CLARITY
vulnerability insight

User Guide

Requirements:

1. docker
2. Internet connection
3. Admin / root privilege

Docker installation

Clarity.VI docker page: **https://hub.docker.com/r/clarityvi/vmd**

To run Clarity.VI straight in docker, run the command below:

```
docker run --name vmd -p 8443:443 clarityvi/vmd:latest
```

Now open your browser to https://localhost:8443 and login using: admin/manager

or

for data persistant:

```
docker volume create mariadb-data
docker volume create es-data
docker volume create vmd

docker run -d --name vmd \
--mount source=mariadb-data,target=/var/lib/mysql \
--mount source=es-data,target=/var/lib/elasticsearch \
--mount source=vmd,target=/var/www/vmd \
-p 8443:443 clarityvi/vmd:latest
```

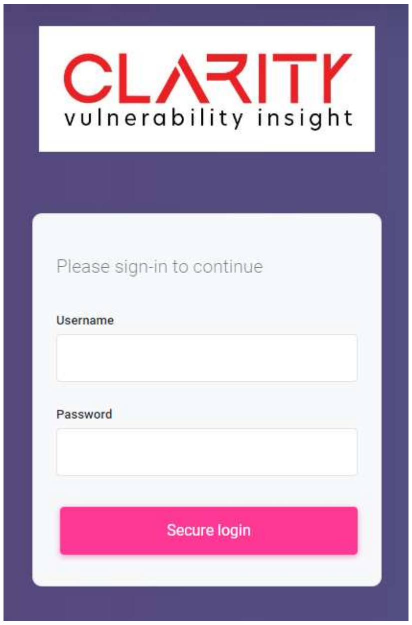
Open your browser to https://localhost:8443 and login using: admin/manager

Send email to info@rnflabs.com to request for trial license.

Using Clarity.VI

1. Login to Clarity.VI dashboard.

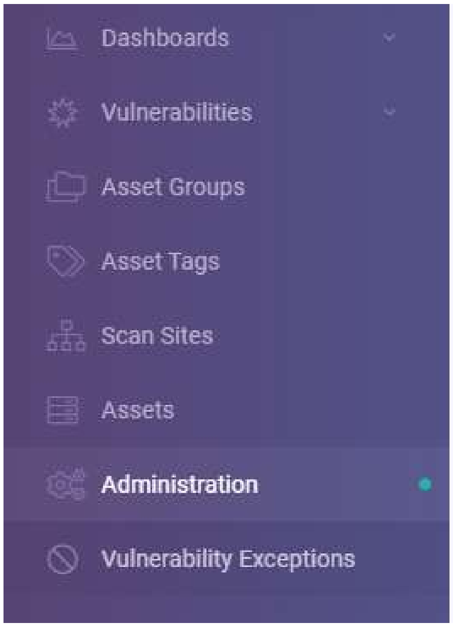
Open your browser to https://localhost:8443 and login using: admin/manager or the password you have set.



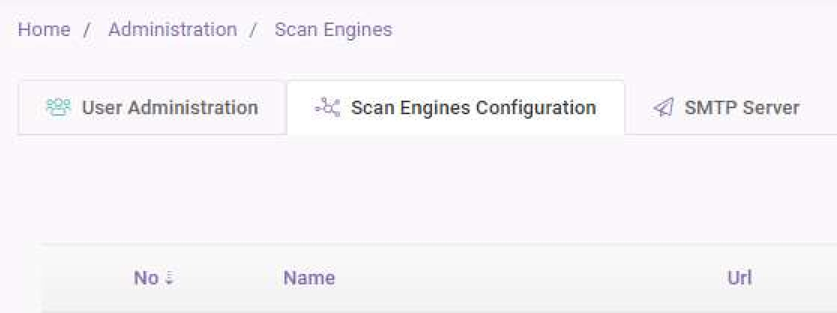
Enter the user & password you created during the installation.

2. Adding Nessus scanner to the Dashboard

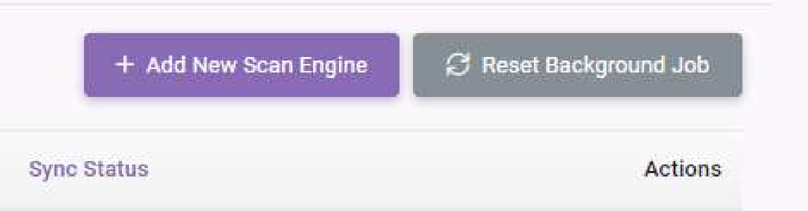
Go to the “Administration” page.



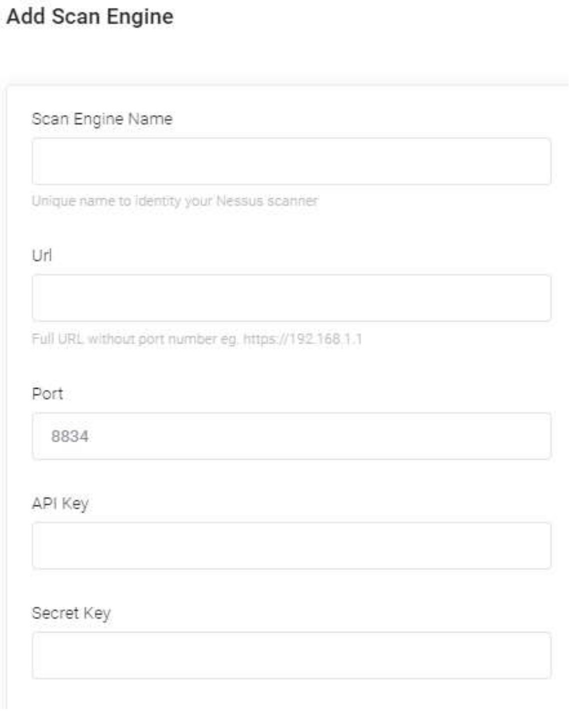
Click the “Scan Engine Configuration” tab.


Home / Administration / Scan Engines
User Administration
Scan Engines Configuration
SMTP Server
No
Name
Url

Click “+ Add New Scan Engine”.



Enter the Scan engine name
The URL of the Nessus – https://xxx.xxx.xxx.xxx
Default port is 8834, change the port if you Nessus port if different.
Enter the API Key and the Secret Key.



Add Scan Engine

Scan Engine Name

Unique name to identity your Nessus scanner

Url

Full URL without port number eg. https://192.168.1.1

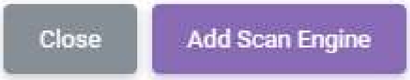
Port

8834

API Key

Secret Key

Click “Add Scan Engine”.



