

 RiskTech  
100 2019 Gartner 2015  
CoolVendor

# NG | Screener UI Dashboard creation

Ljupce Nikolov  
June 2019

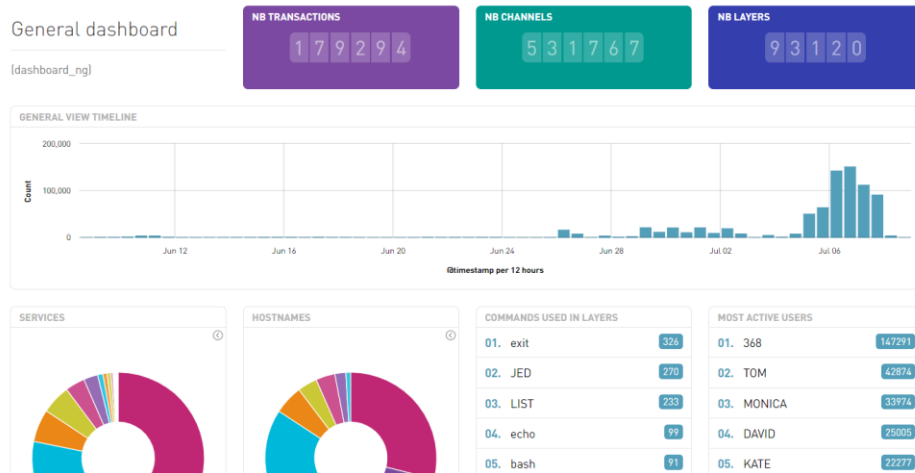


## Summary

- What is a dashboard
- Global picture
- Index Patterns
- Saved search
- Dashboard and Visualizations
- Dashboard administration commands

# What is a dashboard?

- Combination of charts and table element
- Defined to highlight important piece of information
- Could be both defined for controls output as well as Forensic investigation

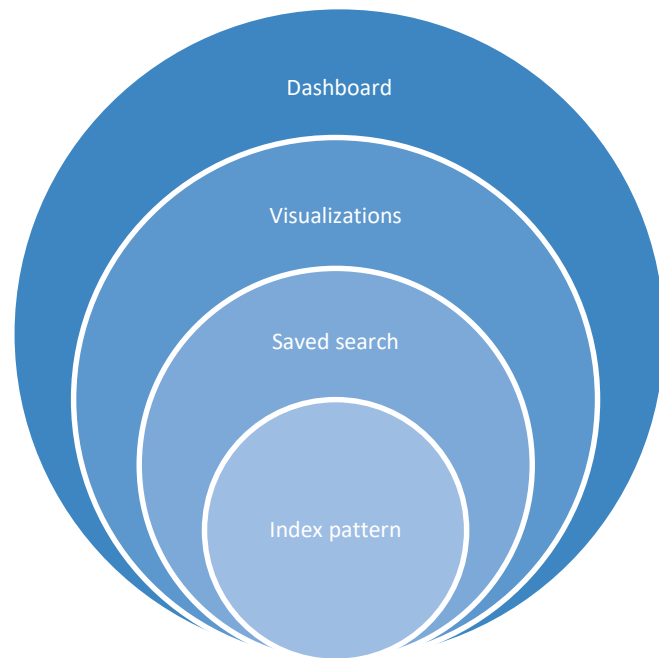




## Global picture

### Links between elements

- Dashboard contains Visualizations
- Visualizations are built on Saved search
- Saved search uses Index pattern



