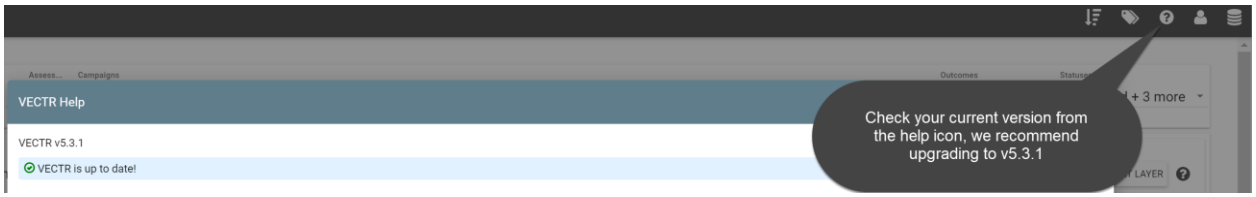
Importing CTI into VECTR

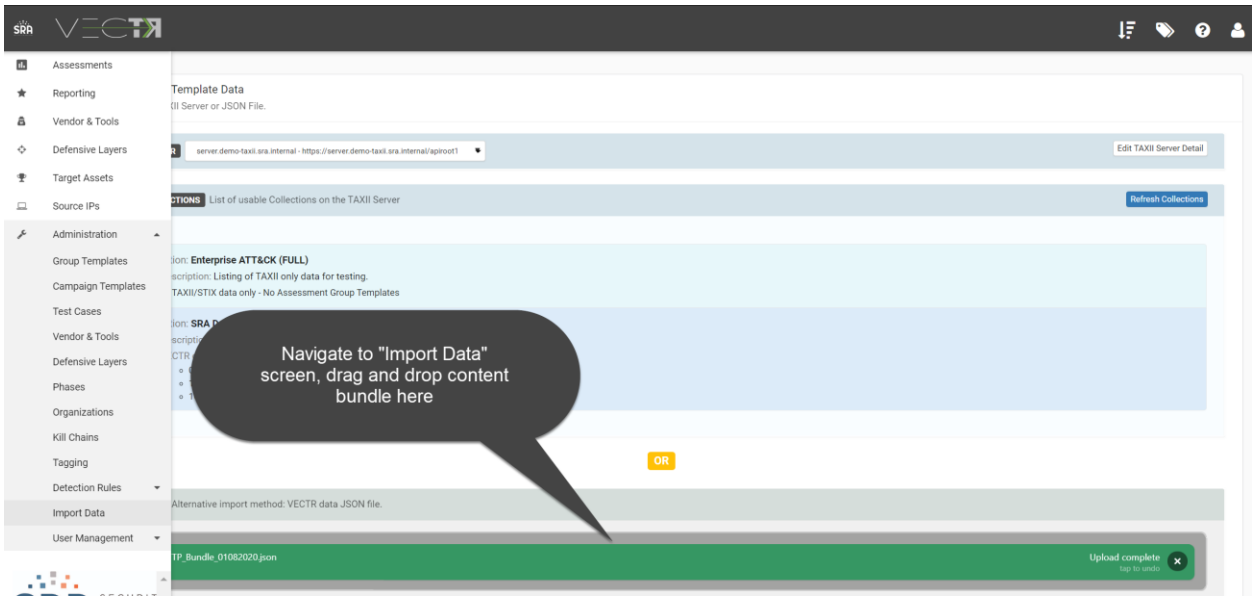
1. Confirm you're on the latest VECTR release



