VECTR v5.4 Feature Breakdown

Table of Contents

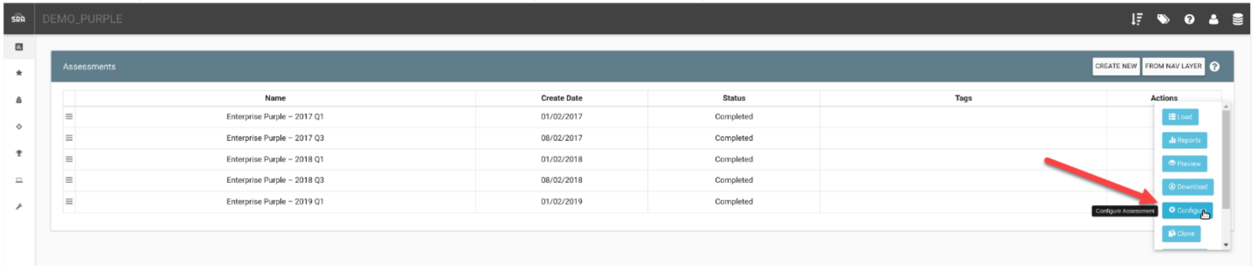
Custom Escalation Path Start Icon

What is it?

Allows users to set the icon for the start of their escalation paths in a campaign view.

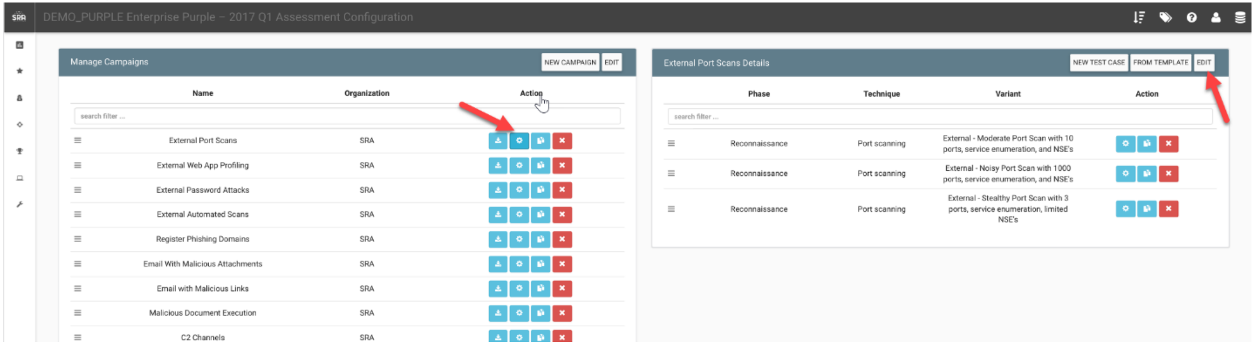
How does it work?

Click configure on an Assessment housing the campaign:



Name	Create Date	Status	Tags	Actions
Enterprise Purple – 2017 Q1	01/02/2017	Completed		
Enterprise Purple – 2017 Q3	08/02/2017	Completed		
Enterprise Purple – 2018 Q1	01/02/2018	Completed		
Enterprise Purple – 2018 Q3	08/02/2018	Completed		
Enterprise Purple – 2019 Q1	01/02/2019	Completed		

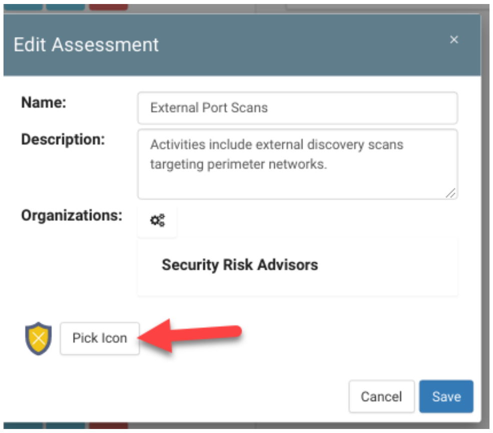
Click the Cog next to the Campaign you want to edit, then the Edit button at the top of the Campaign:



Name	Organization	Action
External Port Scans	SRA	
External Web App Profiling	SRA	
External Password Attacks	SRA	
External Automated Scans	SRA	
Register Phishing Domains	SRA	
Email With Malicious Attachments	SRA	
Email with Malicious Links	SRA	
Malicious Document Execution	SRA	
C2 Channels	SRA	

Phase	Technique	Variant	Action
Reconnaissance	Port scanning	External - Moderate Port Scan with 10 ports, service enumeration, and NSE's	
Reconnaissance	Port scanning	External - Noisy Port Scan with 1000 ports, service enumeration, and NSE's	
Reconnaissance	Port scanning	External - Stealthy Port Scan with 3 ports, service enumeration, limited NSE's	

Click the Pick Icon button:



Name: External Port Scans

Description: Activities include external discovery scans targeting perimeter networks.

Organizations: Security Risk Advisors

How can this feature help me?

Allows for customization of escalation path for screenshots.

Database Upgrades on Application Start

What is it?

This feature allows VECTR to automatically update its databases prior to web application startup.

How does it work?

VECTR checks the state of any existing application databases on startup and updates them if necessary. Logs are stored in a separate database for auditing and debugging. This feature may contribute to slightly longer application startup times when databases are being updated.

How can this feature help me?

Users will no longer need to click through upgrade screens after the application is updated.

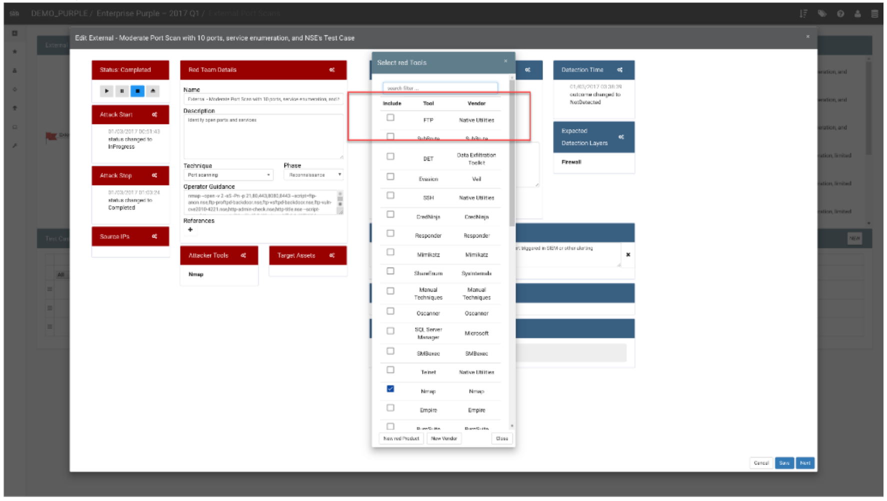
Disable Tools

What is it?

Allows tools to not show up in dropdowns, if disabled. Will still show up in reporting.

How does it work?

Example here shows a tool that is still enabled, FTP:

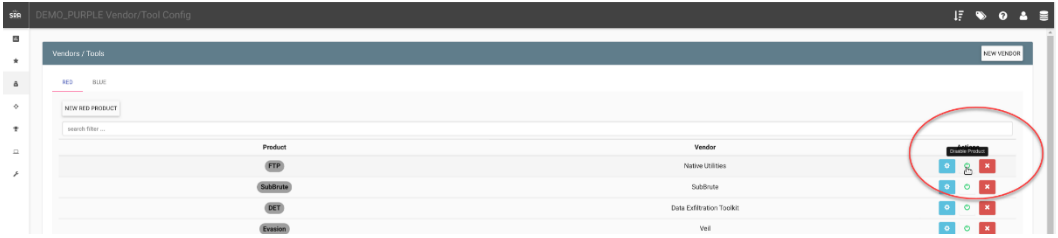


Select red Tools

Include	Tool	Vendor
□	FTP	Native Utilities
□	SubBrute	SubBrute
□	DET	Data Exfiltration Toolkit
□	Evasion	Veil
□	SSH	Native Utilities
□	CredNinja	CredNinja
□	Responder	Responder
□	Mimikatz	Mimikatz
□	ShareEnum	Sysinternals
□	Manual Techniques	Manual Techniques
□	Oscanner	Oscanner
□	SQL Server Manager	Microsoft
□	SMBexec	SMBexec
□	Telnet	Native Utilities
☑	Nmap	Nmap
□	Empire	Empire
□	BurpSuite	BurpSuite

Edit External - Moderate Port Scan with 10 ports, service enumeration, and NSEs Test Case
Status: Completed
Red Team Details
Attack Start
Attack Stop
Source IPs
Attacker Tools
Nmap
Target Assets
Detection Time
01/03/2017 03:38:39 outcome changed to NotDetected
Expected Detection Layers
Firewall
New red Product
New Vendor
Close
Cancel
Save

From the Vendors & Tools on the left Nav panel, you can disable tools:

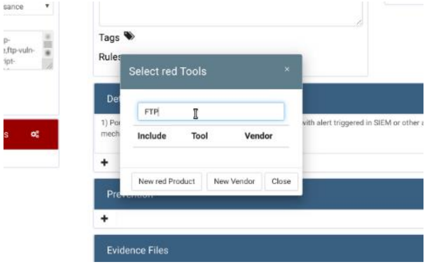


DEMO_PURPLE Vendor/Tool Config

Vendors / Tools

Product	Vendor	Actions
FTP	Native Utilities	
SubBrute	SubBrute	
DET	Data Exfiltration Toolkit	
Evasion	Veil	

This will prevent the Tool FTP from showing up in the selection screen:



Select red Tools

FTP

Include	Tool	Vendor

How can this feature help me?