# Index Pattern

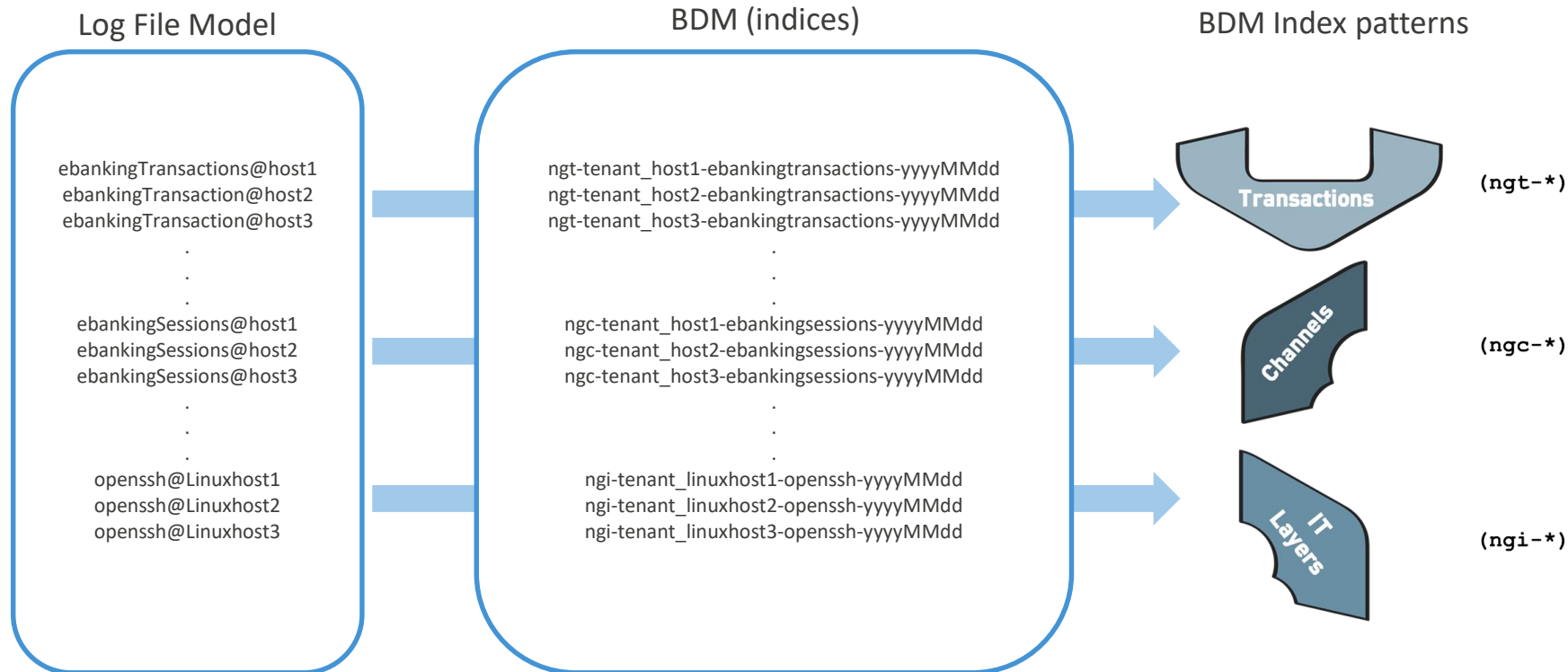




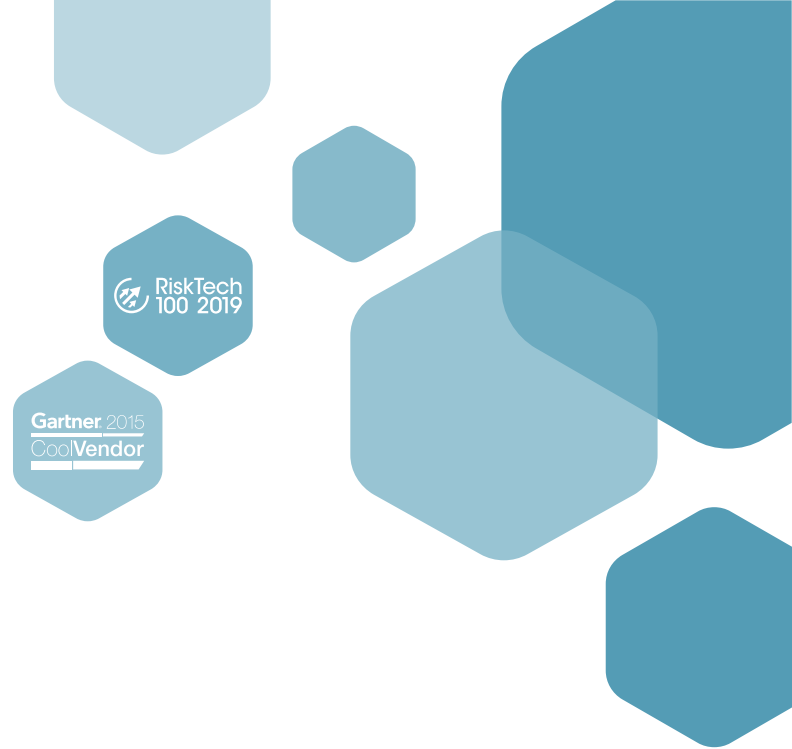
# Index Pattern

- Way to identify underlying indexes to perform searches on
- Work on a set of indexes sharing same type of data
  - Index pattern instead of individual index
  - Sets should share similar data type
- On NG|Screener, 5 default events index patterns are part of the convention
  - `ngt-*` matching all "Transaction" data types
  - `ngc-*` matching all "Channel" data types
  - `ngi-*` matching all "IT Layers" data types
  - `ngv-*` matching all "Violations" data types
  - `ng*` matching everything
- Index name format is `ng[tciv]-tenantname_host-service-date`
  - Specific indexes will be created for each tenant defined for data segregation
- Will be specified when creating saved search

# Index Pattern



# Saved Search







## Saved Search

- Saved searches have 2 main purposes
  - Basis for data visualization
  - Used as a table to show events
    - Fields Mapping to change header column name
- Most commonly one saved search will be used across one dashboard
  - Consistently show the data through the whole dashboard

# Saved Search - View

The screenshot displays the NGIScreener interface. On the left, a sidebar contains a list of filters: Channels - (ngc-\*), Generic - (ng\*), Layers - (ngi-\*), Transactions - (ngt-\*), and Violations - (ngv-\*). A blue callout box points to the 'Generic - (ng\*)' filter, with the text 'Access Saved search part'. The main area shows a 'Discover' view with a timeline from June 06 to June 03, a search bar, and a table of results. The table has a header '@timestamp' and a list of timestamps. The total hits are 318,075. The bottom of the table shows 'Total entries: 500' and a pagination bar with numbers 1 through 5.

NGIScreener Discover

Channels - (ngc-\*)

Generic - (ng\*)

Layers - (ngi-\*)

Transactions - (ngt-\*)

Violations - (ngv-\*)

200,000  
200,000

Jun 06 Jun 09 Jun 12 Jun 15 Jun 18 Jun 21 Jun 24 Jun 27 Jun 30 Jun 03

⏪ Last 1M ⏩

DROP DATA HERE OR CLICK ON BUTTON TO ADD FILTERS

Search

TOTAL HITS: 318,075

@timestamp

> 2019-06-30T00:00:06+02:00

> 2019-06-30T00:00:10+02:00

> 2019-06-30T00:00:22+02:00

> 2019-06-30T00:01:23+02:00

> 2019-06-30T00:02:00+02:00

> 2019-06-30T00:02:37+02:00

> 2019-06-30T00:02:57+02:00

> 2019-06-30T00:03:22+02:00

> 2019-06-30T00:03:45+02:00

> 2019-06-30T00:04:17+02:00

> 2019-06-30T00:05:21+02:00

> 2019-06-30T00:08:27+02:00

> 2019-06-30T00:09:11+02:00

Total entries: 500

« 1 2 3 4 5 »

Access Saved search part



## Saved Search - View

The screenshot shows the NGIScreener interface. On the left is a sidebar with a list of defined saved searches:

- Channels - (ngc-\*)
- Generic - (ng\*)
- Layers - (ngi-\*)
- Transactions - (ngt-\*)
- Violations - (ngv-\*)

At the bottom of the sidebar is a button with a plus sign (+) to add a new saved search.

The main area displays the 'Discover' view, showing a list of hits with a timestamp column. The first few entries are:

- > 2019-06-30T00:00:06+02:00
- > 2019-06-30T00:00:06+02:00
- > 2019-06-30T00:00:22+02:00
- > 2019-06-30T00:01:33+02:00

The interface also includes a top navigation bar with 'Discover', a search bar, and a bottom status bar showing 'Total entries: 500'.

## Saved Search – Create new

- Create Saved search with
  - Name for the saved search
  - Index pattern
- Convention specifies these index patterns
  - **ngt**-\* Financial Transactions
  - **ngc**-\* Channels
  - **ngi**-\* IT Layers
  - **ngv**-\* Violations
  - **ng**\* Generic
- Shows indices match specified index pattern
- Once created filter can be added (as when using dashboard view)

Saved search ×

**Name** (required)

**Index pattern** (required)

**MATCHED INDICES**

ngt-default_finnova-swisscomfinnovacorebankingtransaction-201906
ngt-default_finnova-swisscomfinnovacorebankingtransaction-201907
ngt-default_finnova_open-swisscomfinnovacorebankingtransaction-201906
ngt-default_finnova_open-swisscomfinnovacorebankingtransaction-201907

Total entries: 4 « 1 »

**Save**

# Saved Search – Create new

Filtering same as in dashboard view (cf. NG | Screener UI Usage)

The screenshot displays the NG|Screener interface. On the left, a sidebar contains navigation icons and labels: Channels - (ngc-\*), Generic - (ng\*), Layers - (ngi-\*), Transactions - (ngt-\*), and Violations - (ngv-\*). The top bar shows a timeline from June 06 to July 03, with a 'Last 1M' filter and a search bar. The main area displays a table of results for the 'Discover' search. The table has a header row with '@timestamp' and a list of available columns: account\_category, account\_id, account\_name, counterparty\_account\_id, counterparty\_bank\_country, counterparty\_bank\_id, and counterparty\_customer\_id. The table shows 149,364 total hits and 500 total entries. A callout box points to the 'Discover' search name, and another points to the 'AVAILABLE COLUMNS' list.

