

# VECTR v5.1.2 Feature Breakdown

## Table of Contents

Reporting Screen .....	2
User Management .....	4
Tagging Management .....	6
System Flags .....	8

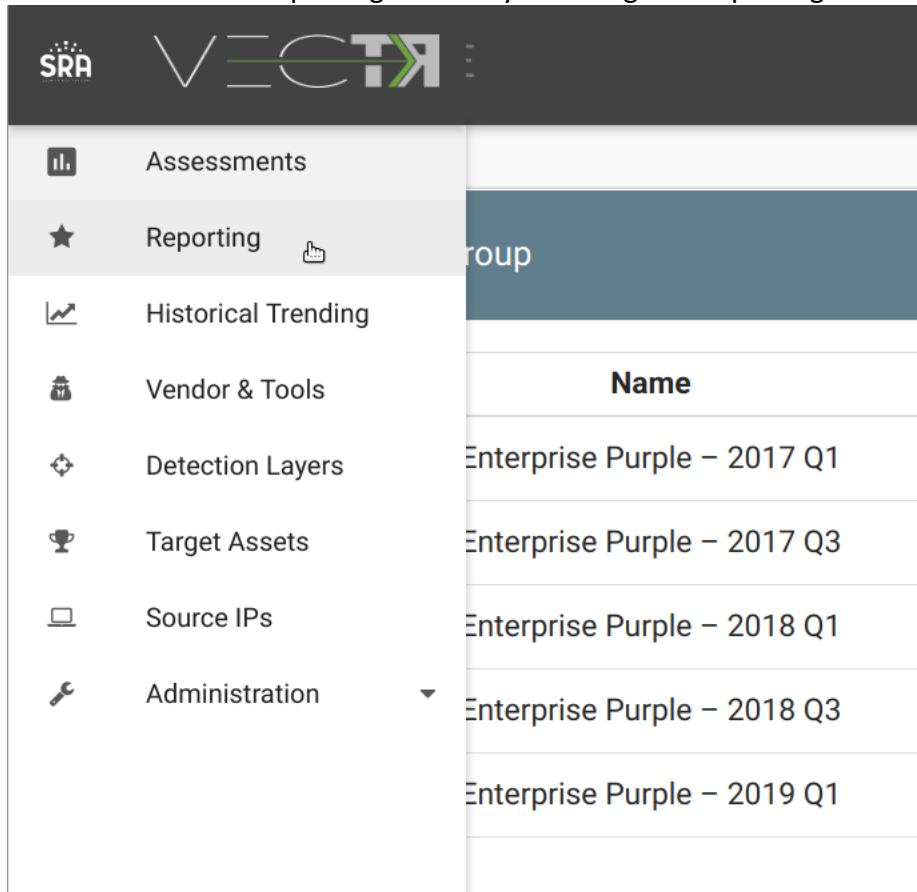
# Reporting Screen

## What is it?

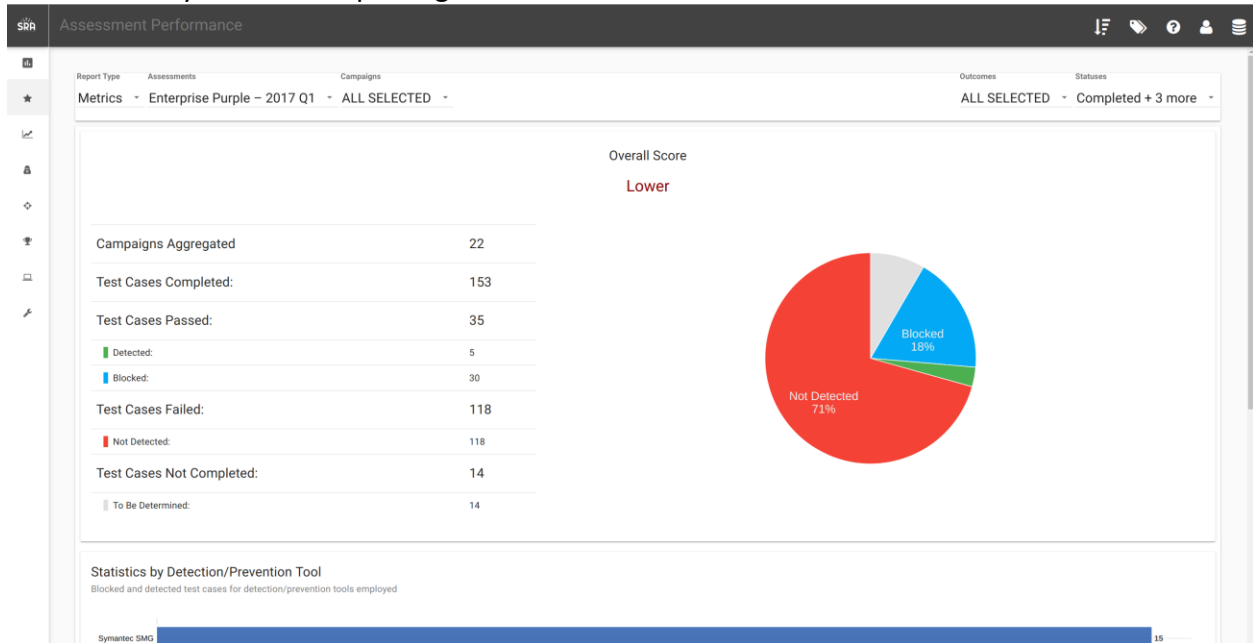
Single reporting view that allows you to cycle through reporting views and view aggregations of Assessments and Campaigns, along with filtering on status/outcomes.