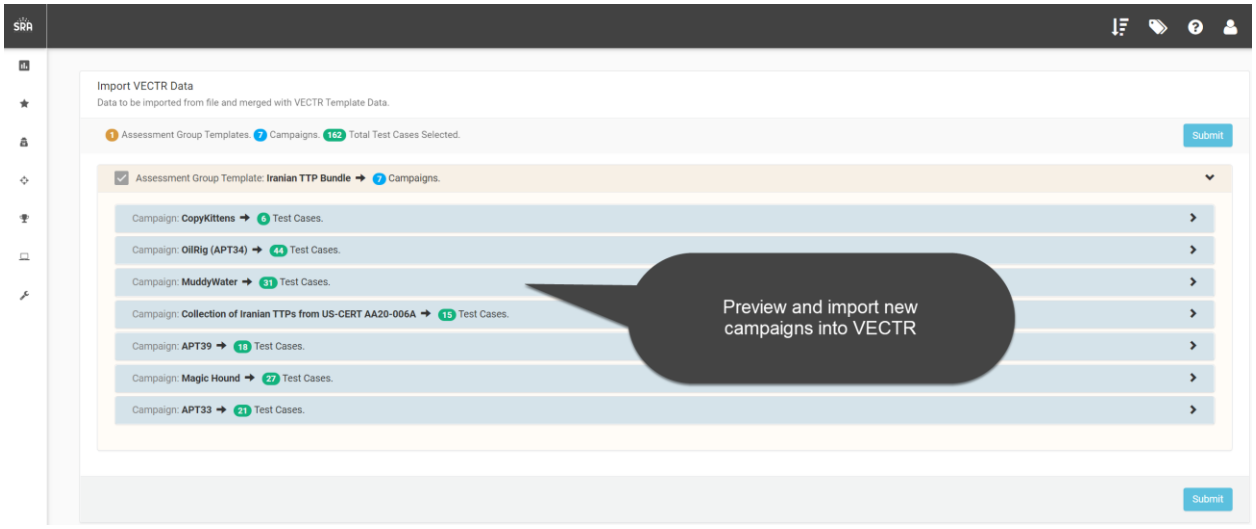
2. Download the "Iranian TTP Bundle" here
   https://github.com/SecurityRiskAdvisors/VECTR/blob/master/cti/Iranian_TTP_Bundle_010920.json

   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.

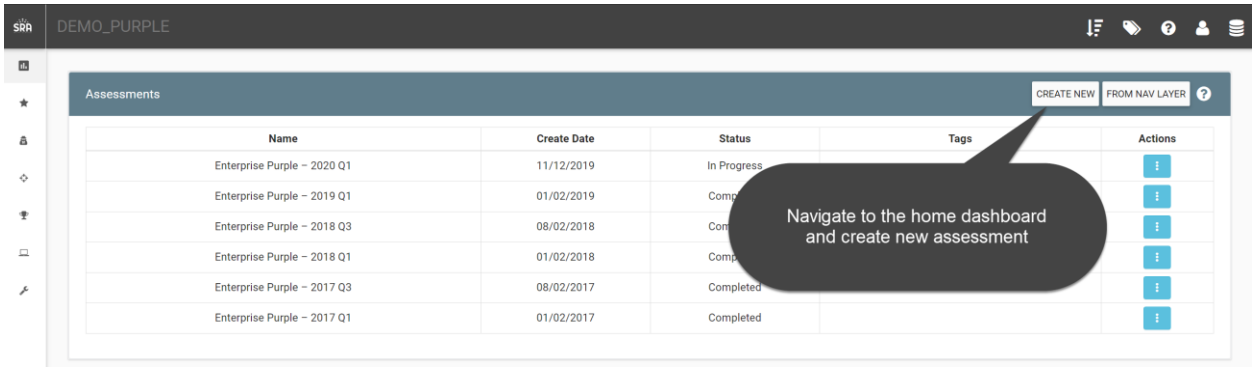
3. Import data into VECTR



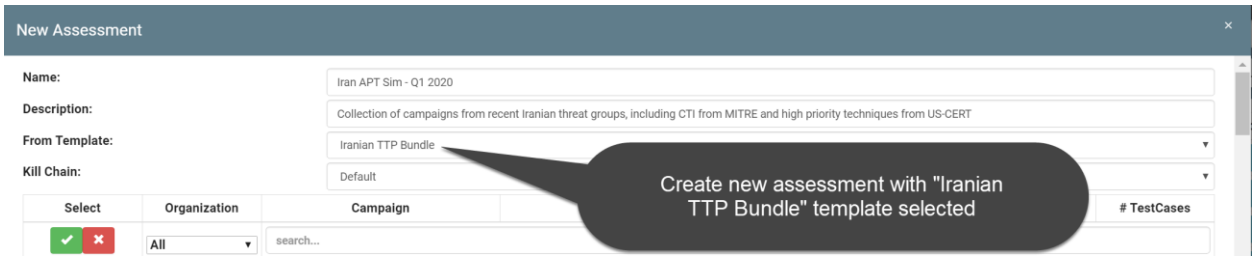
4. Preview and import campaign templates