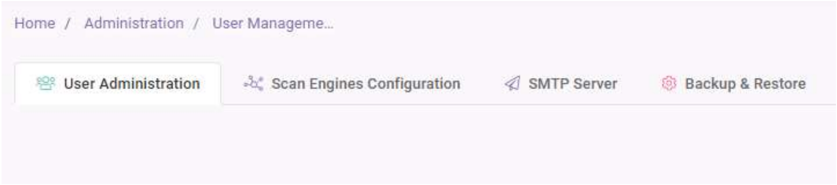
<u>Getting the Nessus API keys.</u>

- Login to Nessus
- Go to “Settings” and click “My Account” page.
- Go to the “API Keys” tab and click the “Generate” button.
- Copy the API and Secret Keys.

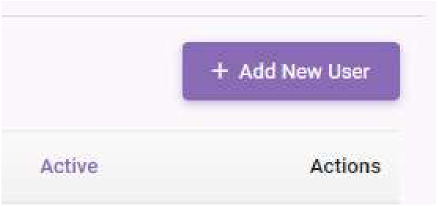
3. Adding user in Dashboard

Go to the “Administration” page.

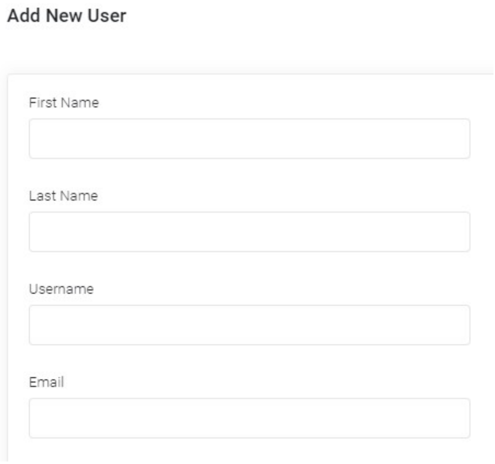
Click the “User Administration” tab.


Home / Administration / User Manageme...
User Administration
Scan Engines Configuration
SMTP Server
Backup & Restore

Click “+ Add New user”.



Enter the details.



Add New User

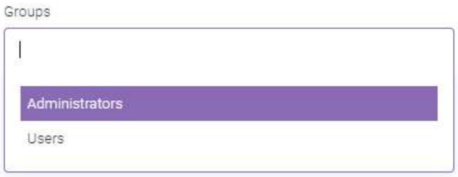
First Name

Last Name

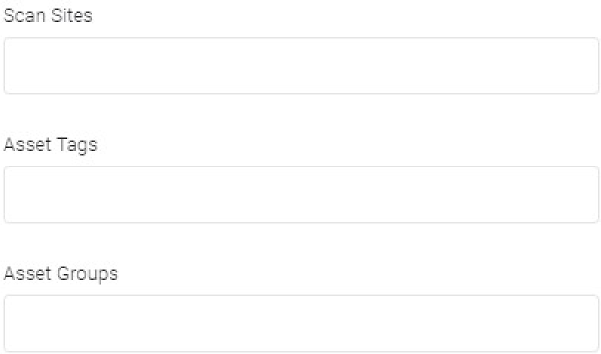
Username

Email

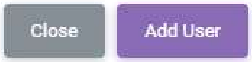
Select the group for the users.



Select the “Scan sites”, “Asset Tags” and the “Asset Groups” the user will have access to.

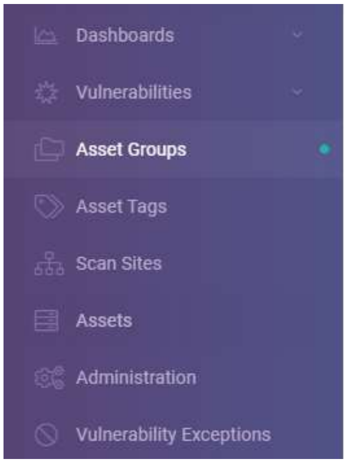


Click “Add User” to complete.

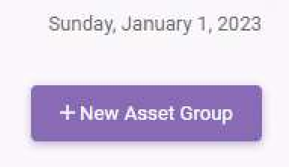


4. Create Asset Group.

Go to “Asset Groups” page.

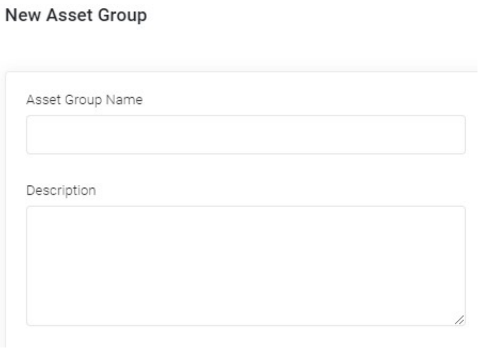


Click “+ New Asset Group”.



Sunday, January 1, 2023

Enter the Asset group name & the description.

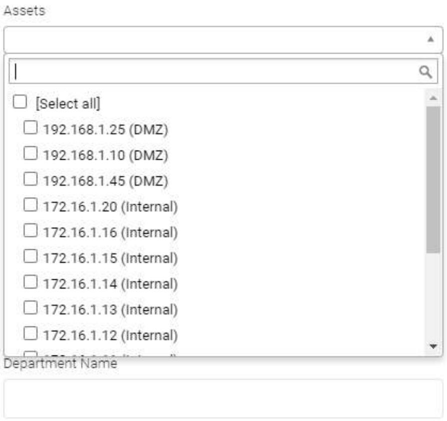


New Asset Group

Asset Group Name

Description

Select the assets for the group.

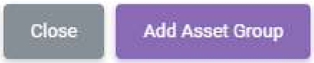


Assets

- □ [Select all]
  - □ 192.168.1.25 (DMZ)
  - □ 192.168.1.10 (DMZ)
  - □ 192.168.1.45 (DMZ)
  - □ 172.16.1.20 (Internal)
  - □ 172.16.1.16 (Internal)
  - □ 172.16.1.15 (Internal)
  - □ 172.16.1.14 (Internal)
  - □ 172.16.1.13 (Internal)
  - □ 172.16.1.12 (Internal)

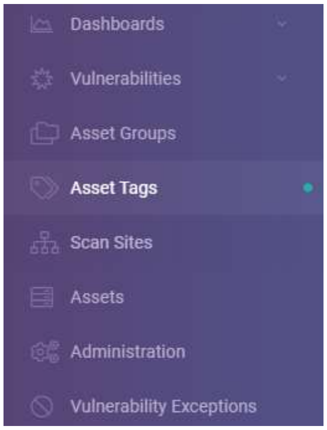
Department Name

Click “Add Asset Group” to complete.

