

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.

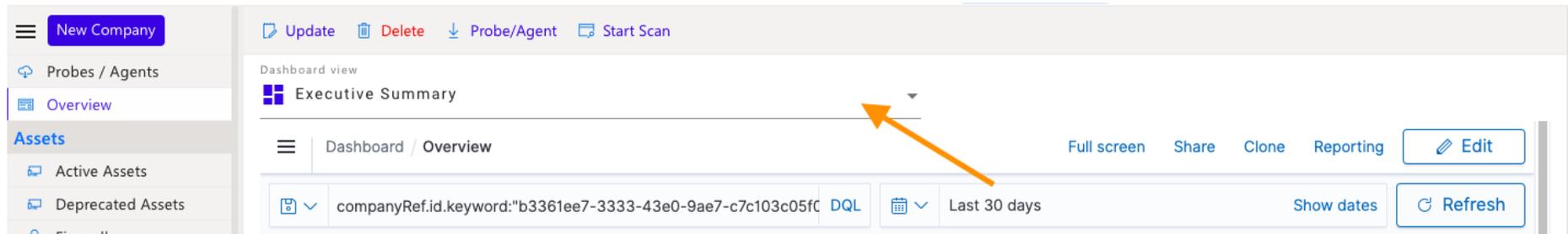
However, if you are in another tab and want to see dashboards, click on the Overview tab in the left side panel, as shown below.

The screenshot displays a security dashboard interface. On the left is a navigation sidebar with a 'New Company' button at the top. Below it are sections for 'Probes / Agents', 'Overview' (highlighted with an orange arrow), 'Assets' (containing 'Active Assets', 'Deprecated Assets', and 'Firewalls'), and 'Scan Results' (containing 'Remediation Plan', 'Standard Reports', 'Vulnerabilities', 'Compliance', 'Active Directory', 'Azure Active Directory', 'Microsoft Secure Score', 'Network Scan Findings', and 'External Scan'). The main content area has a top bar with 'Update', 'Delete', 'Probe/Agent', and 'Start Scan' actions. Below this is a 'Dashboard view' section with a breadcrumb 'Dashboard / Overview' and buttons for 'Full screen', 'Share', 'Clone', 'Reporting', and 'Edit'. A search bar contains the filter 'companyRef.id.keyword:"f1869af1-f0ad-476b-8090-b1dc3a04d00"; DQL' and a date range of 'Last 1 year'. A '+ Add filter' button is also present. The main content area features two panels: 'Active Assets' showing a large number '67', and 'Asset Risk Rating' showing a bar chart with four bars representing vulnerability scores of 77.50, 77.50, 73.70, and 57.70.

Asset Risk Rating	Vulnerability Score
1	77.50
2	77.50
3	73.70
4	57.70

Navigating to Different Dashboards

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



The screenshot displays a web application interface. On the left is a sidebar with navigation items: 'New Company', 'Probes / Agents', 'Overview', and 'Assets' (with sub-items 'Active Assets' and 'Deprecated Assets'). The main content area has a top bar with 'Update', 'Delete', 'Probe/Agent', and 'Start Scan' buttons. Below this is a 'Dashboard view' section with a dropdown menu currently showing 'Executive Summary'. An orange arrow points to this dropdown menu. Below the dropdown is a breadcrumb 'Dashboard / Overview' and buttons for 'Full screen', 'Share', 'Clone', 'Reporting', and 'Edit'. At the bottom, there is a search bar with a dropdown arrow, a text input containing 'companyRef.id.keyword:"b3361ee7-3333-43e0-9ae7-c7c103c05f0', a 'DQL' button, a date range dropdown set to 'Last 30 days', a 'Show dates' button, and a 'Refresh' button.

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

The screenshot displays a security dashboard interface. On the left is a sidebar menu with the following items: 'New Company', 'Probes / Agents', 'Overview', 'Assets' (sub-items: Active Assets, Deprecated Assets, Firewalls), and 'Scan Results' (sub-items: Remediation Plan, Standard Reports, Vulnerabilities, Compliance, Active Directory, Azure Active Directory). A dropdown menu is open, listing dashboard options: 'Application Scan Detailed Dashboard', 'Application Vulnerabilities Detailed Dashboard', 'Assets' (highlighted with an orange arrow), 'Azure Active Directory Audit Logs', and 'Azure Active Directory Computers'. The main dashboard area shows three summary cards: 'Total Assets' with a value of 2,246, 'Critical Assets' with a value of 1, and 'High Risk Assets' with a value of 0. At the top right of the dashboard, there are controls for 'Full screen', 'Share', 'Clone', 'Reporting', 'Edit', a date range of 'Last 30 days', 'Show dates', and 'Refresh'.

