

# VECTR v5.7.0 Feature Breakdown

## Table of Contents

- Added support for Subtechniques in Heatmap ..... 2
- Label configuration in Heatmap ..... 4
- Added ability to identify isolated Test Cases when Assessment Kill Chain is changed ..... 6

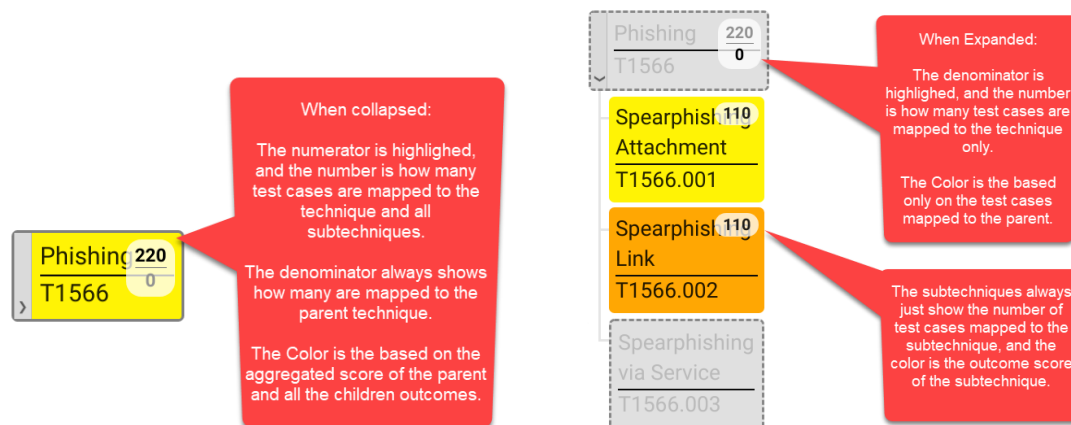
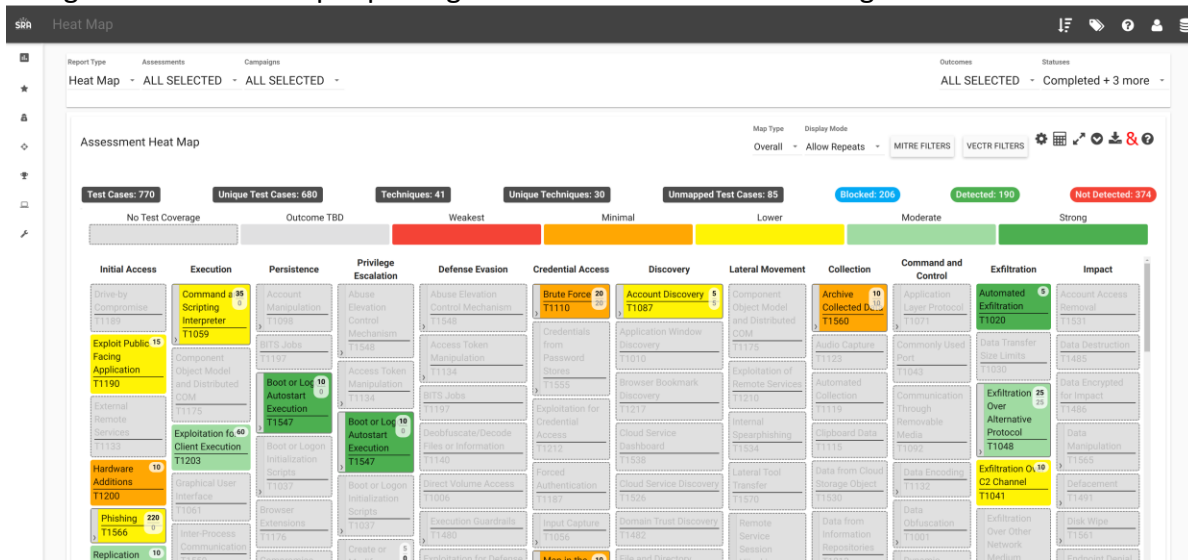
# Added support for Subtechniques in Heatmap

## What is it?

Subtechniques now show up in the Heatmap. Any existing datasets that use “legacy” techniques will be automatically mapped to subtechniques using the [mitre-crosswalk](#).