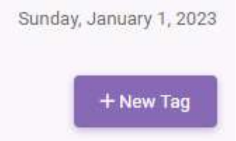


5. Create Asset Tags.

Go to the “Asset Tags” page.

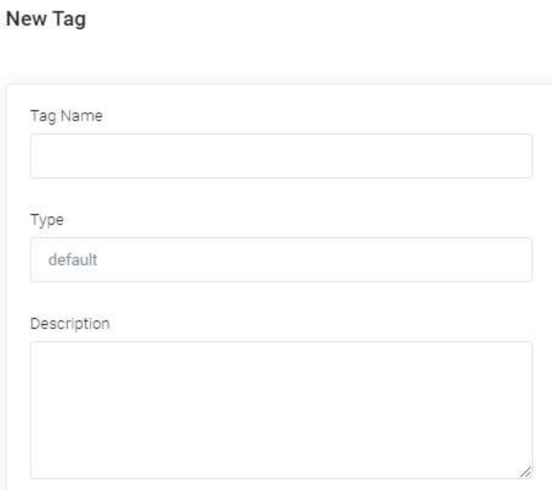


Click “+ New Tag”.



Select the assets for the tag.

Enter the tag details, such as description, tag owner, contacts information.



New Tag

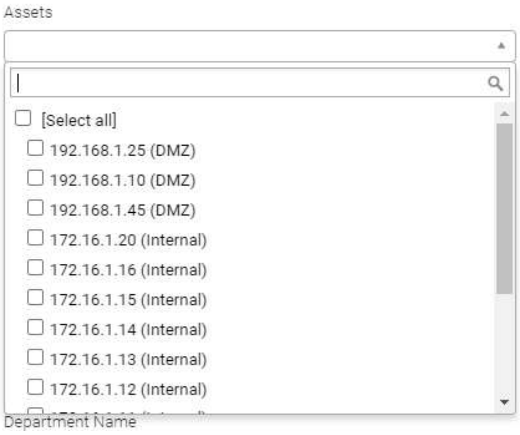
Tag Name

Type

default

Description

Select the assets for the tag.

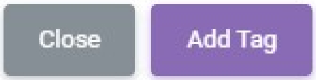


Assets

□ [Select all]
□ 192.168.1.25 (DMZ)
□ 192.168.1.10 (DMZ)
□ 192.168.1.45 (DMZ)
□ 172.16.1.20 (Internal)
□ 172.16.1.16 (Internal)
□ 172.16.1.15 (Internal)
□ 172.16.1.14 (Internal)
□ 172.16.1.13 (Internal)
□ 172.16.1.12 (Internal)

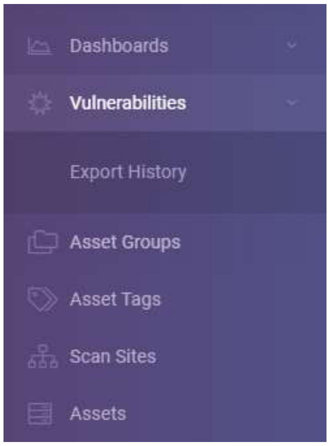
Department Name

Click "Add Tag" to complete.

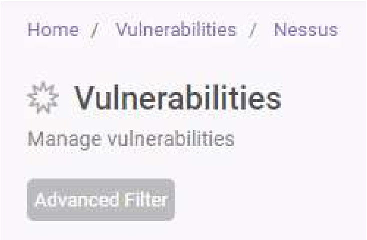


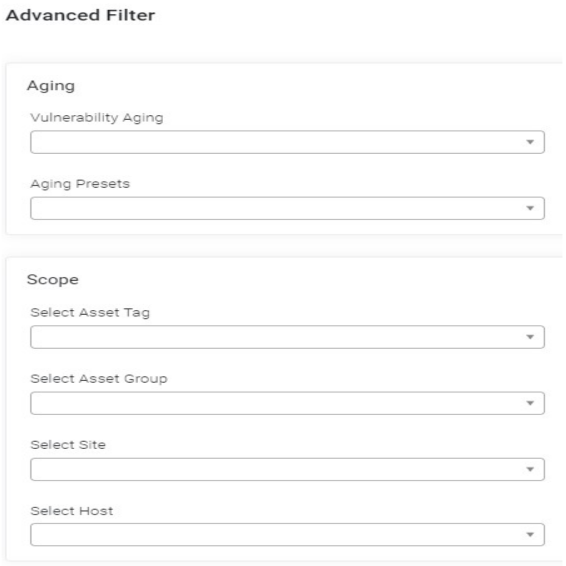
6. Create vulnerability report.

Go to "Vulnerabilities" page.

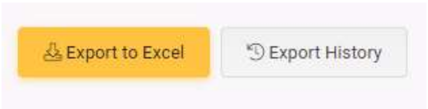


You can select the scope of vulnerabilities you want by using the "Advance Filter" button.

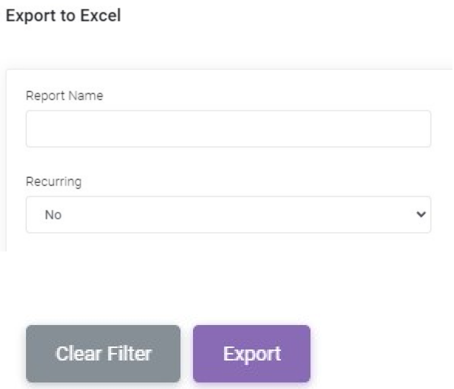




Click “Export to Excel” button.



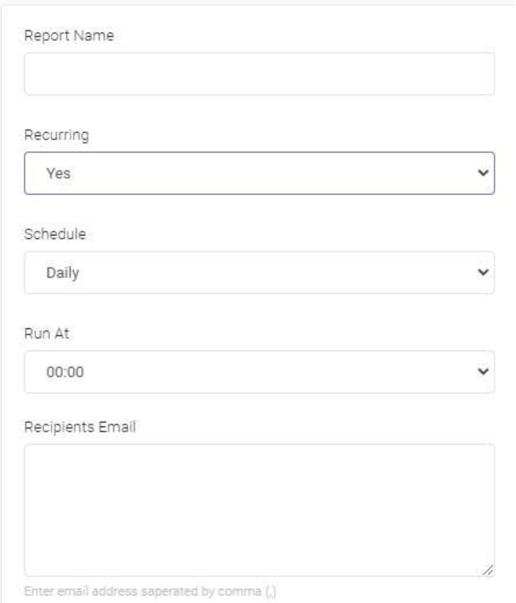
Enter the report name and click “Export”.



