBExec	[Add] [Refresh] [Delete]
SSH	Native Utilities	[Add] [Refresh] [Delete]
Egress-Assess	Egress-Assess	[Add] [Refresh] [Delete]
Evasion	Veil	[Add] [Refresh] [Delete]
SQLping3	SQLping3	[Add] [Refresh] [Delete]
Empire	Empire	[Add] [Refresh] [Delete]
Nmap	Nmap	[Add] [Refresh] [Delete]
ShareEnum	SysInternals	[Add] [Refresh] [Delete]

Clicking the import data button will display data which is not present or differs in the local database:



How can this feature help me?

This feature makes it easier to keep the Administration section up to date with global data and import it into local databases as needed.