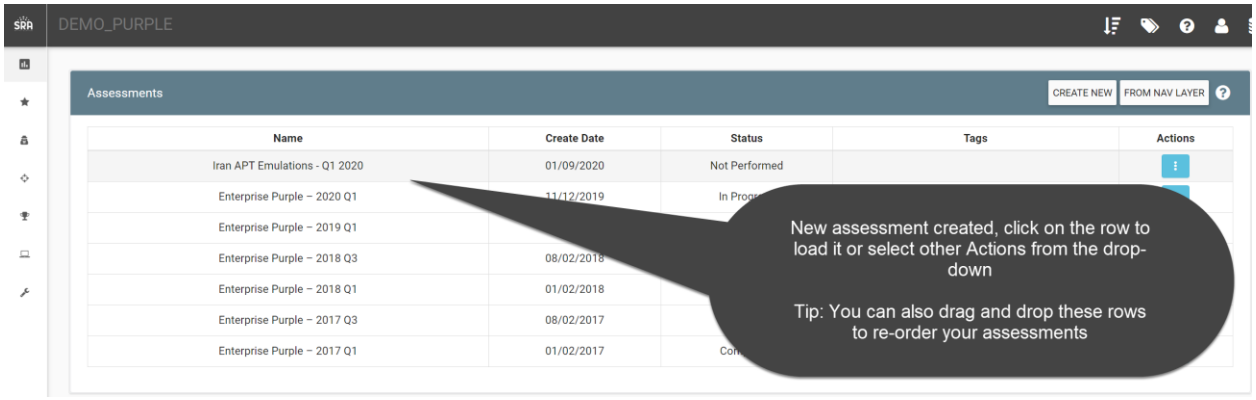
5. Navigate to the home dashboard to create a new assessment



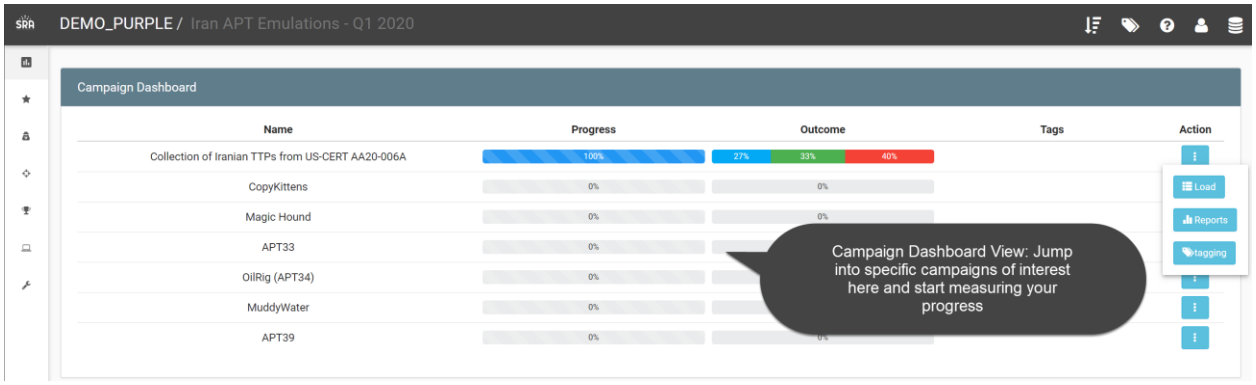
6. Select the newly imported assessment template



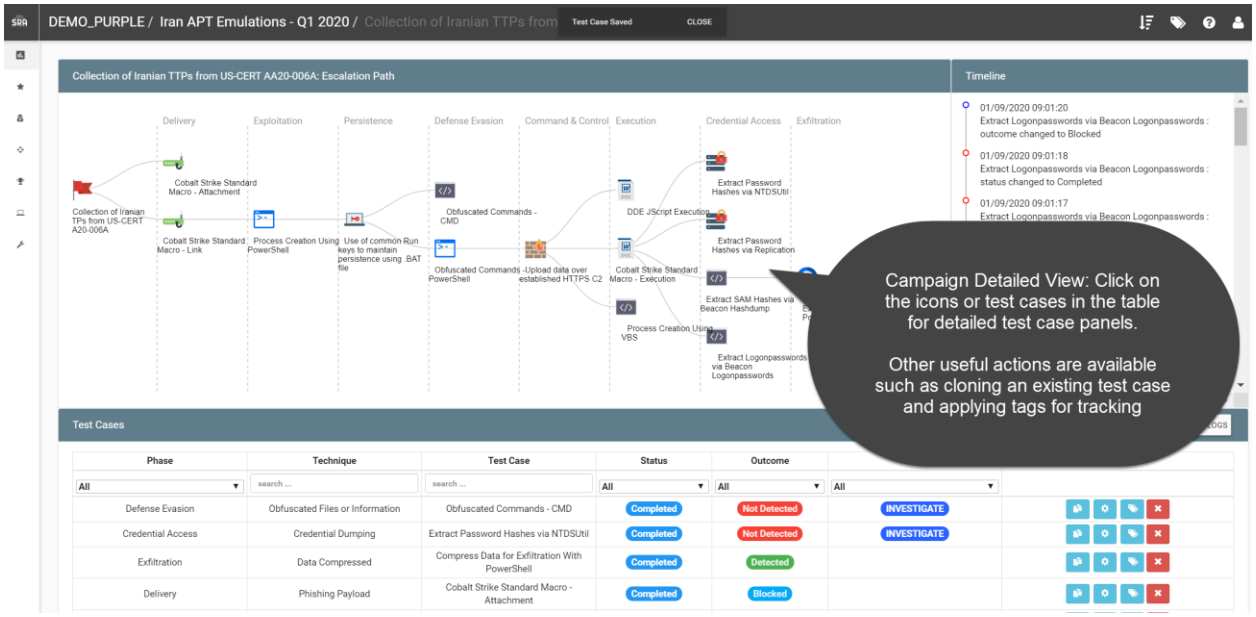
7. Load the assessment from home dashboard view