Recurring: No

7. Create recurring vulnerability report.

Go to “Vulnerabilities” page.
You can select the scope of vulnerabilities you want by using the “Advance Filter” button.
Click “Export to Excel” button.
Enter the report name and select “Recurring” drop-down menu to “Yes”.
Select your preferred schedule time.
Enter list of email, if you want them to be send directly via Email.



Report Name

Recurring: Yes

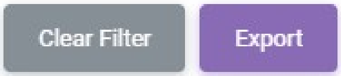
Schedule: Daily

Run At: 00:00

Recipients Email

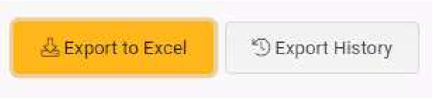
Enter email address saperated by comma (,)

Click “Export” to save.

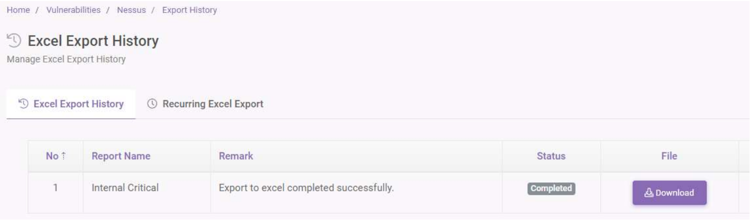


8. Downloading the report.

Go to “Vulnerabilities” page.
Click on the “Export History” button.



Click the “Download” button to download the report.



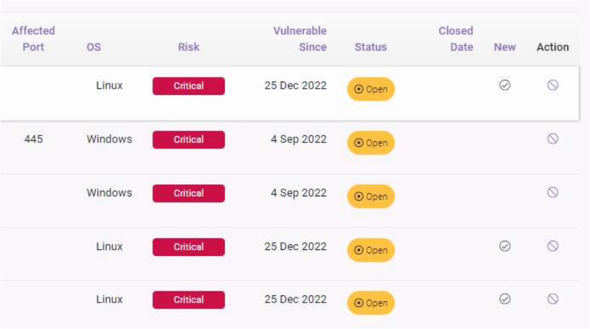
Excel Export History

Manage Excel Export History

No ↑	Report Name	Remark	Status	File
1	Internal Critical	Export to excel completed successfully.	Completed	Download

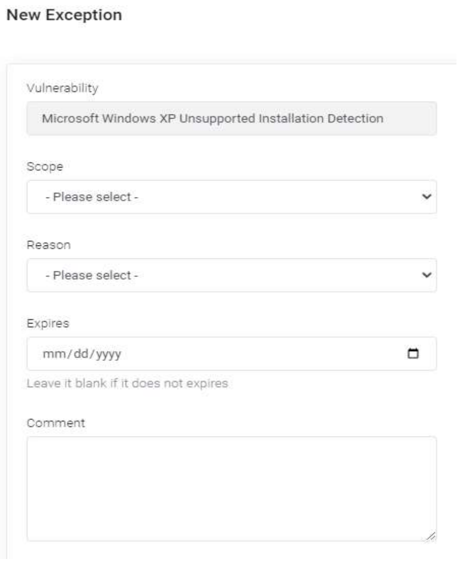
9. Vulnerability Exception.

To create vulnerability exception, click on the “Action” button of the vulnerability and “New Exception” panel will appear.



Affected Port	OS	Risk	Vulnerable Since	Status	Closed Date	New	Action
	Linux	Critical	25 Dec 2022	⊙ Open		✓	⊘
445	Windows	Critical	4 Sep 2022	⊙ Open			⊘
	Windows	Critical	4 Sep 2022	⊙ Open			⊘
	Linux	Critical	25 Dec 2022	⊙ Open		✓	⊘
	Linux	Critical	25 Dec 2022	⊙ Open		✓	⊘

Select the scope of the exception:



New Exception

Vulnerability: Microsoft Windows XP Unsupported Installation Detection

Scope: - Please select -

Reason: - Please select -

Expires: mm/dd/yyyy

Leave it blank if it does not expires

Comment:

- This instance only – the exception will apply only to this specific vulnerability on this host.
- All instances on this asset – the exception will apply to all the same vulnerability on this host.
- All instances on this asset’s site – the exception will apply to all the same vulnerability on the defined “Scan site”.
- All instances in asset group – the exception will apply to all the same vulnerability in the defined “Asset groups”.
- Global (All instances) – the exception will apply to all the same vulnerability globally.

Select the “Reason”.
Define the expiry of the exception. Leave it blank if it does not expires.
Enter the comments or your reference / details of your exception and click “Submit”.

Do note if the exception is created by user, it will need to be review by administrator before the exception if approved.

If the exception is created by administrator, it will automatically approved.

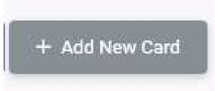
10. Dashboard.

By default the dashboard is blank. You can add in the cards to create a customize view for you dashboard.

You can create multiple dashboard with different view by clicking the "Create new dashboard Page" button.

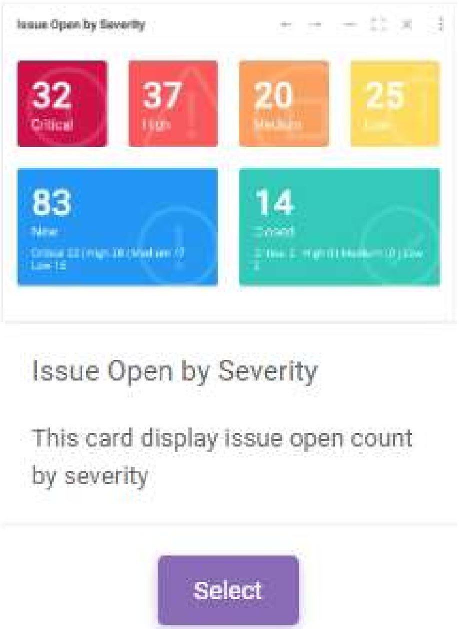
11. Dashboard cards.