Channels - (ngc-\*)

Generic - (ng\*)

Layers - (ngi-\*)

Transactions - (ngt-\*)

Violations - (ngv-\*)

Discover

100,000

100,000

Jun 06 Jun 09 Jun 12 Jun 15 Jun 18 Jun 21 Jun 24 Jun 27 Jun 30 Jul 03

Drop data here or click on the button to add filters

Search

LAST 1M

TOTAL HITS: 149,364

@timestamp

2019-06-30T00:00:52+02:00

2019-06-30T00:00:59+02:00

2019-06-30T00:01:33+02:00

2019-06-30T00:02:04+02:00

2019-06-30T00:02:44+02:00

2019-06-30T00:03:33+02:00

2019-06-30T00:04:03+02:00

2019-06-30T00:04:43+02:00

2019-06-30T00:04:55+02:00

2019-06-30T00:05:04+02:00

2019-06-30T00:06:04+02:00

2019-06-30T00:08:03+02:00

2019-06-30T00:08:24+02:00

Total entries: 500

AVAILABLE COLUMNS

account\_category

account\_id

account\_name

counterparty\_account\_id

counterparty\_bank\_country

counterparty\_bank\_id

counterparty\_customer\_id

SELECTED COLUMNS

@timestamp

1 2 3 4 5

Add columns in the table.  
Important if shown as a  
data table

## Saved search – Create new

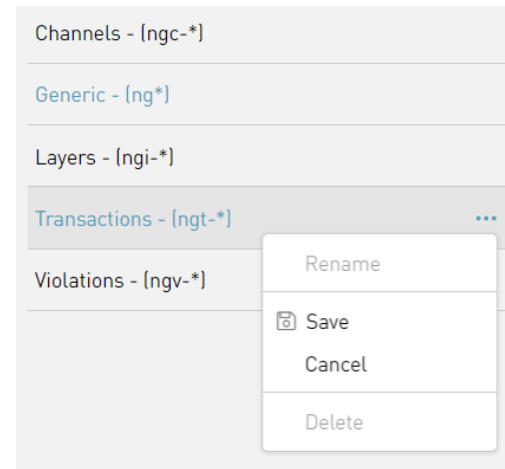
Field Mappings will only be shown in the widget in a dashboard

TOTAL HITS: 149,364								
@timestamp	account_category	account_name	customer_name	transaction_converted...	transaction_currency	transaction_direction		
> 2019-06-30T00:00:52+02:00	NG-SCREENER Private	P 9296.75.49	099242	1536	CHF	out		
> 2019-06-30T00:00:59+02:00	NG-SCREENER c/c Companies	6022.53.56	8187882	352.85	EUR	out		
> 2019-06-30T00:01:33+02:00	Vostro account	6489.40.96	6928922	905263.44	USD	out		
> 2019-06-30T00:02:04+02:00	NG-SCREENER Private	K 4277.90.13	2705319	45.5	CHF	out		
> 2019-06-30T00:02:44+02:00	NG-SCREENER Business Partner	3160.66.11	0529038	62	CHF	out		
> 2019-06-30T00:03:33+02:00	Current account	4679.25.19	0694447	4796.2	CHF	out		
> 2019-06-30T00:04:03+02:00	Vostro account	6489.40.96	6928922	22393.99	USD	out		
> 2019-06-30T00:04:43+02:00	Vostro account	6489.40.96	6928922	65766.59	USD	out		
Total entries: 500							« 1 2 3 4 5 »	



## Saved Search – Create new

- When finished saved search can be saved (cf. printscreen)
- Saved search is ready to be used:
  - As basis for visualizations in dashboards
  - Directly as data table



# Dashboard and Visualizations







# Dashboard and Visualization

## Dashboard

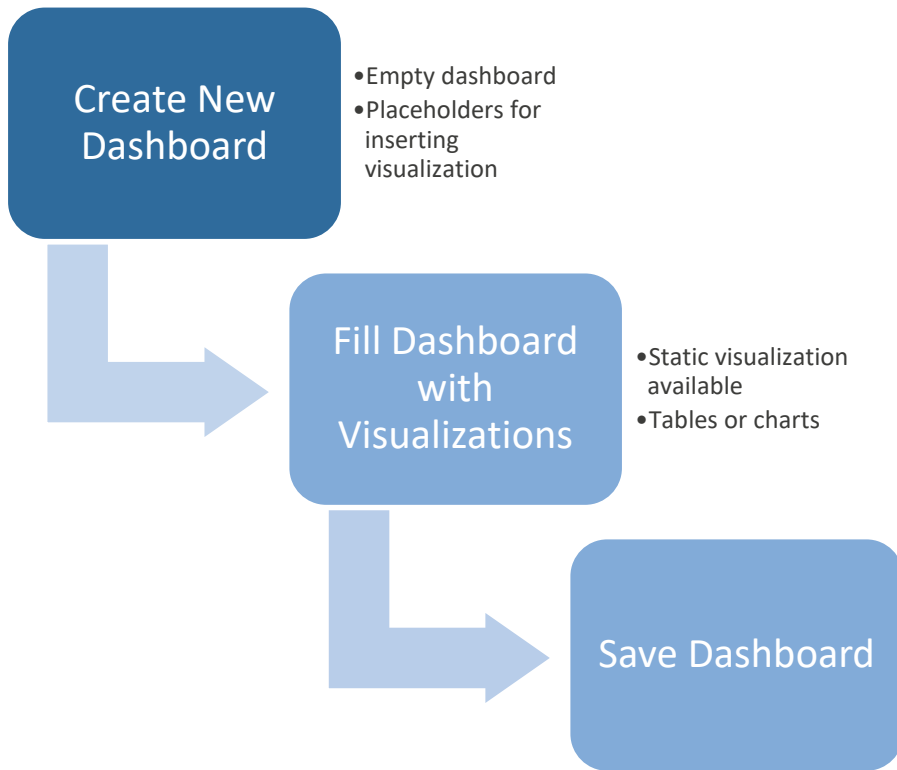
- Collection of visualization put together
- Will be used for
  - Forensic Views
  - Violation Dashboard
  - Control output dashboards

## Visualization

- Biggest part when creating Dashboards
- Different type of visualization available
  - Vertical bar chart
  - Pie chart
  - Heatmap
  - ...