This allows for cleaner dropdowns if your team is using a subset of the tools provided, making it easier to find what you’re using.

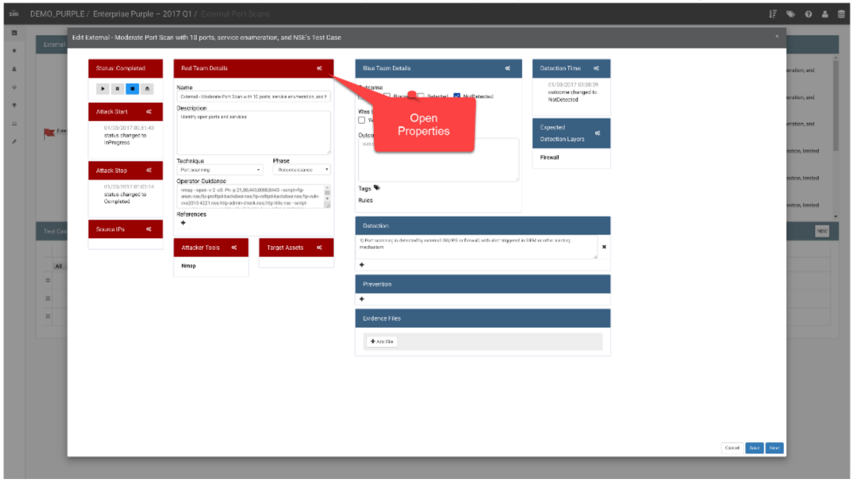
Display Selected Template on Red Team Details

What is it?

Allows for the user to more easily see which admin template is assigned to the test case.

How does it work?

From the Test Case panel, open the properties clicking the Red Team Details cog:



DEMO_PURPLE / Enterprise Purple – 2017 Q1 / External Port Scans
Edit External - Moderate Port Scan with 10 ports, service enumeration, and NSE's Test Case
Status: Completed
Attack Start
Attack Stop
Source IPs
Red Team Details
Attacker Tools
Target Assets
Blue Team Details
Detection Time
Expected Detection Layers
Detection
Prevention
Evidence Files
Cancel
Save
Next

Name: External - Moderate Port Scan with 10 ports, service enumeration, and N

Description: Identify open ports and services

Technique: Port scanning

Phase: Reconnaissance

Attack Start: 01/03/2017 00:51:43 status changed to InProgress

Attack Stop: 01/03/2017 01:03:24 status changed to Completed

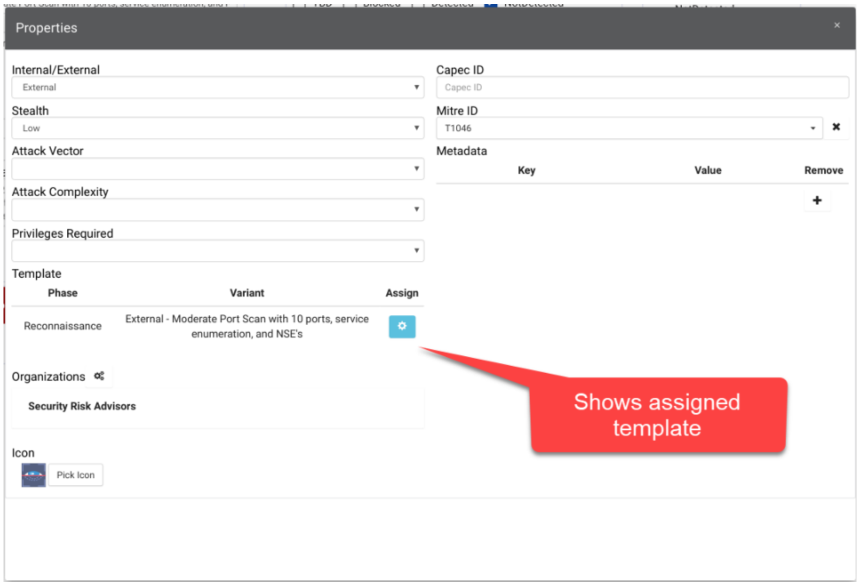
Detection Time: 01/03/2017 03:38:39 outcome changed to NotDetected

Expected Detection Layers: Firewall

Attacker Tools: Nmap

Detection: 1) Port scanning is detected by external IDS/IPS or firewall, with alert triggered in SIEM or other alerting mechanism

Open Properties



Internal/External: External

Stealth: Low

Attack Vector:

Attack Complexity:

Privileges Required:

Capec ID: Capec ID

Mitre ID: T1046

Metadata

Key	Value	Remove

Template

Phase	Variant	Assign
Reconnaissance	External - Moderate Port Scan with 10 ports, service enumeration, and NSE's	⚙

Organizations

Security Risk Advisors

Icon

Shows assigned template

How can this feature help me?

Will allow the user to more easily know which template is assigned to a test case. The template is used in various screens (like Heatmap filters, Detection Rules, etc), and this needs to be more easily extracted from the app.

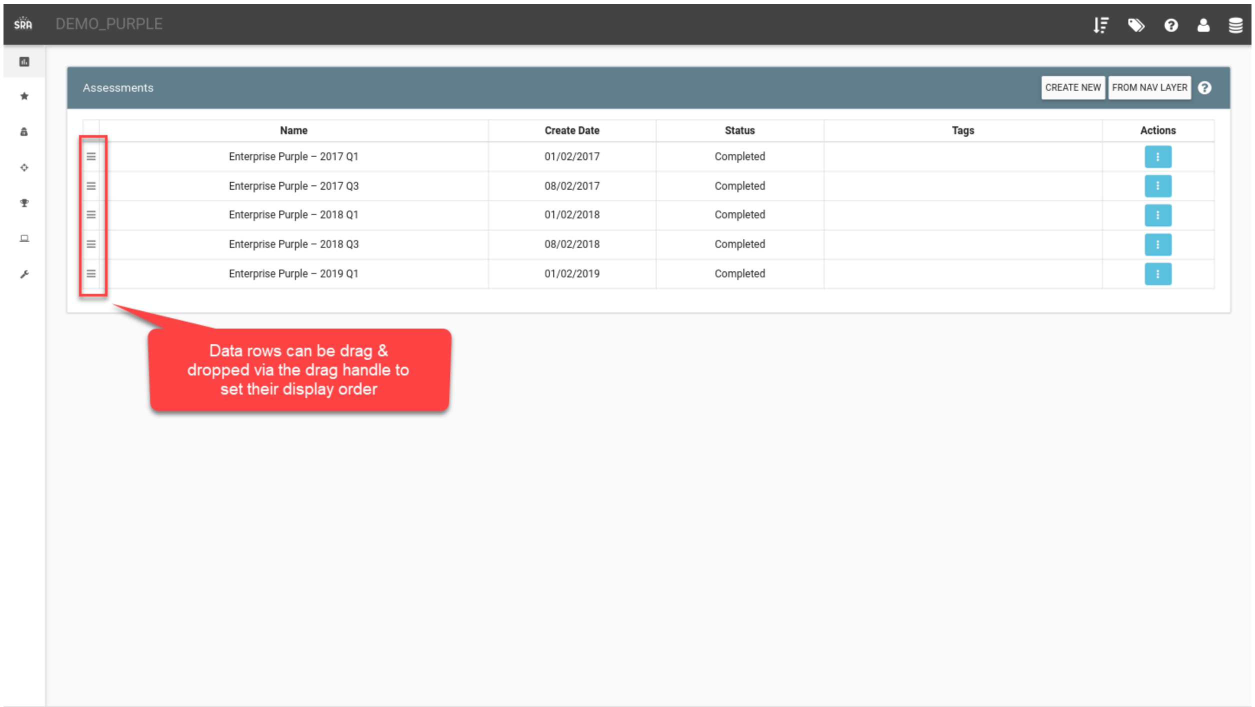
Drag/Drop Handle UI Tweak

What is it?

Data that can be ordered in VECTR is now moved by dragging and dropping a drag handle in the UI.

How does it work?

Reorder data row items by using the drag and drop handle on appropriate data.



	Name	Create Date	Status	Tags	Actions
≡	Enterprise Purple – 2017 Q1	01/02/2017	Completed		⋮
≡	Enterprise Purple – 2017 Q3	08/02/2017	Completed		⋮
≡	Enterprise Purple – 2018 Q1	01/02/2018	Completed		⋮
≡	Enterprise Purple – 2018 Q3	08/02/2018	Completed		⋮
≡	Enterprise Purple – 2019 Q1	01/02/2019	Completed		⋮

Data rows can be drag & dropped via the drag handle to set their display order

How can this feature help me?