You can add card by clicking the "Add New Card" button.



12. Issue Open by Severity.

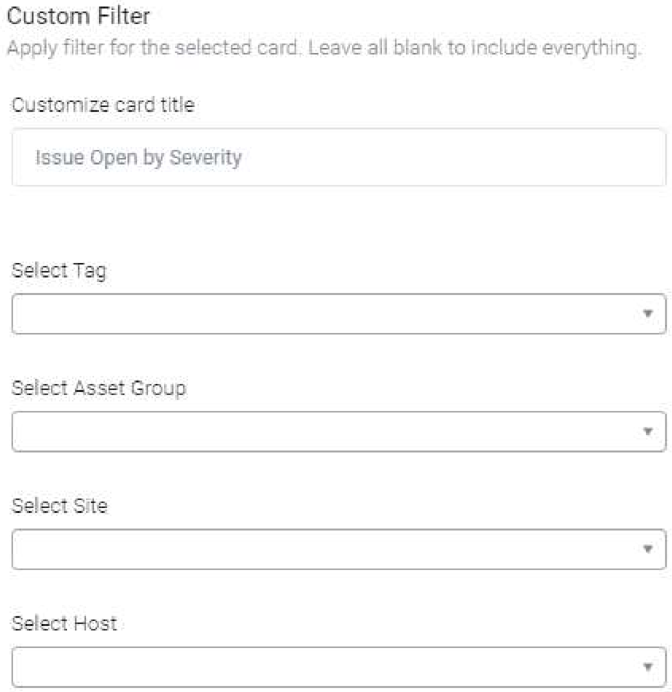
This card provides the total number of vulnerability found by severity.



Issue Open by Severity

This card display issue open count by severity

You can select the scope by selecting the tag, asset groups, scan sites or hosts.



Custom Filter

Apply filter for the selected card. Leave all blank to include everything.

Customize card title

Issue Open by Severity

Select Tag

Select Asset Group

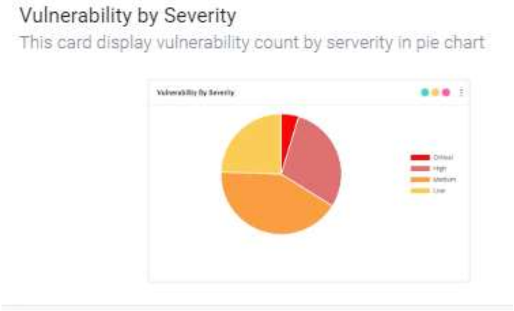
Select Site

Select Host

To get an overview of all the assets, leave the scope blank.

13. Vulnerability by Severity.

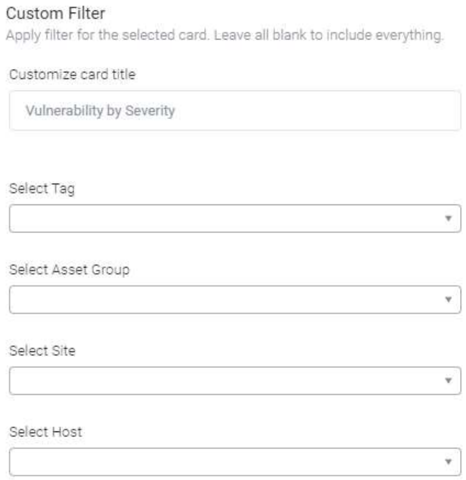
This card provides a pie chart of the total number of vulnerability found by severity.



Vulnerability by Severity

This card display vulnerability count by serverity in pie chart

You can select the scope by selecting the tag, asset groups, scan sites or hosts.



Custom Filter

Apply filter for the selected card. Leave all blank to include everything.

Customize card title

Vulnerability by Severity

Select Tag

Select Asset Group

Select Site

Select Host

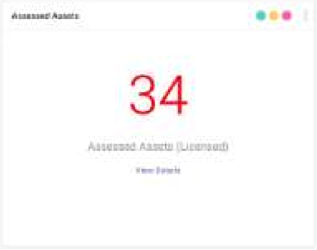
To get an overview of all assets, leave the scope blank.

14. Assessed Assets.

This card provide the number of assets that have been scanned.

Assessed Assets

This card display the number of assessed assets



Assessed Assets

34

Assessed Assets (Licensed)

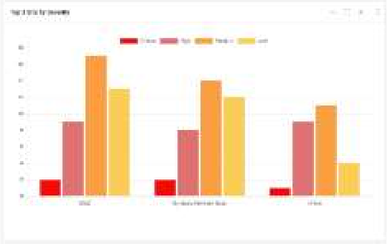
To get an overview of all the assets, leave the scope blank.

15. Top X Bar Chart.

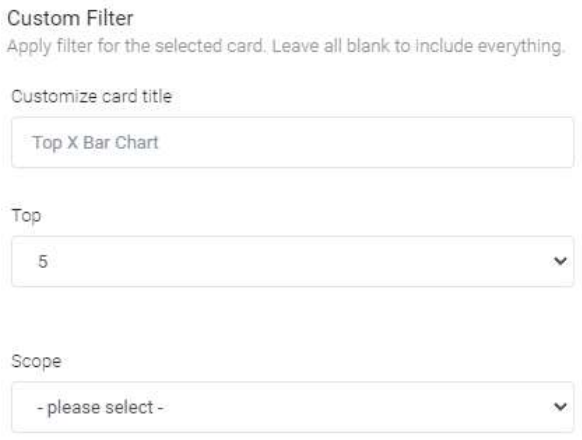
This card provide a bar chart view of vulnerability found by your selected scope.

Top X Bar Chart

This card display top X bar chart



You can select the scope by selecting the tag, asset groups, scan sites or hosts.



Custom Filter

Apply filter for the selected card. Leave all blank to include everything.

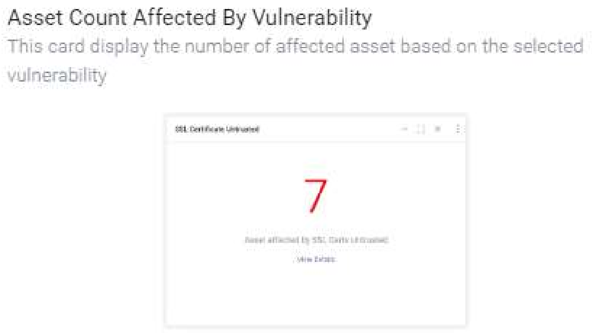
Customize card title: Top X Bar Chart

Top: 5

Scope: - please select -

16. Asset Count Affected By {Vulnerability}.

This card provide the number of hosts / assets affected by specific vulnerability.