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 frame 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:

The screenshot displays a dashboard titled "Vulnerability" with a sub-section "Dashboard / Overview". The main content area is divided into two panels: "Critical Risk Vulnerabilities" showing a count of 0, and "High Risk Vulnerabilities" showing a count of 38. A search bar at the top contains the query "companyRef.id.keyword:"525e4b7a-7272-4d55-a971-8e917f6c21c" and a "DQL" button. A date range selector is set to "Nov 25, 2022 @ 00:00:00.0" to "Dec 25, 2022 @ 00:00:00.0". A calendar pop-up is open, showing the month of December 2022. The date "25" is selected, and the time "00:00" is chosen from a list of hourly options. An orange arrow points from the date range selector to the calendar. The "End date" field shows "Dec 25, 2022 @ 00:00:00.000". A user name "NIKHIL (42.48%)" is visible in the bottom right corner.

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.

The screenshot displays a security dashboard interface. On the left is a navigation sidebar with sections for Probes / Agents, Assets, Scan Results, and Settings. The 'Overview' tab is selected. The main content area shows a dashboard view with a filter condition: `companyRef.id.keyword:"dedced6d-d4f8-4cea-9810-570894bfd2ae"`. A modal dialog titled 'EDIT FILTER' is open, showing the configuration for the filter: Field is 'AccountDomain', Operator is 'exists', and the 'Create custom label?' checkbox is checked. The dialog has 'Cancel' and 'Save' buttons. To the right, a table lists vulnerable files, and a bar chart titled 'Top 10 Assets by Vulnerabilities' shows the count of vulnerabilities for various assets, categorized by severity (Critical, High, Medium, Low).

Asset Name	Critical	High	Medium	Low
WIN-KA4K0HKMG00	10	500	500	100
WIN-I0RDSMDL7P3	10	500	500	100
WIN-NOU6Y0aDL6	10	500	500	100
HASHWIN16	10	500	500	100
log4j-api-2.16.0.jar	10	500	500	100
log4j-api-2.11.1.jar	10	500	500	100
log4j-api-2.11.1.jar	10	500	500	100

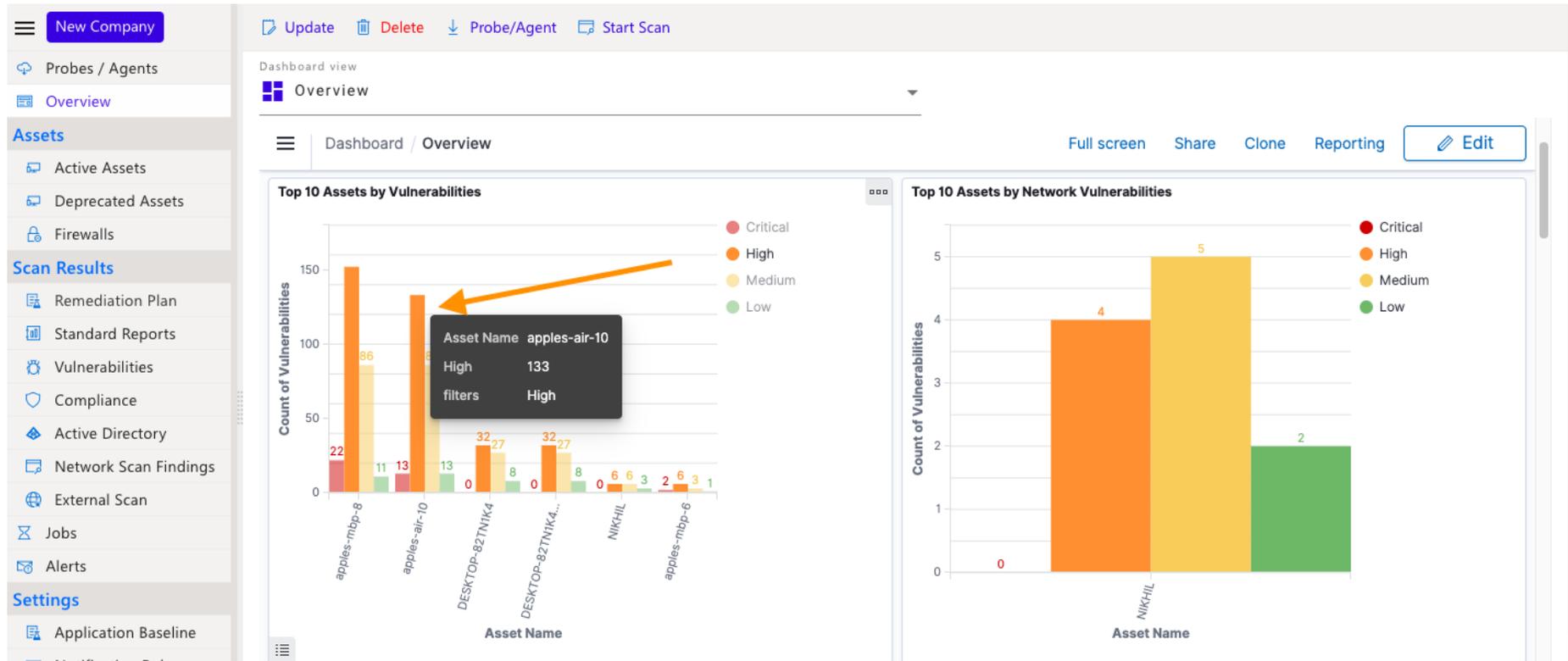
- You can also filter the values by clicking on the '+' sign next to the value in the data tables, as shown below:

The screenshot shows a dashboard interface with a sidebar on the left containing navigation options like 'Probes / Agents', 'Overview', 'Assets', and 'Scan Results'. The main content area displays a table titled 'Newly Discovered Assets in last 48 hours Details'. The table has columns for 'Asset Name', 'IP Address', 'Name', 'Last Discovered Time', and 'Count of Assets'. An orange arrow points to a magnifying glass icon in the 'Name' column header, which is labeled 'Filter for value'.

Asset Name ↕	IP Address ↕	Filter for value	Name ↕	Last Discovered Time ↕	Count of Assets ↕
apples-mbp-8.hashinclude	172.16.1.117	🔍	macOS	Dec 27, 2022 @ 11:03:30.781	1
apples-mbp-6.hashinclude	172.16.1.123	🔍	macOS	Dec 27, 2022 @ 10:52:22.642	1
apples-air-10.hashinclude	172.16.1.135	🔍	MacOS Big Sur	Dec 27, 2022 @ 12:43:54.468	1
					3

Export: [Raw](#) [Formatted](#)

- 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.

The screenshot displays a security dashboard interface. On the left, a sidebar menu is visible with categories: 'New Company', 'Probes / Agents', 'Overview', 'Assets', 'Scan Results', and 'Settings'. The 'Assets' section is expanded, showing 'Active Assets', 'Deprecated Assets', and 'Firewalls'. The 'Scan Results' section includes 'Remediation Plan', 'Standard Reports', 'Vulnerabilities', 'Compliance', 'Active Directory', 'Azure Active Directory', 'Microsoft Secure Score', 'Network Scan Findings', and 'External Scan'. The 'Settings' section includes 'Application Baseline'. The main dashboard area shows a top navigation bar with 'Update', 'Delete', 'Probe/Agent', and 'Start Scan' buttons. Below this, the dashboard title is 'Executive Summary'. A dropdown menu is open, showing 'Dashboard / Overview' and 'Home' options. An orange arrow points to the 'Dashboard / Overview' option. Below the dropdown, a 'Recently viewed' list includes 'Executive Summary', 'Assets', 'Overview', 'OpenSSL Critical Vulnerability', and 'Network Scan Findings #global'. Another orange arrow points to the 'Dashboard' option in the 'OpenSearch Dashboards' section. The main dashboard content area displays several metrics: 'Critical Assets' (1), 'High Risk Assets' (0), 'Avg Vulnerability Score' (37.61), 'Min Vulnerability Score' (0.00), and 'Attention Required Assets' (18). The 'Dashboard / Overview' page also features buttons for 'Full screen', 'Share', 'Clone', 'Reporting', and 'Edit'.