Previously the data rows themselves where able to be drag and dropped by clicking and dragging the row, but this was confusing users and causing unintended ordering behavior. This new feature should make the drag and drop action easier to use and more deliberate.

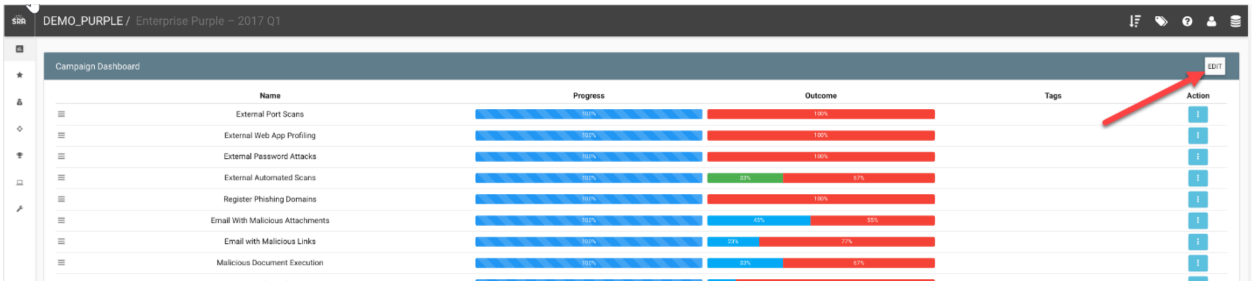
Edit Assessment Description from Campaign Dashboard

What is it?

Allows for editing an Assessment from the Campaign Dashboard

How does it work?

Click the Edit button:



	Name	Progress	Outcome	Tags	Action
≡	External Port Scans	100%	100%		⋮
≡	External Web App Profiling	100%	100%		⋮
≡	External Password Attacks	100%	100%		⋮
≡	External Automated Scans	100%	33% 67%		⋮
≡	Register Phishing Domains	100%	100%		⋮
≡	Email With Malicious Attachments	100%	45% 55%		⋮
≡	Email with Malicious Links	100%	23% 77%		⋮
≡	Malicious Document Execution	100%	33% 67%		⋮

How can this feature help me?

Allows for easier access to editing an Assessment

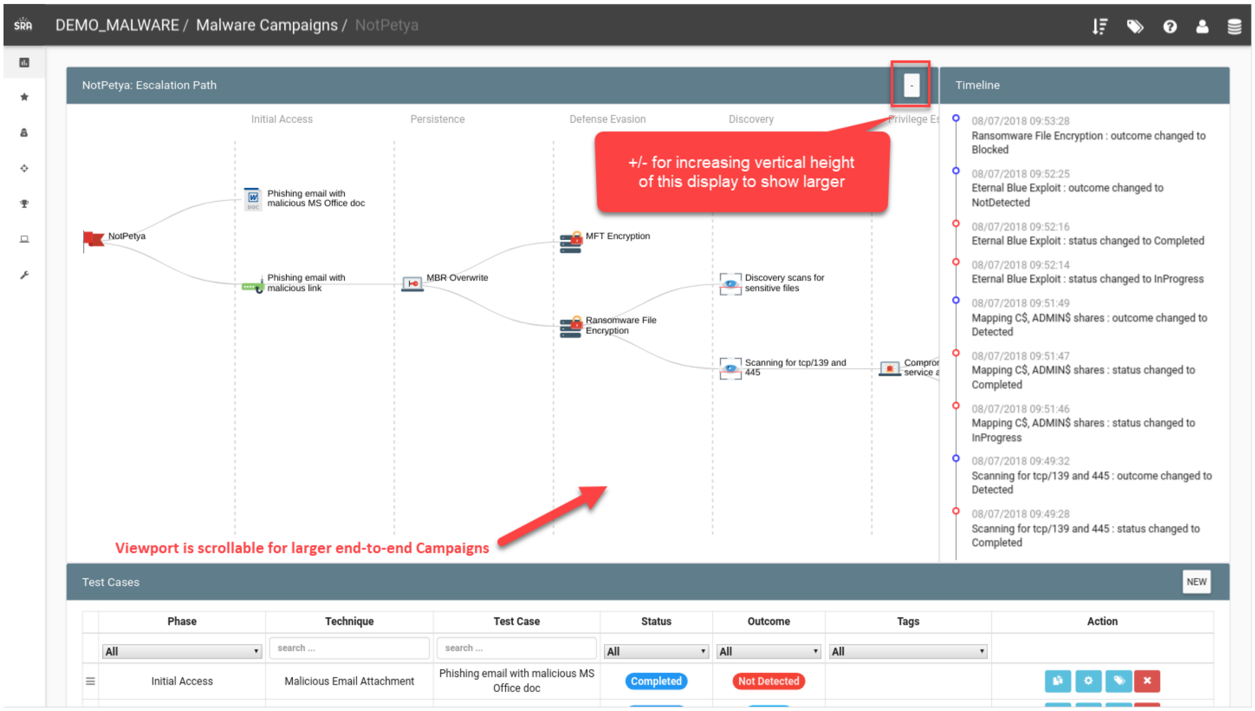
Escalation Path Tweaks

What is it?

This feature improves the spacing and visibility of the Escalation Path on the Campaign detailed view.

How does it work?

The Escalation Path has been modified to limit the amount of text overlap shown. Additionally, the Escalation Path viewport height can be modified via a +/- button in the UI and the horizontal length of the diagram is now scrollable in a user's web browser.


SRA
DEMO_MALWARE / Malware Campaigns / NotPetya
NotPetya: Escalation Path
-
Initial Access
Persistence
Defense Evasion
Discovery
Privilege Es
NotPetya
Phishing email with malicious MS Office doc
Phishing email with malicious link
MBR Overwrite
MFT Encryption
Ransomware File Encryption
Discovery scans for sensitive files
Scanning for tcp/139 and 445
Compror service a
Timeline
Test Cases
NEW

+/- for increasing vertical height of this display to show larger

Viewport is scrollable for larger end-to-end Campaigns

08/07/2018 09:53:28
Ransomware File Encryption : outcome changed to Blocked

08/07/2018 09:52:25
Eternal Blue Exploit : outcome changed to NotDetected

08/07/2018 09:52:16
Eternal Blue Exploit : status changed to Completed

08/07/2018 09:52:14
Eternal Blue Exploit : status changed to InProgress

08/07/2018 09:51:49
Mapping C$, ADMIN$ shares : outcome changed to Detected

08/07/2018 09:51:47
Mapping C$, ADMIN$ shares : status changed to Completed

08/07/2018 09:51:46
Mapping C$, ADMIN$ shares : status changed to InProgress

08/07/2018 09:49:32
Scanning for tcp/139 and 445 : outcome changed to Detected

08/07/2018 09:49:28
Scanning for tcp/139 and 445 : status changed to Completed

	Phase	Technique	Test Case	Status	Outcome	Tags	Action
	All	search ...	search ...	All	All	All	
≡	Initial Access	Malicious Email Attachment	Phishing email with malicious MS Office doc	Completed	Not Detected		

How can this feature help me?

The Escalation Path should be easier to visually navigate and understand how a Campaign's Test Cases are divided among Kill Chain Phases.

Filesize Limit Increase for Evidence Files

What is it?

A 190 MB file size limit has been added to VECTR’s evidence files upload feature.

How does it work?

The UI will display a warning if a user tries to upload a file greater than 190MB.

How can this feature help me?

Previously, uploading large files could cause the front-end to become unstable, and there was no visual indicator of what the application was doing. Until the VECTR team adds a configurable file size limit, this makes the interface more manageable.

Fix Database Creation Bug

What is it?

This fixes a bug where empty databases could be created by a combination of users accessing previously deleted databases.

How does it work?

This corrects the issue of empty databases being created.

How can this feature help me?

If you have encountered this issue it will now be fixed. There may be some instances where previously created empty databases will need to be manually deleted.

