Introduction

- Dashboards Overview:

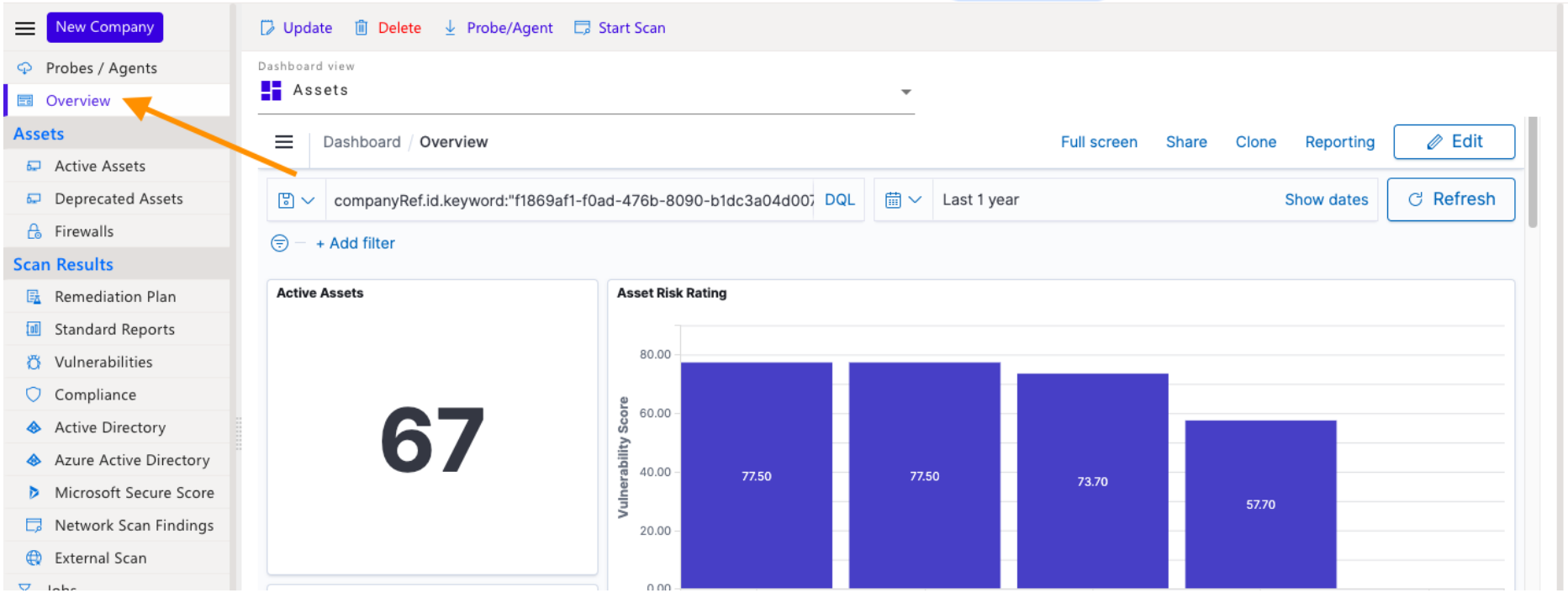
Dashboards are the most useful tool for visualising data that has been stored without the need to code an entire framework that consumes data from the engine. Dashboards provide an attractive visualisation or interactive chart.

- **Use cases for Dashboards**

A data dashboard is a collection of charts, graphs, gauges, and other visualisations that provide an overview of the data that you're interested in and interact with. Real-time search, monitoring, and analysis of business and operational data can be tracked, analysed, and displayed.

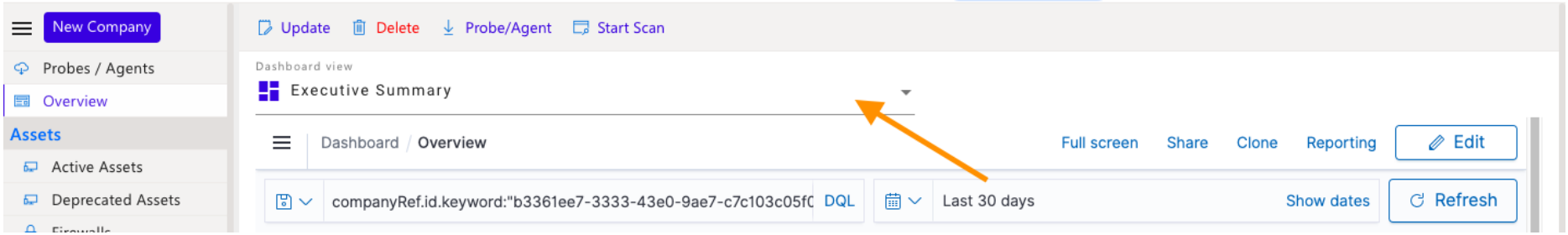
- **Dashboards:**

Dashboards are the default view when you log in.
However, if you are in another tab and want to see dashboards, click on the Overview tab in the left side panel, as shown below.

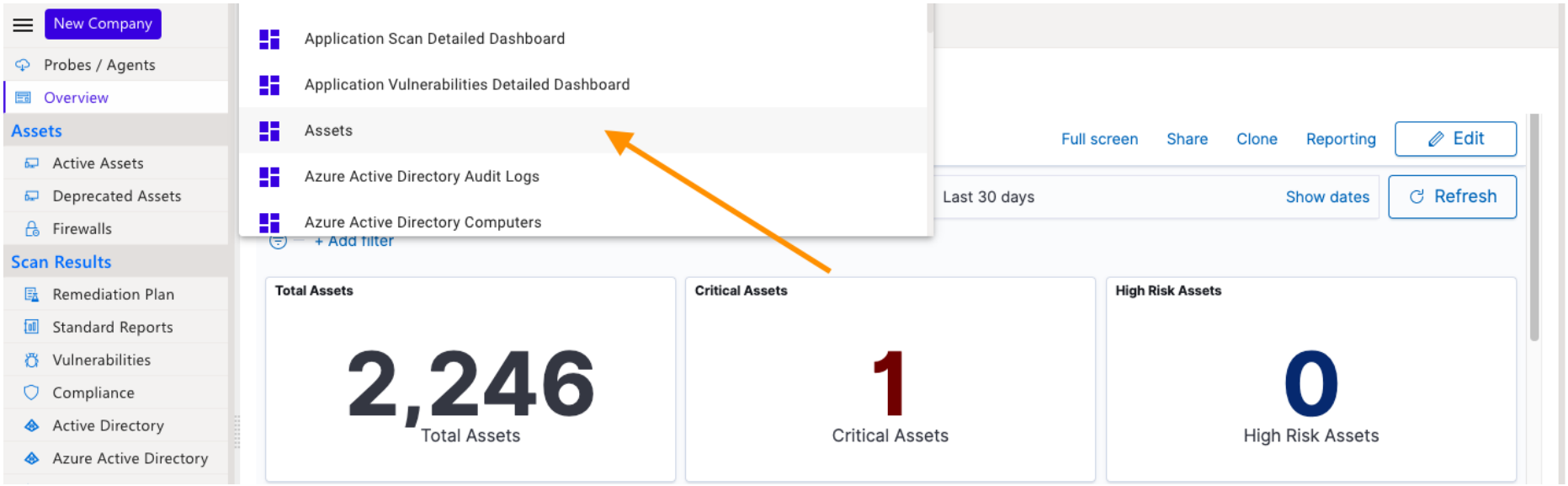


Navigating to Different Dashboards

- If you want to see a different dashboard, click the dropdown menu below the Dashboard view and select the dashboard.

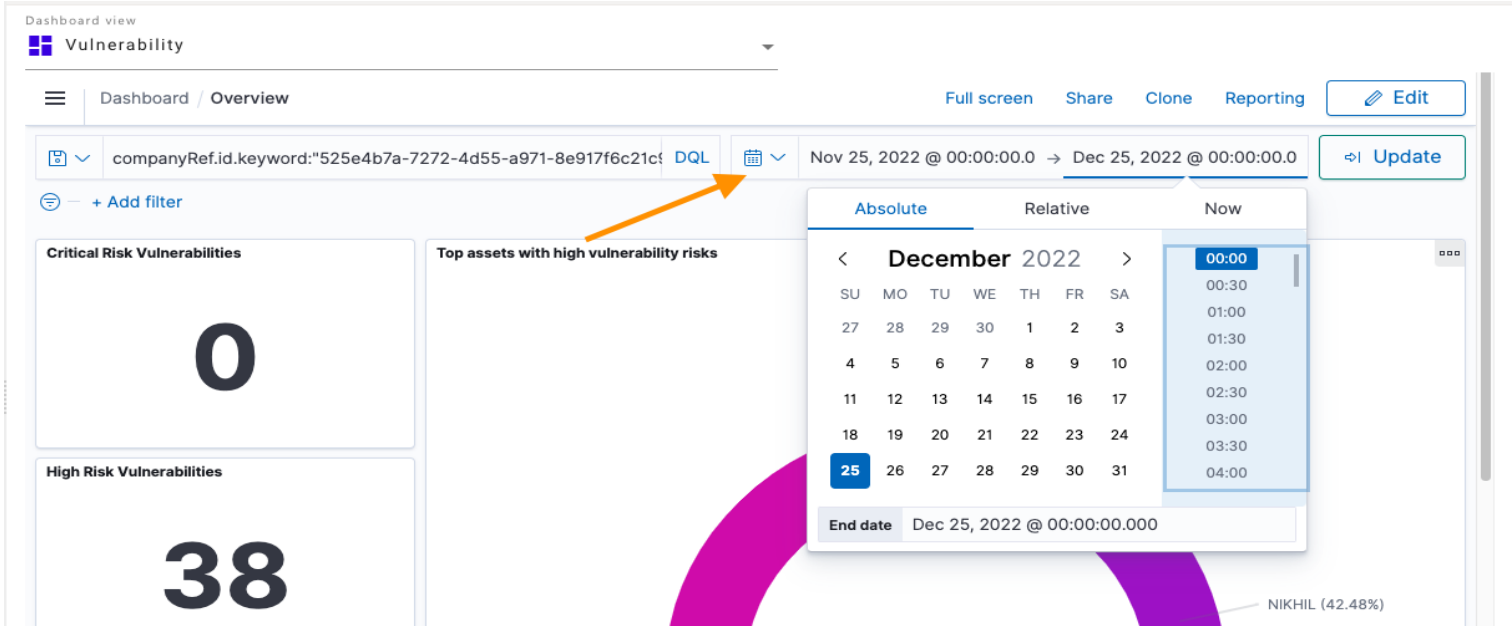


- Choose the dashboard that you want to view. Then, as shown below, you will be able to view the selected dashboard.