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

The screenshot displays a dashboard editor interface. On the left is a sidebar with navigation options: Overview, Assets (Active Assets, Deprecated Assets, Firewalls), Scan Results (Remediation Plan, Standard Reports, Vulnerabilities, Compliance, Active Directory, Azure Active Directory, Microsoft Secure Score, Network Scan Findings, External Scan), Jobs, and Alerts. The main area is titled 'Dashboard view' and 'Executive Summary'. It shows a breadcrumb 'Dashboard / Editing New Dashboard' and a toolbar with 'Options', 'Share', 'Add', 'Cancel', 'Save', 'Reporting', and a '+ Create new' button. Below the toolbar are search and filter controls: a search box, a 'DQL' button, a date range selector set to 'Last 30 days', a 'Show dates' button, and a 'Refresh' button. A '+ Add filter' button is also visible. The main content area contains a dashed box with the text 'Add an existing or new object to this dashboard' and a '+ Create new' button.

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

The screenshot shows a dashboard interface for a security tool. On the left is a sidebar with navigation menus: 'Probes / Agents', 'Overview', 'Assets' (with sub-items: Active Assets, Deprecated Assets, Firewalls), 'Scan Results' (with sub-items: Remediation Plan, Standard Reports, Vulnerabilities, Compliance, Active Directory, Network Scan Findings, External Scan), 'Jobs', 'Alerts', and 'Settings' (with sub-items: Application Baseline, Notification Rules, Settings). The main content area is titled 'Dashboard view' and 'Overview'. It features a breadcrumb 'Dashboard / Editing New Dashboard (unsaved)' and a toolbar with buttons for 'Options', 'Share', 'Add', 'Cancel', 'Save', 'Reporting', and 'Create new'. Below the toolbar is a search bar with 'DQL' and a date filter set to 'Last 30 days'. A table titled 'OS by Assets' is displayed with columns: Operating System Name, Asset Name, OS Full Name, OS Platform, OS Version, and Updated Time. An orange arrow points to the 'Save' button in the toolbar. At the bottom right, there is a pagination control showing '1 2 3 4 5 ... 13 »'. Below the table, there are export options: 'Export: Raw' and 'Formatted'.

Operating System Name	Asset Name	OS Full Name	OS Platform	OS Version	Updated Time
windows	WIN7PRO-PC	windows	windows		Dec 9, 2022 @ 05:32
windows	WIN-TAT8MLJGBEJ	windows	windows		Dec 20, 2022 @ 15:37
windows	WIN-RL54PT1R3UH	windows	windows		Dec 20, 2022 @ 15:36
windows	WIN-MNDA87FDIOG	windows	windows		Dec 9, 2022 @ 05:35
windows	WIN-FGDST65B8P6	windows	windows		Dec 13, 2022 @ 13:03
windows	WIN-CIUDK9OCGKB	windows	windows		Dec 13, 2022 @ 13:00
windows	WIN-8D86E515VJF	windows	windows		Dec 20, 2022 @ 15:35
windows	WIN-1TL95BRLCNM		windows		Dec 20, 2022 @ 13:00
windows	WIN-19EXCHANGE	windows	windows		Dec 20, 2022 @ 15:35
windows	WIN-0706MMRQOL8	windows	windows		Dec 20, 2022 @ 15:34

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.

The screenshot displays a dashboard editing interface. The left sidebar contains navigation options: Probes / Agents, Overview (highlighted), Assets (Active Assets, Deprecated Assets, Firewalls), Scan Results (Remediation Plan, Standard Reports, Vulnerabilities, Compliance, Active Directory, Azure Active Directory, Microsoft Secure Score, Network Scan Findings, External Scan), Jobs, Alerts, and Settings (Application Baseline, Notification Rules, Settings).

The main dashboard area shows a 'Dashboard view' for 'Overview'. The breadcrumb path is 'Dashboard / Editing Overview Copy', with an arrow pointing to the text. Action buttons include 'Update', 'Delete', 'Probe/Agent', 'Start Scan', 'Options', 'Share', 'Add', 'Reporting', 'Cancel', 'Save', and 'Create new' (highlighted with an arrow). A search filter is set to 'companyRef.id.keyword:"dedced6d-d4f8-4cea-9810-570894bfd2ae"' with a 'KQL' button. A date filter is set to 'Last 30 days' with a 'Show dates' button and a 'Refresh' button.