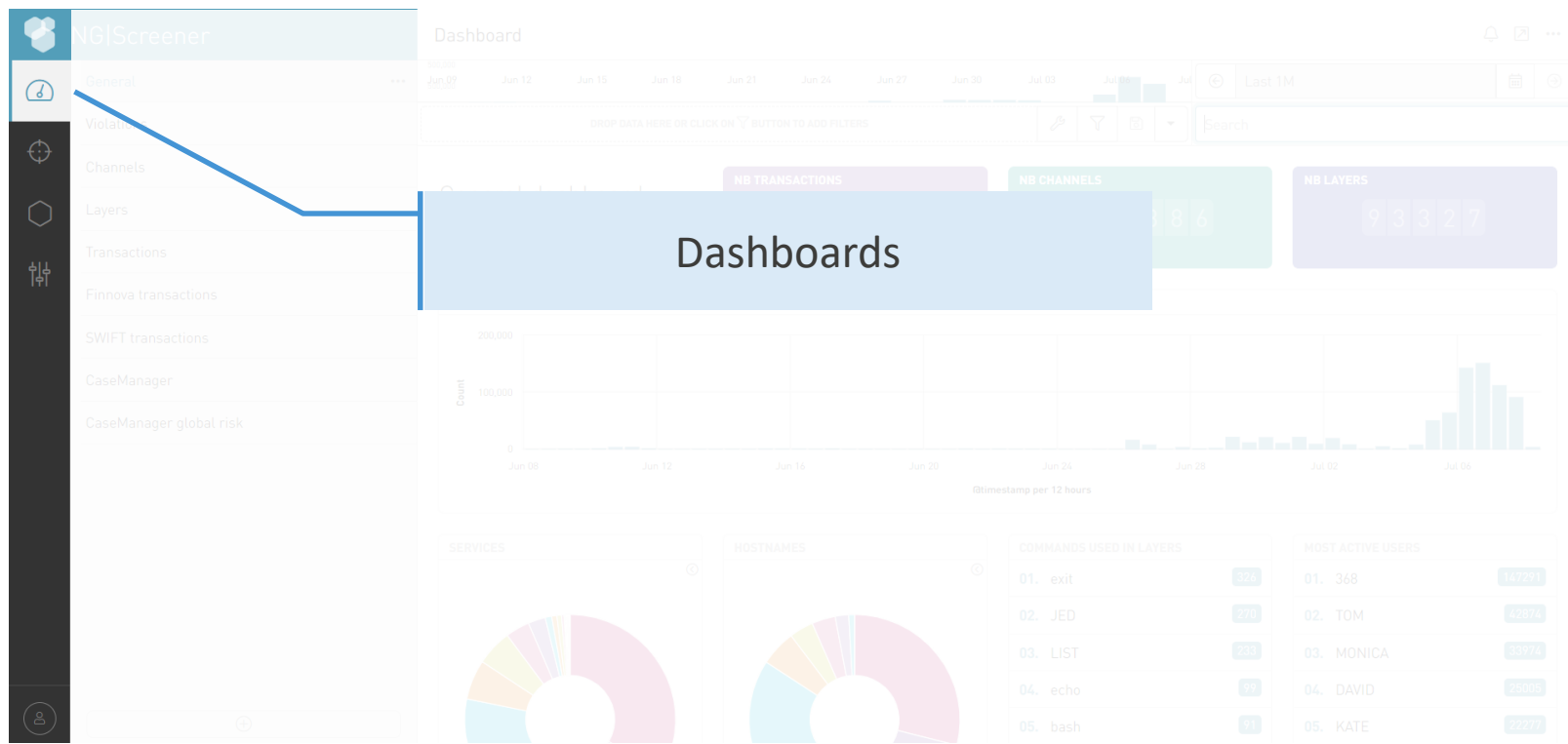


## Dashboard and visualizations





# Create a new Dashboard





# Create a new Dashboard

NG|Screener

Dashboard

General

Violations

Channels

Layers

Transactions

Finnova transactions

SWIFT transactions

CaseManager

CaseManager global risk

General dashboard

(dashboard\_ng)