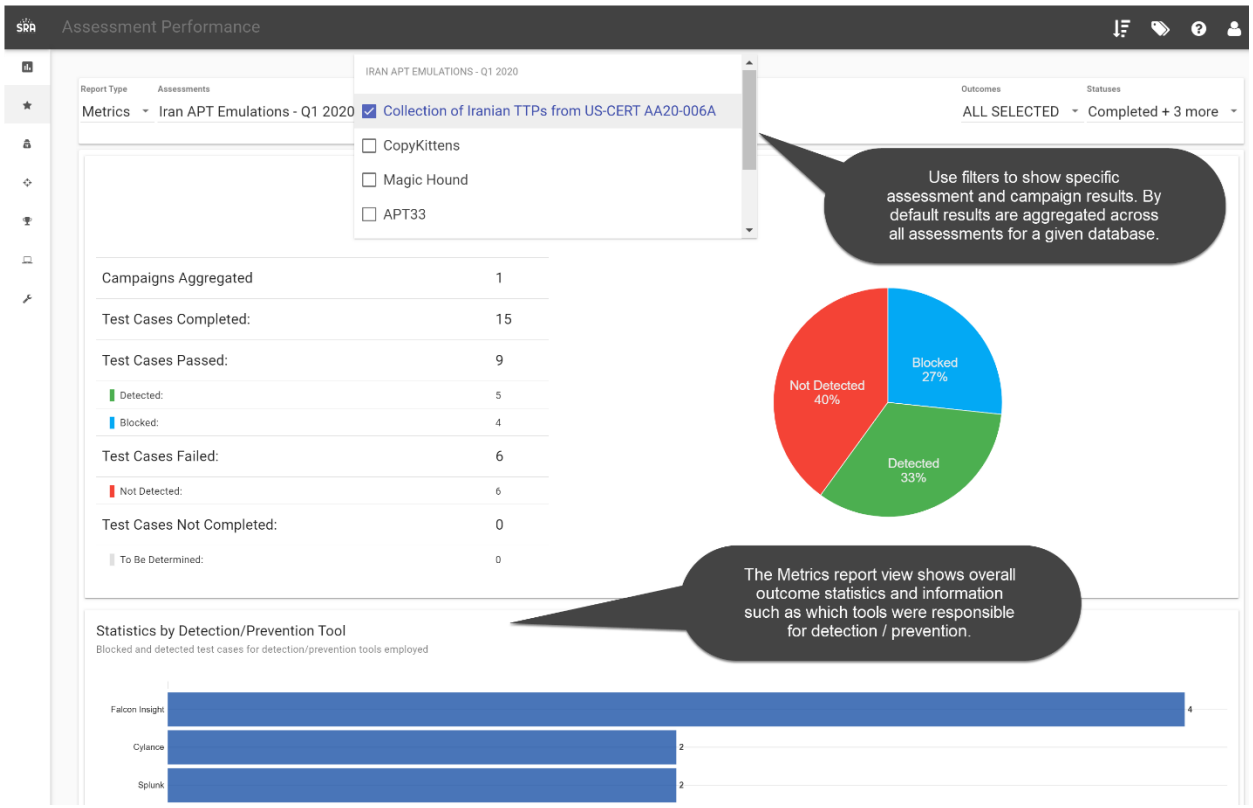
8. Load different campaigns/APT groups from campaign dashboard



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)



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