The 'Log4j Vulnerability Analysis' widget contains a table:

Asset Name	Application Directory	Vulnerable	File
hash	/usr/share/elasticsearch/lib	No	log4j-api-2.16.0.jar
apples-macbook-air-8	/usr/local/Cellar/elasticsearch-full/7.11.2/libexec/lib	Yes	log4j-api-2.11.1.jar
apples-macbook-air-8	/usr/local/Cellar/sonarqube/9.1.0.47736/libexec/elasticsearch/lib	Yes	log4j-api-2.11.1.jar

Export options: Raw, Formatted.

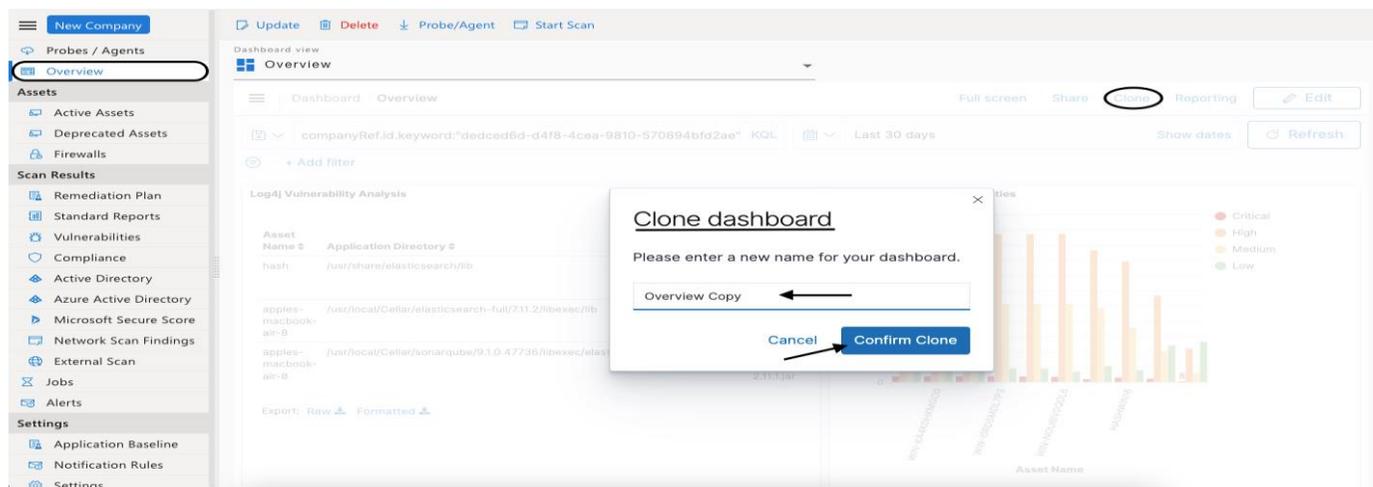
The 'Top 10 Assets by Vulnerabilities' widget is a bar chart showing the count of vulnerabilities for various assets. The y-axis is 'Count of Vulnerabilities' (0 to 1,000). The x-axis is 'Asset Name'. The legend indicates severity levels: Critical (red), High (orange), Medium (yellow), and Low (green). Assets shown include WIN-K44K0HKMG00, WIN-0RDSMDL7P3, WIN-N0U6I00DL6, and HASHWIN16.

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.