NB TRANSACTIONS

179,294

NB CHANNELS

531,386

NB LAYERS

933,27

GENERAL VIEW TIMELINE

SERVICES

HOSTNAMES

COMMANDS USED IN LAYERS

MOST ACTIVE USERS

01. exit 35%

02. TOM 49%

03. MONICA 39%

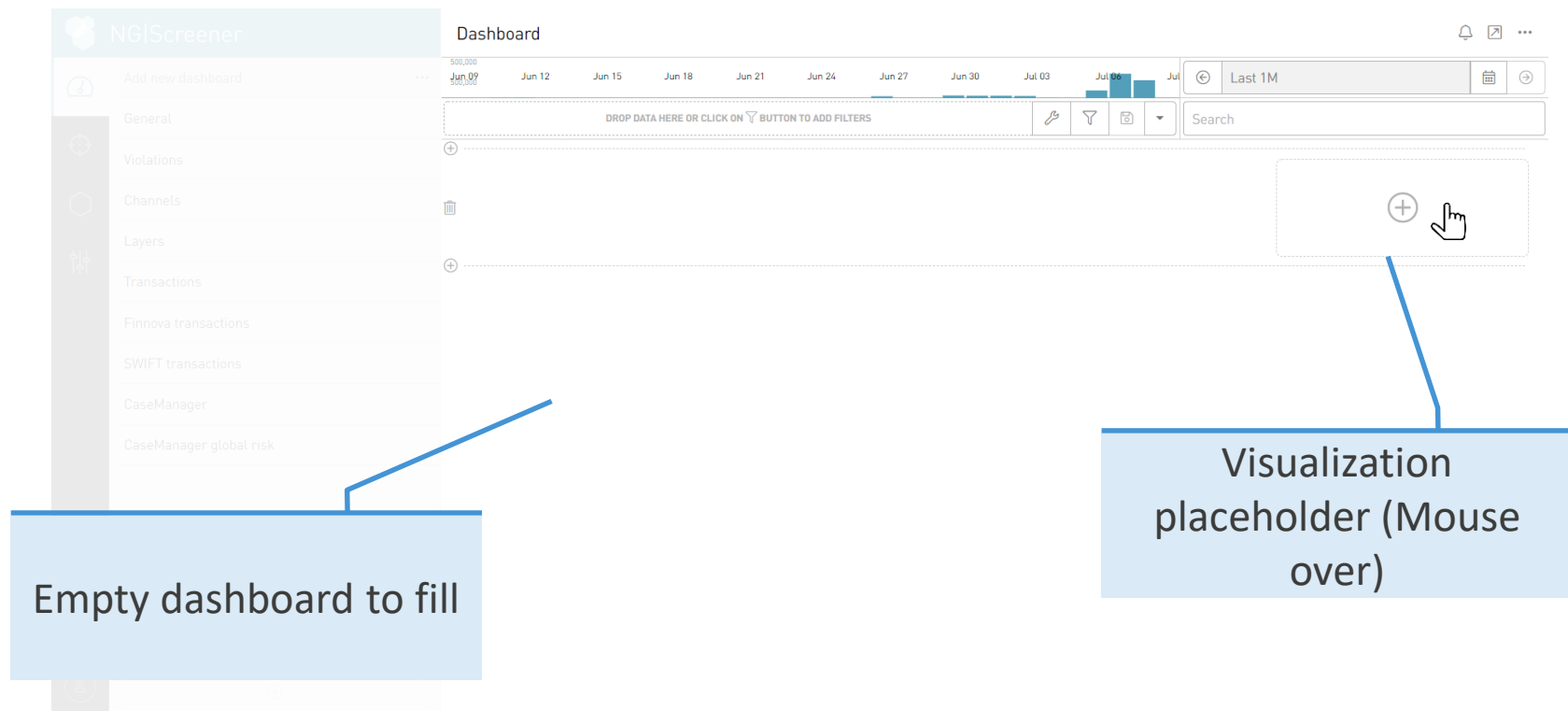
04. DAVID 20%

05. bash 1%

05. KATE 22%

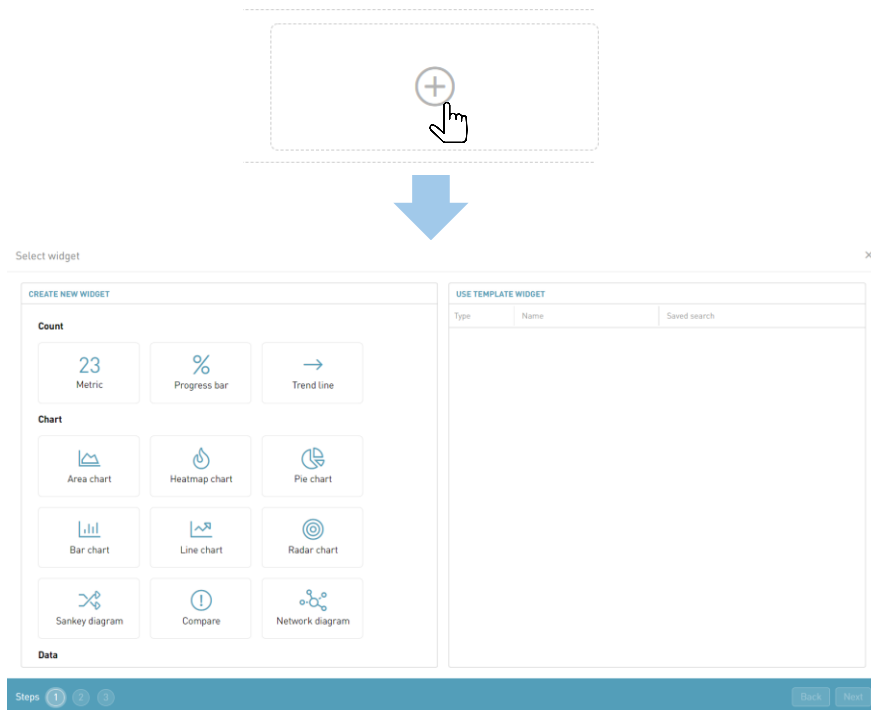
Create new dashboard

## Create a new Dashboard



# Create Visualizations

- Click on placeholder to add a visualization
- Wizard will appear to define the content of the visualization
  - Type
  - Saved Search
  - Configuration
- Configuration depend on type of visualization
- Size of visualization could be changed afterwards





# Example of a pie chart

Select widget

×

## CREATE NEW WIDGET

### Count

23  
Metric

%  
Progress bar

→  
Trend line

### Chart

Area chart

Heatmap chart

Pie chart

Bar chart

Line chart

Radar chart

Sankey diagram

Compare

Network diagram

### Data

## USE TEMPLATE WIDGET

Type

Name

Saved search

Select "Pie chart" as  
visualization

Steps

1

2

3

Back

Next



## Example of a pie chart

Select saved search



SAVED SEARCH	
Name	Index pattern
Generic	ng*
Channels	ngc-*
Transactions	ngt-*
Layers	ngi-*
Violations	ngv-*

Total entries: 5

Select Transaction Saved search (previously created) on ngt-\* index pattern

Steps

1

2

3

Back

Next












## Example of a pie chart

Configure widget



**METRICS**   

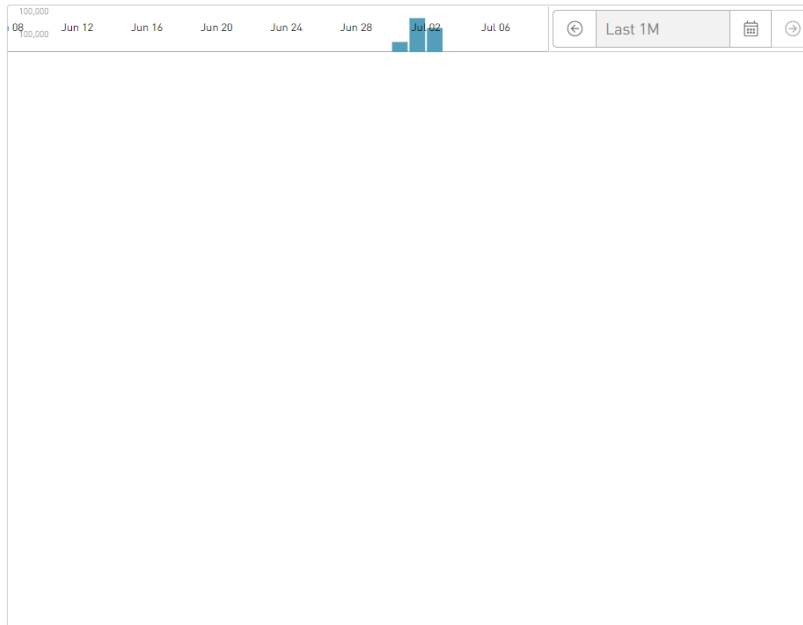


**BUCKETS**   

**PROPERTIES**

**Widget title** (required)

☒ Donut



Steps

1

2

3

Back

Save



## Example of a pie chart

- Metrics define what will be used for sizing the chart elements
  - For a pie the size of the slices
- Options
  - Count
  - Unique Count
  - Sum
  - ...
- More option depending on what has been selected

