VECTR v5.1.3 Feature Breakdown

Table of Contents

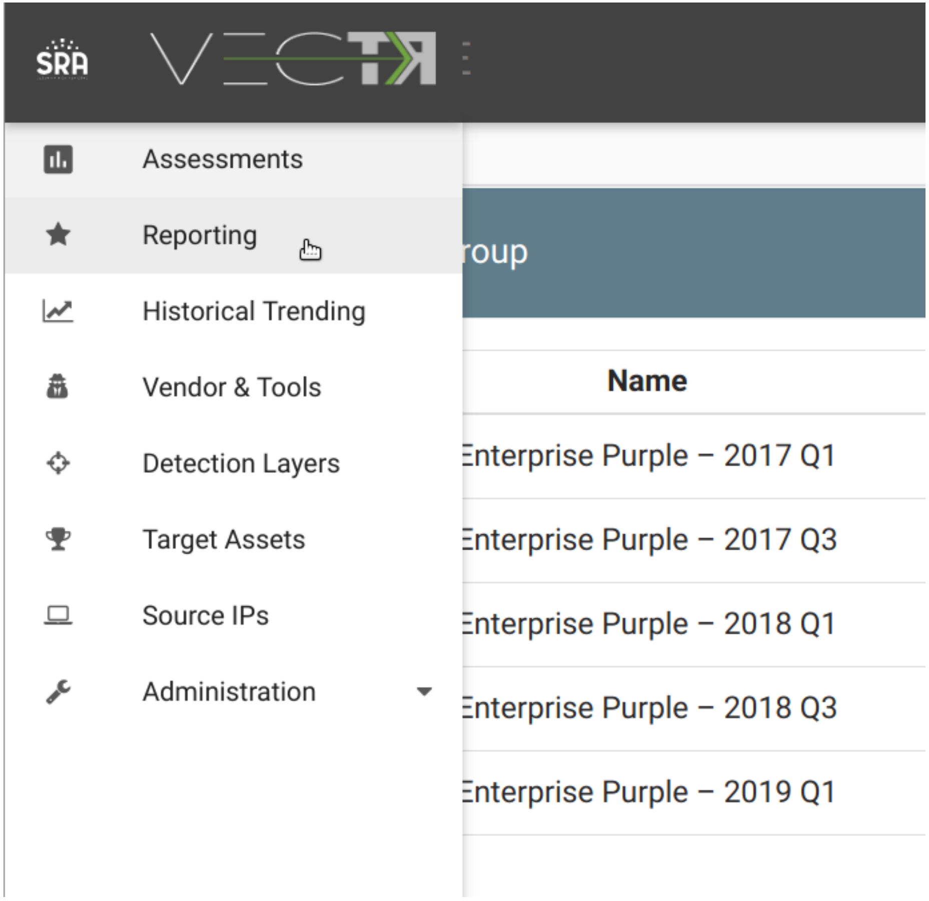
Reporting Screen

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.