## How does it work?

Navigate to the Heatmap reporting screen. You will see something like this:



## How can this feature help me?

This will allow users to map test cases to subtechniques and visualize outcomes

## Additional Comments:

When there is a scenario where a legacy mitre id can map to multiple subtechniques, we take the first item in the list of the crosswalk file. For example, if a test case was mapped to mitre id T1034, it will now be mapped to T1574.007.

```
{
  "T1034": [
    {
      "id": "T1574.007",
      "explanation": "Deprecated and split into separate Unquoted Path, PATH Environment Variable, and Search Order Hijacking sub-techniques."
    },
    {
      "id": "T1574.008",
      "explanation": "Deprecated and split into separate Unquoted Path, PATH Environment Variable, and Search Order Hijacking sub-techniques."
    },
    {
      "id": "T1574.009",
      "explanation": "Deprecated and split into separate Unquoted Path, PATH Environment Variable, and Search Order Hijacking sub-techniques."
    }
  ],
  "change-type": "Became Multiple Sub-Techniques"
},
```

There are some cases where legacy ids have been deprecated:

```
{
  "T1051": [
    {
      "id": "N/A",
      "explanation": "Deprecated from ATT&CK due to lack of in the wild use"
    }
  ],
  "change-type": "Deprecated"
},
```

These will show up in the Data Integrity screen as “MITRE ID UNRECOGNIZED”

10 - Macro - MSBuild	Phishing Payload	Enterprise Purple – 2019 Q1	Email With Malicious Attachments	Completed	Blocked	MITRE ID UNRECOGNIZED	⚙
----------------------	------------------	-----------------------------	----------------------------------	-----------	---------	-----------------------	---

