

VECTR v4.4.1 Feature Breakdown

Table of Contents

- Tagging System 2
- Assessment Group Templates 4
- Running SSL in Docker..... 6

Tagging System

What is it?

VECTR can now tag Test Cases for easy access and organization.

How does it work?

There is now a “tags” section in the Test Case popup:

Edit External - Stealthy Port Scan with 3 ports, service enumeration, limited NSE's Test Case

Status: Completed

Attack Start: 11/03/2015 00:26:20 status changed to InProgress

Attack Stop: 11/03/2015 00:46:30 status changed to Completed

Source IPs

Red Team Details

Name: External - Stealthy Port Scan with 3 ports, service enumeration, limiter

Description: Identify open ports and services

Attack Pattern: Targeted Port Scanning

Phase: External Recon

Command: command

References: +

Blue Team Details

Outcome: ☐ TBD ☐ Blocked ☐ Detected ☒ NotDetected

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

Outcome Notes: outcomeNotes

Tags

Detection Time: 11/16/2015 16:11:05 outcome changed to NotDetected

Expected Detection Layers: IDS/IPS, Firewall

Successful Detection Behavior

1) An alert is configured on the External IDS/IPS/NGFW and/or SIEM when port scanning is detected.

2) There is an Incident Response Workflow in place to investigate and block the offending IP address

Cancel Save

Clicking this will bring you to a selection screen with all your tags. If there are no tags created, you can create one by clicking Add/Edit Labels:

SELECT

Click Here

Add/Edit Labels Done

Now you can select a color at the bottom, then give your label custom text:

CONFIGURE

Priority 1

Apply

SELECT

☒ Priority 1

Add/Edit Labels

Done

Status: Completed

Attack Start

11/03/2015 00:26:20

status changed to InProgress

Attack Stop

11/03/2015 00:46:30

status changed to Completed

Source IPs

Red Team Details

Name

External - Stealthy Port Scan with 3 ports, service enumeration, limited NSE's Test Case

Description

Identify open ports and services

Attack Pattern

Targeted Port Scanning

Phase

External Recon

Command

command

References

+

Attacker Tools

Target Assets

Blue Team Details

Outcome

☐ TBD
☐ Blocked
☐ Detected
☒ NotDetected

Was the event source logged?

☐ TBD
☒ Yes
☐ No

Outcome Notes

outcomeNotes

Tags

Priority 1

Successful Detection Behavior

1) An alert is configured on the External IDS/IPS/NGFW and/or SIEM when port scanning is detected.