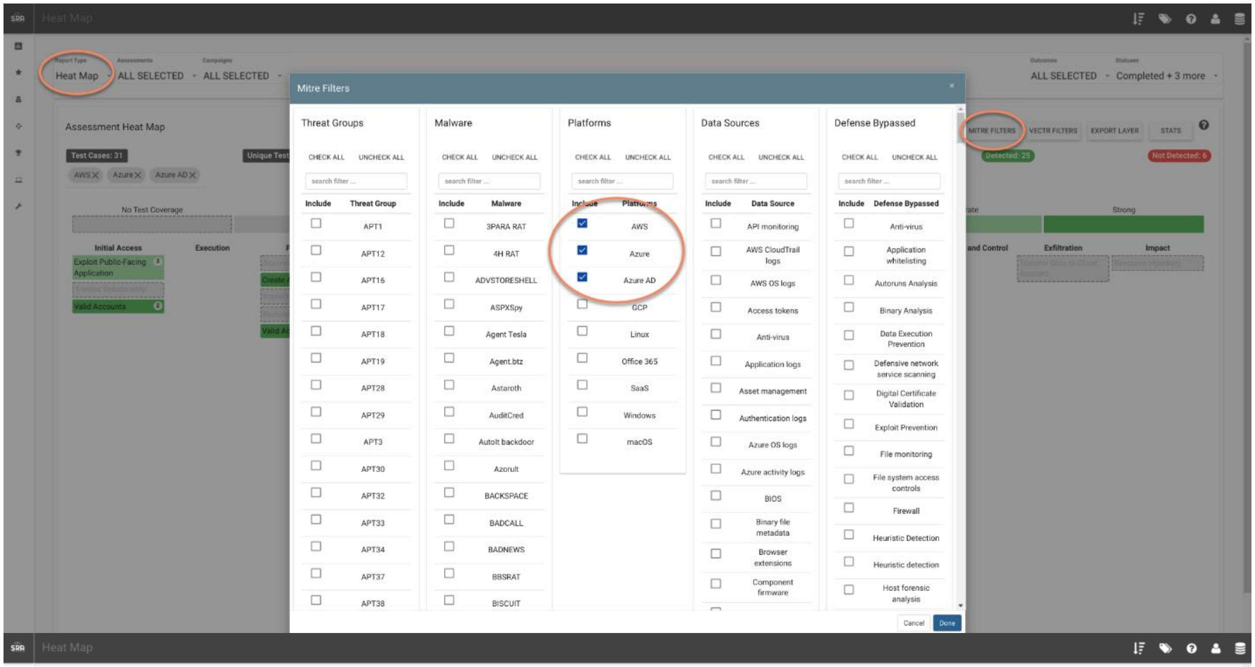
Heatmap Counts and Filter Visualization

What is it?

Shows currently applied data filters to your Heatmap, along with various statistics on the visible data.

How does it work?

Click either MITRE FILTERS and/or VECTR FILTERS, select filters.



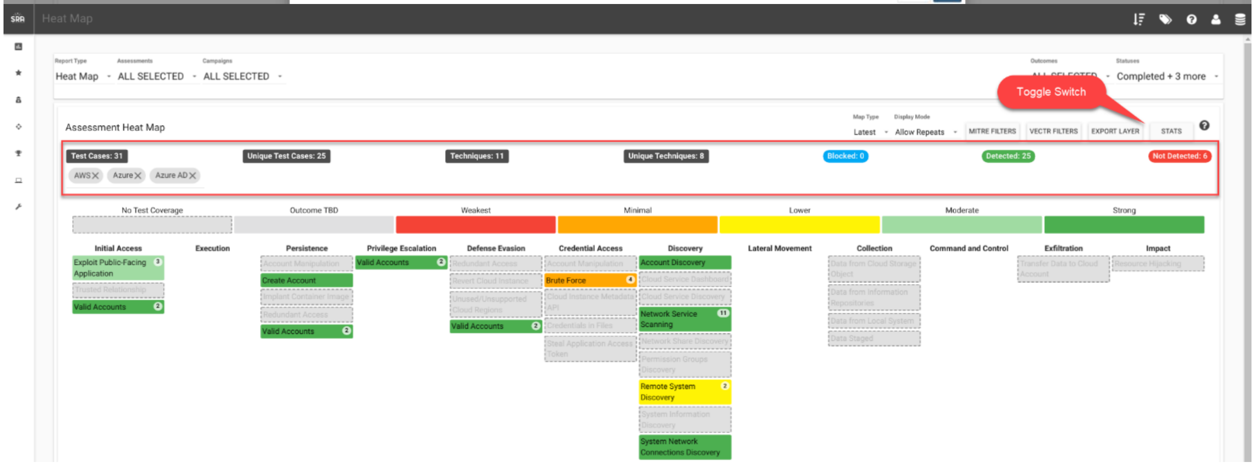
Threat Groups: APT1, APT12, APT16, APT17, APT18, APT19, APT28, APT29, APT3, APT30, APT32, APT33, APT34, APT37, APT38

Malware: 3PARA RAT, 4H RAT, ADVSTORESHELL, ASPXSpy, Agent Tesla, Agent.btz, Astaroth, AuditCred, Autoit backdoor, Azorult, BACKSPACE, BADCALL, BADNEWS, BBSRAT, BISCUIT

Platforms: ☑ AWS, ☑ Azure, ☑ Azure AD, □ GCP, □ Linux, □ Office 365, □ SaaS, □ Windows, □ macOS

Data Sources: API monitoring, AWS CloudTrail logs, AWS OS logs, Access tokens, Anti-virus, Application logs, Asset management, Authentication logs, Azure OS logs, Azure activity logs, BIOS, Binary file metadata, Browser extensions, Component firmware

Defense Bypassed: Anti-virus, Application whitelisting, Autoruns Analysis, Binary Analysis, Data Execution Prevention, Defensive network service scanning, Digital Certificate Validation, Exploit Prevention, File monitoring, File system access controls, Firewall, Heuristic Detection, Heuristic detection, Host forensic analysis



Test Cases: 31 | Unique Test Cases: 25 | Techniques: 11 | Unique Techniques: 8 | Blocked: 0 | Detected: 25 | Not Detected: 6

AWS, Azure, Azure AD

How can this feature help me?

Allows for visuals to show which filters are applied, along with easier to read counts of test cases and techniques.

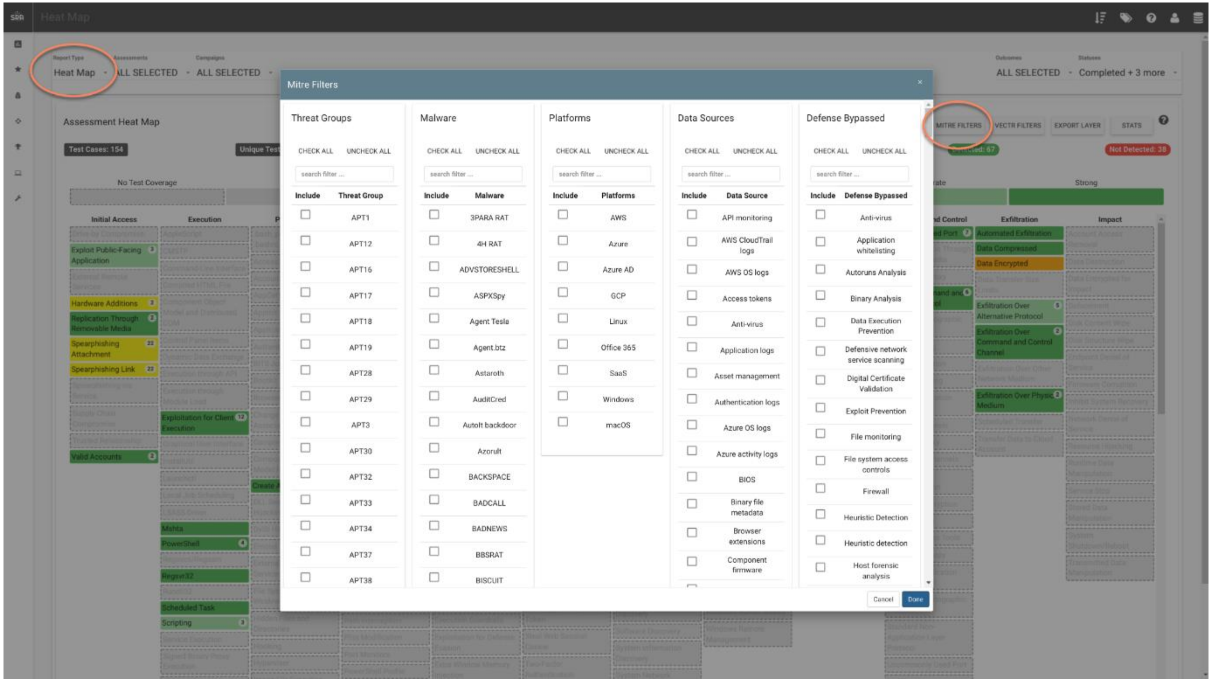
Heatmap Sub-matrix Filters

What is it?

Added different Enterprise filters to the Heatmap that are defined by MITRE Matrices. See https://attack.mitre.org/matrices/enterprise/

How does it work?

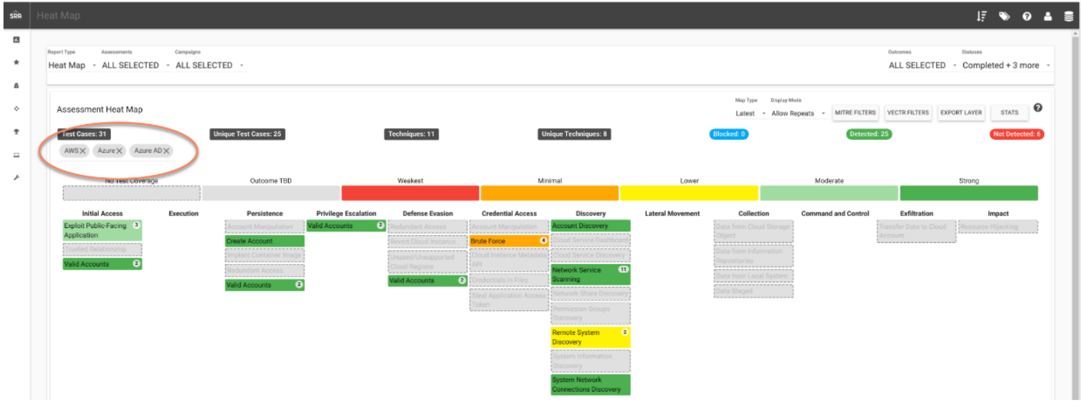
From the Heatmap Reporting screen, click the MITRE FILTERS button:



Report Type: Heat Map · Assessments: ALL SELECTED · Campaigns: ALL SELECTED · Outcomes: ALL SELECTED · Statuses: Completed + 3 more

How can this feature help me?