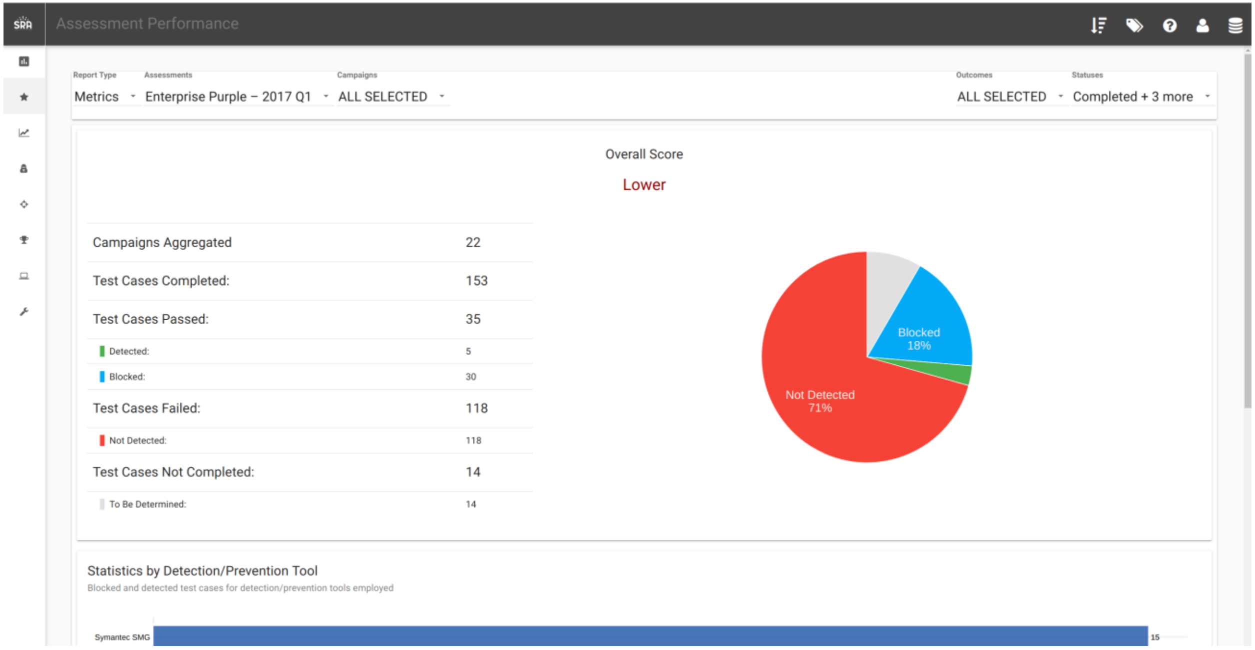
How does it work?

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



Name
Enterprise Purple – 2017 Q1
Enterprise Purple – 2017 Q3
Enterprise Purple – 2018 Q1
Enterprise Purple – 2018 Q3
Enterprise Purple – 2019 Q1

This will take you to the Reporting View:



Assessment Performance

Report Type	Assessments	Campaigns	Outcomes	Statuses
Metrics	Enterprise Purple – 2017 Q1	ALL SELECTED	ALL SELECTED	Completed + 3 more

Overall Score

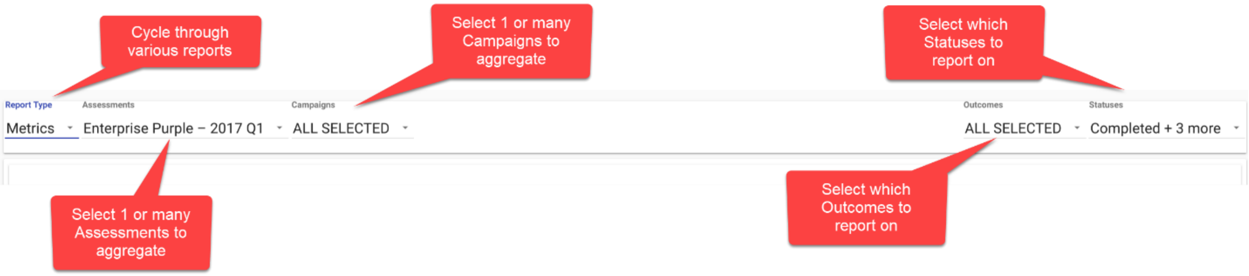
Lower

Campaigns Aggregated	22
Test Cases Completed:	153
Test Cases Passed:	35
🟩 Detected:	5
🟦 Blocked:	30
Test Cases Failed:	118
🟥 Not Detected:	118
Test Cases Not Completed:	14
⬜ To Be Determined:	14

Statistics by Detection/Prevention Tool

Blocked and detected test cases for detection/prevention tools employed

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



Report Type	Assessments	Campaigns	Outcomes	Statuses
Metrics	Enterprise Purple – 2017 Q1	ALL SELECTED	ALL SELECTED	Completed + 3 more