Asset Count Affected By Vulnerability

This card display the number of affected asset based on the selected vulnerability

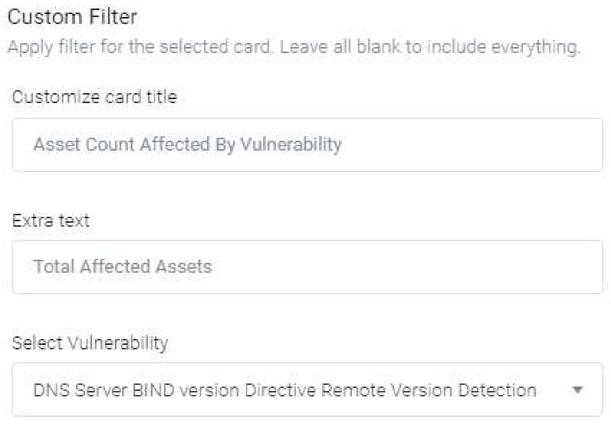
SSL Certificate Untrusted

7

Asset affected by SSL Certs Untrusted

View Details

You can define the vulnerability by “Select Vulnerability” of your choice.



Custom Filter

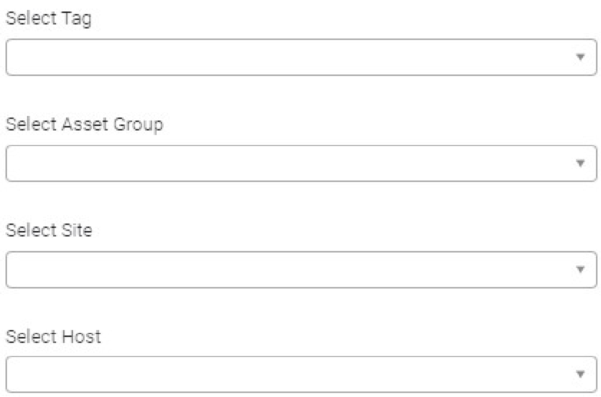
Apply filter for the selected card. Leave all blank to include everything.

Customize card title: Asset Count Affected By Vulnerability

Extra text: Total Affected Assets

Select Vulnerability: DNS Server BIND version Directive Remote Version Detection

Define the scope by selecting the tag, assets groups, scan sites or hosts.



Select Tag

Select Asset Group

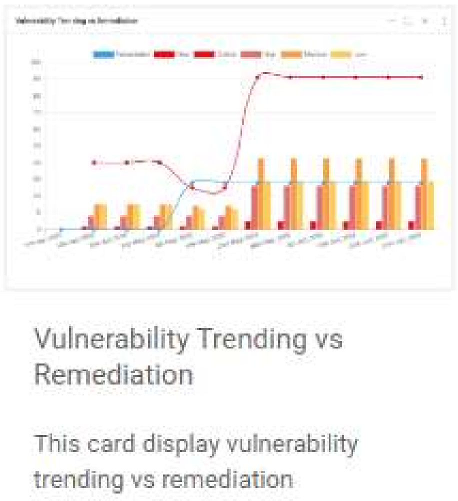
Select Site

Select Host

To get an overview of all assets, leave the scope blank.

17. Vulnerability Trending vs Remediation.

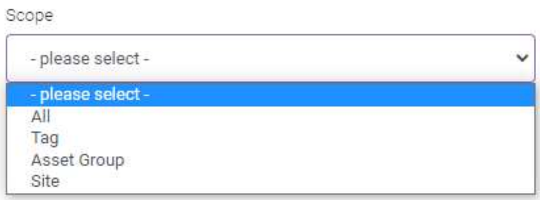
This card provide the vulnerability trending charts.



Vulnerability Trending vs Remediation

This card display vulnerability trending vs remediation

Define the scope by selecting the tags, asset groups or scan sites. Select all, if you want an overview of all the assets.

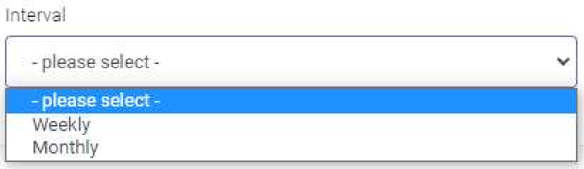


Scope

- please select -

- please select -
All
Tag
Asset Group
Site

Define the interval of the charts, by selecting “Weekly” or “Monthly” interval.



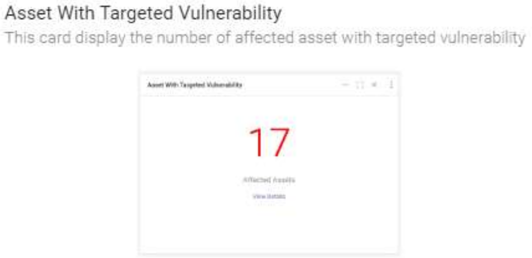
Interval

- please select -

- please select -
Weekly
Monthly

18. Asset with Targeted Vulnerability.

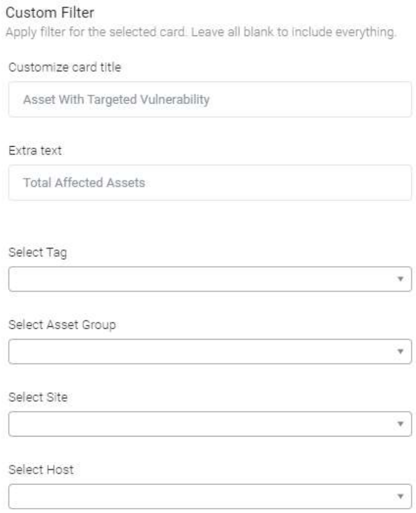
This card shows number of assets with exploitable vulnerability.



Asset With Targeted Vulnerability

This card display the number of affected asset with targeted vulnerability

You can define the scope based on tag, asset groups, scan sites or multiple hosts if you need to be specific.



Custom Filter

Apply filter for the selected card. Leave all blank to include everything.