Create aggregation ×

**Type** (required)

Slice size ▼

**Aggregation** (required)

Count ▼

**Custom label**

Save




Cancel






## Example of a pie chart

Configure widget



**METRICS**   

**BUCKETS**   

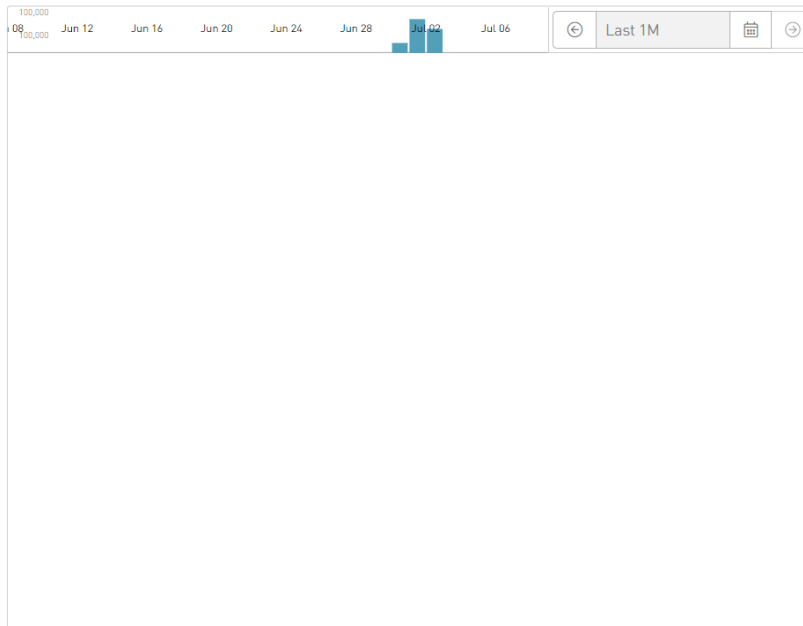


**PROPERTIES**

**Widget title** (required)

Widget title

☒ Donut



Steps

1

2

3

Back

Save



## Example of a pie chart

- Buckets defines how to split the chart
  - For a pie it means what will be used to split it
- In this example, the different terms in the field `transaction_currency` will be used to specify slices (most common case)
  - CHF
  - USD
  - EUR
  - ...

Create aggregation



Type (required)

Split slices

Aggregation (required)

Terms

Field (required)

transaction\_currency

Order by (required)

Metric: count

Order (required)

Descending

Size (required)

10



Custom label

Save

Cancel



# Example of a pie chart

Configure widget



**METRICS** + ✎ 🗑

```
{ "id": "m1", "type": "count", "schema": "metric", "params": {} }
```

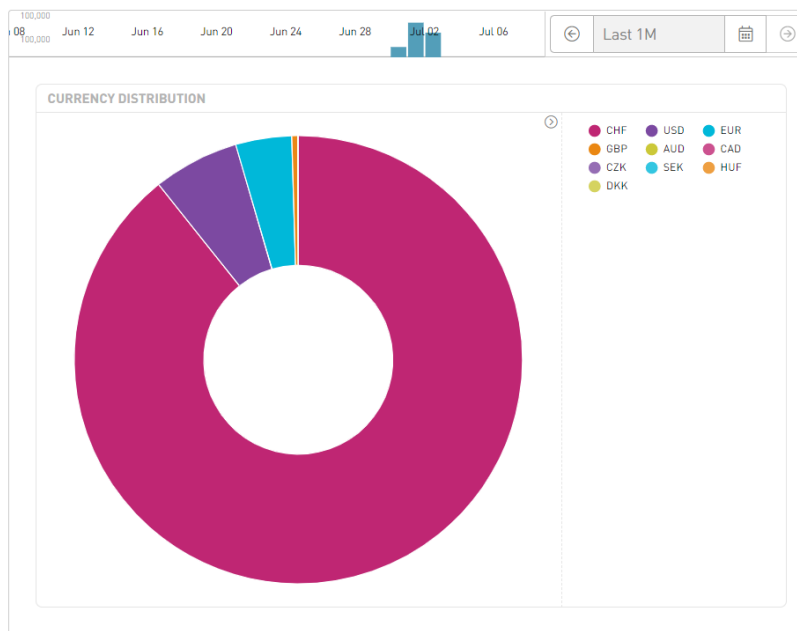
**BUCKETS** + ✎ 🗑

```
{ "id": "b1", "type": "terms", "schema": "split", "params": { "field": "transac..." }
```