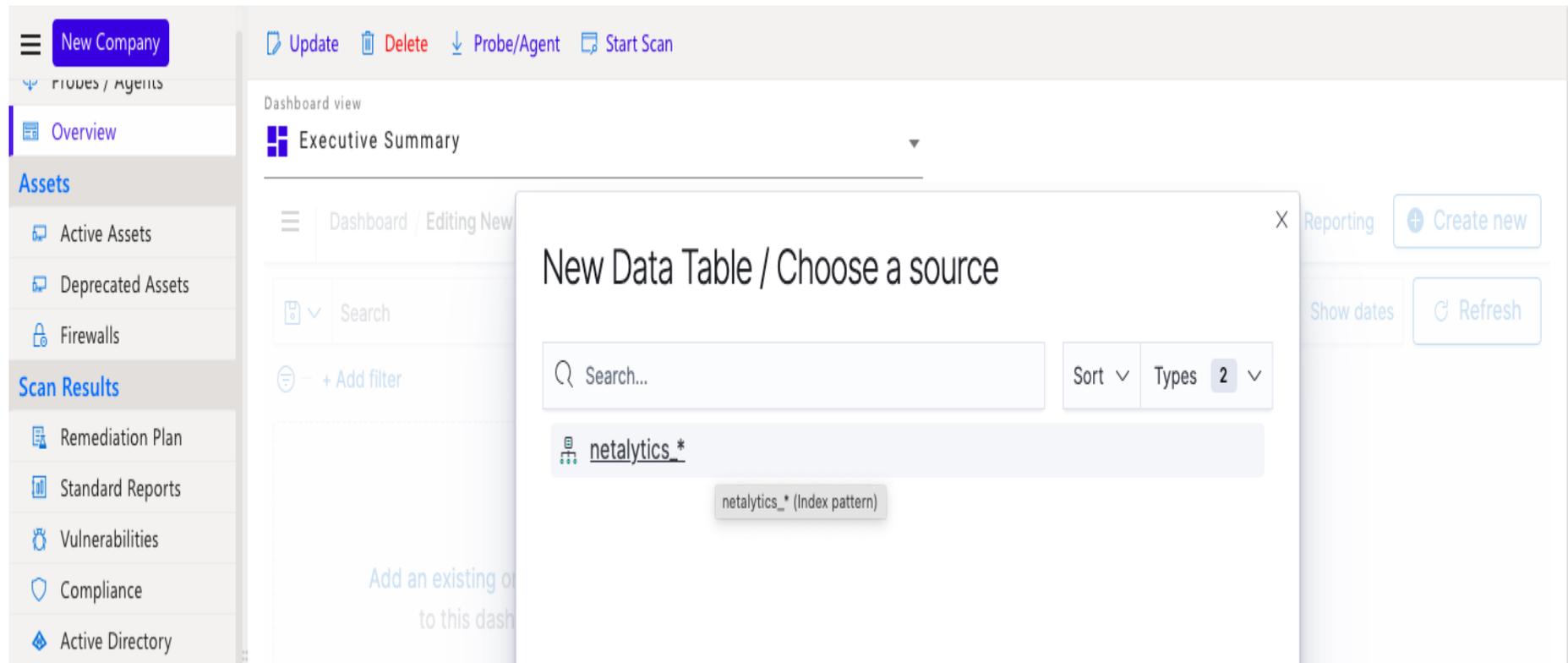
Creating Custom visualization:

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

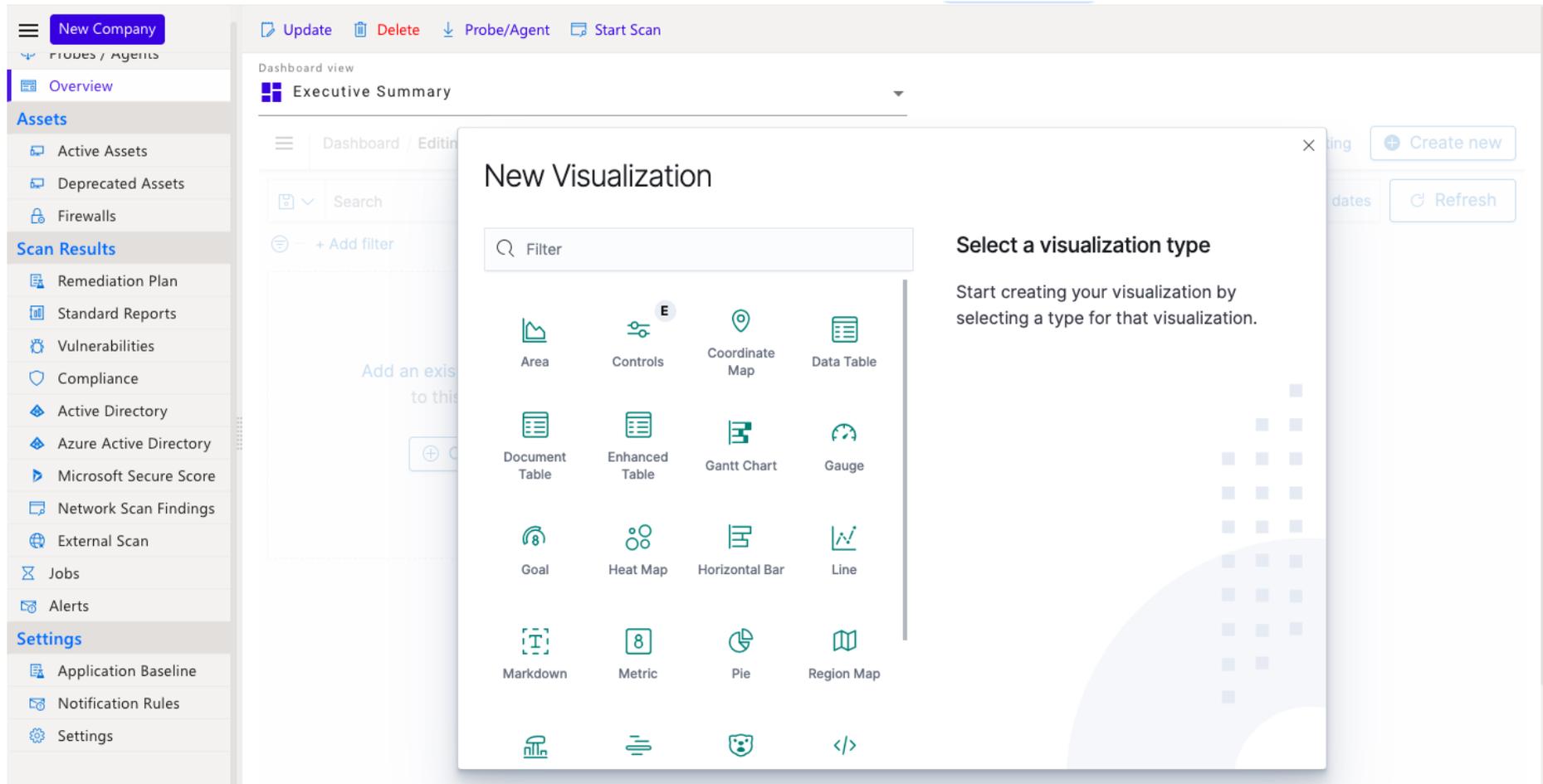
The screenshot displays a web application interface for a security dashboard. On the left is a navigation sidebar with sections: 'Probes / Agents', 'Overview', 'Assets' (with sub-items: Active Assets, Deprecated Assets, Firewalls), 'Scan Results' (with sub-items: Remediation Plan, Standard Reports, Vulnerabilities, Compliance, Active Directory, Network Scan Findings, External Scan), 'Jobs', 'Alerts', and 'Settings' (with sub-items: Application Baseline, Notification Rules). The main content area at the top has a header with 'New Company' and action buttons: 'Update', 'Delete', 'Probe/Agent', and 'Start Scan'. Below this is a 'Dashboard view' section with a dropdown menu currently showing 'Overview'. A 'Visualize' menu icon is highlighted with an orange arrow. A secondary dropdown menu is open, listing 'Home', 'Recently viewed' (with 'Overview' listed below), 'OpenSearch Dashboards' (with sub-items: Overview, Discover, Dashboard, and 'Visualize' highlighted with an orange arrow), and 'OpenSearch Plugins' (with sub-items: Query Workbench, Reporting). In the background, a 'Create visualization' dialog is visible, featuring a table with the following structure:

Type	Description	Actions
Data Table		
Data Table		
Enhanced Table		
Horizontal Bar		
Pie		
Enhanced Table		

- 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.

The screenshot displays a security dashboard interface. On the left is a navigation sidebar with sections for 'Assets', 'Scan Results', and 'Settings'. The main area shows a table of 'Asset IP address' and 'Count'. Below the table are 'Export' options and a pagination control. On the right, a configuration panel for 'netalytics_*' is open, showing settings for a bucket aggregation: 'Split rows' is checked, 'Aggregation' is set to 'Terms', 'Field' is 'host.ip.keyword', 'Order by' is 'Metric: Count', 'Order' is 'Descending', and 'Size' is '1000'. There are also options for 'Group other values in separate bucket' and 'Show missing values', both of which are unchecked. A 'Custom label' field contains 'Asset IP address'. At the bottom of the panel are 'Discard' and 'Update' buttons.

Asset IP address ↕	Count ↕
192.168.1.44	10
192.168.1.129	7
192.168.1.205	7
192.168.1.1	6
192.168.1.110	6
192.168.1.158	6
192.168.1.121	5
192.168.1.150	5
192.168.1.69	5
192.168.1.84	5

Export: [Raw](#) [Formatted](#)

1 2 3 4 5 ... 100 »

netalytics_*

Data Options

Split rows 👁️ ✕

Aggregation [Terms help](#)

Terms ⌵

Field

host.ip.keyword ⌵

Order by

Metric: Count ⌵

Order **Size**

Descending ⌵ 1000

Group other values in separate bucket

Show missing values

Custom label

Asset IP address

✕ Discard ▶ Update

- 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.