Cycle through various reports

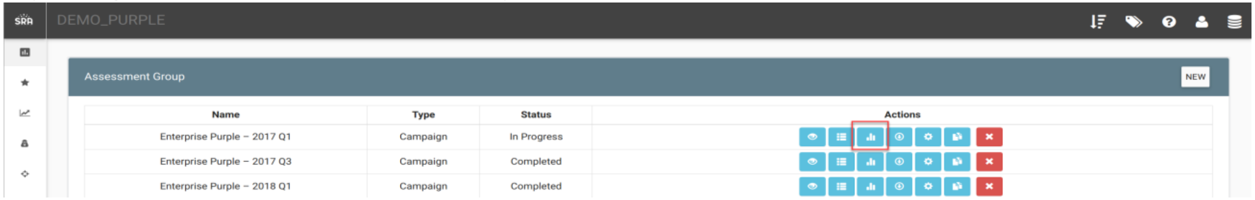
Select 1 or many Campaigns to aggregate

Select which Statuses to report on

Select 1 or many Assessments to aggregate

Select which Outcomes to report on

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

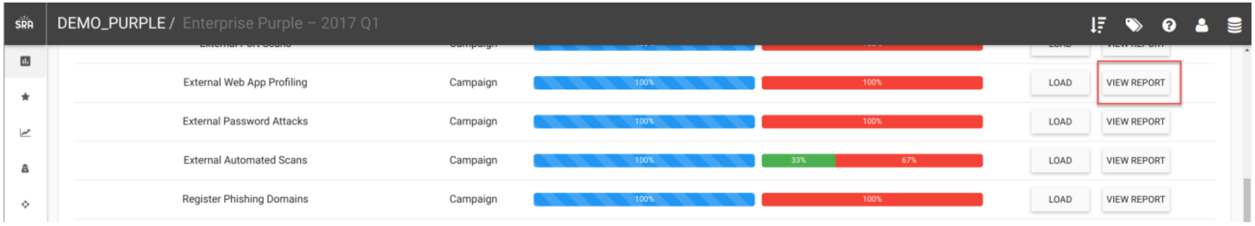


DEMO_PURPLE

Assessment Group

Name	Type	Status	Actions
Enterprise Purple – 2017 Q1	Campaign	In Progress	
Enterprise Purple – 2017 Q3	Campaign	Completed	
Enterprise Purple – 2018 Q1	Campaign	Completed	

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



DEMO_PURPLE / Enterprise Purple – 2017 Q1

External Web App Profiling	Campaign	100%	100%	LOAD	VIEW REPORT
External Password Attacks	Campaign	100%	100%	LOAD	VIEW REPORT
External Automated Scans	Campaign	100%	33% 67%	LOAD	VIEW REPORT
Register Phishing Domains	Campaign	100%	100%	LOAD	VIEW REPORT

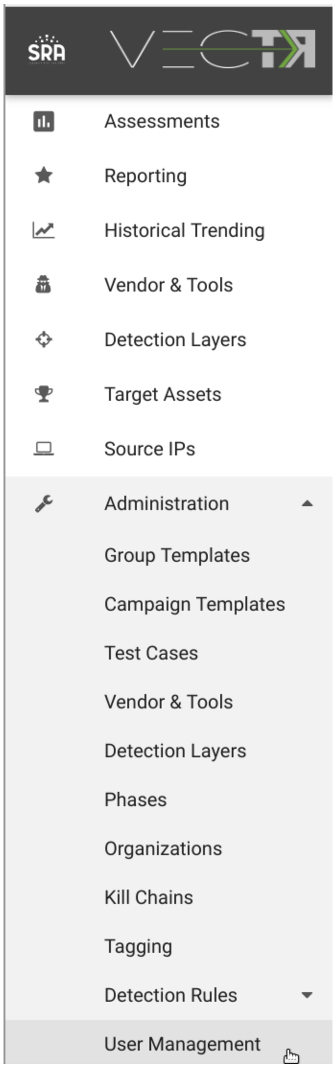
User Management

What is it?