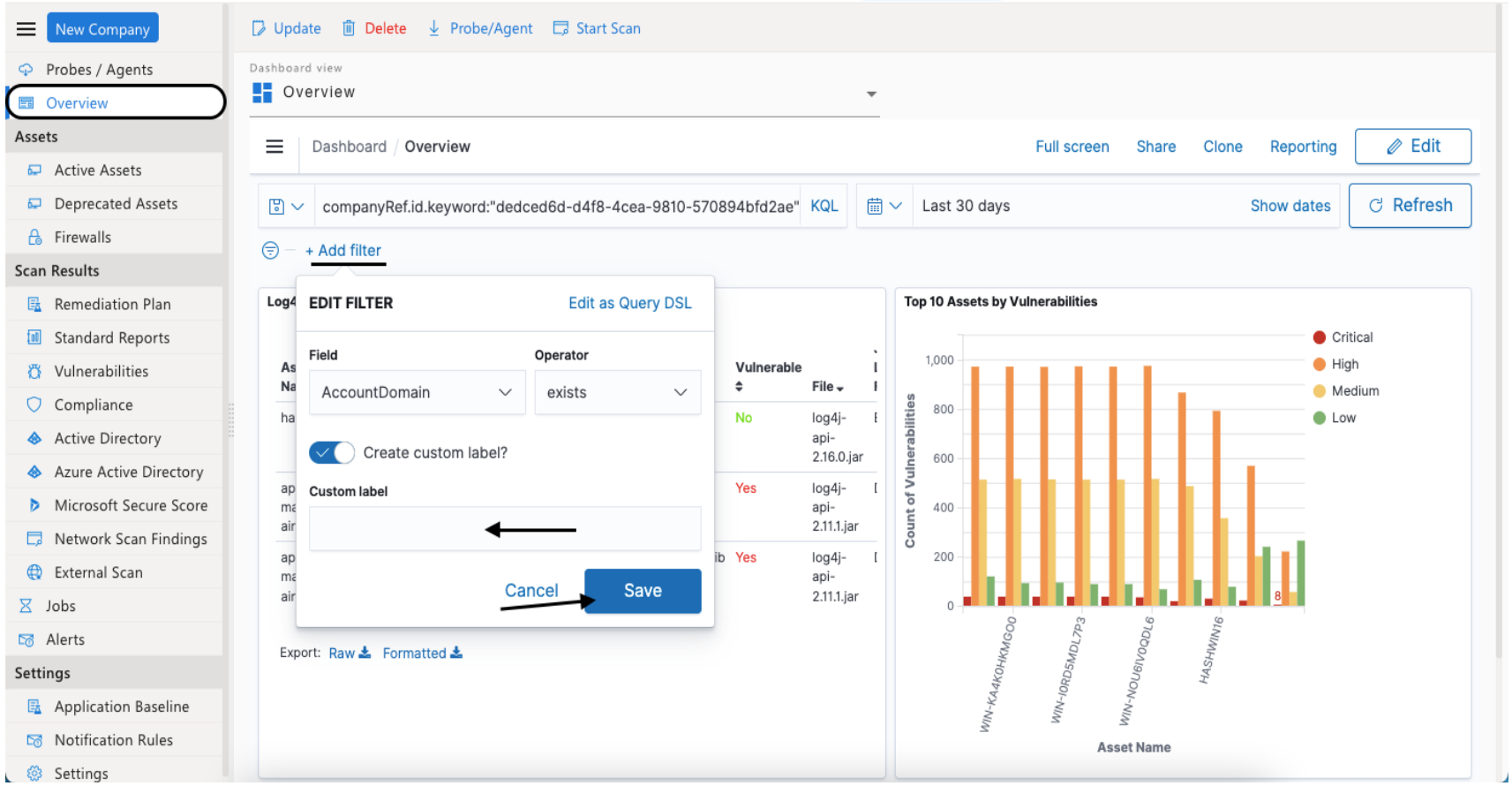
Viewing Dashboards

- By selecting a time period, you can view the dashboard.
- You can customize the dashboard's time frame to view time for a specific time period. You can choose an absolute time frame like calendar format, or you can choose a relative time format like "Last 30 days".
- You can also choose a filter condition by adding a field in the "Add filter" section. The dashboard's time frame can be changed as shown below:

