

VECTR v7.1.1 Feature Breakdown

[Table of Contents](#)

Advanced Reporting Features.....2

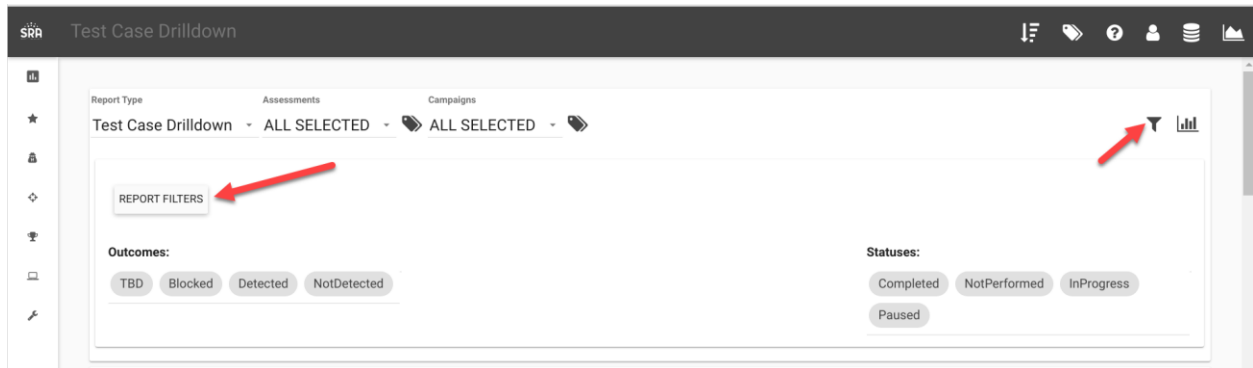
Advanced Reporting Features

What is it?

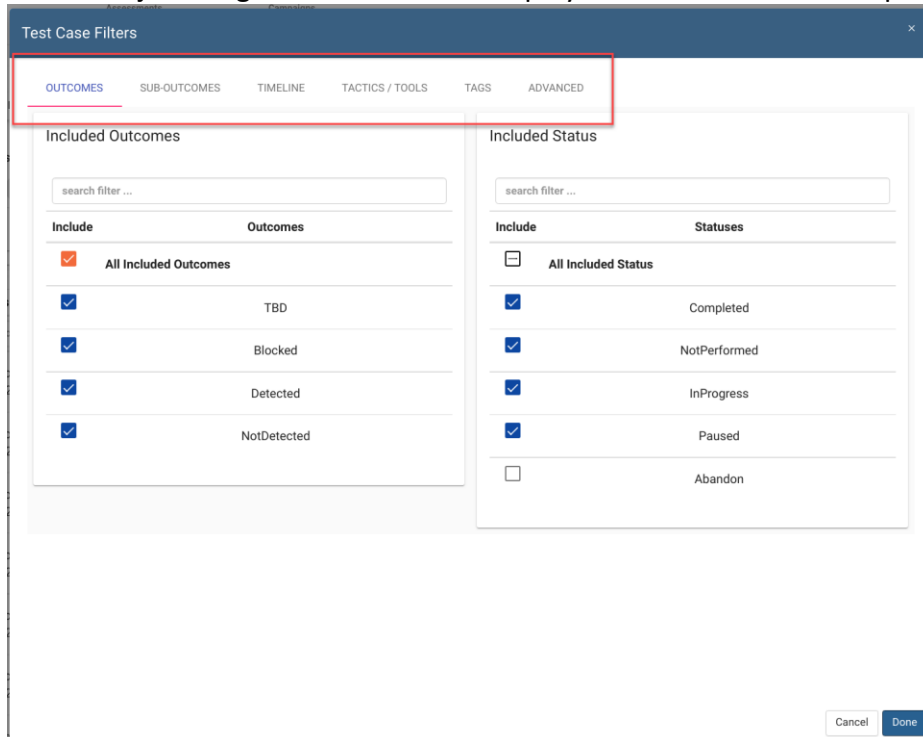
Allows for more granular control of reporting to show the exact statistics needed for your reports.

How does it work?