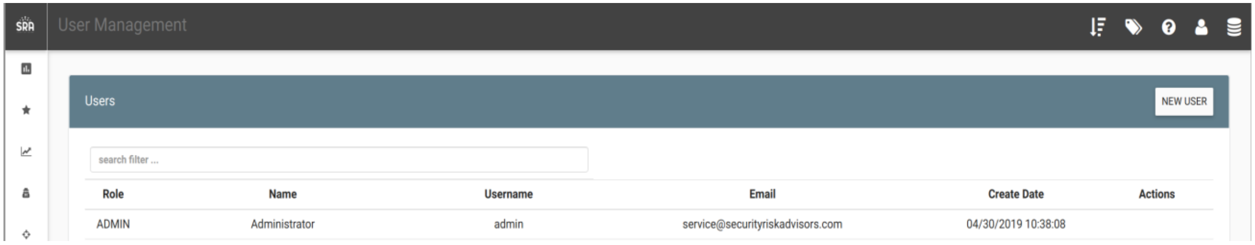
Allows for an ADMIN to add users with either the Role of USER or ADMIN. Users with USER will be able to use the platform, but not create users or escalate Roles.

How does it work?

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

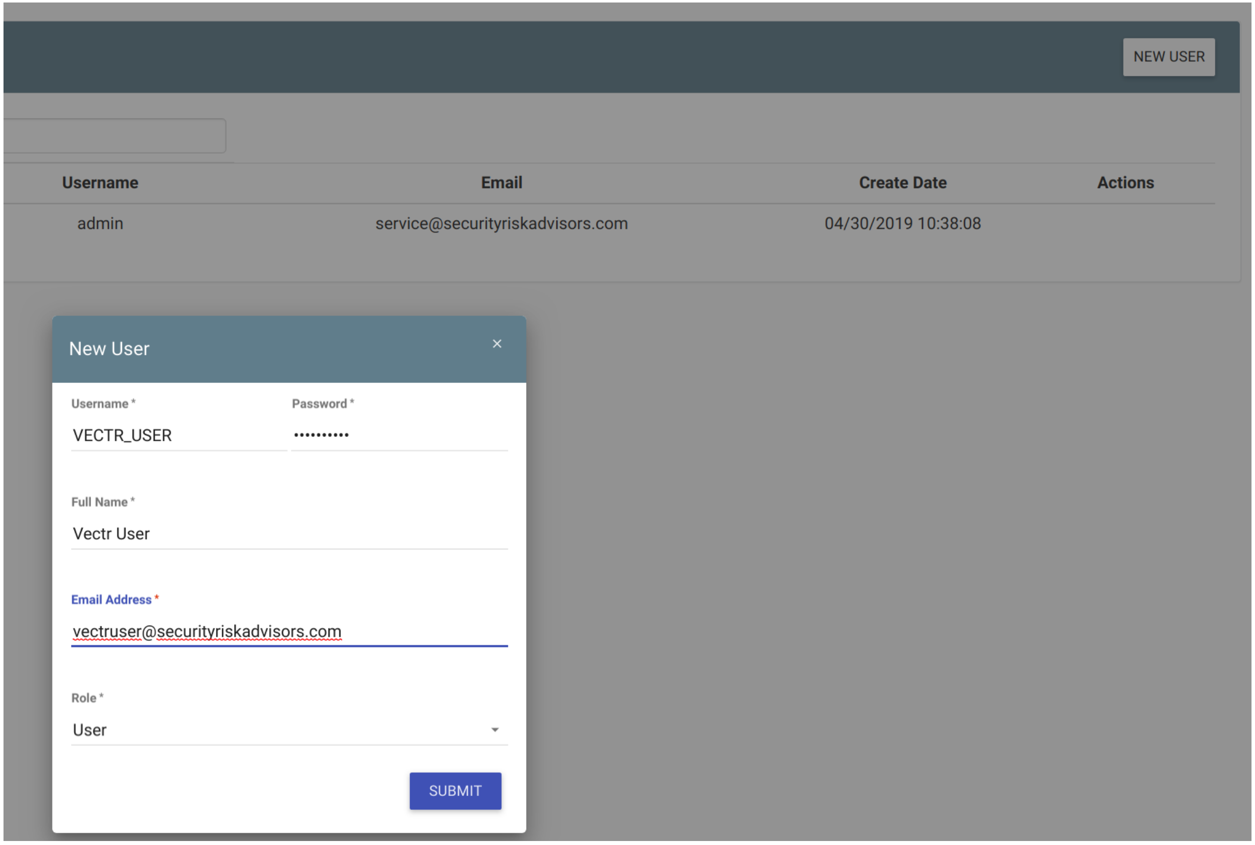


This will take you to the User Management page.



Role	Name	Username	Email	Create Date	Actions
ADMIN	Administrator	admin	service@securityriskadvisors.com	04/30/2019 10:38:08	

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.