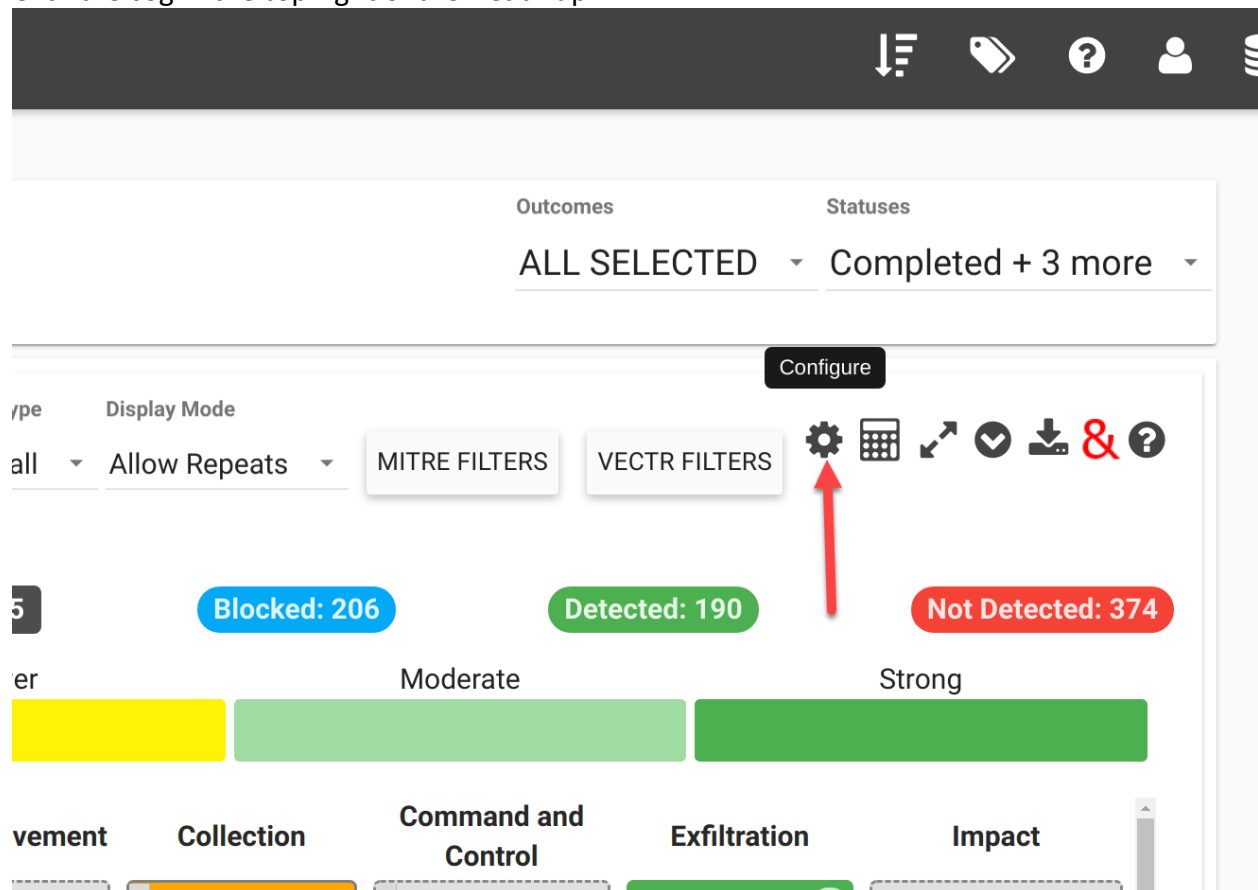
# Label configuration in Heatmap

## What is it?

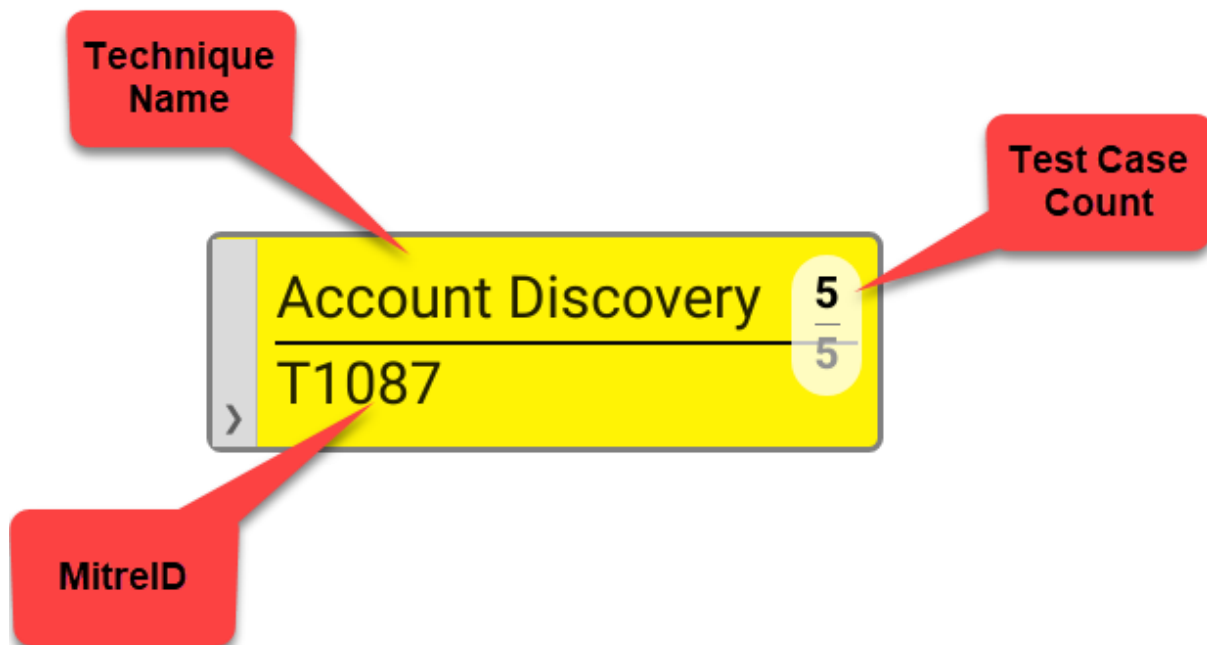
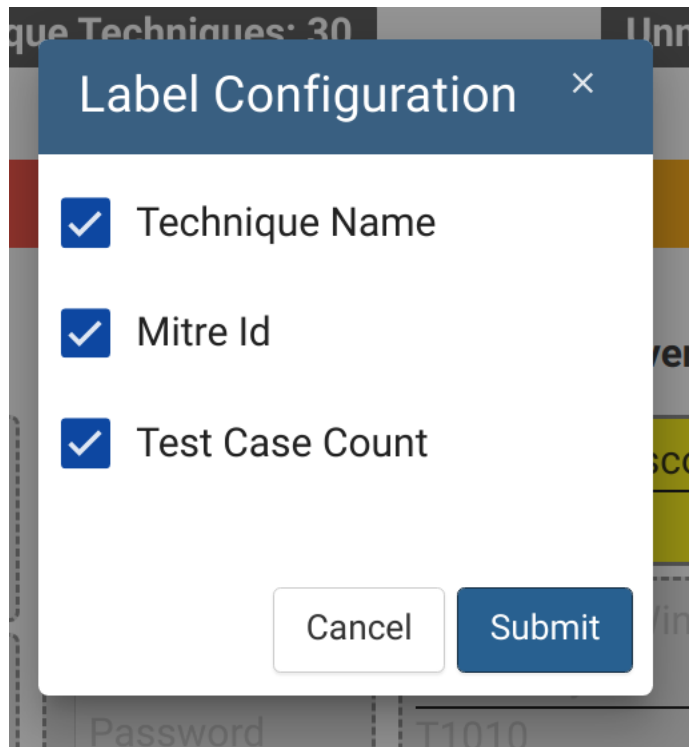
Allow for some customization of the labels that show up on the Heatmap.

## How does it work?

Click the cog in the top right of the Heatmap:



This will bring up the label config widget:



### How can this feature help me?

This will allow for screenshots or visuals to be customized.

