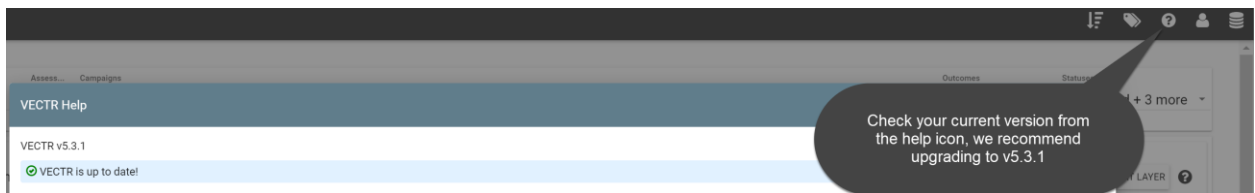


Importing CTI into VECTR

1. Confirm you're on the latest VECTR release

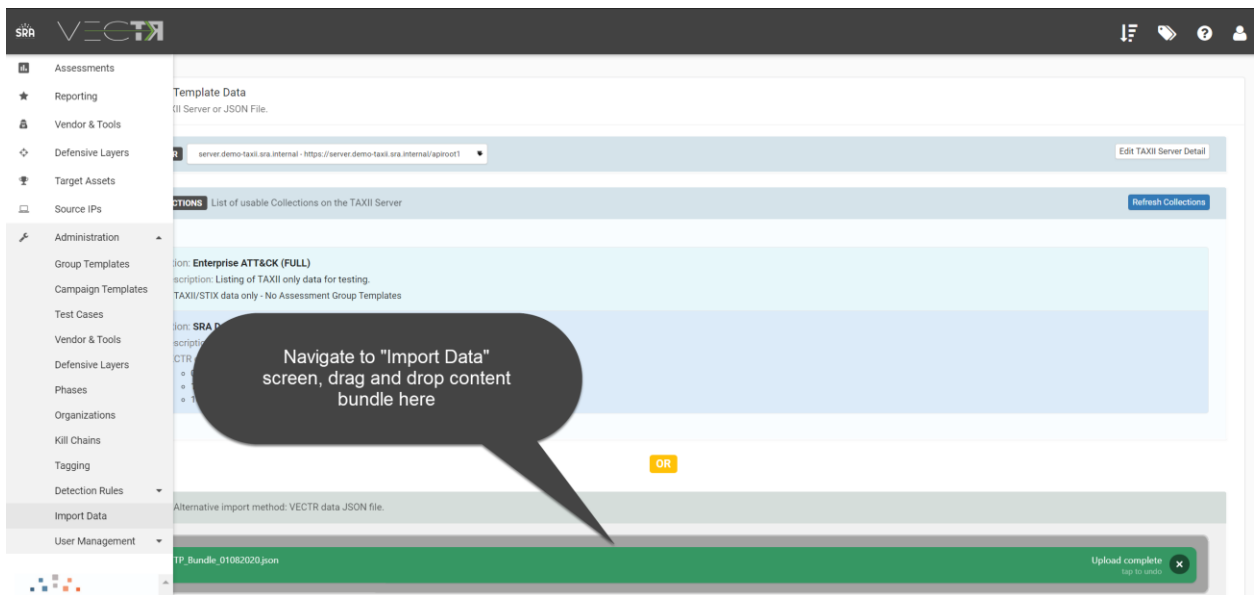


2. Download the “Iranian TTP Bundle” here

https://github.com/SecurityRiskAdvisors/VECTR/blob/master/cti/Iranian_TTP_Bundle_010920.json

Note: STIX 2.0 bundles from MITRE can also be downloaded from MITRE’s CTI GitHub page and imported into VECTR. For example the following bundle can be downloaded and imported to bring in the entire ATT&CK framework or only selected content (<https://github.com/mitre/cti/blob/master/enterprise-attack/enterprise-attack.json>). This will create many campaign templates in VECTR that can be used for further assessment planning and targeted APT emulation purposes. Other framework bundles such as PRE-ATT&CK and MOBILE can also be imported in the same fashion.