## How does it work?

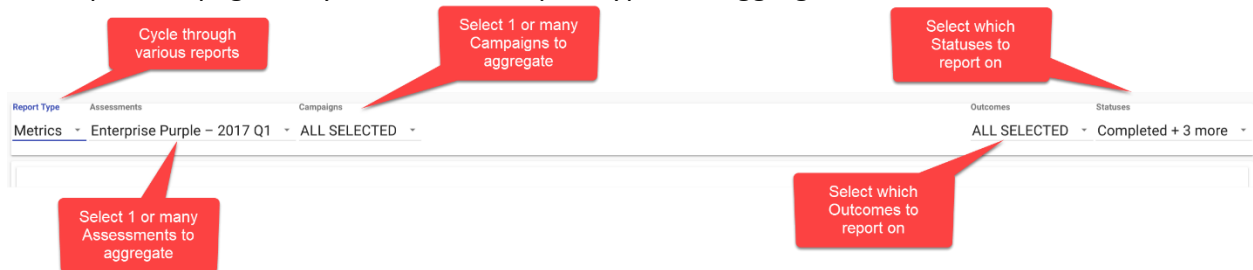
You can access the Reporting screen by selecting the Reporting tab on the Left Nav:



This will take you to the Reporting View:



The top of the page lets you select the report type and aggregate/filter data:



You can get to the Reporting screen with the proper Assessment selected by clicking the reporting icon in the Assessment Group selection screen:

Name	Type	Status	Actions
Enterprise Purple - 2017 Q1	Campaign	In Progress	[Icons]
Enterprise Purple - 2017 Q3	Campaign	Completed	[Icons]
Enterprise Purple - 2018 Q1	Campaign	Completed	[Icons]

You can get to the Reporting screen with the proper Assessment and Campaign selected by clicking the reporting icon in the Campaign selection screen:

Name	Type	Progress	Actions
External Web App Profiling	Campaign	100% / 100%	LOAD VIEW REPORT
External Password Attacks	Campaign	100% / 100%	LOAD VIEW REPORT
External Automated Scans	Campaign	100% / 32% / 67%	LOAD VIEW REPORT
Register Phishing Domains	Campaign	100% / 100%	LOAD VIEW REPORT