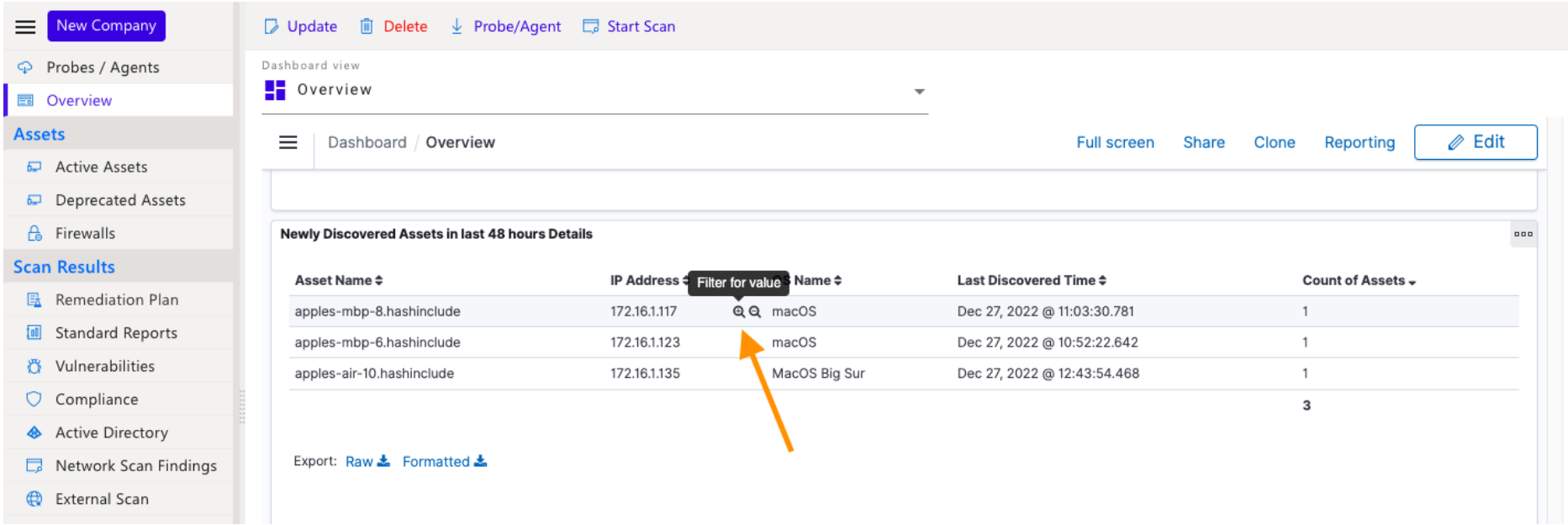


Filtering for Values

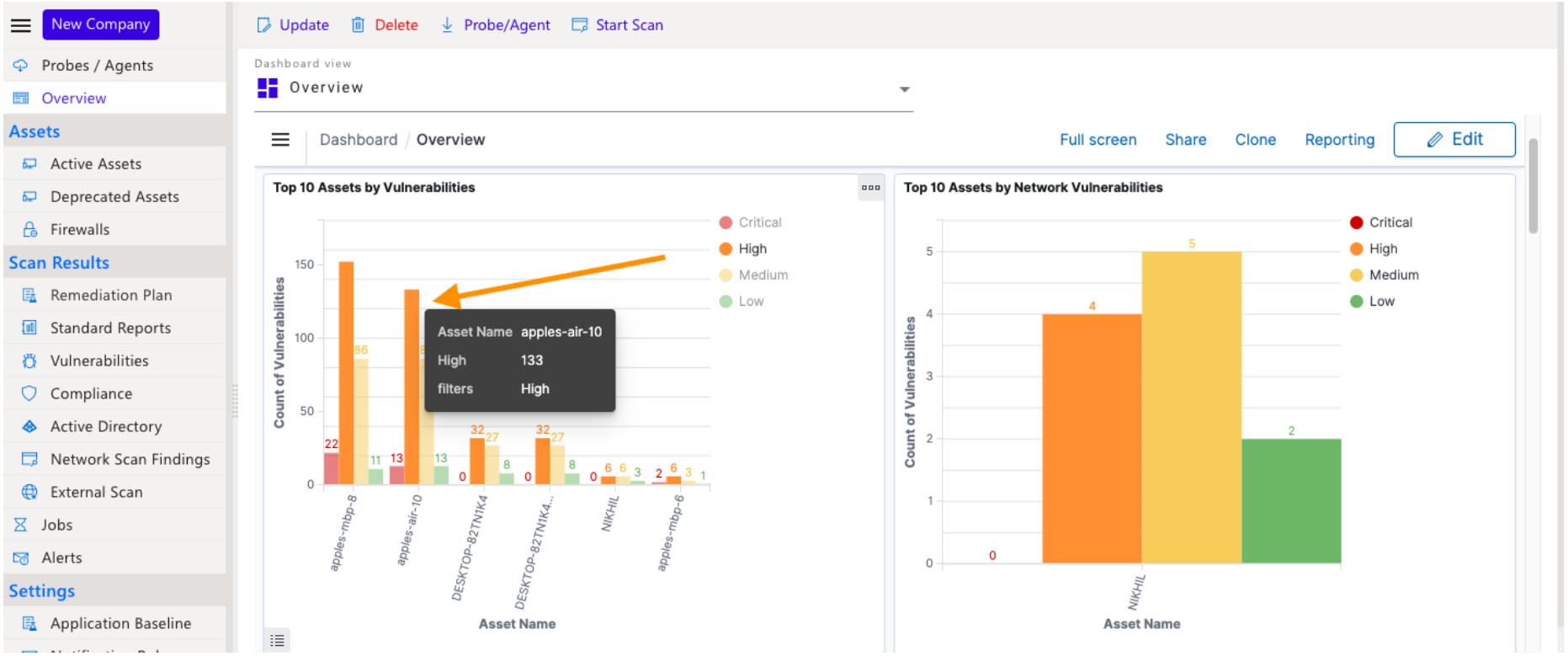
- By using a filter, you can view a specific set of data.
- This can be accomplished by adding a filter condition and entering a value in the "Add filter" field.



- You can also filter the values by clicking on the '+ 'sign next to the value in the data tables, as shown below:



- You can also filter values by clicking on the section of graphs, as shown below:



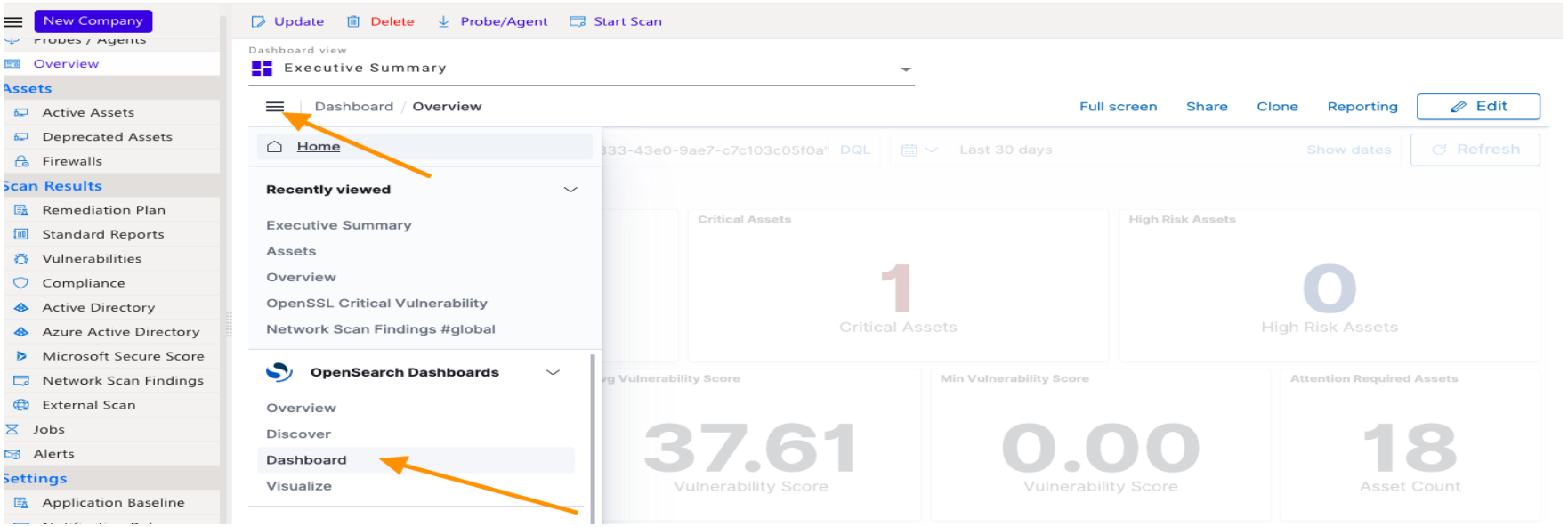
To create a new custom Dashboard with values

Building Your Custom Dashboard

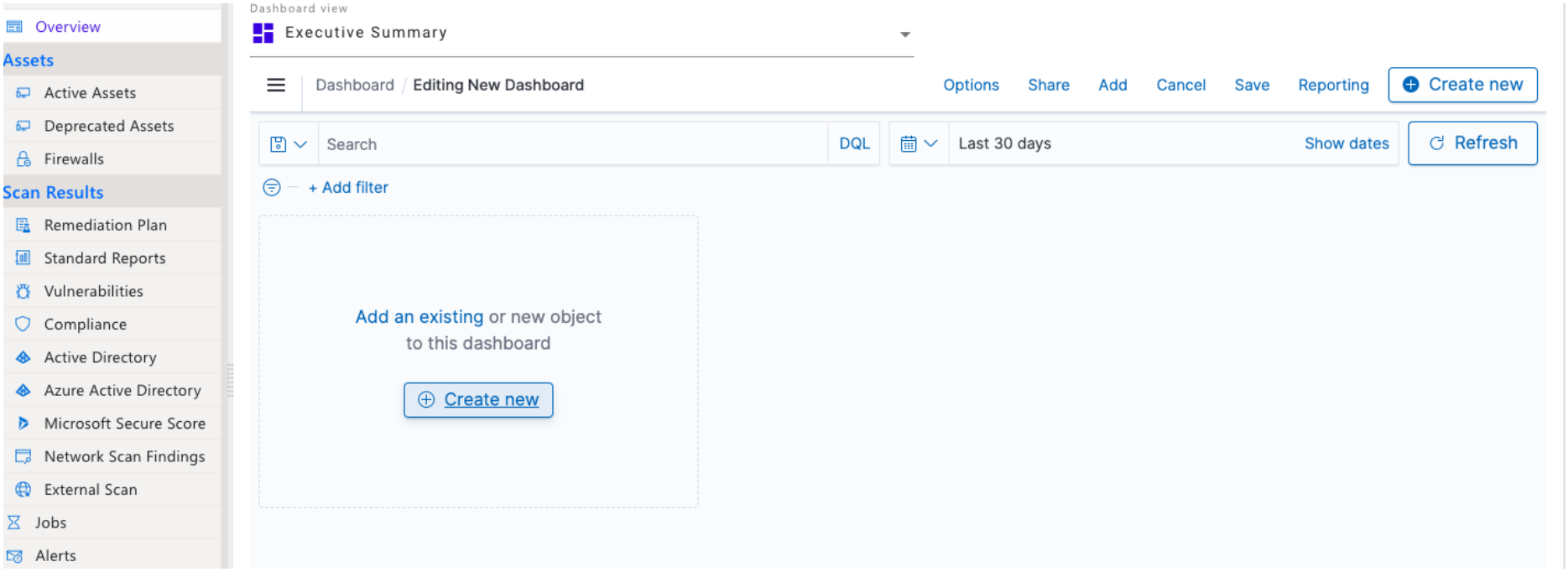
• You can view existing dashboards, but if you want to create your own, follow the steps below:

Create a new custom dashboard:

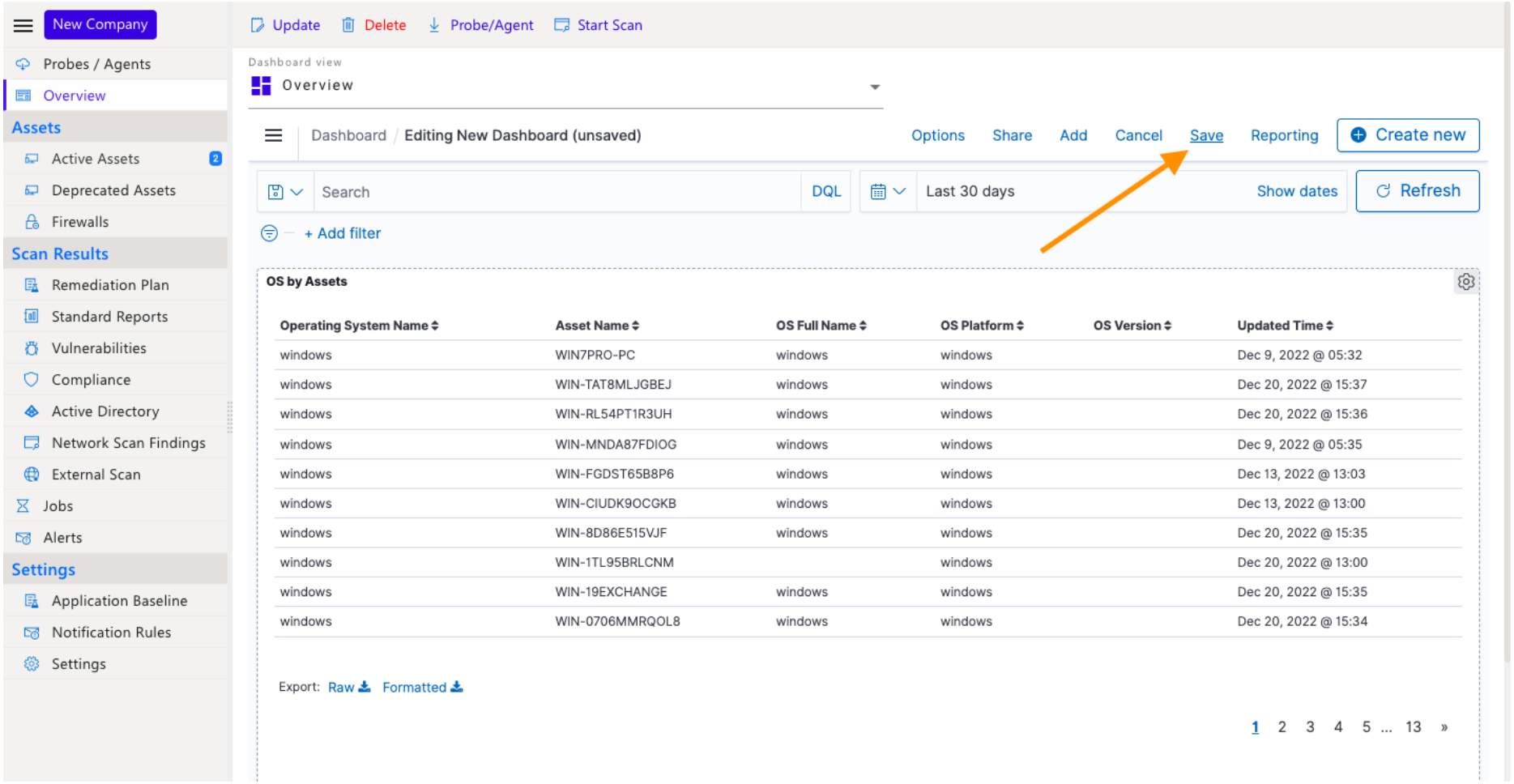
- As shown below, click on the menu icon and then on the Dashboard option.



• As shown below, you can add an existing visualization/chart or create a new one for your custom dashboard.

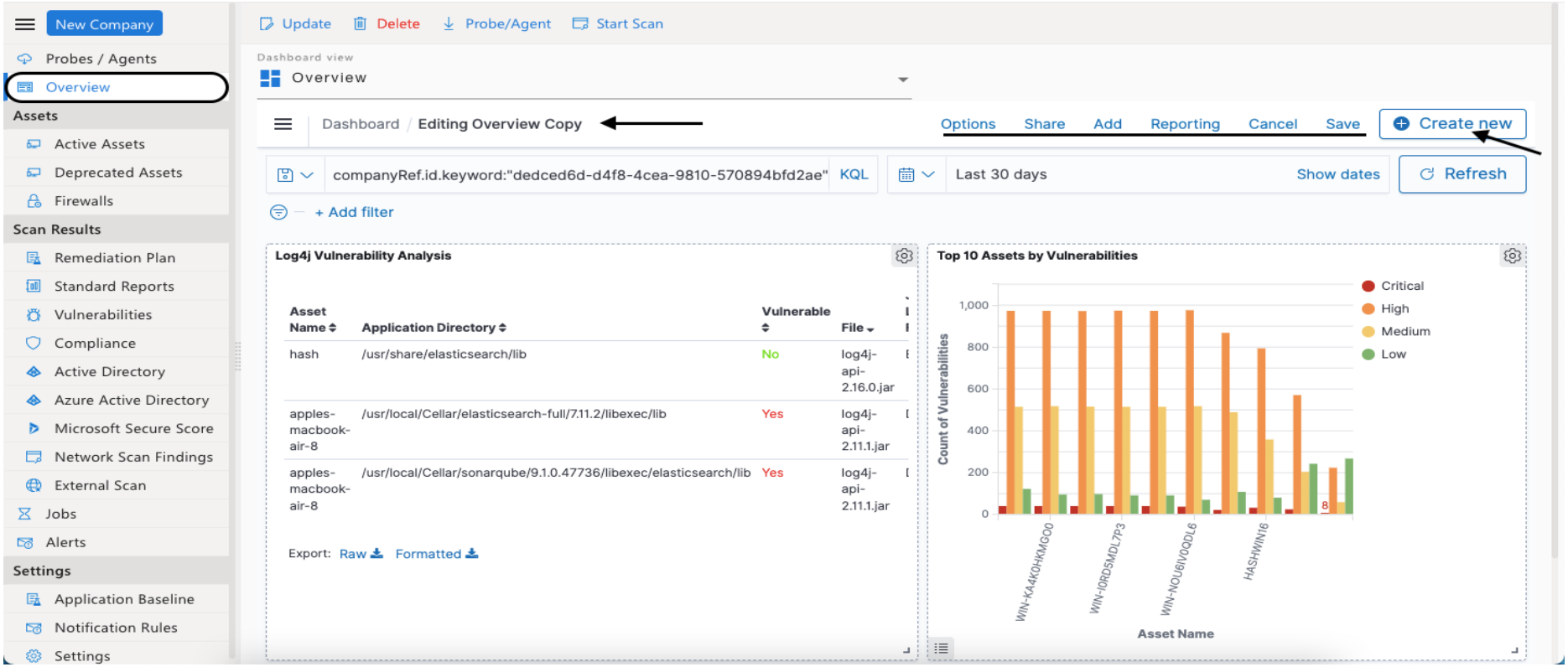


- After adding a visualization, save it and name it as shown below.



Editing a Dashboard:

• As shown in the image below, it is possible to clone an existing dashboard by giving it a new name.
• The Edit function allows you to change the appearance of any widget on the dashboard. After editing, save the dashboard with changes.

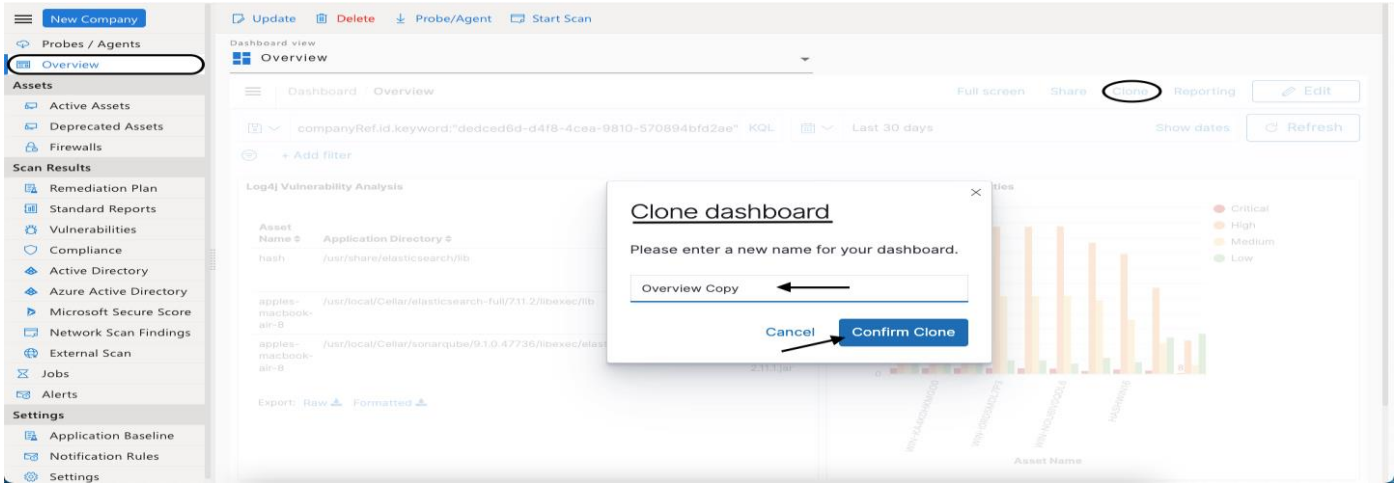


Full Screen:

- You can view the dashboard in full screen by clicking the "Full Screen" button on the top right.

Cloning Dashboards

- You can clone a dashboard.
- As shown in the image below, it is possible to clone an existing dashboard by giving it a new name.