3. Import data into VECTR



4. Preview and import campaign templates

The screenshot shows the 'Import VECTR Data' interface. At the top, it says 'Data to be imported from file and merged with VECTR Template Data.' Below this, a summary bar indicates '1 Assessment Group Templates', '7 Campaigns', and '162 Total Test Cases Selected.' A 'Submit' button is on the right. The main area shows a list of campaign templates under the heading 'Assessment Group Template: Iranian TTP Bundle → 7 Campaigns.' The list includes:

- Campaign: CopyKittens → 3 Test Cases.
- Campaign: OilRig (APT34) → 44 Test Cases.
- Campaign: MuddyWater → 31 Test Cases.
- Campaign: Collection of Iranian TTPs from US-CERT AA20-006A → 15 Test Cases.
- Campaign: APT39 → 11 Test Cases.
- Campaign: Magic Hound → 27 Test Cases.
- Campaign: APT33 → 21 Test Cases.

A callout bubble points to the list with the text: 'Preview and import new campaigns into VECTR'. A 'Submit' button is at the bottom right.

5. Navigate to the home dashboard to create a new assessment

The screenshot shows the 'Assessments' dashboard. At the top, there's a header 'DEMO_PURPLE' and a 'CREATE NEW' button. Below the header is a table of assessments:

Name	Create Date	Status	Tags	Actions
Enterprise Purple - 2020 Q1	11/12/2019	In Progress		⋮
Enterprise Purple - 2019 Q1	01/02/2019	Completed		⋮
Enterprise Purple - 2018 Q3	08/02/2018	Completed		⋮
Enterprise Purple - 2018 Q1	01/02/2018	Completed		⋮
Enterprise Purple - 2017 Q3	08/02/2017	Completed		⋮
Enterprise Purple - 2017 Q1	01/02/2017	Completed		⋮

A callout bubble points to the 'CREATE NEW' button with the text: 'Navigate to the home dashboard and create new assessment'.

6. Select the newly imported assessment template

The screenshot shows the 'New Assessment' form. It has fields for 'Name', 'Description', 'From Template', and 'Kill Chain'. The 'From Template' dropdown is set to 'Iranian TTP Bundle'. Below these fields is a table with columns 'Select', 'Organization', 'Campaign', and '# TestCases'.

Select	Organization	Campaign	# TestCases
<input checked="" type="checkbox"/>	All		

A callout bubble points to the 'From Template' dropdown with the text: 'Create new assessment with "Iranian TTP Bundle" template selected'.

7. Load the assessment from home dashboard view

Assessments

Name	Create Date	Status	Tags	Actions
Iran APT Emulations - Q1 2020	01/09/2020	Not Performed		
Enterprise Purple - 2020 Q1	11/12/2019	In Progress		
Enterprise Purple - 2019 Q1				
Enterprise Purple - 2018 Q3	08/02/2018			
Enterprise Purple - 2018 Q1	01/02/2018			
Enterprise Purple - 2017 Q3	08/02/2017			
Enterprise Purple - 2017 Q1	01/02/2017	Completed		

CREATE NEW FROM NAV LAYER ?

New assessment created, click on the row to load it or select other Actions from the drop-down

Tip: You can also drag and drop these rows to re-order your assessments

8. Load different campaigns/APT groups from campaign dashboard

Campaign Dashboard

Name	Progress	Outcome	Tags	Action
Collection of Iranian TTPs from US-CERT AA20-006A	100%	27% 33% 40%		
Copy Kittens	0%	0%		
Magic Hound	0%	0%		
APT33	0%			
OilRig (APT34)	0%			
MuddyWater	0%			
APT39	0%	0%		

Campaign Dashboard View: Jump into specific campaigns of interest here and start measuring your progress

Load Reports Tagging

9. Detailed Campaign View: In this example, we are tracking test cases against some common TTPs used in the past by Iranian threat groups as recommended in US-CERT Alert (AA20-006A)

Collection of Iranian TTPs from US-CERT AA20-006A: Escalation Path

Timeline

- 01/09/2020 09:01:20 Extract Logonpasswords via Beacon Logonpasswords : outcome changed to Blocked
- 01/09/2020 09:01:18 Extract Logonpasswords via Beacon Logonpasswords : status changed to Completed
- 01/09/2020 09:01:17 Extract Logonpasswords via Beacon Logonpasswords :