Username	Email	Create Date	Actions
admin	service@securityriskadvisors.com	04/30/2019 10:38:08	

New User

Username * VECTR_USER

Password * ••••••••••

Full Name * Vectr User

Email Address * vectruser@securityriskadvisors.com

Role * User

How can this feature help me?

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

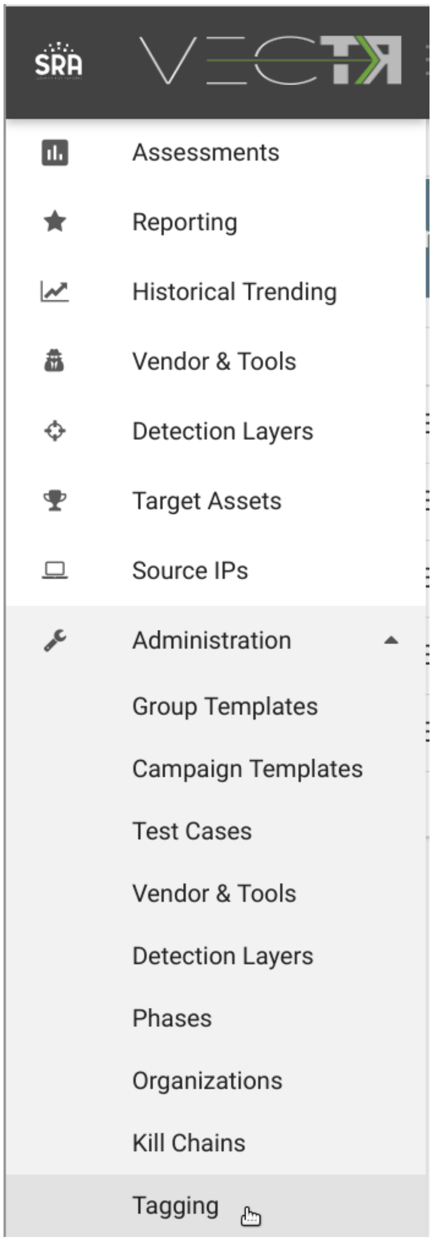
Tagging Management

What is it?

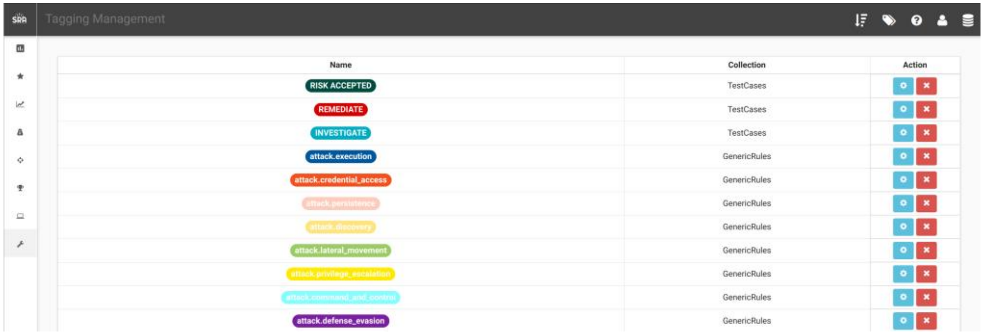
Allows for editing and deleting of existing system tags.