This will allow you to see theoretical coverage of techniques run by test cases from various assessments and campaigns.



Report Type: Heat Map · Assessments: ALL SELECTED · Campaigns: ALL SELECTED · Outcomes: ALL SELECTED · Statuses: Completed + 3 more

Map Type: Latest · Display Mode: Allow Repeats

Test Cases: 31 · Unique Test Cases: 25 · Techniques: 11 · Unique Techniques: 8 · Blocked: 0 · Detected: 25 · Not Detected: 6

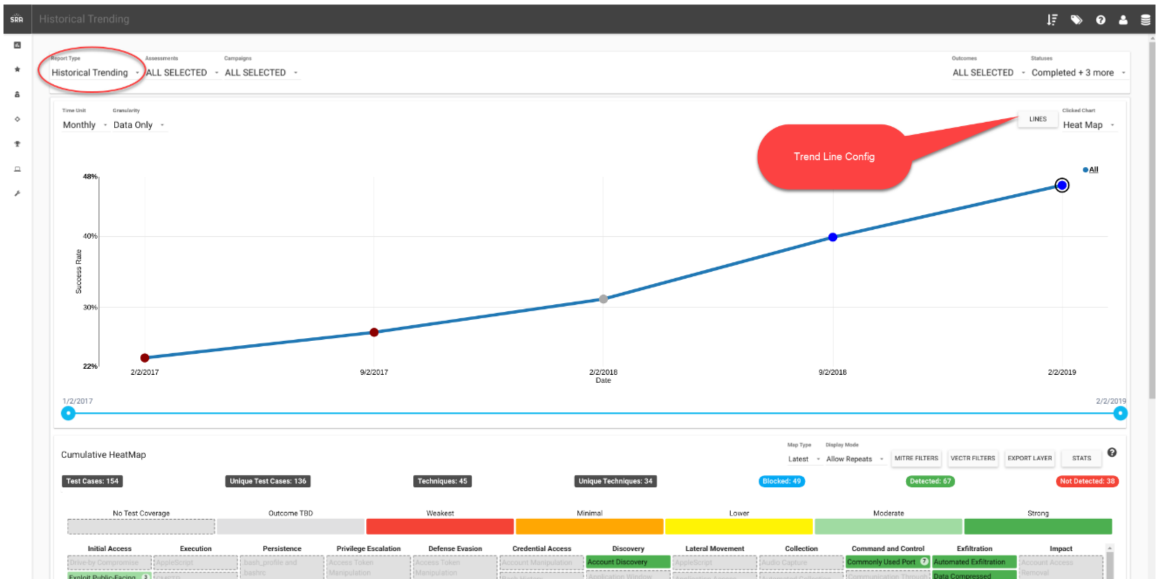
AWS ✕ Azure ✕ Azure AD ✕

Historical Trending Screen Multiple Trendlines

What is it?

Allows users to see how data is trending over time based on a Phases/Tactics, Attacker Tools, Tags, or Defensive Layers

How does it work?



Historical Trending

Report Type: Historical Trending
Assessments: ALL SELECTED
Campaigns: ALL SELECTED
Outcomes: ALL SELECTED
Statuses: Completed + 3 more

Time Unit: Monthly
Granularity: Data Only
Clicked Chart: Heat Map

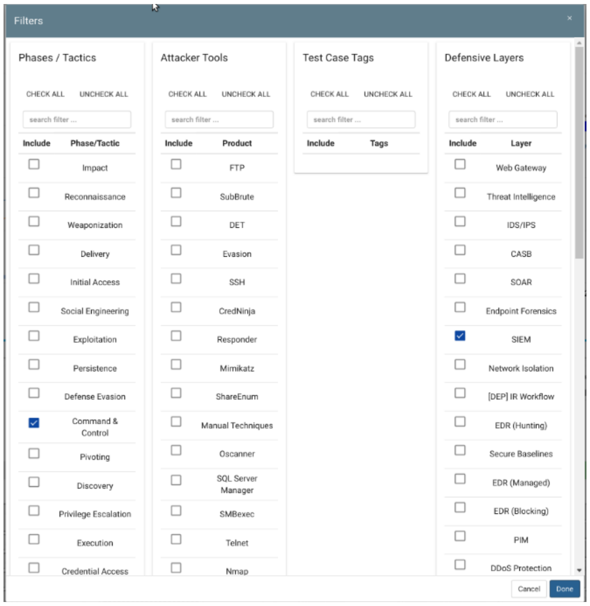
Trend Line Config

Cumulative HeatMap

Map Type: Latest
Display Mode: Allow Repeats

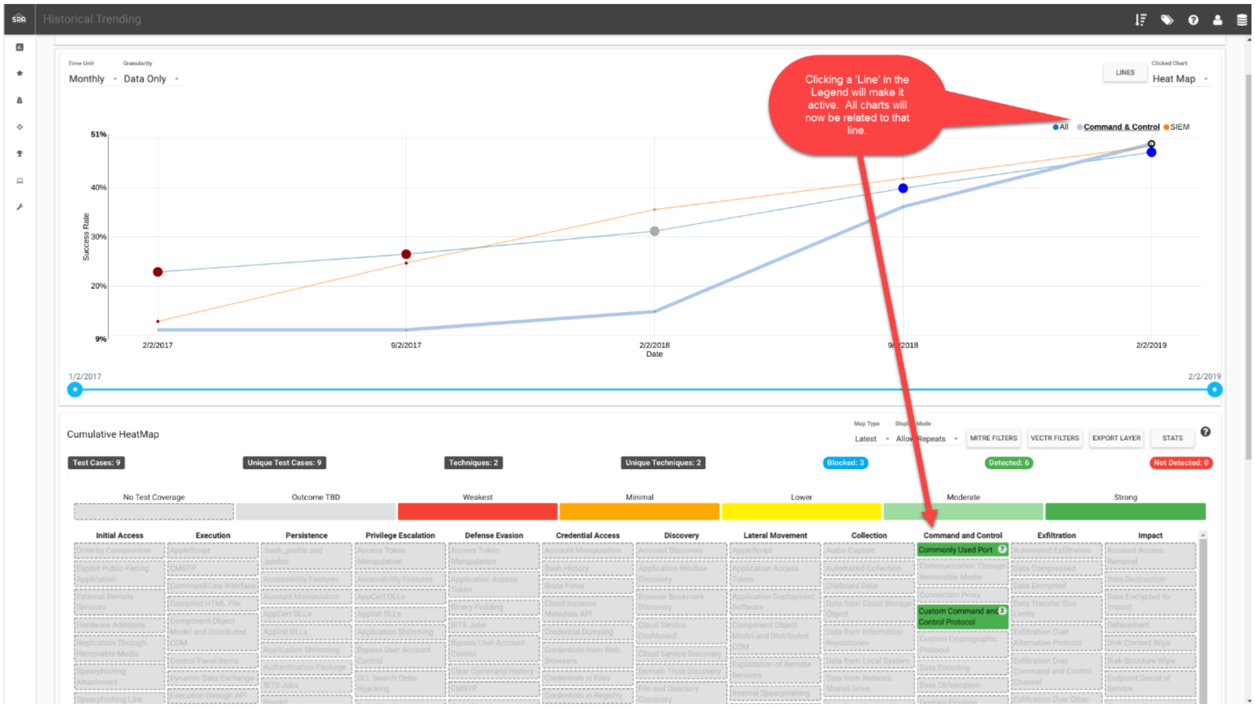
Test Cases: 154 | Unique Test Cases: 136 | Techniques: 45 | Unique Techniques: 34 | Blocked: 49 | Detected: 67 | Not Detected: 38

Click on data that you want to see historically trended:



Filters

Phases / Tactics		Attacker Tools		Test Case Tags		Defensive Layers	
Include	Phase/Tactic	Include	Product	Include	Tags	Include	Layer
☐	Impact	☐	FTP			☐	Web Gateway
☐	Reconnaissance	☐	SubBrute			☐	Threat Intelligence
☐	Weaponization	☐	DET			☐	IDS/IPS
☐	Delivery	☐	Evasion			☐	CASB
☐	Initial Access	☐	SSH			☐	SOAR
☐	Social Engineering	☐	CredNinja			☐	Endpoint Forensics
☐	Exploitation	☐	Responder			☑	SIEM
☐	Persistence	☐	Mimikatz			☐	Network Isolation
☐	Defense Evasion	☐	ShareEnum			☐	[DEP] IR Workflow
☑	Command & Control	☐	Manual Techniques			☐	EDR (Hunting)
☐	Pivoting	☐	Oscanner			☐	Secure Baselines
☐	Discovery	☐	SQL Server Manager			☐	EDR (Managed)
☐	Privilege Escalation	☐	SMBexec			☐	EDR (Blocking)
☐	Execution	☐	Telnet			☐	PIM
☐	Credential Access	☐	Nmap			☐	DDoS Protection



Time Unit: Monthly

Granularity: Data Only

Clicked Chart: Heat Map

Clicking a 'Line' in the Legend will make it active. All charts will now be related to that line.