Customize card title

Asset With Targeted Vulnerability

Extra text

Total Affected Assets

Select Tag

Select Asset Group

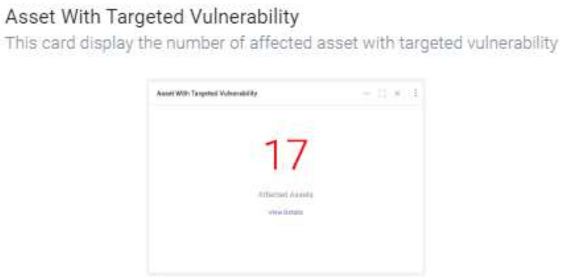
Select Site

Select Host

Leave the scope blank if you can to cover all assets.

19. New Discovered Assets.

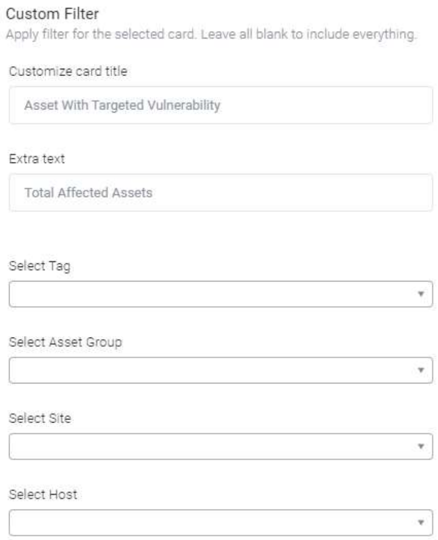
This card provide the number of new found assets in the latest scan.



Asset With Targeted Vulnerability

This card display the number of affected asset with targeted vulnerability

You can define the scope based on tag, asset groups, scan sites or multiple hosts if you need to be specific.



Custom Filter

Apply filter for the selected card. Leave all blank to include everything.

Customize card title

Asset With Targeted Vulnerability

Extra text

Total Affected Assets

Select Tag

Select Asset Group

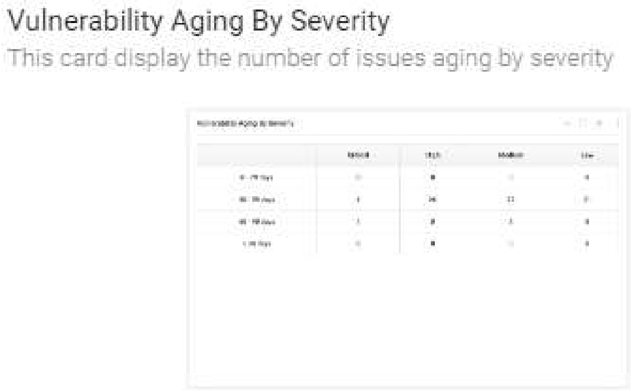
Select Site

Select Host

Leave the scope blank if you can to cover all assets.

20. Vulnerability Aging By Severity.

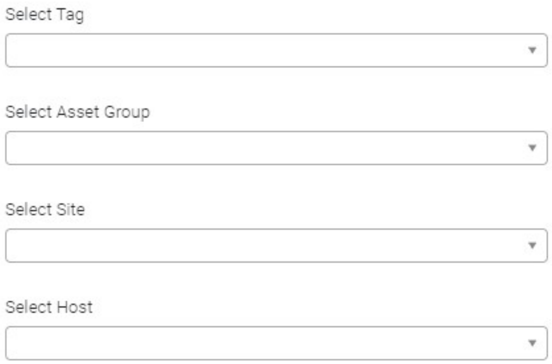
This card provide the view of aging vulnerability by severity.



Vulnerability Aging By Severity

This card display the number of issues aging by severity

Define the scope by selecting the tag, assets groups, scan sites or hosts.



Select Tag

Select Asset Group

Select Site

Select Host

To get an overview of all assets, leave the scope blank.

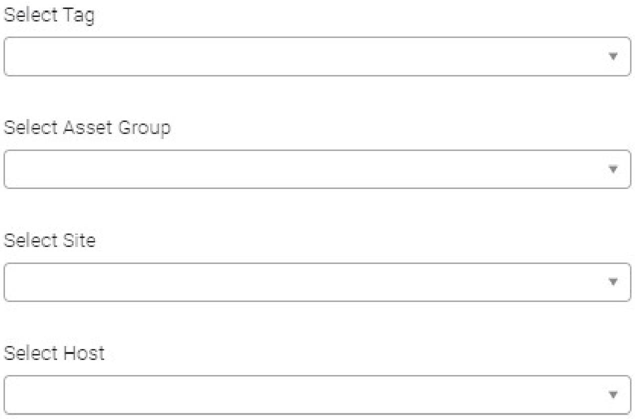
21. Mitigated Host By Severity.

This card shows the number of remediated vulnerability by assets and severity.

Mitigated Host By Severity

This card display the number of issues closed by host and severity

You can define the scope by selecting tags, assets groups, scan sites or hosts.



Select Tag

Select Asset Group

Select Site

Select Host

To get an overview of all assets, leave the scope blank.

22. Top X Table.

This card provide the top 3 – top 10 view of your most vulnerable assets, tags, asset groups or scan sites.

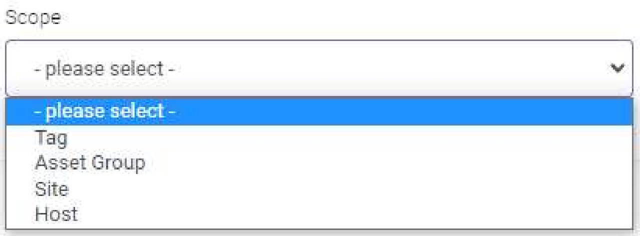
Top X Table

This card display the top x table base on user selected scope

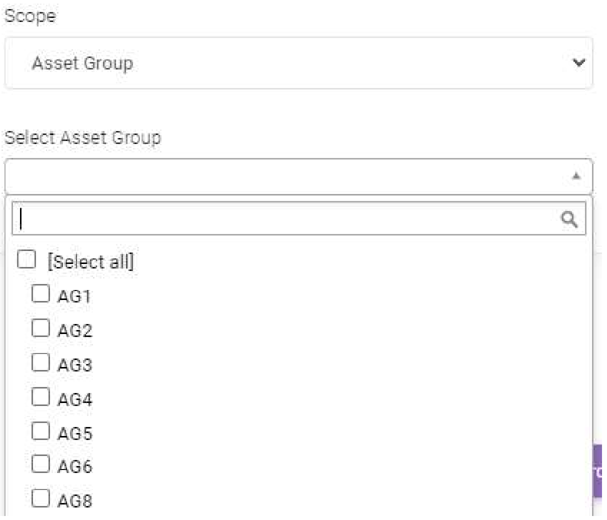
You can customize the view according to what scope you define.