# Added ability to identify isolated Test Cases when Assessment Kill Chain is changed

## What is it?

Test Cases that are used in a Campaign but are not mapped to the Assessment Kill Chain are now displayed in a warning screen when the Assessment Kill Chain is changed, and also show up in the Data Integrity reporting screen.

## How does it work?

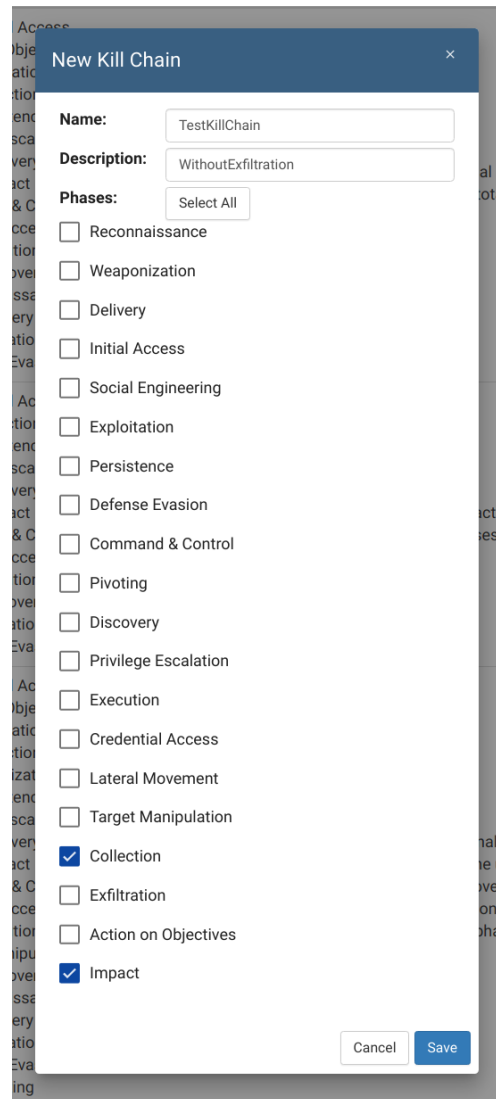
Here's an example of a campaign with 3 Test Cases mapped to Exfiltration