**PROPERTIES**

**Widget title** (required)

☒ Donut



Steps

1

2

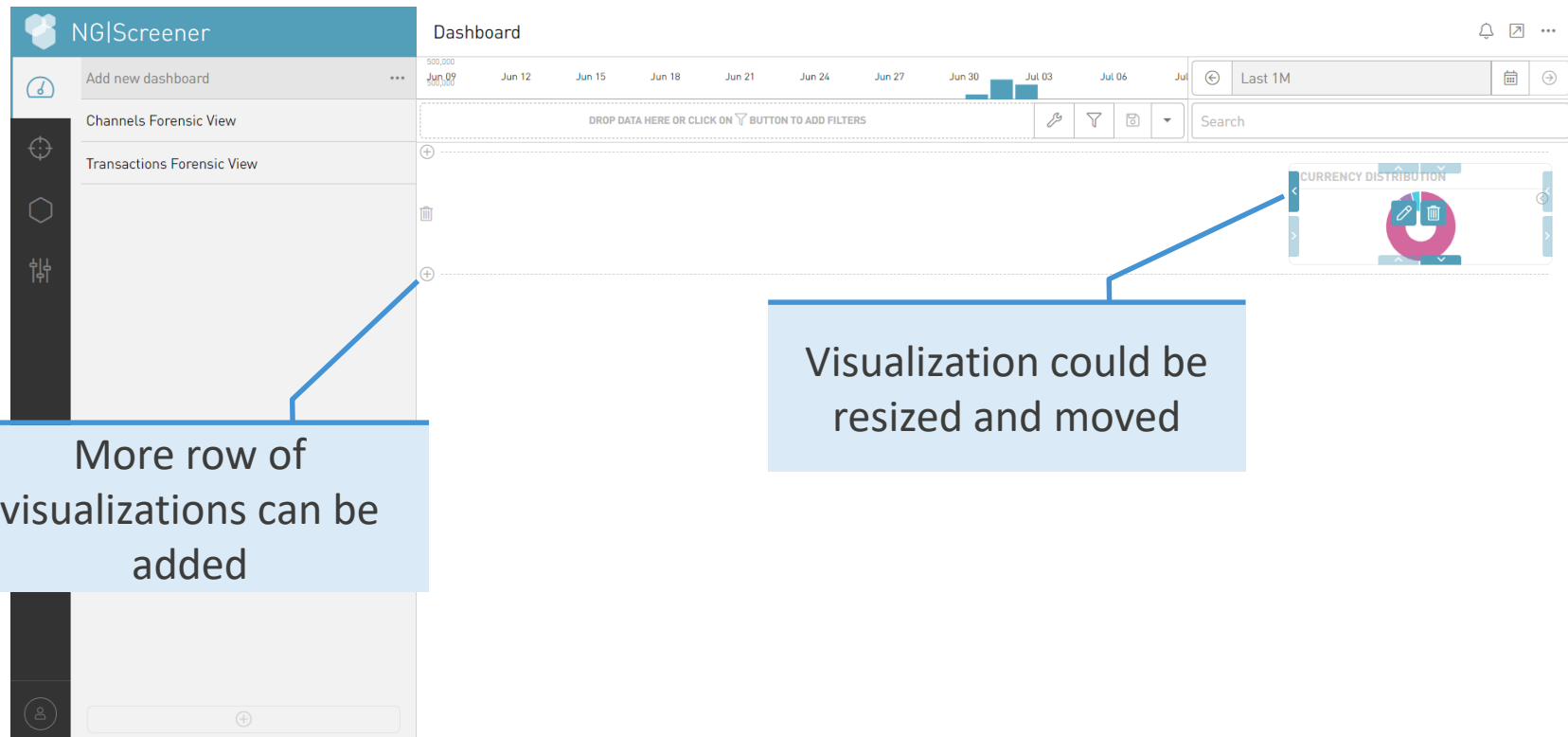
3

Back

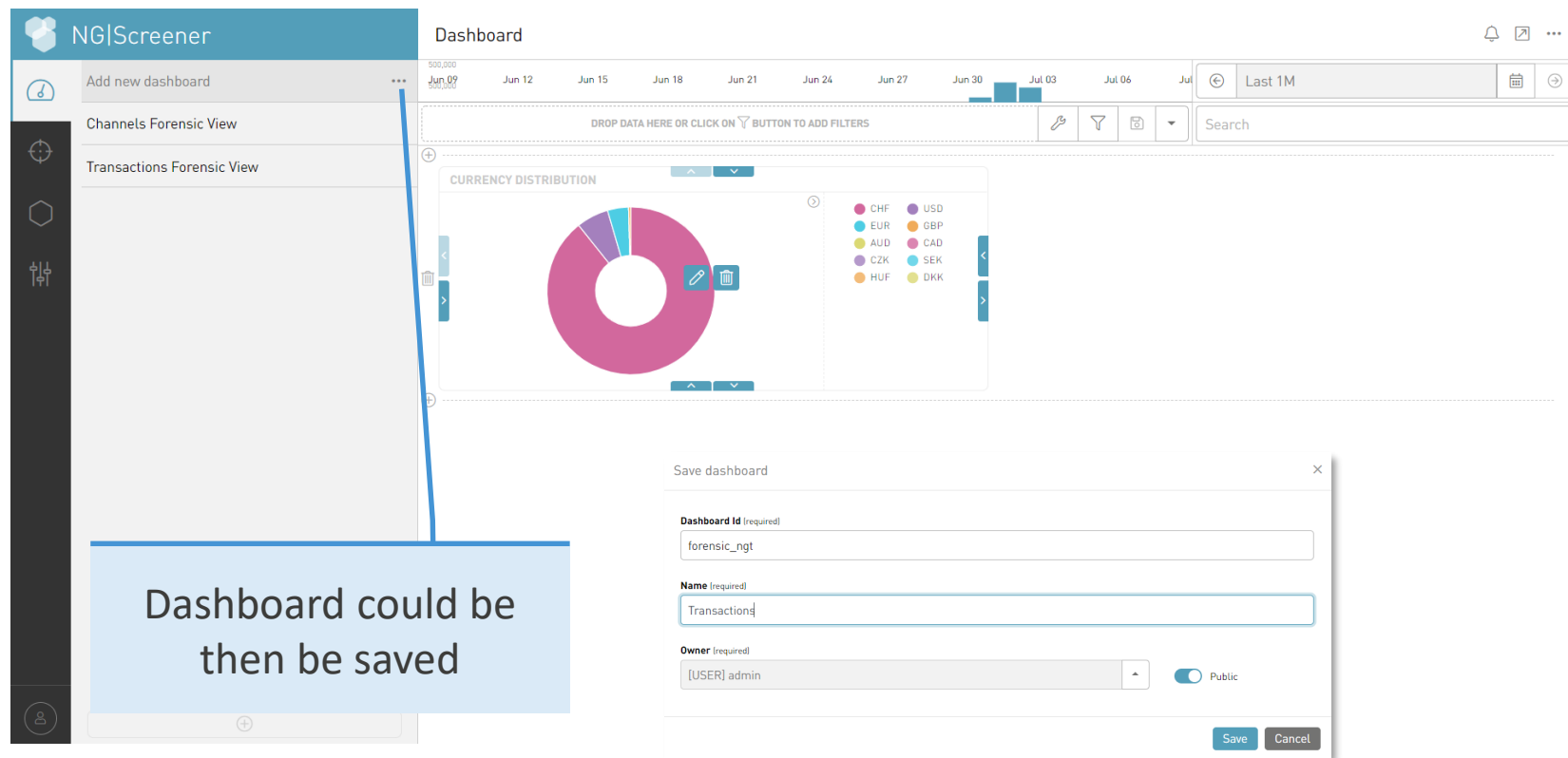
Save



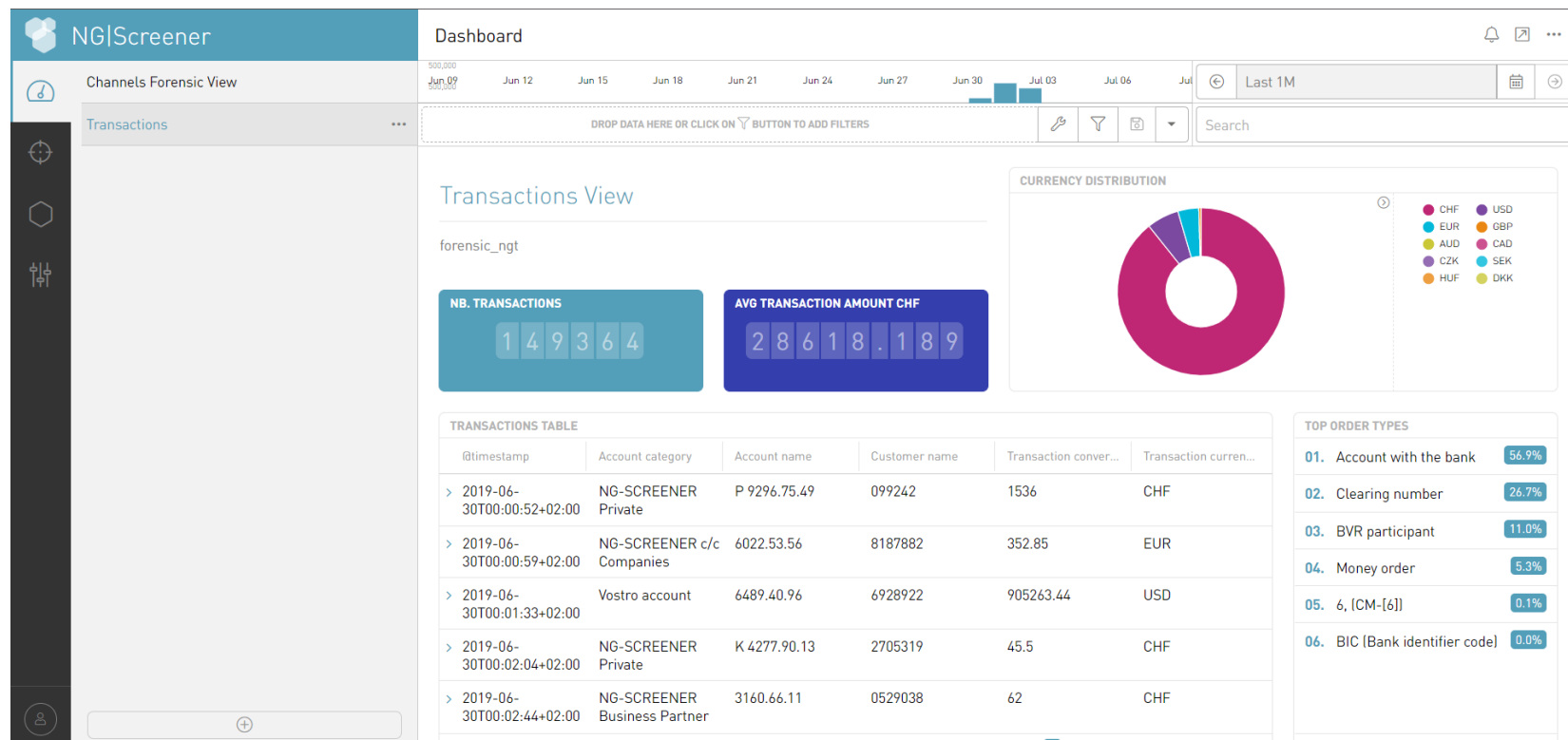
## Example of a pie chart



## Example of a pie chart



# Example of a pie chart





# Dashboard administration commands





## Dashboard administration command

- Using ngadmin command line tool
  - List dashboards
    - `ngadmin dashboard_listDashboards`
  - Export Dashboards
    - `ngadmin dashboard_exportDashboards`
  - Import Dashboards
    - `ngadmin dashboard_importDashboards`



## Dashboard administration command

```
[root@NG-SCREENER dashboards]# ngadmin dashboard_listDashboards
```

DASHBOARD_ID	TYPE	NAME
-----	-----	-----
forensic_ngc	FORENSIC	Channels Forensic View
forensic_ngt	FORENSIC	Transactions

(2 dashboards found)



## Dashboard administration command

- Export dashboards
  - `ngadmin dashboard_exportDashboards -d out_dir [-t type] [filter criteria]`
- Parameters
  - `-d`: Directory where to write output (Mandatory, should be writeable by ng-screener user)
  - `-t` : Type of dashboards to be exported (forensic, control, all (DEFAULT))
  - Filter criteria: Filter which dashboards to be exported (ex. forensic\_\*)



## Dashboard administration command

- Import dashboards