Cumulative HeatMap

Map Type: Latest

Display Mode: Allow Repeats

Test Cases: 9

Unique Test Cases: 9

Techniques: 2

Unique Techniques: 2

Blocked: 3

Detected: 6

Not Detected: 0

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port 7	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Application Access Token	Bash History	Application Window Discovery	Application Access Token	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Application Deployment Software	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	BITS Jobs	Cloud Instance Metadata API	Cloud Service Dashboard	Component Object Model and Distributed COM	Data from Cloud Storage Object	Custom Command and Control Protocol 2	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Bypass User Account Control	Credential Dumping	Cloud Service Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Clear Command History	Credentials from Web Browsers	Domain Trust Discovery	Internal Spearphishing	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	CMSTP	Credentials in Files	File and Directory Discovery		Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other	Endpoint Denial of Service
	Execution through API	BITS Jobs			Credentials in Registry				Domain Fronting		
		Bootkit									

How can this feature help me?

This allows users to see how they are trending to different aspects of their program, whether it be tagged data, a specific phase/tactic, or a defensive tool.

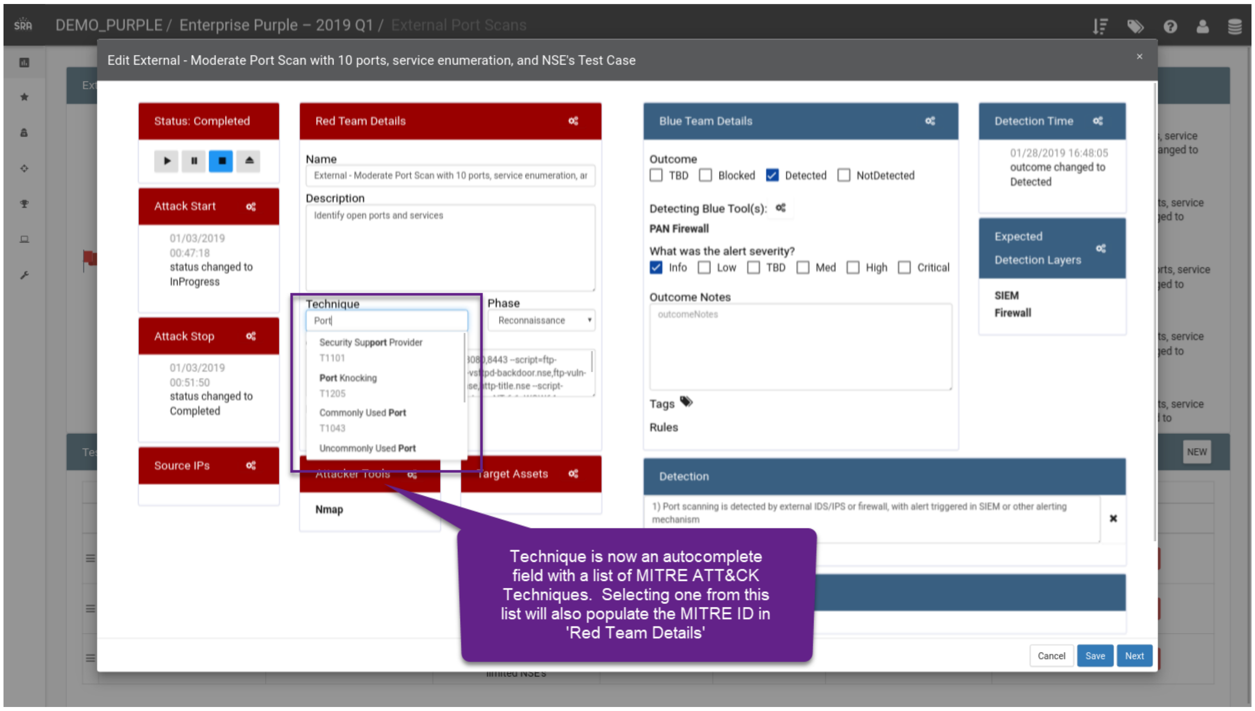
MITRE ATT&CK Technique Autocomplete

What is it?

This feature adds autocomplete capability to the Technique dropdown on the Test Case screen.

How does it work?

When entering a Technique on the Test Case screen the UI will now show a list of matching MITRE ATT&CK Techniques and ID's. Entering data here will automatically populate the Red Team Details so that the Test Case shows up appropriately in the Heatmap view.



DEMO_PURPLE / Enterprise Purple – 2019 Q1 / External Port Scans

Edit External - Moderate Port Scan with 10 ports, service enumeration, and NSE's Test Case

Status: Completed

Attack Start: 01/03/2019 00:47:18 status changed to InProgress

Attack Stop: 01/03/2019 00:51:50 status changed to Completed

Source IPs

Red Team Details

Name: External - Moderate Port Scan with 10 ports, service enumeration, ar

Description: Identify open ports and services

Technique: Port

- Security Support Provider T1101
- Port Knocking T1205
- Commonly Used Port T1043
- Uncommonly Used Port

Phase: Reconnaissance

Attacker Tools: Nmap

Target Assets

Blue Team Details

Outcome: ☐ TBD ☐ Blocked ☑ Detected ☐ NotDetected

Detecting Blue Tool(s): PAN Firewall

What was the alert severity? ☑ Info ☐ Low ☐ TBD ☐ Med ☐ High ☐ Critical

Outcome Notes: outcomeNotes

Tags

Rules

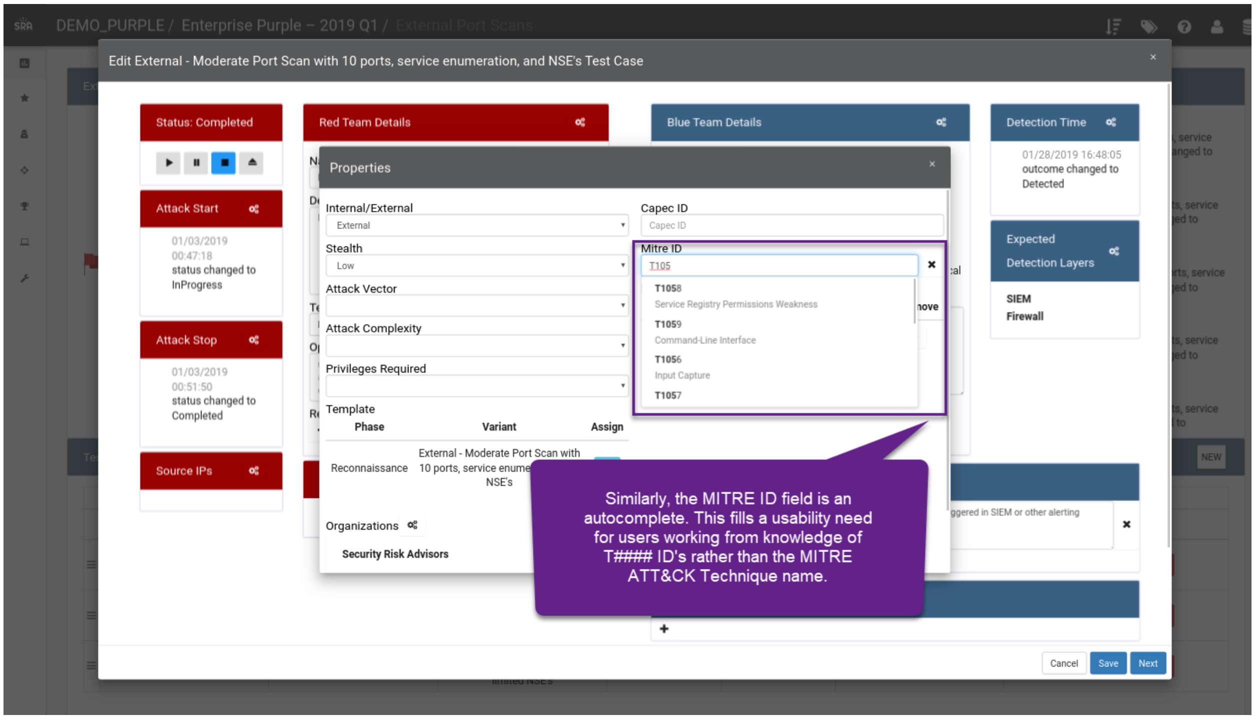
Detection Time: 01/28/2019 16:48:05 outcome changed to Detected

Expected Detection Layers: SIEM Firewall

Detection: 1) Port scanning is detected by external IDS/IPS or firewall, with alert triggered in SIEM or other alerting mechanism

Technique is now an autocomplete field with a list of MITRE ATT&CK Techniques. Selecting one from this list will also populate the MITRE ID in 'Red Team Details'

Additionally, when manually entering a Mitre ID on the Red Team Details screen (by clicking the cog in the Red Team Details header on the Test Case Screen) the Mitre ID will show an autocomplete list.