Detection Time

11/16/2015 16:11:05

outcome changed to NotDetected

Expected Detection Layers

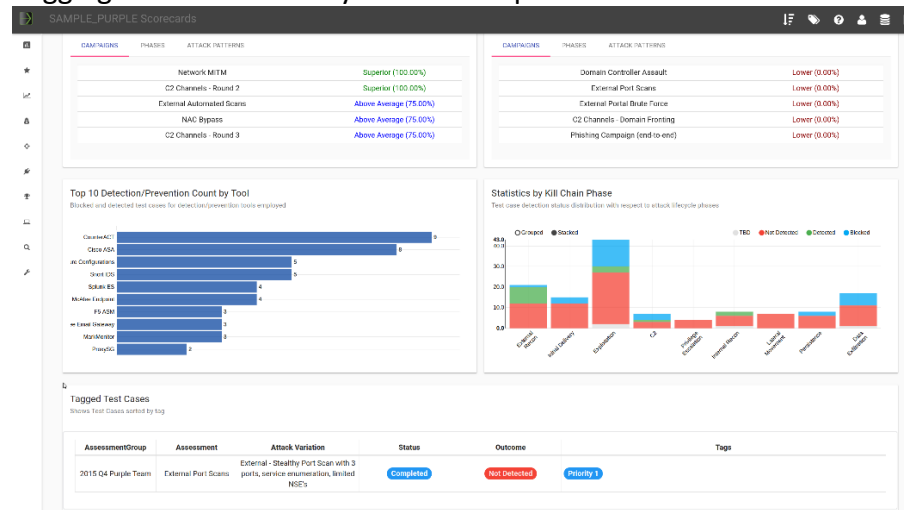
IDS/IPS

Firewall

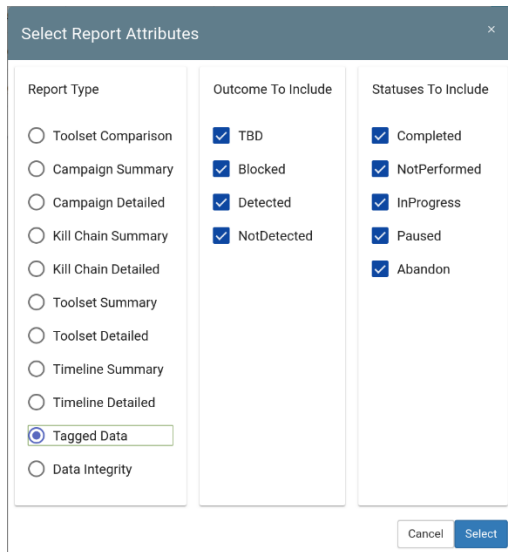
Cancel

Save

Tagging Test Cases allow you to see important information in the scorecard:

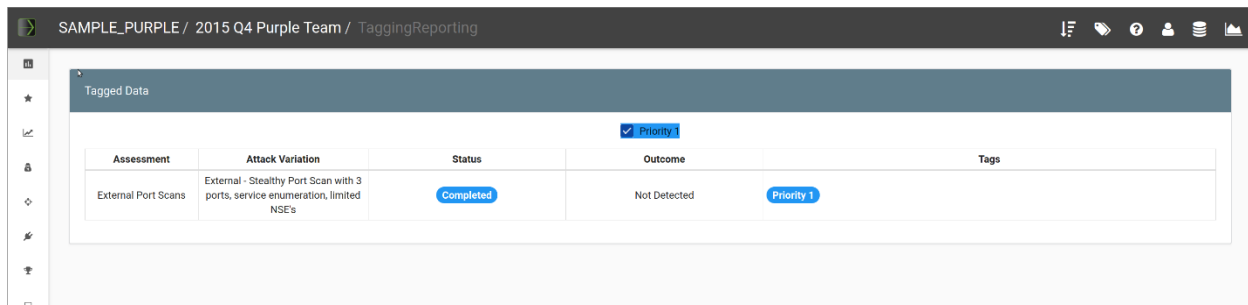


You can also access a view dedicated to tags:



The 'Select Report Attributes' dialog box allows users to configure report types, outcomes, and statuses. The 'Report Type' section on the left lists various report categories, with 'Tagged Data' selected. The 'Outcome To Include' section in the middle has checkboxes for TBD, Blocked, Detected, and NotDetected, all of which are checked. The 'Statuses To Include' section on the right has checkboxes for Completed, NotPerformed, InProgress, Paused, and Abandon, all of which are checked. At the bottom right, there are 'Cancel' and 'Select' buttons.

Report Type	Outcome To Include	Statuses To Include
<input type="radio"/> Toolset Comparison	<input checked="" type="checkbox"/> TBD	<input checked="" type="checkbox"/> Completed
<input type="radio"/> Campaign Summary	<input checked="" type="checkbox"/> Blocked	<input checked="" type="checkbox"/> NotPerformed
<input type="radio"/> Campaign Detailed	<input checked="" type="checkbox"/> Detected	<input checked="" type="checkbox"/> InProgress
<input type="radio"/> Kill Chain Summary	<input checked="" type="checkbox"/> NotDetected	<input checked="" type="checkbox"/> Paused
<input type="radio"/> Kill Chain Detailed		<input checked="" type="checkbox"/> Abandon
<input type="radio"/> Toolset Summary		
<input type="radio"/> Toolset Detailed		
<input type="radio"/> Timeline Summary		
<input type="radio"/> Timeline Detailed		
<input checked="" type="radio"/> Tagged Data		
<input type="radio"/> Data Integrity		



The screenshot shows the 'Tagged Data' view within the application. The breadcrumb navigation at the top reads 'SAMPLE_PURPLE / 2015 Q4 Purple Team / TaggingReporting'. A sidebar on the left contains navigation icons. The main content area displays a table with the following data:

Assessment	Attack Variation	Status	Outcome	Tags
External Port Scans	External - Stealthy Port Scan with 3 ports, service enumeration, limited NSE's	Completed	Not Detected	Priority 1

You can quickly navigate to your tagged data by accessing the quick launch in the top right of the display:



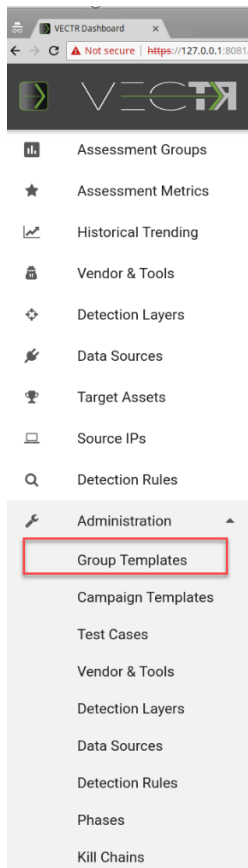
Assessment Group Templates

What is it?

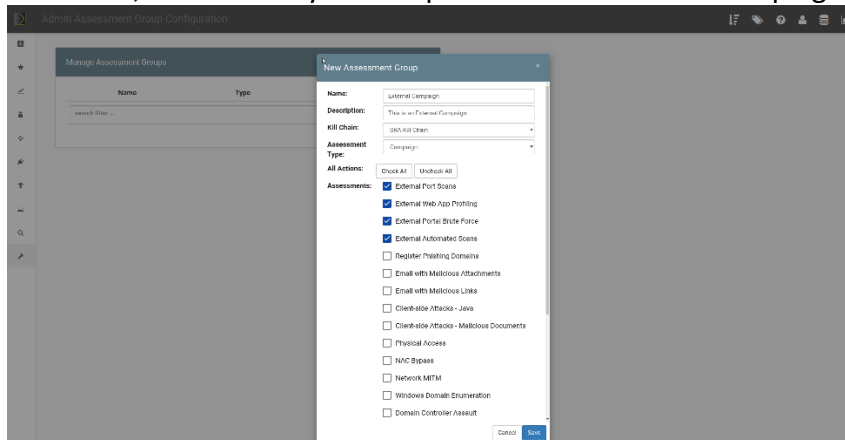
Assessment Group Templates allow you to logically group campaigns together into reusable templates.

How does it work?

In your Administration, click on Group Templates



Click New, then fill out your template with the desired campaigns:



Back in the Assessment Group screen, when you click “New”, you’ll be able to select from your Template:

The screenshot shows a web application interface with a sidebar on the left and a main content area. The sidebar contains a list of assessment groups. The main content area displays a table of assessment groups and a 'New Assessment Group' dialog box. The dialog box is open, showing fields for Name, Description, From, Template, Kill Chain, Assessment Type, All Actions, and Assessments. The 'From' and 'Template' fields are highlighted with a red box. The 'Assessments' section contains a list of checkboxes for various security tests.

Name	Type
2015 Q4 Purple Team	Campaign
2016 Q2 Purple Team	Campaign
2017 Q1 Purple Team	Campaign

New Assessment Group

Name: 2018_ExternalCampaigns

Description: Running through External Campaigns

From: External Campaign

Template: External Campaign

Kill Chain: SRA Kill Chain

Assessment Type: Campaign

All Actions: ☒ Check All ☐ Uncheck All

Assessments:

- ☒ External Port Scans
- ☒ External Web App Profiling
- ☒ External Portal Brute Force
- ☒ External Automated Scans
- ☐ Register Phishing Domains
- ☐ Email with Malicious Attachments
- ☐ Email with Malicious Links
- ☐ Client-side Attacks - Java
- ☐ Client-side Attacks - Malicious Documents
- ☐ Physical Access
- ☐ NAC Bypass
- ☐ Network MITM
- ☐ Windows Domain Enumeration

Cancel Save

Running SSL in Docker

What is it?

Allows you to run HTTPS from your docker container.

How does it work?

See <https://github.com/SecurityRiskAdvisors/VECTR>, section #4.

How can this feature help me?

This feature allows you to communicate to the Tomcat server on the docker container via https using a certificate of your choice.