  - `ngadmin dashboard_importDashboards -d in_dir [-f input XML file]`
  - Parameters
    - `-d`: Directory where to read dashboards (Mandatory, should be readable by ng-screener user)
    - `-f` : Dashboard XML file to be imported (if not specified, all files in directory)



# Thank you!

## NetGuardians



+41 24 425 97 60



[info@netguardians.ch](mailto:info@netguardians.ch)



[www.netguardians.ch](http://www.netguardians.ch)



[Linkedin.com/company/netguardians](https://www.linkedin.com/company/netguardians)



[Facebook.com/NetGuardians](https://www.facebook.com/NetGuardians)



[@netguardians](https://twitter.com/netguardians)



<https://www.youtube.com/netguardians>

## Ljupce Nikolov



+41 24 425 97 60



[nikolov@netguardians.ch](mailto:nikolov@netguardians.ch)



# Contact us

## NetGuardians Headquarters

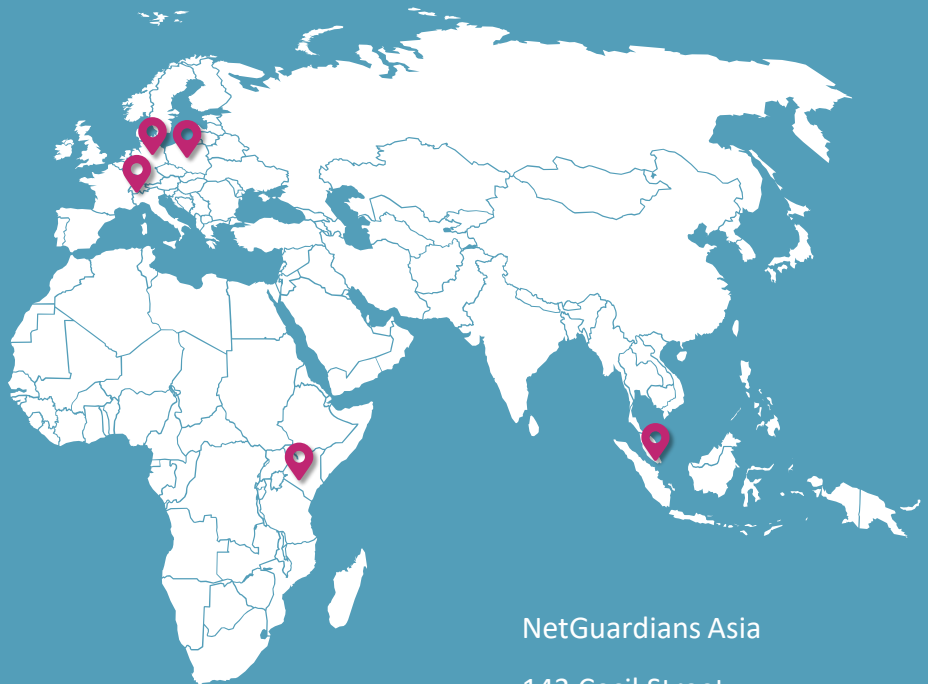
Y-Parc, Av. des Sciences 13  
1400 Yverdon-les-Bains  
Switzerland

T +41 24 425 97 60

## NetGuardians Africa

Vienna Court  
State House Rd  
Nairobi, Kenya

+254 205 138539



## NetGuardians Germany

Rhein-Main Gebiet  
Germany

T +49 172 3799003

## NetGuardians Eastern Europe

Koszykowa 61, 00-667  
Warsaw, Poland

## NetGuardians Asia

143 Cecil Street  
#09-01 GB Building  
069542 Singapore

T +65 6224 0987