The screenshot displays the SRA interface for a campaign named 'demo / Data Exfil / Data Exfil'. The main view is titled 'Data Exfil: Escalation Path' and shows a diagram of the kill chain. A red flag icon labeled 'Data Exfil' is connected by three lines to three target icons: 'Extract data via Bluetooth', 'T1022 - Data Encrypted', and 'T1048 - Exfiltration Over Alternative Protocol - SSH'. The 'Exfiltration' phase is highlighted in the diagram. A 'Timeline' tab is visible on the right.

Below the diagram is a 'Test Cases' table with columns: Phase, Technique, Test Case, Status, Outcome, Tags, and Action. The table lists three test cases, all with a status of 'NotPerformed' and an outcome of 'TBD'. The 'Phase' column is highlighted with a red box.

Phase	Technique	Test Case	Status	Outcome	Tags	Action
All	search ...	search ...	All	All	All	
Exfiltration	Exfiltration Over Other Network Medium	Extract data via Bluetooth	NotPerformed	TBD		[Icons]
Exfiltration	Data Encrypted	T1022 - Data Encrypted	NotPerformed	TBD		[Icons]
Exfiltration	Exfiltration Over Alternative Protocol	T1048 - Exfiltration Over Alternative Protocol - SSH	NotPerformed	TBD		[Icons]

Create a Kill Chain without Exfiltration as a Phase:



A dialog box titled "New Kill Chain" with a close button (X) in the top right corner. It contains three input fields: "Name" with the value "TestKillChain", "Description" with the value "WithoutExfiltration", and "Phases" with a dropdown menu showing "Select All". Below these fields is a list of 20 phases, each with a checkbox. The phases are: Reconnaissance, Weaponization, Delivery, Initial Access, Social Engineering, Exploitation, Persistence, Defense Evasion, Command & Control, Pivoting, Discovery, Privilege Escalation, Execution, Credential Access, Lateral Movement, Target Manipulation, Collection (checked), Exfiltration, Action on Objectives, and Impact (checked). At the bottom right are "Cancel" and "Save" buttons.