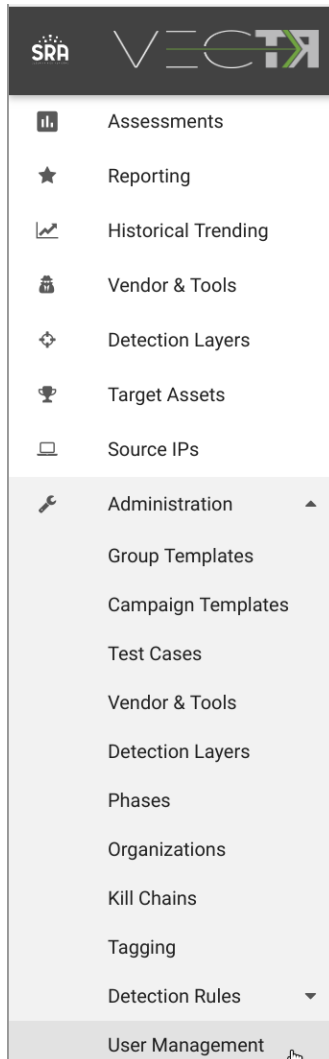
# User Management

## What is it?

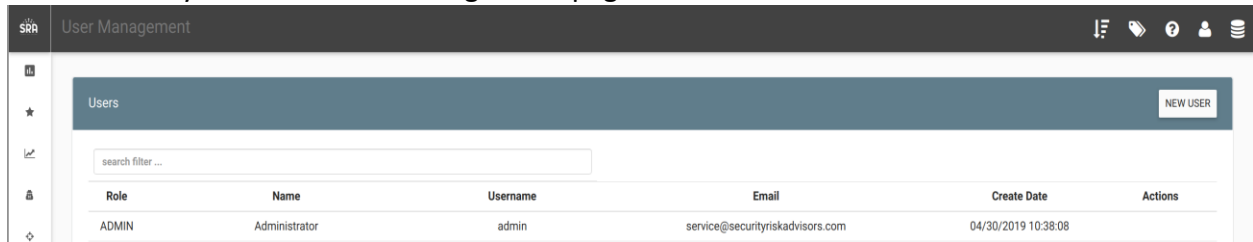
Allows for an ADMIN to add users with either the Role of USER or ADMIN. Users with USER will be able to use the platform, but not create users or escalate Roles.

## How does it work?

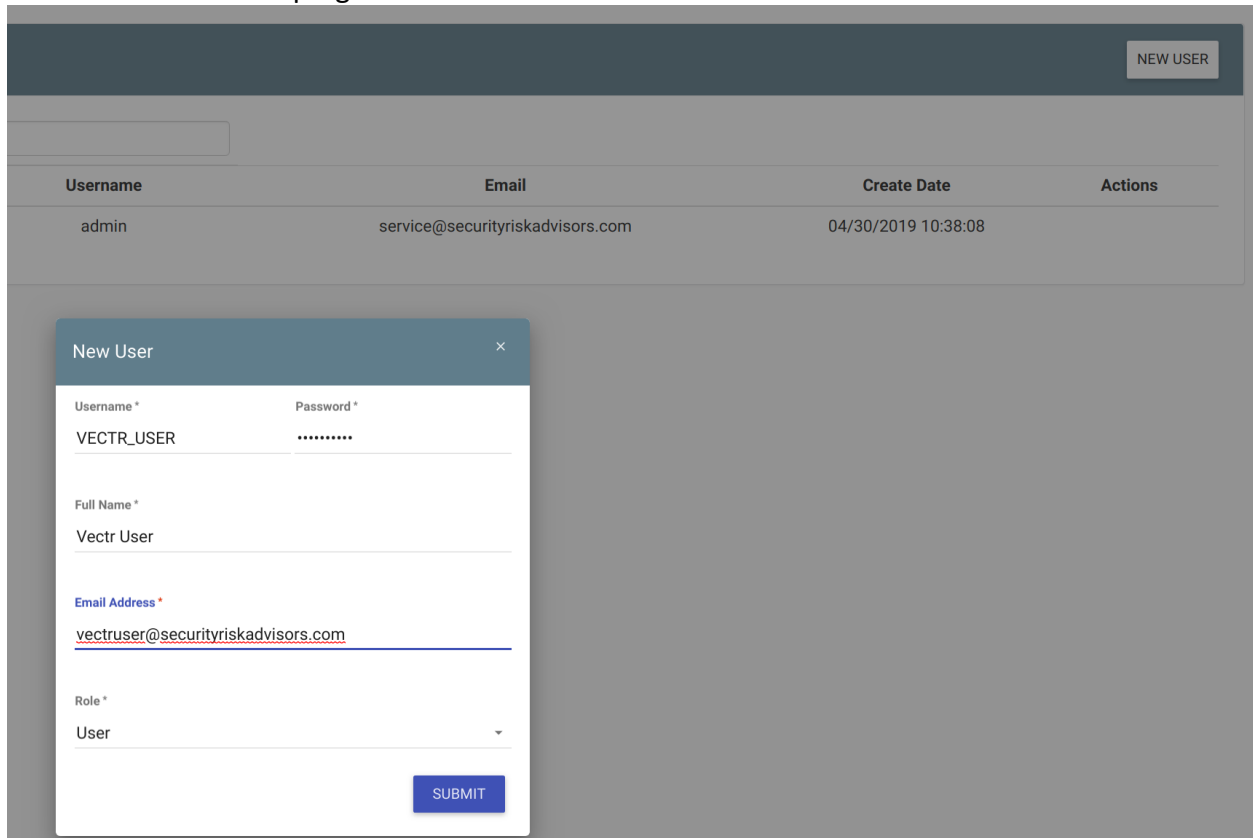
You can access the User Management screen by selecting the User Management tab on the Left Nav:



This will take you to the User Management page.