How does it work?

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

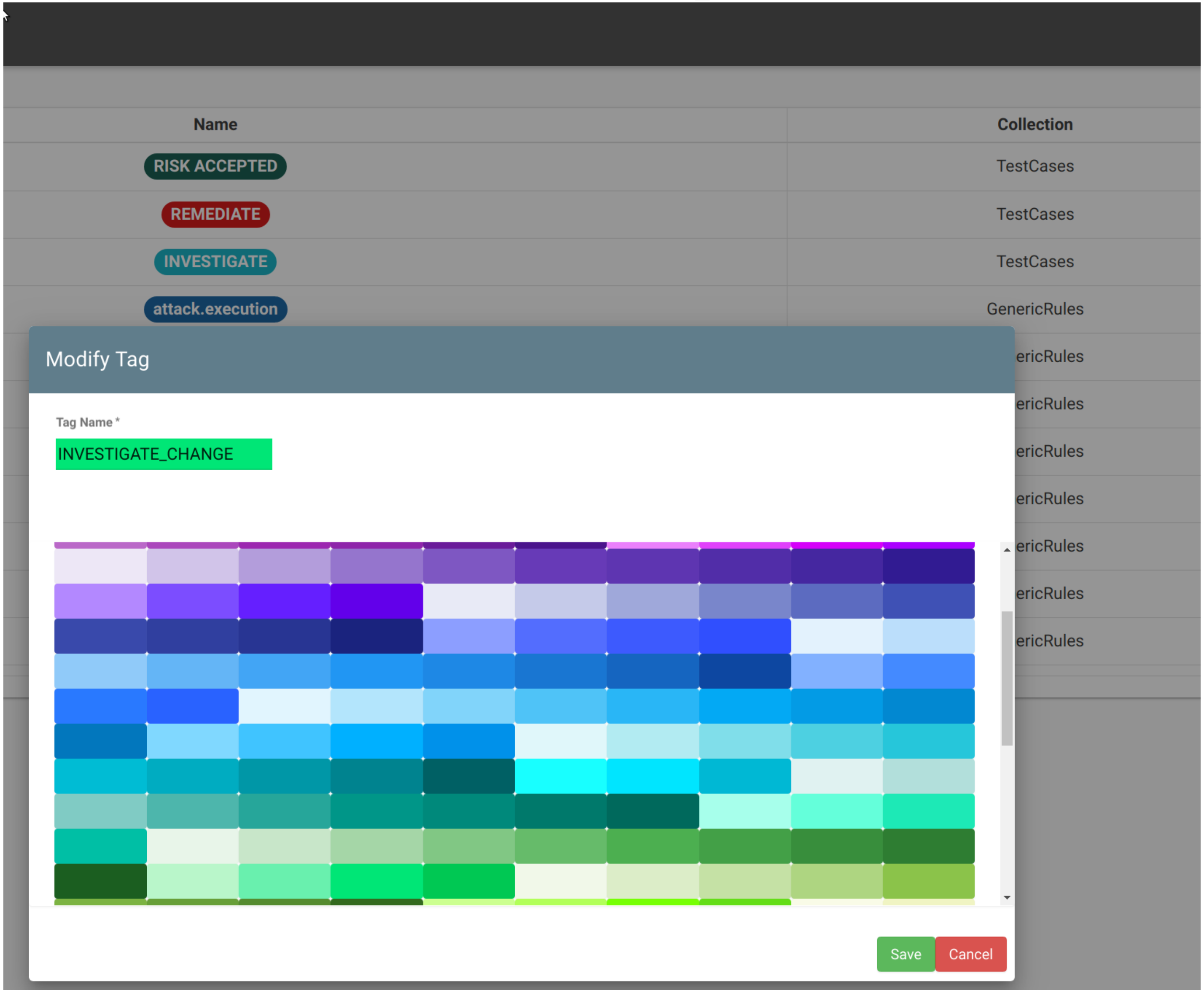


This will take you to the Tagging Management page. From here you can edit one of your Tags by clicking the cog on the right, or delete the tag by clicking the red X on the right:



Name	Collection	Action
RISK ACCEPTED	TestCases	⚙ ✖
REMEDIATE	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.command_and_control	GenericRules	⚙ ✖
attack.defense_evasion	GenericRules	⚙ ✖

You can change the Name and Color by clicking the cog on the right. In this example, we changed the name “INVESTIGATE” tag to “INVESTIGATE_CHANGE” and color to green.



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

Modify Tag

Tag Name *

INVESTIGATE_CHANGE

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.

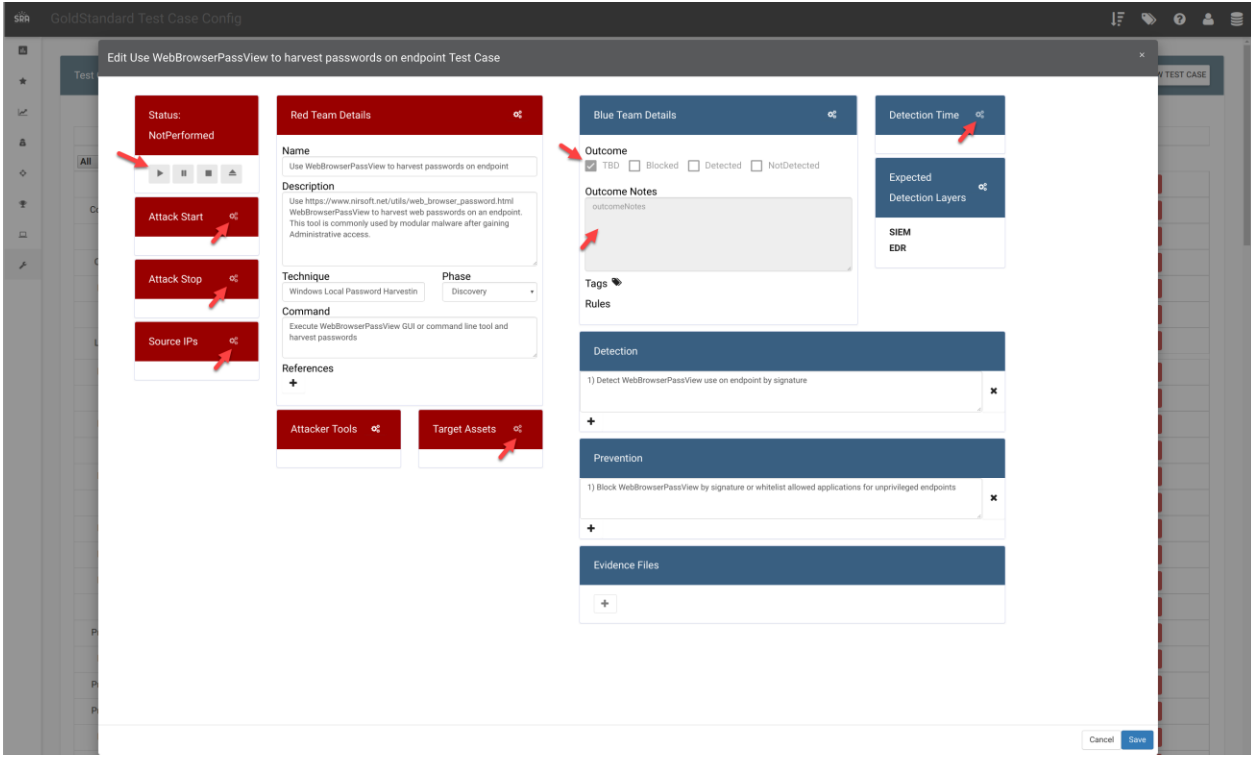
System Flags

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:



Edit Use WebBrowserPassView to harvest passwords on endpoint Test Case

Status: NotPerformed

Name: Use WebBrowserPassView to harvest passwords on endpoint

Description: Use https://www.nirsoft.net/utils/web_browser_password.html WebBrowserPassView to harvest web passwords on an endpoint. This tool is commonly used by modular malware after gaining Administrative access.