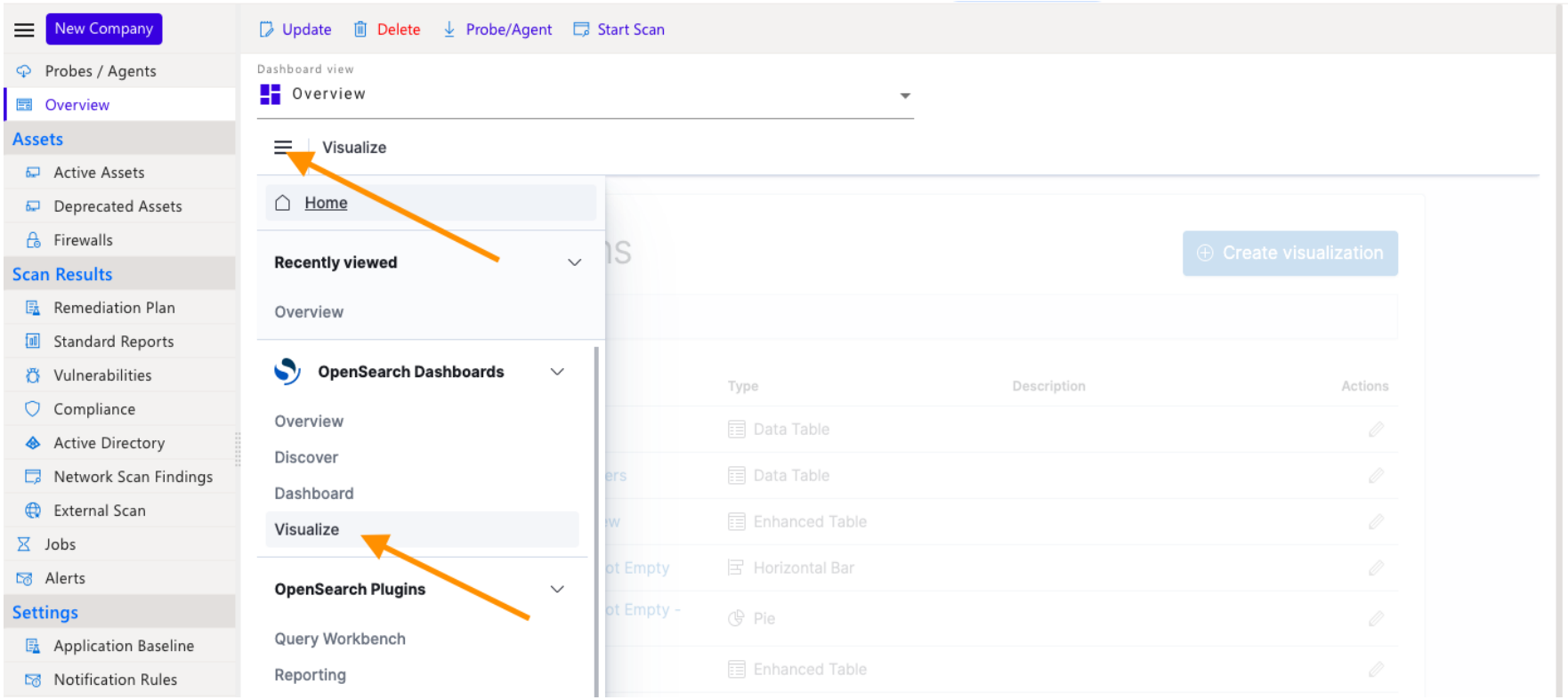


Creating Visualization/Table/Chart

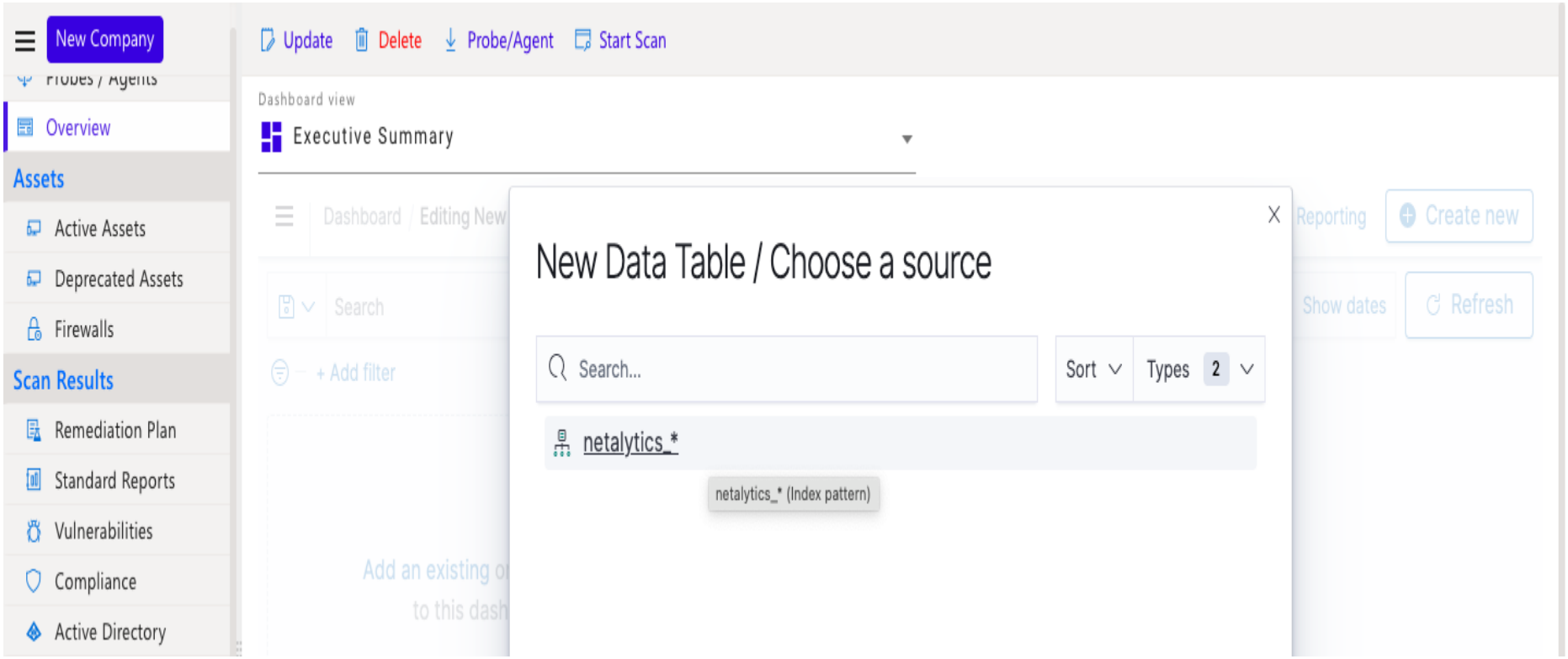
- To view dashboards, you must first add visualizations/charts.
- You can either add an existing visualization or create a new one.
- Data tables, bar charts, line charts, pie charts, area charts, metric, gauge charts, heat maps, TSVB charts (Time series charts), Markdown (Text Visualization), Control (Options Dropdown chart), and so on are examples of visualizations.

Creating Custom visualization:

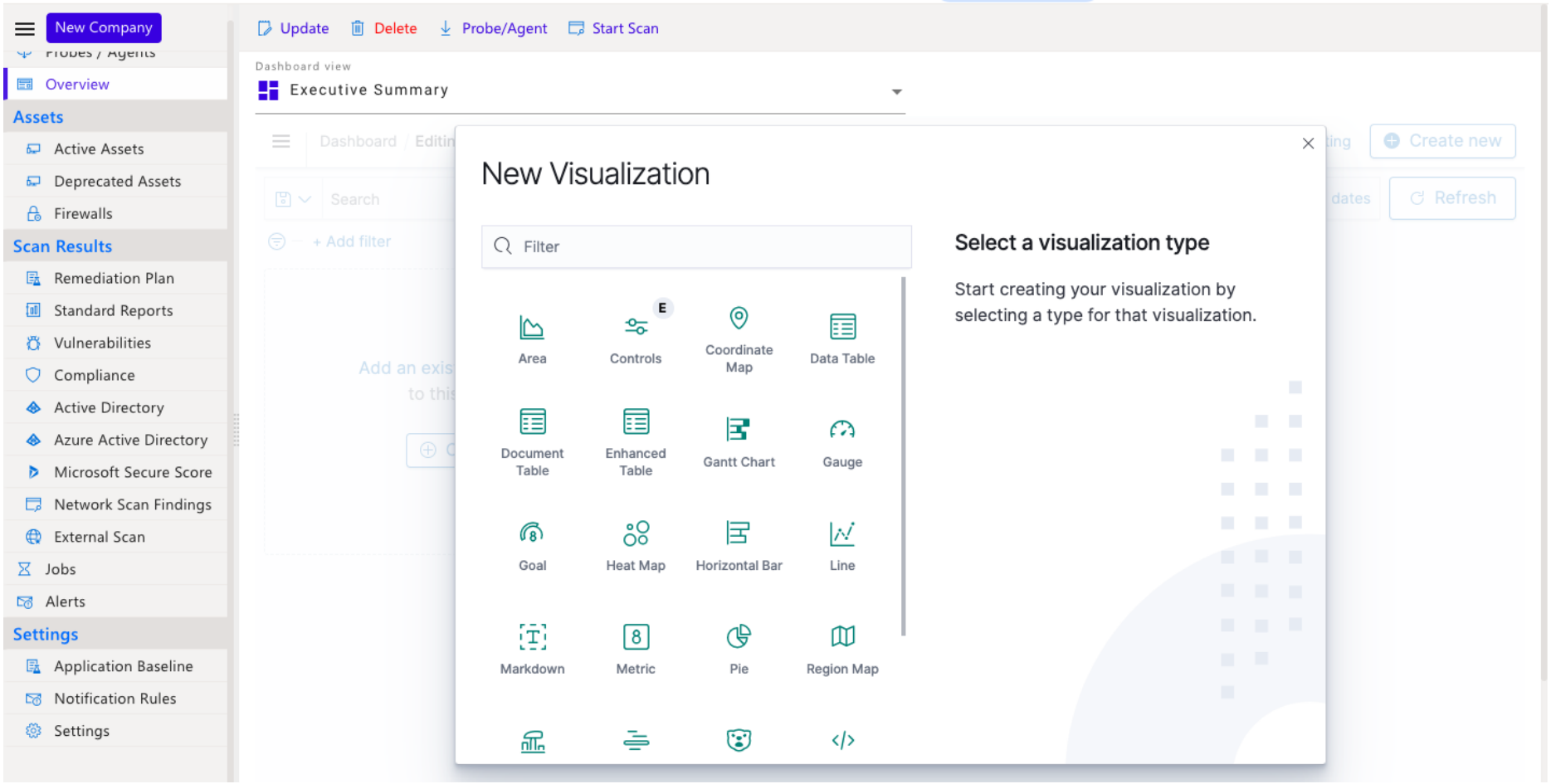
• To make your own custom visualization, click the menu icon and then the visualize option, as shown below.