If you're logged in as a user with Role "ADMIN", you can create new user by clicking the "New User" button in the top right.



## How can this feature help me?

This will allow an Administrator to grant/deny different users access to the platform.

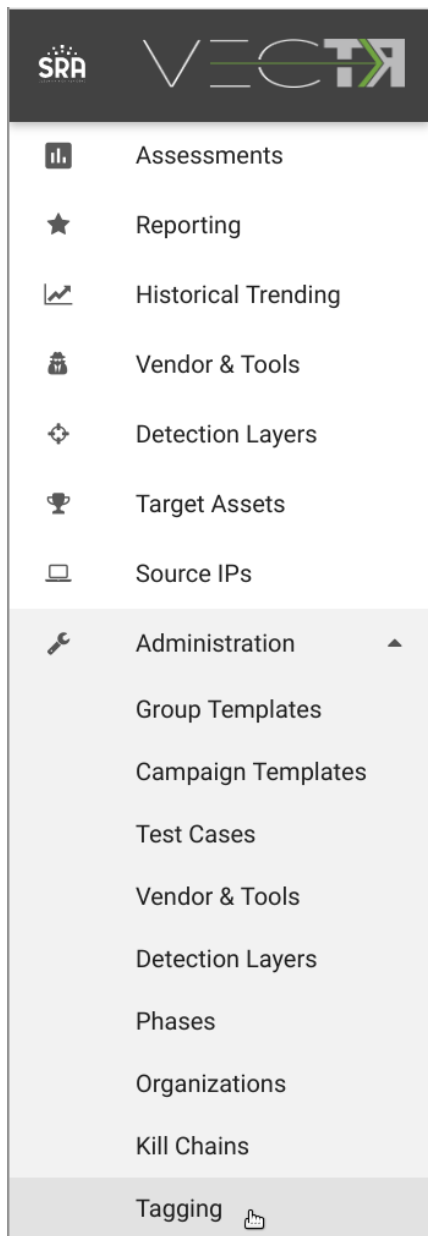
# Tagging Management





















## What is it?

Allows for editing and deleting of existing system tags.

## How does it work?

You can access the Tagging Management screen by selecting the Tagging tab on the Left Nav:



Name	Collection	Action
RISK ACCEPTED	TestCases	 
REMIEDIATE	TestCases	 
INVESTIGATE	TestCases	 
attack_execution	GenericRules	 
attack_credential_access	GenericRules	 
attack_persistence	GenericRules	 
attack_discovery	GenericRules	 
attack_lateral_movement	GenericRules	 
attack_privilege_escalation	GenericRules	 
attack_defense_evasion	GenericRules	 

Name	Collection
RISK ACCEPTED	TestCases
REMEDIATE	TestCases
INVESTIGATE	TestCases
attack.execution	GenericRules

Modify Tag

Tag Name \*

INVESTIGATE\_CHANGE

Save

Cancel

You can only delete a tag if it's not currently in use. If you attempt to, a popup will appear informing you of the database that the tag is located in. If you navigate to that database (DB

icon in the top right), then select the tag shortcut (Tag icon in the top right), you can quickly find the tagged data.