From the Reporting screen, make sure the Filters screen is visible, then click the Report Filters button:



All the major categories of filters are displayed in Tabs across the top:



These applied filters will be used against all Report Type pages. For example, if you want to see all tests that have an Expected Defensive Layer of SIEM:

Test Case Filters

OUTCOMES SUB-OUTCOMES TIMELINE **TACTICS / TOOLS** TAGS ADVANCED

Phases / Tactics

search filter ...

Include	Phase/Tactic
<input type="checkbox"/>	All Phases / Tactics
<input type="checkbox"/>	Reconnaissance
<input type="checkbox"/>	Resource Development
<input type="checkbox"/>	Weaponization
<input type="checkbox"/>	Delivery
<input type="checkbox"/>	Social Engineering
<input type="checkbox"/>	Initial Access
<input type="checkbox"/>	Execution
<input type="checkbox"/>	Exploitation

Defensive Tools

search filter ...

Include	Product
<input type="checkbox"/>	All Defensive Tools
<input type="checkbox"/>	Hadoop
<input type="checkbox"/>	McAfee DLP
<input type="checkbox"/>	CounterACT
<input type="checkbox"/>	Honeyd
<input type="checkbox"/>	ThreatStream
<input type="checkbox"/>	Vectra
<input type="checkbox"/>	PAN AutoFocus
<input type="checkbox"/>	Falcon Overwatch

Expected Defensive Layers

siem

Include	Layer
<input type="checkbox"/>	All Expected Defensive Layers
<input checked="" type="checkbox"/>	SIEM

Offensive Tools

search filter ...

Include	Product
<input type="checkbox"/>	All Offensive Tools
<input type="checkbox"/>	Get-GPPPassword
<input type="checkbox"/>	FTP
<input type="checkbox"/>	Egress Buster
<input type="checkbox"/>	SMB
<input type="checkbox"/>	Netcat
<input type="checkbox"/>	Responder
<input type="checkbox"/>	Telnet
<input type="checkbox"/>	Nessus

Cancel Done

This will only retrieve data that has a Test Case “Defenses” that contains SIEM:

Edit Extract Password Hashes via VSS Test Case

Status: Completed

Attack Start: 01/19/2018 03:44:54 status changed to InProgress

Attack Stop: 01/19/2018 04:43:43 status changed to Completed

Sources

Red Team Details

Name: Extract Password Hashes via VSS

Description: Dump domain hashes for all domain users on the domain controller via VSS (Volume Shadow Services).

Technique: Compromise a DC - T1003 Phase: Lateral Movement

Operator Guidance: wmic /node:DC /user:DOMAIN\User /password:UserPassword process call create "cmd /c vssadmin list shadows 2>&1 > C:\Temp\output.txt"

Blue Team Details

Outcome: ☐ TBD ☐ Blocked ☐ Detected ☒ NotDetected

Was the event source logged? ☐ TBD ☐ Yes ☒ No

Outcome Notes: outcomeNotes

Tags: Rules

Detection Time: 01/19/2018 06:25:29 outcome changed to NotDetected

Defenses: **SIEM EDR**

How can this feature help me?

This allows for more granular control of reporting. Here is a guide for how the reporting filters map up to the Test Case fields:

Filter:

Test Case Filters

OUTCOMES

SUB-OUTCOMES

TIMELINE

TACTICS / TOOLS

T

Included Outcomes

search filter ...

Include	Outcomes
<input checked="" type="checkbox"/>	All Included Outcomes
<input checked="" type="checkbox"/>	TBD
<input checked="" type="checkbox"/>	Blocked
<input checked="" type="checkbox"/>	Detected
<input checked="" type="checkbox"/>	NotDetected

Field:

Blue Team Details

Outcome

☐ TBD ☐ Blocked ☐ Detected ☒ NotDetected

Filter:

Included Status

search filter ...

Include	Statuses
<input type="checkbox"/>	All Included Status
<input checked="" type="checkbox"/>	Completed
<input checked="" type="checkbox"/>	NotPerformed
<input checked="" type="checkbox"/>	InProgress
<input checked="" type="checkbox"/>	Paused
<input type="checkbox"/>	Abandon

Field:

Status: Completed

▶

⏸

■

⏶

Filter:

Included Activity Logged

search filter ...