Technique: Windows Local Password Harvestin

Phase: Discovery

Command: Execute WebBrowserPassView GUI or command line tool and harvest passwords

References

Outcome: ☑ TBD □ Blocked □ Detected □ NotDetected

Outcome Notes: outcomeNotes

Tags

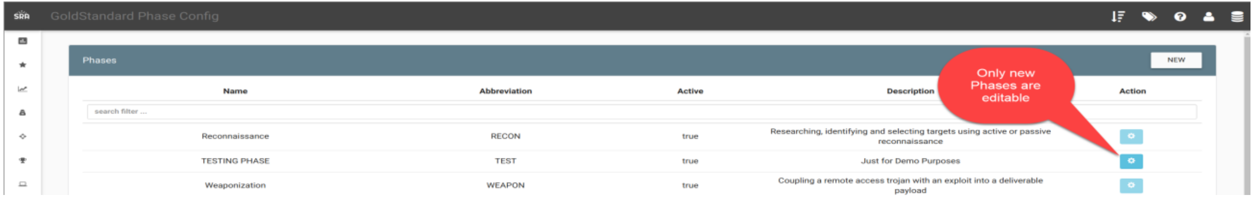
Rules

SIEM
EDR

1) Detect WebBrowserPassView use on endpoint by signature

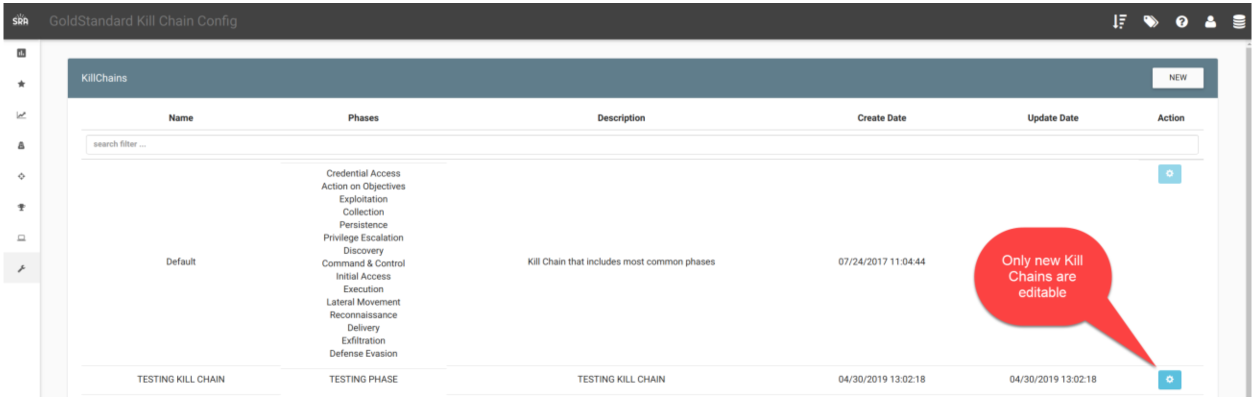
1) Block WebBrowserPassView by signature or whitelist allowed applications for unprivileged endpoints

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



Name	Abbreviation	Active	Description	Action
Reconnaissance	RECON	true	Researching, identifying and selecting targets using active or passive reconnaissance	
TESTING PHASE	TEST	true	Just for Demo Purposes	
Weaponization	WEAPON	true	Coupling a remote access trojan with an exploit into a deliverable payload	

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



GoldStandard Kill Chain Config
KillChains
NEW
search filter ...
Only new Kill Chains are editable

Name	Phases	Description	Create Date	Update Date	Action
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	⚙