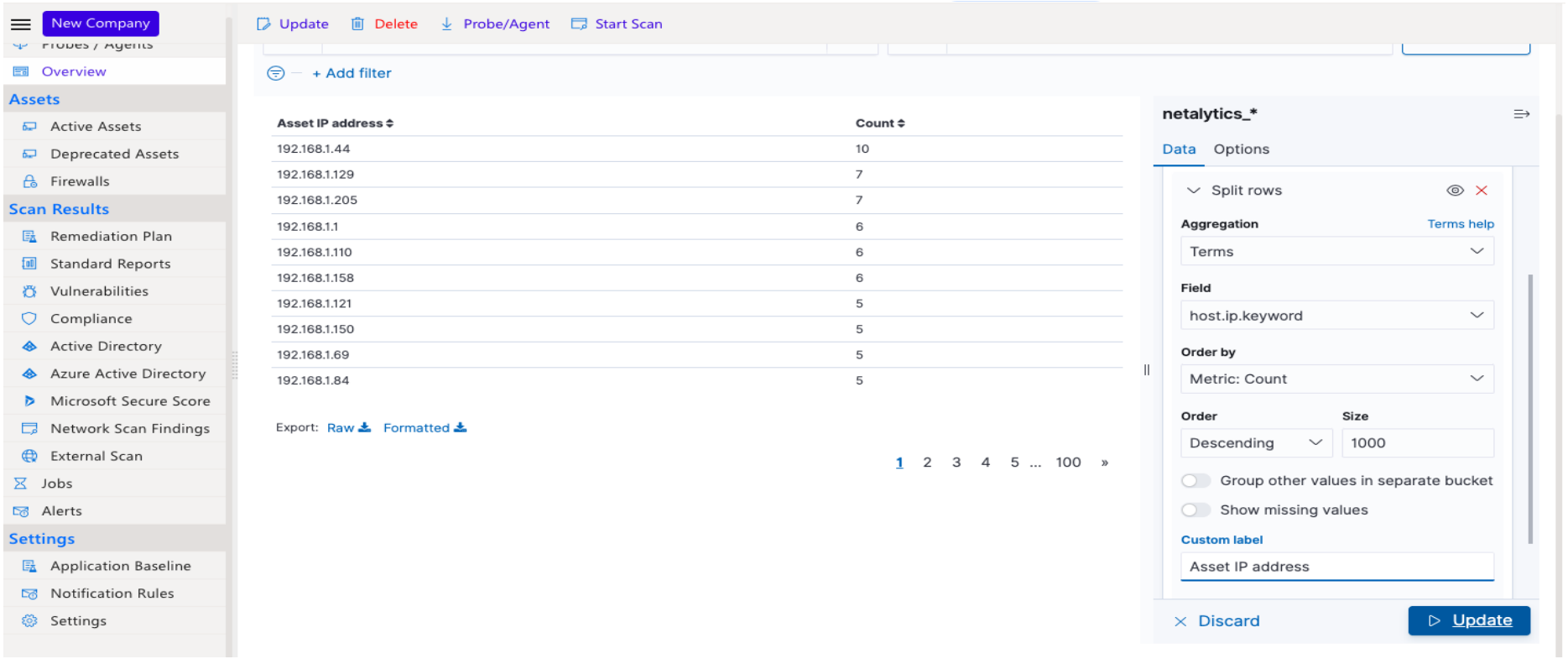
- Choose the dataset/index pattern from which the visualization will be built.



- Now select the type of visualization you want to build.

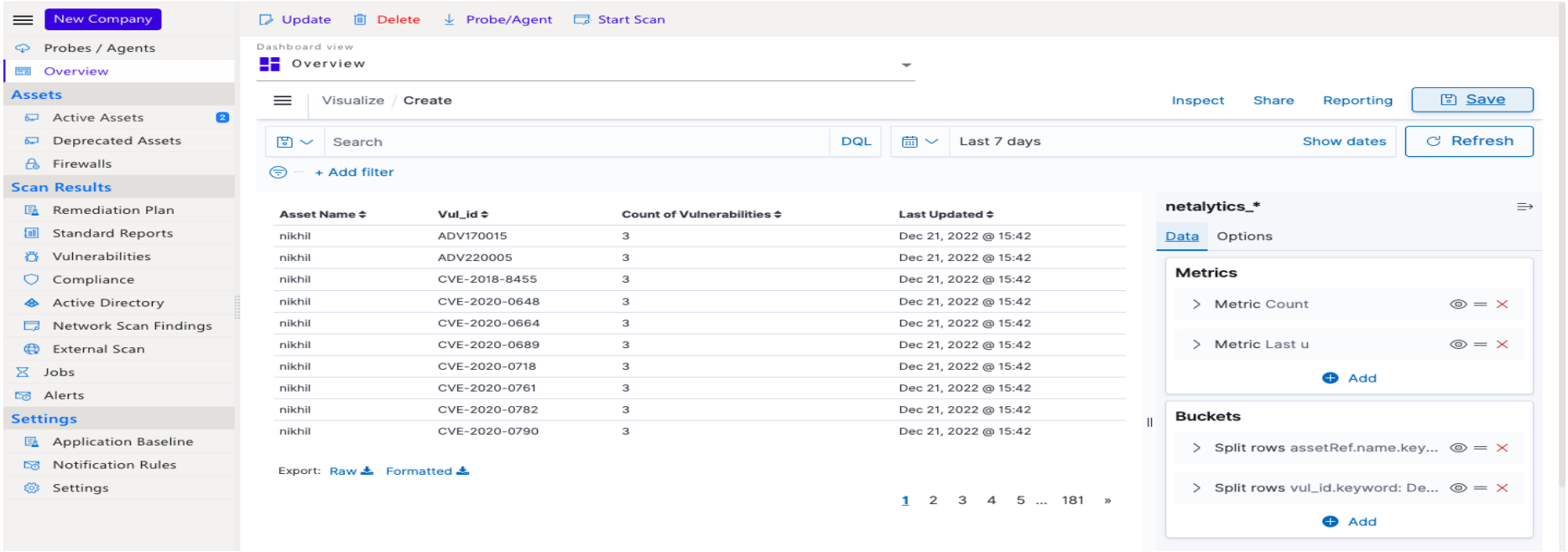


- Now you can see the visualisation view. In this section, you'll find buckets and metrics in data tables.
- Aggregation in buckets is built using field keys.
- You use "terms" for general aggregation. You can also use other bucket aggregation methods such as date histograms, date ranges, and so on. In metrics, you define the type of metric that will be used, such as count, sum, and so on.



- For Buckets - select “split rows” – select “terms” – select your “field_key_name” – select “size of field_key_name – add a “custom label” – select “update”.
- For metrics – select one of count/sum/average/max/min/Top hit (Latest values) – select “update”.

You can add a conditional filter by clicking on “add filter” with a field key assigned a value. If the visualisation meets your requirements, save it with a custom name. Once the visualisation is finished, you can add it to your custom dashboard.



Bucket Aggregations:

- **Date Histogram -** A date histogram is created by organising a numeric field by date. Intervals can be specified in seconds, minutes, hours, days, weeks, months, or years. You can also specify a custom interval frame in the text field by selecting Custom as the interval and entering a number and a time unit. The time units for custom intervals are s for seconds, m for minutes, h for hours, d for days, w for weeks, and y for years. Precision levels as low as one second are supported by various units. The date-key returned by Elasticsearch is used to label intervals at the beginning of the interval. The tooltip for a monthly interval, for example, will display the first day of the month.

- **Histogram -** A numeric field is used to construct a standard histogram. For this field, specify an integer interval. To include empty intervals in the histogram, select the Show empty buckets checkbox.

- **Range -** A range aggregation allows you to specify value ranges for a numeric field. To add a set of range endpoints, click Add Range. To remove a range, click the red (x) symbol.

- **Date Range -** A date range aggregation reports values that fall within a specified range of dates. Date math expressions can be used to specify date ranges. To add a set of range endpoints, click Add Range. To remove a range, click the red (x) symbol.