DEMO_PURPLE / Enterprise Purple – 2019 Q1 / External Port Scans

Edit External - Moderate Port Scan with 10 ports, service enumeration, and NSE's Test Case

Status: Completed

Attack Start: 01/03/2019 00:47:18 status changed to InProgress

Attack Stop: 01/03/2019 00:51:50 status changed to Completed

Detection Time: 01/28/2019 16:48:05 outcome changed to Detected

Expected Detection Layers: SIEM, Firewall

Properties

Internal/External: External

Stealth: Low

Attack Vector:

Attack Complexity:

Privileges Required:

Capec ID: Capec ID

Mitre ID: T105

T1058 Service Registry Permissions Weakness

T1059 Command-Line Interface

T1056 Input Capture

T1057

Template

Phase	Variant	Assign
Reconnaissance	External - Moderate Port Scan with 10 ports, service enume… NSE's	

Organizations: Security Risk Advisors

Similarly, the MITRE ID field is an autocomplete. This fills a usability need for users working from knowledge of T#### ID's rather than the MITRE ATT&CK Technique name.

How can this feature help me?

This will make it easier for Red Team operators to create new Test Cases and assign them to the appropriate MITRE ATT&CK Technique.

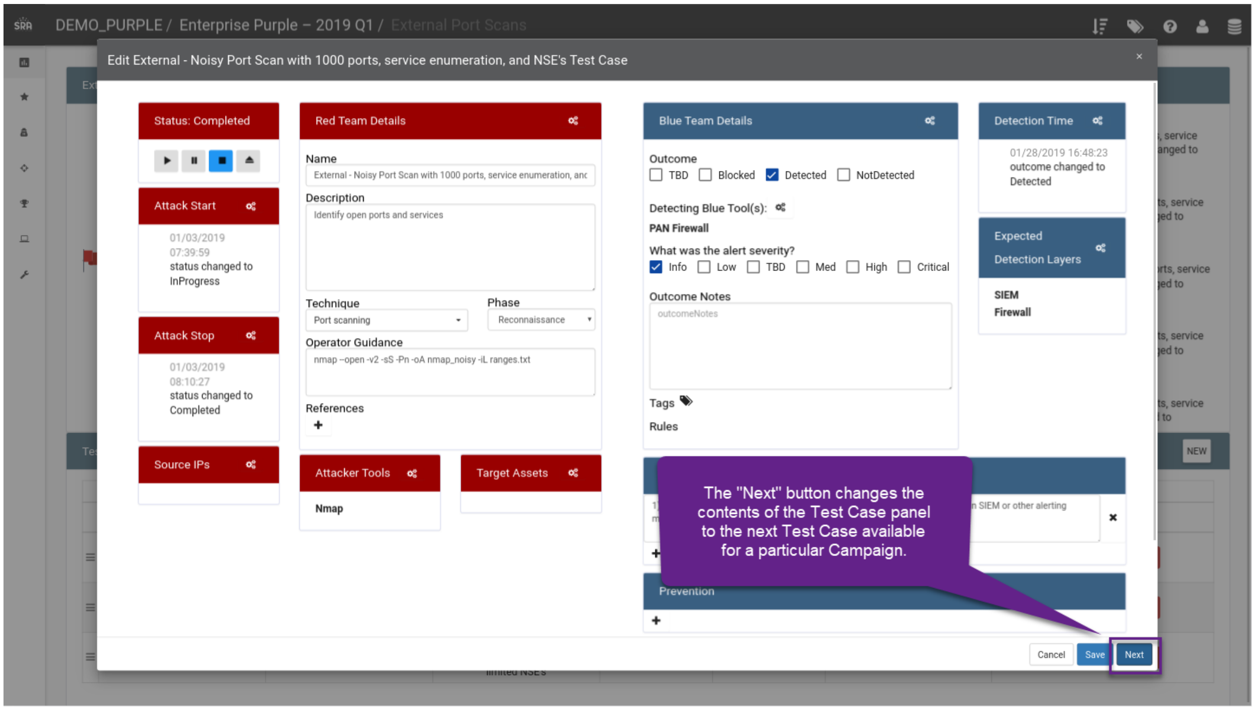
Next Test Case Button

What is it?

A Next button has been added to the Test Case panel to cycle through Test Cases in a campaign.

How does it work?

Clicking the "Next" button on the Test Case panel will update the view with the next available Test Case for a Campaign.



DEMO_PURPLE / Enterprise Purple – 2019 Q1 / External Port Scans

Edit External - Noisy Port Scan with 1000 ports, service enumeration, and NSE's Test Case

Status: Completed

Attack Start

01/03/2019 07:39:59 status changed to InProgress

Attack Stop

01/03/2019 08:10:27 status changed to Completed

Source IPs

Red Team Details

Name: External - Noisy Port Scan with 1000 ports, service enumeration, anc

Description: Identify open ports and services

Technique: Port scanning

Phase: Reconnaissance

Operator Guidance: nmap --open -v2 -sS -Pn -oA nmap_noisy -iL ranges.txt

References

Attacker Tools: Nmap

Target Assets

Blue Team Details

Outcome: □ TBD □ Blocked ☑ Detected □ NotDetected

Detecting Blue Tool(s): PAN Firewall

What was the alert severity? ☑ Info □ Low □ TBD □ Med □ High □ Critical

Outcome Notes: outcomeNotes

Tags

Rules

Detection Time

01/28/2019 16:48:23 outcome changed to Detected

Expected Detection Layers

SIEM
Firewall

Prevention

The "Next" button changes the contents of the Test Case panel to the next Test Case available for a particular Campaign.

How can this feature help me?

This feature makes it easier for users to navigate Test Cases during a comprehensive Purple Team exercise.

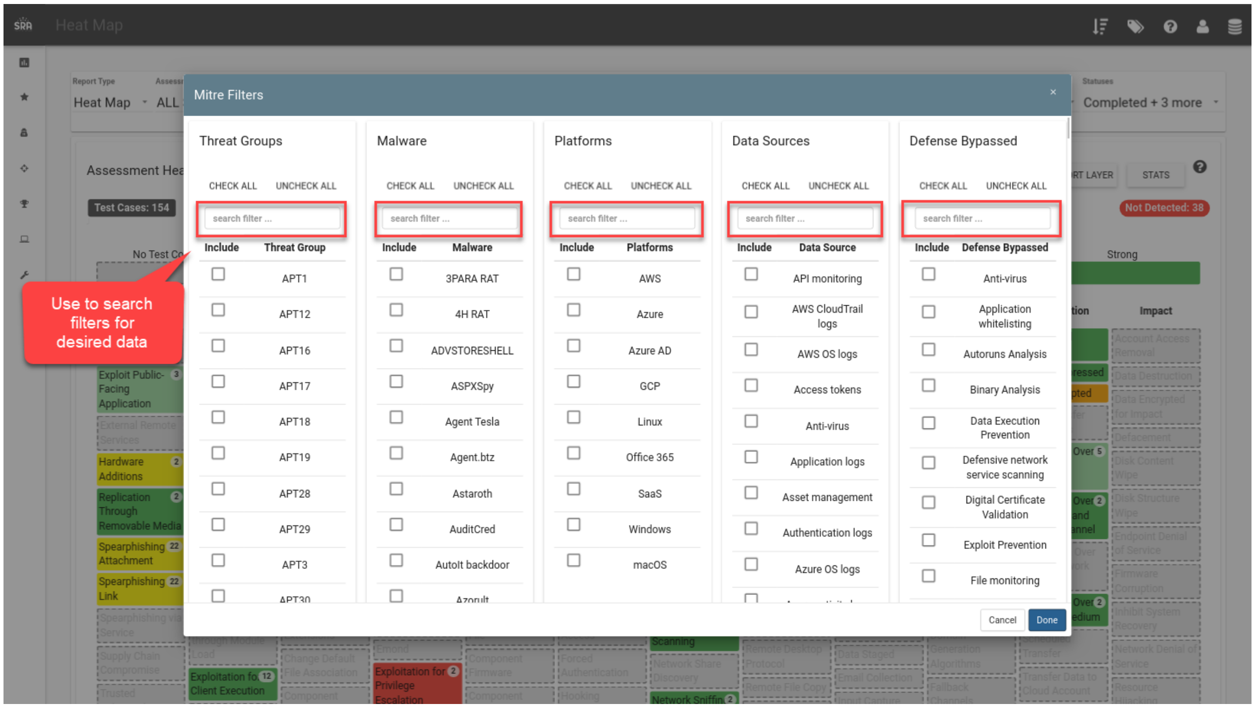
Search Filters for Target Assets and Heatmap Filters

What is it?

Search filter fields have been added for Heatmap filters and the Target Assets screen.

How does it work?

Type a word or characters to refine data shown in the following data tables. Then select your desired data. This example shows a listing of searchable Heatmap filters.