The screenshot shows a security dashboard interface. On the left is a navigation sidebar with sections like 'Assets', 'Scan Results', and 'Settings'. The main area displays a table of vulnerabilities with columns for Asset Name, Vul_id, Count of Vulnerabilities, and Last Updated. Below the table are 'Export' options and a pagination bar. On the right, there are configuration panels for 'netalytics_*' with 'Data' and 'Options' tabs. The 'Metrics' panel shows 'Metric Count' and 'Metric Last u' with visibility and delete icons. The 'Buckets' panel shows 'Split rows assetRef.name.key...' and 'Split rows vul_id.keyword: De...' with visibility and delete icons.

Asset Name	Vul_id	Count of Vulnerabilities	Last Updated
nikhil	ADV170015	3	Dec 21, 2022 @ 15:42
nikhil	ADV220005	3	Dec 21, 2022 @ 15:42
nikhil	CVE-2018-8455	3	Dec 21, 2022 @ 15:42
nikhil	CVE-2020-0648	3	Dec 21, 2022 @ 15:42
nikhil	CVE-2020-0664	3	Dec 21, 2022 @ 15:42
nikhil	CVE-2020-0689	3	Dec 21, 2022 @ 15:42
nikhil	CVE-2020-0718	3	Dec 21, 2022 @ 15:42
nikhil	CVE-2020-0761	3	Dec 21, 2022 @ 15:42
nikhil	CVE-2020-0782	3	Dec 21, 2022 @ 15:42
nikhil	CVE-2020-0790	3	Dec 21, 2022 @ 15:42

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.

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.

The screenshot displays a security dashboard interface. On the left is a navigation sidebar with sections like 'Assets', 'Scan Results', and 'Settings'. The main area shows a 'Log4j Vulnerability Analysis' table and a 'Top 10 Assets by Vulnerabilities' bar chart. A 'SHARE THIS DASHBOARD' menu is open, showing options for 'Embed code' and 'Permalinks'.

Asset Name	Application Directory	Vulnerable	File
hash	/usr/share/elasticsearch/lib	No	log4j-api-2.16.0.jar
apples-macbook-air-8	/usr/local/Cellar/elasticsearch-full/7.11.2/libexec/lib	Yes	log4j-api-2.11.1.jar
apples-macbook-air-8	/usr/local/Cellar/sonarqube/9.1.0.47736/libexec/elasticsearch/lib	Yes	log4j-api-2.11.1.jar

Export: Raw | Formatted

Top 10 Assets by Vulnerabilities

Count of Vulnerabilities

Asset Name

Legend: Critical (Red), High (Orange), Medium (Yellow), Low (Green)

SHARE THIS DASHBOARD

- Embed code
- Permalinks

- 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.

The screenshot displays the Discover interface with the following components:

- Left Sidebar:** Contains navigation menus for 'Probes / Agents', 'Overview', 'Assets' (Active Assets, Deprecated Assets, Firewalls), 'Scan Results' (Remediation Plan, Standard Reports, Vulnerabilities, Compliance, Active Directory, Network Scan Findings, External Scan), 'Jobs', 'Alerts', and 'Settings' (Application Baseline, Notification Rules, Settings).
- Top Bar:** Includes 'Update', 'Delete', 'Probe/Agent', 'Start Scan', and 'Discover' tabs. Action buttons for 'New', 'Save', 'Open', 'Share', 'Reporting', and 'Inspect' are also present.
- Search and Filter Area:** Shows a search query 'assetRef.name.keyword: WIN-RL54PT1R3UH' with a filter icon and '+ Add filter' button. A date range of 'Last 7 days' and a 'Refresh' button are also visible.
- Results Section:**
 - Summary:** '309 hits' for the query 'assetRef.name.keyword: WIN-RL54PT1R3UH'.
 - Chart:** A bar chart titled 'u per 3 hours' showing a significant spike on Dec 21, 2022, with a count of approximately 250.
 - Table:** A table with columns 'Time', 'assetRef.name', and 'description'. It lists three entries for Dec 21, 2022 @ 08:06, all for asset 'WIN-RL54PT1R3UH', describing 'Open Port 593', 'Open Port 21', and 'Open Port 135' discovered for the asset.

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.