- **IPv4 Range -** You can specify IPv4 address ranges using IPv4 range aggregation. Click Add Range to add a set of range endpoints. To delete a range, click the red (x) symbol.

- **Terms -** You can use a terms aggregation to display the top or bottom n elements of a given field, ordered by count or a custom metric.

- **Filters -** A terms aggregation allows you to display the top or bottom n elements of a given field, ordered by count or a custom metric.

- **Significant Terms -** The results of the experimental significant terms aggregation are displayed.

Metric Aggregations:

1. **Count -** The count aggregation returns a raw count of the elements in the selected index pattern.

2. **Average -** The average of a numeric field is returned by this aggregation. Choose a field from the drop-down menu.

3. **Sum -** The total sum of a numeric field is returned by the sum aggregation. Choose a field from the drop-down menu.

4. **Min -** The min aggregation returns the numeric field's minimum value. Choose a field from the drop-down menu.

5. **Max -** A numeric field's maximum value is returned by the max aggregation. Choose a field from the drop-down menu.

Unique Count - The number of unique values in a field is returned by the cardinality aggregation. Choose a field from the drop-down menu.

Standard Deviation - The standard deviation of data in a numeric field is returned by the extended stats aggregation. Choose a field from the drop-down menu.

Top Hit - The top hits aggregation returns one or more of the most important values from a particular field in your documents. Choose a field from the drop-down menu, how you want to sort the documents and which fields should be prioritised, and how many values should be returned.

Percentiles - The percentile aggregation divides values in a numeric field into the percentile bands you specify. Choose a field from the drop-down menu, then enter one or more percentage ranges in the Percentiles fields. To remove a percentile field, click the X. To add a percentile field, click + Add.

Percentile Rank - The aggregation percentile ranks returns the percentile rankings for the values in the numeric field you specify. Choose a numeric field from the drop-down menu, then fill in the Values fields with one or more percentile rank values. To remove a values field, click the X. To add a values field, click +Add.

Different Type of Visualizations:

Below are the major types of visualizations that can be built as per one's needs:

1) **Data Table**: This is one of the most common visualisations. Data is typically displayed in the form of a table with rows and columns. This table can be built using field keys in aggregation buckets and metrics as needed.

2) **Enhanced Table:** Similar to Data Table, but with additional features such as computed columns, a filter bar, and a pivot table.

3) **Document Table**: This table is similar to the data table, but it only contains single documents (not aggregations).

4) **Controls**: This is useful for adding dropdowns and Range Sliders to the top of dashboards.

5) **Pie Chart:** A pie chart is a circular statistical graphic divided into slices to show numerical proportion. This graph is used to compare parts of a whole or to represent data in percentages.

6) **Vertical Bar Chart:** A vertical bar chart is used to display values in the form of vertical bars in the X and Y axis.

7) **Horizontal Bar Chart:** A horizontal bar chart is used to display values in the form of horizontal bars in the X and Y axis.

8) **Line Chart:** A line chart is used to display values in form of lines in X and Y Axis.

9) **Area Chart:** An area chart is used to display values in form of area in X and Y Axis.

10) **Heat Map:** Heatmap charts allow you to plot individual bucket values as a colour.

11) **Metric:** Metric visualisation can be used to display key values or indicators in the form of distinct values.

12) **Gauge:** A gauge visualisation shows where your metric on the data falls within a predefined range.

13) **Goal:** A goal visualisation describes your goal and how your metric on your data progresses toward it.

14) **Markdown:** This visualisation is a widget for displaying formatted text.

15) **TSVB Chart:** A Time Series Data Visualizer(TSVB) chart provides options to view the features of timeseries data and gives many ways of showing data.

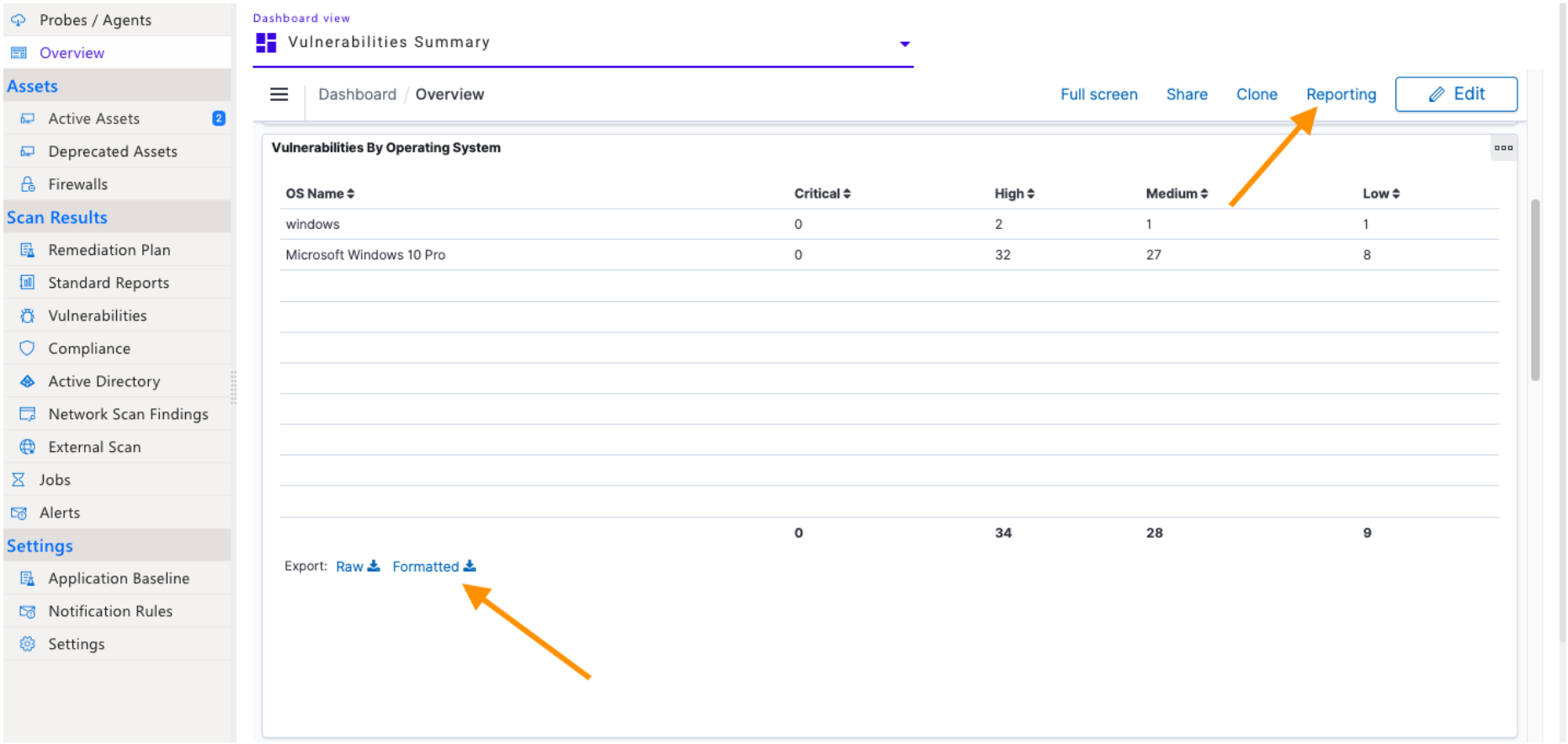
16) **Tag Cloud:** A group of words, sized according to their importance.

Additional Abilities of Dashboards

Downloading Reports from Dashboard & Visualizations

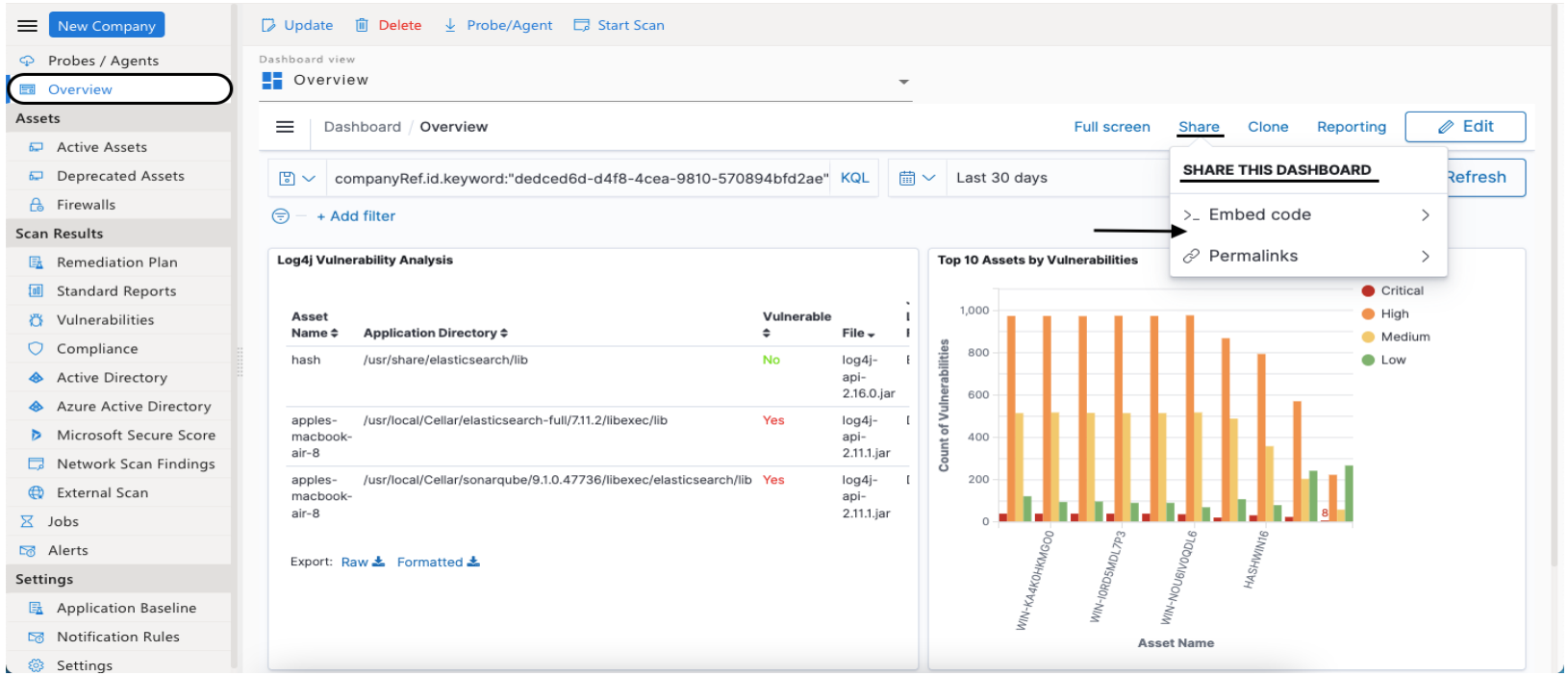
• We can download the report from the dashboard as follows:

1. First, specify the time frame for which the report must be downloaded.
2. By clicking on the "Raw" and "Formatted" buttons in data tables, we can download visualisation as CSV Reports.
3. To download CSV reports from bar charts and other charts, click the gear icon and then "inspect" before downloading the CSV report.
4. To download the dashboard as a PDF or PNG report, go to the top menu and select the option to download the dashboard as a report.
5. As illustrated below, we can download reports.


Probes / Agents
Overview
Assets
Active Assets
2
Deprecated Assets
Firewalls
Scan Results
Remediation Plan
Standard Reports
Vulnerabilities
Compliance
Active Directory
Network Scan Findings
External Scan
Jobs
Alerts
Settings
Application Baseline
Notification Rules
Settings
Dashboard view
Vulnerabilities Summary
Dashboard / Overview
Full screen
Share
Clone
Reporting
Edit
Vulnerabilities By Operating System
OS Name
Critical
High
Medium
Low
windows
0
2
1
1
Microsoft Windows 10 Pro
0
32
27
8
0
34
28
9
Export: Raw Formatted

Sharing Dashboards as Links:

- Dashboards can be shared as links and viewed.
- When you select Share the dashboard, you will be given two options: Embed code and Permalinks. You will be able to select relevant options in the future.
- Use the "embed" code to share a Link in iframe format with various options. Use "permalinks" to share a link in plain text.

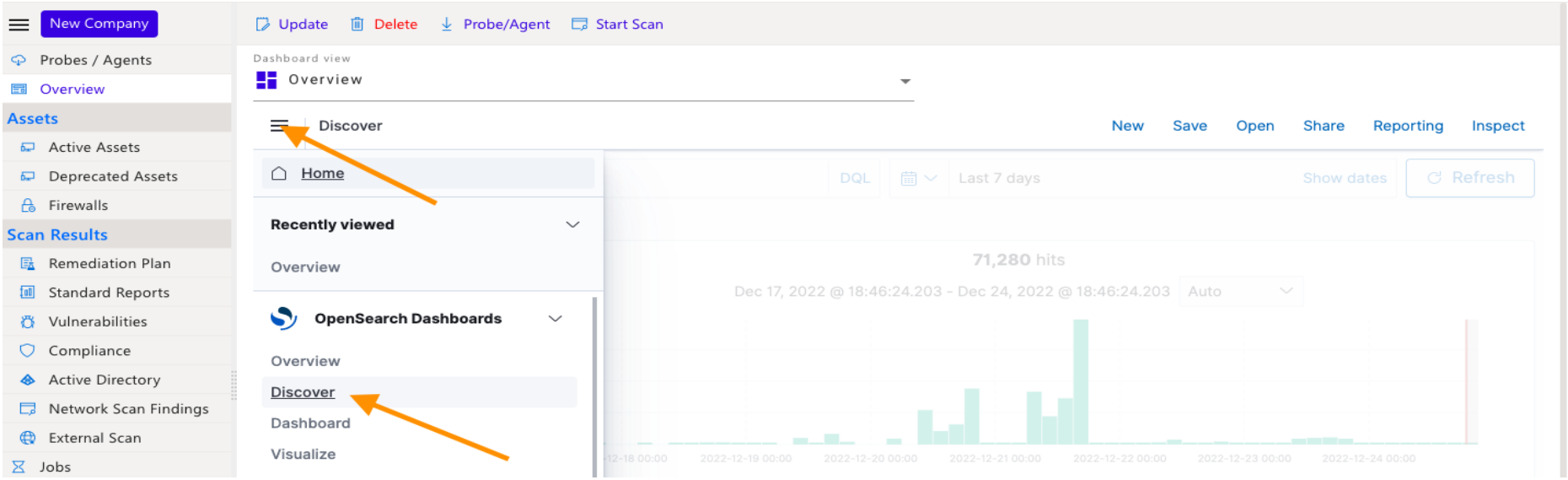


Exploring Raw Data

Discover - Discover in Dashboards helps you extract insights and get value out of data assets across your organization. You can quickly ingest and query your data, display that data in visualizations and interactive dashboards, and deliver insights to your organization.

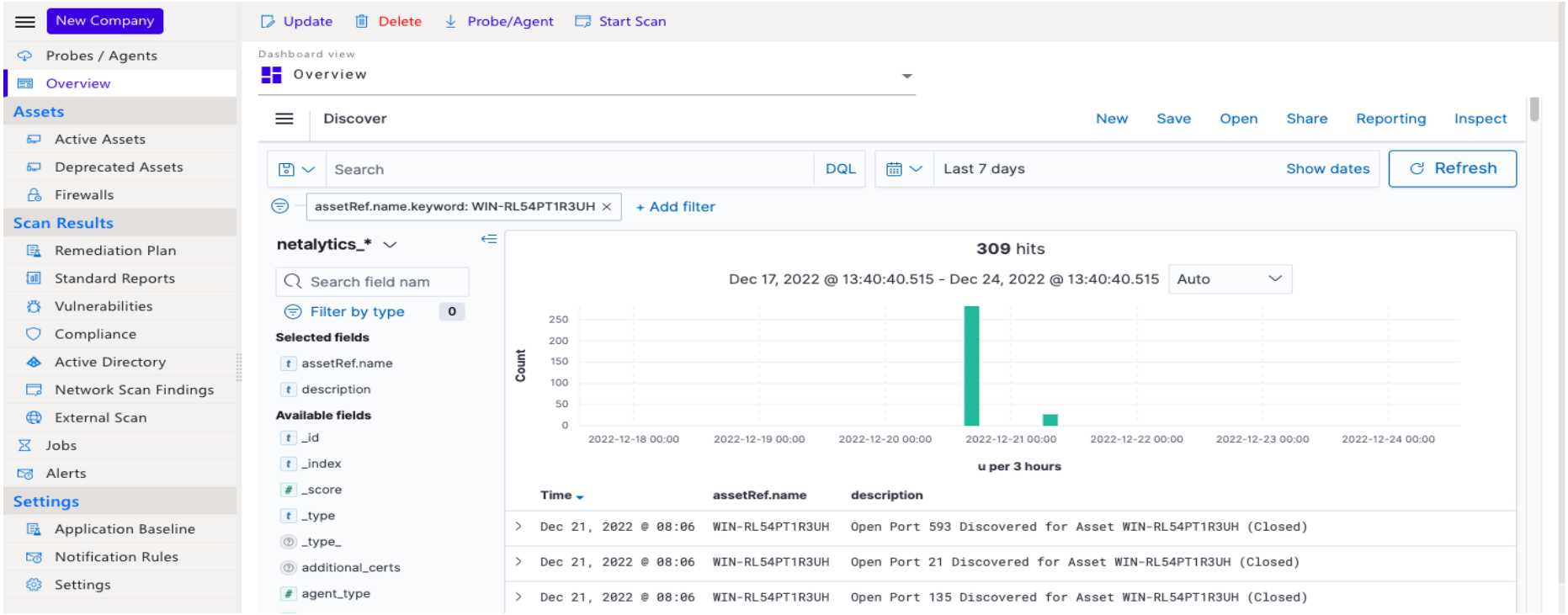
Navigating and view Discover section:

- You can view raw data in Dashboards' Discover section, as shown below:



- In Discover, you can view raw data and explore fields as shown below:

1. Documents are available here. Expand each document by clicking on the right-arrow icon.
2. Add columns from the left column to see columns in the view.
3. Each document has field columns and values associated with it.
4. You can also filter a field value to see a specific set of data.



Saved Search:

- You can save your custom conditional search and view it later.
- Apply the conditional filter and time period, then click "Save" and give this saved search a unique name. You can access your saved search at any time by clicking "open" and then selecting your saved search.