Use to search filters for desired data

Mitre Filters

Threat Groups

Include	Threat Group
☐	APT1
☐	APT12
☐	APT16
☐	APT17
☐	APT18
☐	APT19
☐	APT28
☐	APT29
☐	APT3
☐	APT30

Malware

Include	Malware
☐	3PARA RAT
☐	4H RAT
☐	ADVSTORESHELL
☐	ASPXSpy
☐	Agent Tesla
☐	Agent.btz
☐	Astaroth
☐	AuditCred
☐	AutoIt backdoor
☐	Azorult

Platforms

Include	Platforms
☐	AWS
☐	Azure
☐	Azure AD
☐	GCP
☐	Linux
☐	Office 365
☐	SaaS
☐	Windows
☐	macOS

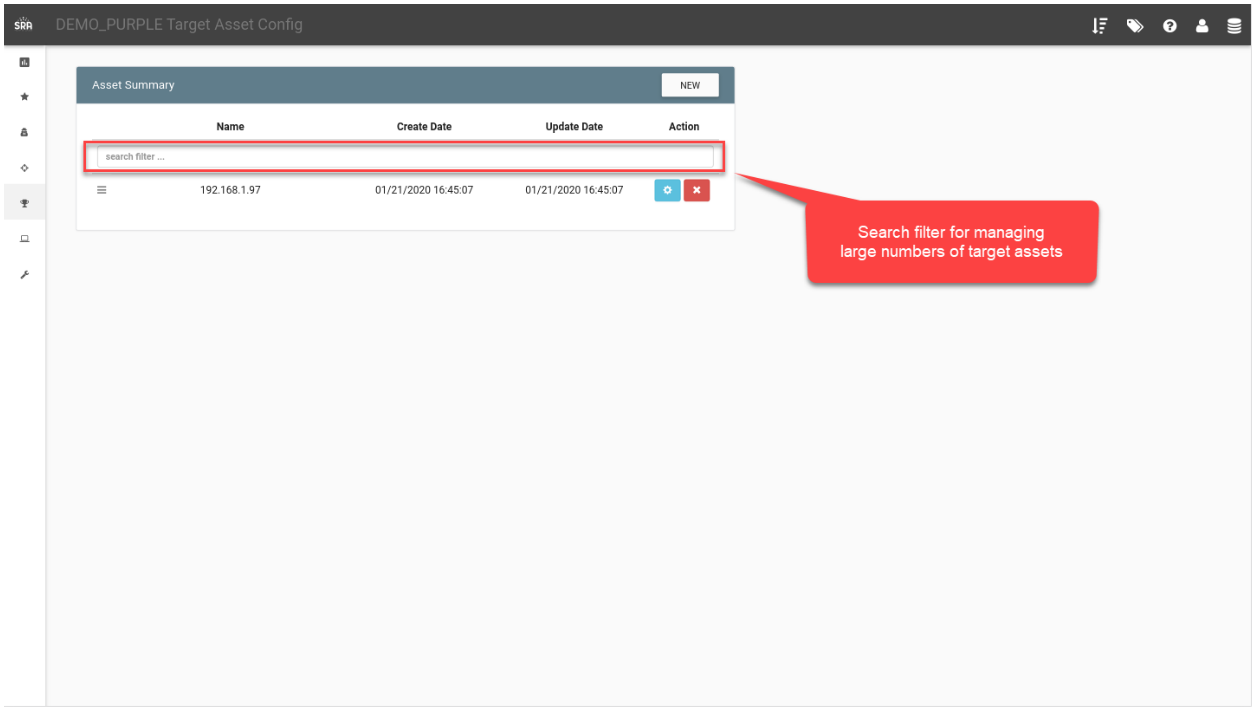
Data Sources

Include	Data Source
☐	API monitoring
☐	AWS CloudTrail logs
☐	AWS OS logs
☐	Access tokens
☐	Anti-virus
☐	Application logs
☐	Asset management
☐	Authentication logs
☐	Azure OS logs

Defense Bypassed

Include	Defense Bypassed
☐	Anti-virus
☐	Application whitelisting
☐	Autoruns Analysis
☐	Binary Analysis
☐	Data Execution Prevention
☐	Defensive network service scanning
☐	Digital Certificate Validation
☐	Exploit Prevention
☐	File monitoring

The Target Assets screen is also searchable to make it easier to manage larger data sets.



Name	Create Date	Update Date	Action
192.168.1.97	01/21/2020 16:45:07	01/21/2020 16:45:07	

Search filter for managing large numbers of target assets

How can this feature help me?

This feature makes it quicker to find and select desired data in the system.

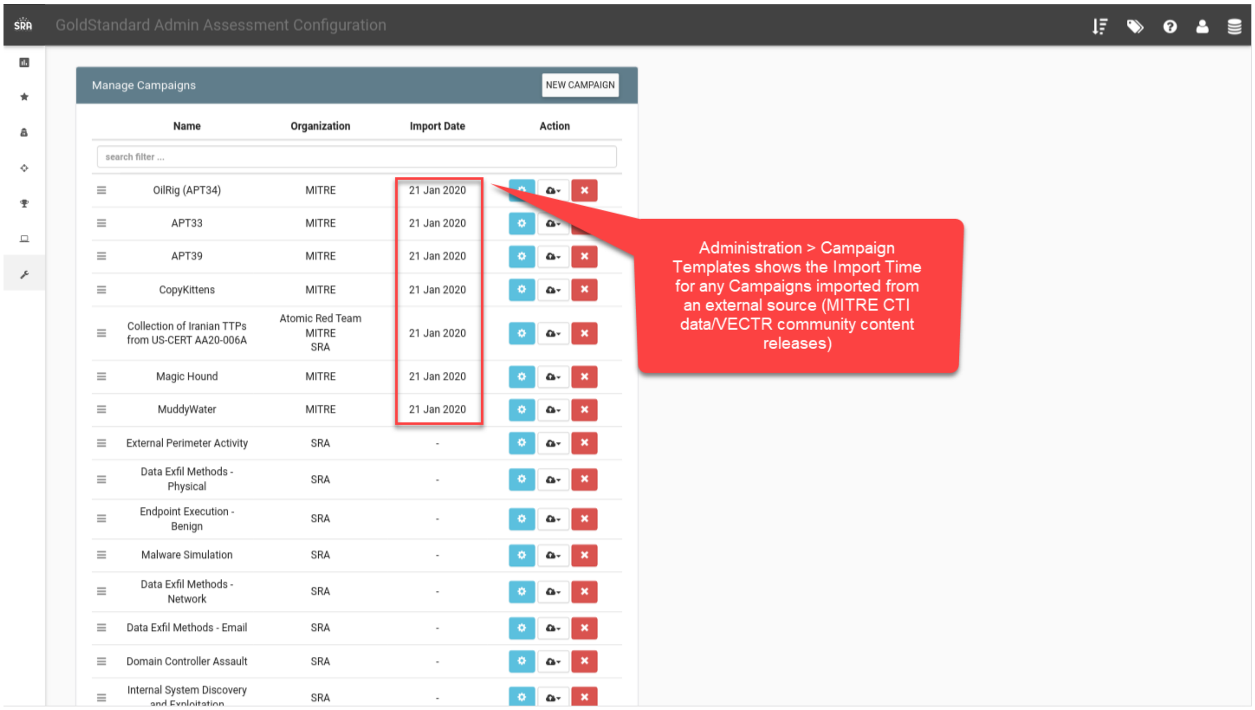
Show Import Date and Time for Campaigns

What is it?

The Campaign Templates screen will now show an Import Date column.

How does it work?

Import Date is populated for any campaigns that have been imported from an external source like the MITRE CTI enterprise-attack json file.



Name	Organization	Import Date	Action
OilRig (APT34)	MITRE	21 Jan 2020	
APT33	MITRE	21 Jan 2020	
APT39	MITRE	21 Jan 2020	
CopyKittens	MITRE	21 Jan 2020	
Collection of Iranian TTPs from US-CERT AA20-006A	Atomic Red Team MITRE SRA	21 Jan 2020	
Magic Hound	MITRE	21 Jan 2020	
MuddyWater	MITRE	21 Jan 2020	
External Perimeter Activity	SRA	-	
Data Exfil Methods - Physical	SRA	-	
Endpoint Execution - Benign	SRA	-	
Malware Simulation	SRA	-	
Data Exfil Methods - Network	SRA	-	
Data Exfil Methods - Email	SRA	-	
Domain Controller Assault	SRA	-	
Internal System Discovery and Exploitation	SRA	-	

Administration > Campaign Templates shows the Import Time for any Campaigns imported from an external source (MITRE CTI data/VECTR community content releases)

How can this feature help me?

It's helpful for operators to know when a campaign was last imported to determine if there have been updates or if a campaign may be out of date.

Tooltips Improved

What is it?

Tooltips have been standardized and added to more fields in VECTR.

How does it work?

Hover over a field to see a tooltip with a name or description of the control. VECTR previously had tooltips, but they were uncommon and not attached to all controls that might need explanation.

How can this feature help me?

Additional tooltips were added to improve the usability of the application.