This cards depends on a properly created tags and asset groups if you wanted an accurate presentation of your environment.

Select the “Scope” and leave the box below blank if you want an overall view.

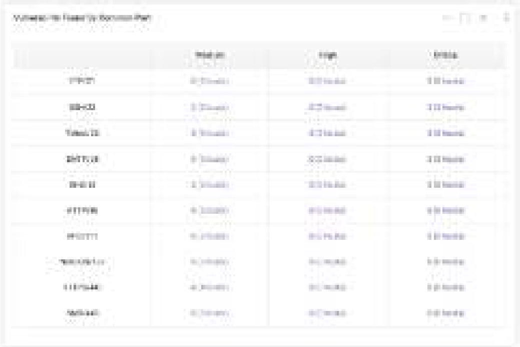


Check the items in the box below the “Scope” if you wanted to select only the relevant view according to your environment.



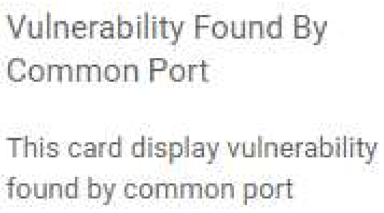
23. Vulnerability Found By Common Port.

This card provide view of vulnerability found by ports / services.



Vulnerability Found By Common Port

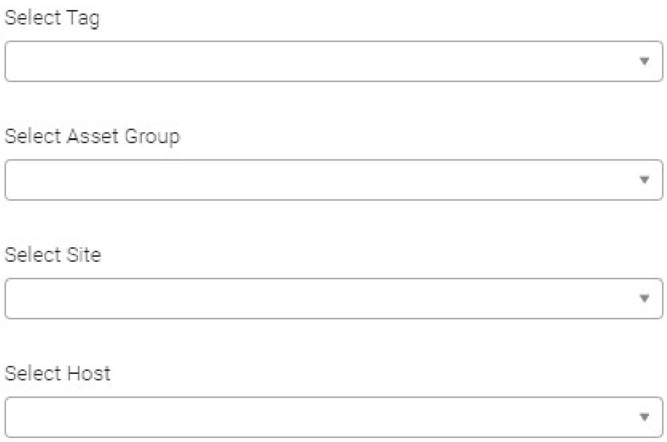
	Medium	High	Critical
FTP/21	[illegible]	[illegible]	[illegible]
SSH/22	[illegible]	[illegible]	[illegible]
Telnet/23	[illegible]	[illegible]	[illegible]
SMTP/25	[illegible]	[illegible]	[illegible]
DNS/53	[illegible]	[illegible]	[illegible]
HTTP/80	[illegible]	[illegible]	[illegible]
POP3/110	[illegible]	[illegible]	[illegible]
NetBIOS/139	[illegible]	[illegible]	[illegible]
HTTPS/443	[illegible]	[illegible]	[illegible]
SMB/445	[illegible]	[illegible]	[illegible]



Vulnerability Found By Common Port

This card display vulnerability found by common port

You can define the scope by selecting tags, assets groups, scan sites or hosts.



Select Tag

Select Asset Group

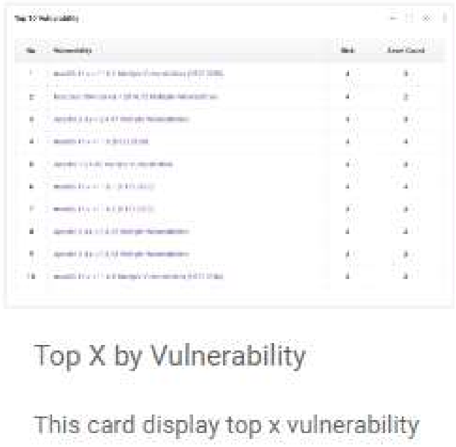
Select Site

Select Host

To get an overview of all assets, leave the scope blank.

24. Top X by Vulnerability.

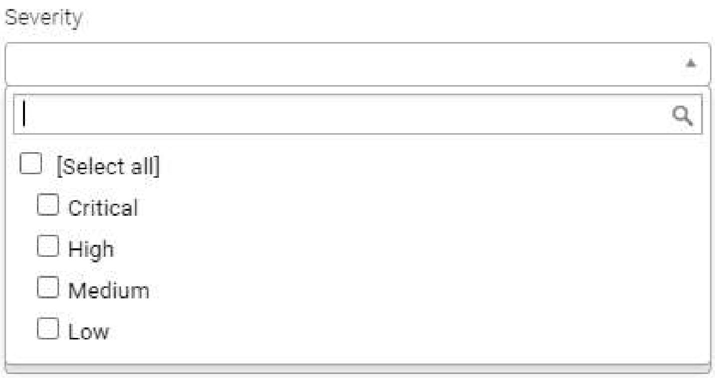
This card provide the top 3 – top 10 view of most common vulnerability found by severity.



Top X by Vulnerability

This card display top x vulnerability

You can define the scope by selecting the “Severity”. If you wanted an overall view, leave other menu blank.



Severity

☐ [Select all]

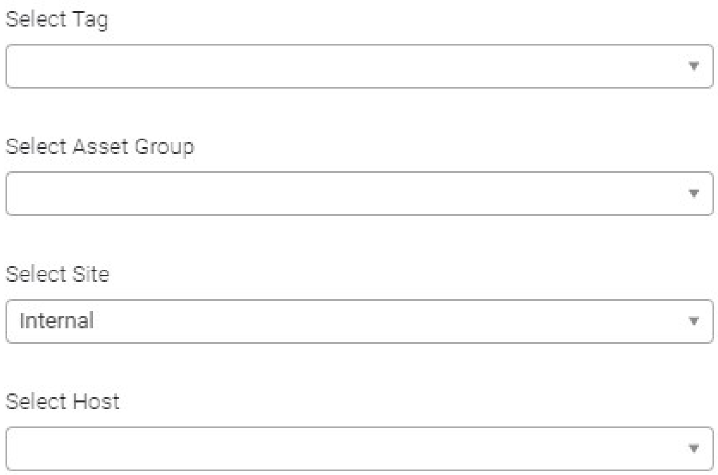
☐ Critical

☐ High

☐ Medium

☐ Low

If you want a specific view based on tags, assets groups, scan sites or hosts. Select the items you wanted and click “Add card”.



Select Tag

Select Asset Group

Select Site: Internal

Select Host