**New Kill Chain**

**Name:** TestKillChain

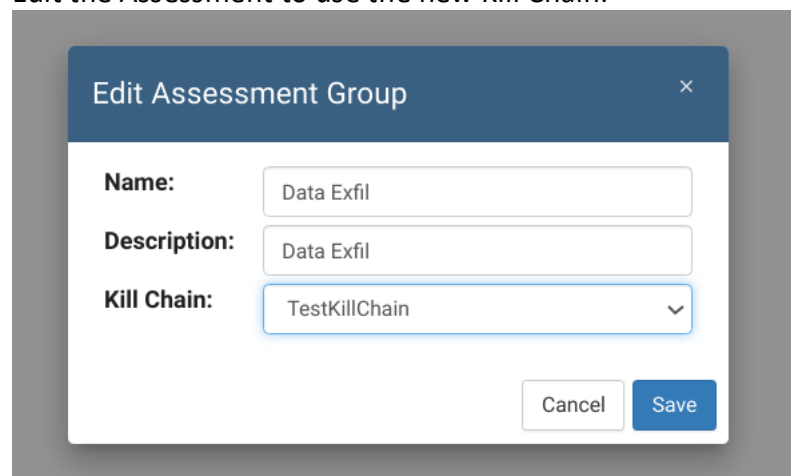
**Description:** WithoutExfiltration

**Phases:** Select All

- ☐ Reconnaissance
- ☐ Weaponization
- ☐ Delivery
- ☐ Initial Access
- ☐ Social Engineering
- ☐ Exploitation
- ☐ Persistence
- ☐ Defense Evasion
- ☐ Command & Control
- ☐ Pivoting
- ☐ Discovery
- ☐ Privilege Escalation
- ☐ Execution
- ☐ Credential Access
- ☐ Lateral Movement
- ☐ Target Manipulation
- ☒ Collection
- ☐ Exfiltration
- ☐ Action on Objectives
- ☒ Impact

Cancel Save

Edit the Assessment to use the new Kill Chain:



A dialog box titled "Edit Assessment Group" with a close button (X) in the top right corner. It contains three input fields: "Name" with the value "Data Exfil", "Description" with the value "Data Exfil", and "Kill Chain" with a dropdown menu showing "TestKillChain". At the bottom right are "Cancel" and "Save" buttons.

**Edit Assessment Group**

**Name:** Data Exfil

**Description:** Data Exfil

**Kill Chain:** TestKillChain

Cancel Save

This will show a conflict report:

Conflict Report

The following phases are not in the "TestKillChain" kill chain. Test cases which belong to these phases will not appear in your assessment if you modify the kill chain. See the list of test cases below that will be effected by this change.

1 Campaigns

3 Total Test Cases

10 Phases

Privilege Escalation

Exfiltration

Defense Evasion

Discovery

Credential Access

Persistence

Lateral Movement

Execution

Initial Access

Command & Control

Campaign: Data Exfil → 3 Test Cases

Test Case: Extract data via Bluetooth | Phase: Exfiltration

Test Case: T1022 - Data Encrypted | Phase: Exfiltration

Test Case: T1048 - Exfiltration Over Alternative Protocol - SSH | Phase: Exfiltration

Click Continue to accept these changes. You can fix the orphaned test cases from the Data Integrity report page. Otherwise, click Cancel.

Cancel

Continue



The Campaign will now not show the Test Cases:

The screenshot shows the SRA interface for a campaign named 'Data Exfil'. The top navigation bar includes 'demo / Data Exfil / Data Exfil'. The main content area is divided into two panels: 'Data Exfil: Escalation Path' (active) and 'Timeline'. The 'Data Exfil: Escalation Path' panel shows a red flag icon labeled 'Data Exfil'. Below this, the 'Test Cases' section is visible, featuring a table with columns: Phase, Technique, Test Case, Status, Outcome, Tags, and Action. The table is currently empty, and a 'CAMPAIGN ACTIONS' button is located to the right of the table header.

You can go to the Data Integrity report to fix the issues:

The screenshot shows the SRA interface for the 'Data Integrity' report. The top navigation bar includes 'Data Integrity'. The main content area is divided into two panels: 'Data Integrity' (active) and 'Test Cases'. The 'Data Integrity' panel shows a table with columns: Report Type, Assessments, Campaigns, Outcomes, and Statuses. The table is currently empty. Below this, the 'Test Cases' section is visible, featuring a table with columns: Test Case, Technique, Assessment, Campaign, Status, Outcome, Integrity Problems, and Action. The table lists three test cases, all with a status of 'NotPerformed' and an outcome of 'TBD'. The 'Integrity Problems' column shows 'EXCLUDED BY ASSESSMENT KILLCHAIN' for each row. A red box highlights the 'Integrity Problems' column.

## How can this feature help me?

This will allow users to not “lose” data when changing a Kill Chain.