Include	Activity Logged
<input type="checkbox"/>	All Included Activity Logged
<input type="checkbox"/>	TBD
<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

Field:

Blue Team Details

Outcome

☐ TBD ☐ Blocked ☐ Detected ☒ NotDetected

Was the event source logged?

☐ TBD ☐ Yes ☒ No

Note:

Activity Logged will only apply for NotDetected Outcome.

Filter:

Included Alert Severity

search filter ...

Include	Alert Severity
<input type="checkbox"/>	All Included Alert Severity
<input type="checkbox"/>	TBD
<input type="checkbox"/>	Info
<input type="checkbox"/>	Low
<input type="checkbox"/>	Med
<input type="checkbox"/>	High
<input type="checkbox"/>	Critical

Field:

Blue Team Details

Outcome

☐ TBD ☐ Blocked ☒ Detected ☐ NotDetected

Detecting Blue Tool(s):

What was the alert severity?

☒ TBD ☐ Info ☐ Low ☐ Med ☐ High ☐ Critical

Note:

Alert Severity will only apply for Detected Outcome.

Filter:

Included Alert Triggered

search filter ...

Include	Alert Triggered
<input type="checkbox"/>	All Included Alert Triggered
<input type="checkbox"/>	TBD
<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

Field:

Blue Team Details



Outcome

☐ TBD ☒ Blocked ☐ Detected ☐ NotDetected

Detecting Blue Tool(s):

Was an alert triggered?

☒ TBD ☐ Yes ☐ No

Note:

Alert Triggered will only apply for Blocked Outcome.

Filter:

Attack Start Timeline



Min Date

Max Date

Field:

Attack Start  

01/19/2018 03:44:54

status changed to
InProgress


Note: MinDate inclusive, MaxDate exclusive

Filter:

Phases / Tactics

Include	Phase/Tactic
<input type="checkbox"/>	All Phases / Tactics
<input type="checkbox"/>	Reconnaissance
<input type="checkbox"/>	Resource Development
<input type="checkbox"/>	Weaponization

Field:

Red Team Details 

Name

Description

Dump domain hashes for all domain users on the domain controller via VSS (Volume Shadow Services).

Technique ?

Phase

Operator Guidance

```
wmic /node:DC /user:DOMAIN\User  
/password:UserPassword process call create "cmd /c  
vssadmin list shadows 2>&1 > C:\Temp\output.txt"
```

Filter:

Defensive Tools

splunk

Include	Product
<input type="checkbox"/>	All Defensive Tools
<input checked="" type="checkbox"/>	Splunk

Field:

Blue Team Details

Outcome

☐ TBD ☐ Blocked ☒ Detected ☐ NotDetected

Detecting Blue Tool(s):

Splunk

What was the alert severity?

☐ TBD ☐ Info ☐ Low ☐ Med ☒ High ☐ Critical

Filter:

Expected Defensive Layers

siem

Include	Layer
<input type="checkbox"/>	All Expected Defensive Layers
<input checked="" type="checkbox"/>	SIEM

Field:

Defenses ? ⚙

SIEM

EDR

Filter:

Offensive Tools

nmap

Include	Product
<input type="checkbox"/>	All Offensive Tools
<input checked="" type="checkbox"/>	Nmap

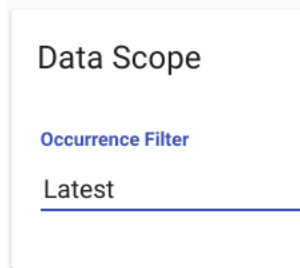
Field:

Attacker

Tools

Nmap

The last filter on the list is the “Latest” flag under ADVANCED / DataScope:



This is one of the more expensive queries and will cause data to load more slowly if you have larger datasets.

The purpose is to only show you the last run test case variant for each template type across all the selected Assessments and Campaigns. There is more extensive documentation on this here:

<https://docs.vectr.io/HistoricalTrending/>