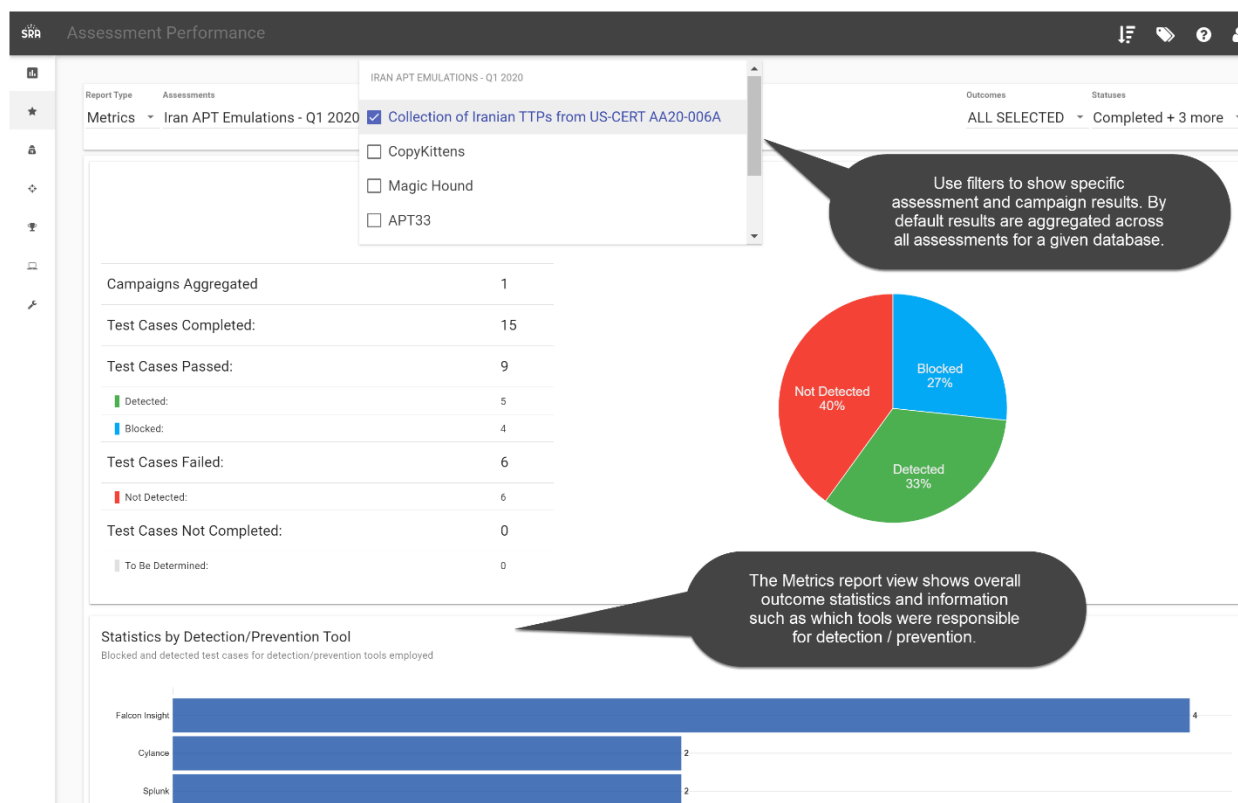
Test Cases

Phase	Technique	Test Case	Status	Outcome	
Defense Evasion	Obfuscated Files or Information	Obfuscated Commands - CMD	Completed	Not Detected	INVESTIGATE
Credential Access	Credential Dumping	Extract Password Hashes via NTDSutil	Completed	Not Detected	INVESTIGATE
Exfiltration	Data Compressed	Compress Data for Exfiltration With PowerShell	Completed	Detected	
Delivery	Phishing Payload	Cobalt Strike Standard Macro - Attachment	Completed	Blocked	

Campaign Detailed View: Click on the icons or test cases in the table for detailed test case panels.

Other useful actions are available such as cloning an existing test case and applying tags for tracking

10. Viewing Reports across multiple assessments or campaigns



11. Viewing assessment results in the dynamic Heat Map view, showing relative coverage across the MITRE ATT&CK™ Enterprise framework