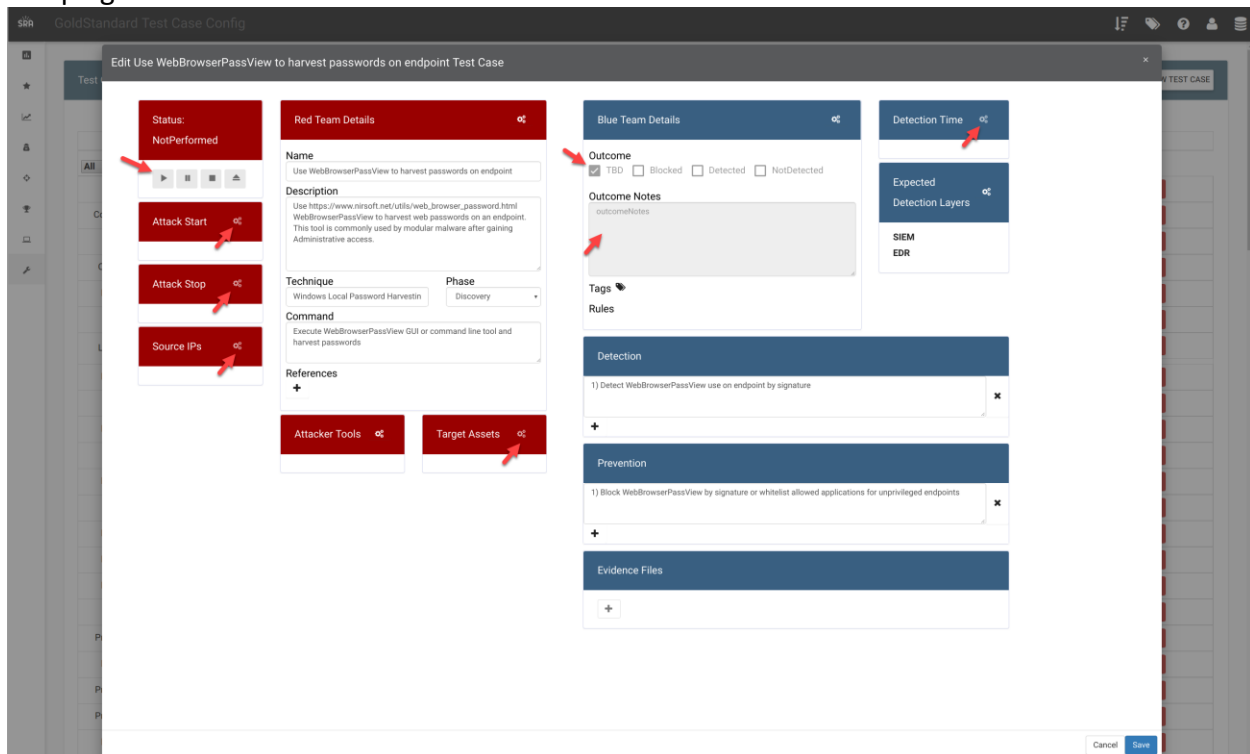
# System Flags

## What is it?

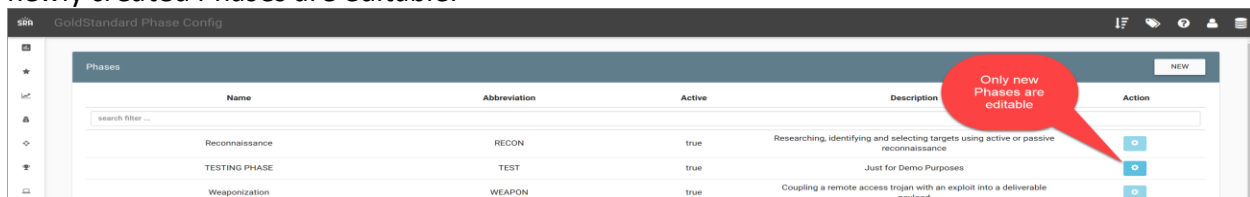
Certain data has been tagged with SystemFlags. This will help guide users in areas of the app where data should not be modified, along with preventing collisions of future data deliveries.

## How does it work?

Tagging of the data with a SystemFlag is done by Security Risk Advisors. We have disabled editing of fields in Administration that should only be edited within the context of a running campaign:



The 19 Phases that are delivered are tagged with SystemFlags, thus cannot be edited. Any newly created Phases are editable:







The 3 Kill Chains that are delivered are tagged as SystemFlags, thus cannot be edited. Any newly created Kill Chains are editable:

snGoldStandard Kill Chain Config

★

KillChains

NEW

Name	Phases	Description	Create Date	Update Date	Action
search filter ...					
Default	Credential Access Action on Objectives Exploitation Collection Persistence Privilege Escalation Discovery Command & Control Initial Access Execution Lateral Movement Reconnaissance Delivery Exfiltration Defense Evasion	Kill Chain that includes most common phases	07/24/2017 11:04:44		
TESTING KILL CHAIN	TESTING PHASE	TESTING KILL CHAIN	04/30/2019 13:02:18	04/30/2019 13:02:18	

Only new Kill Chains are editable