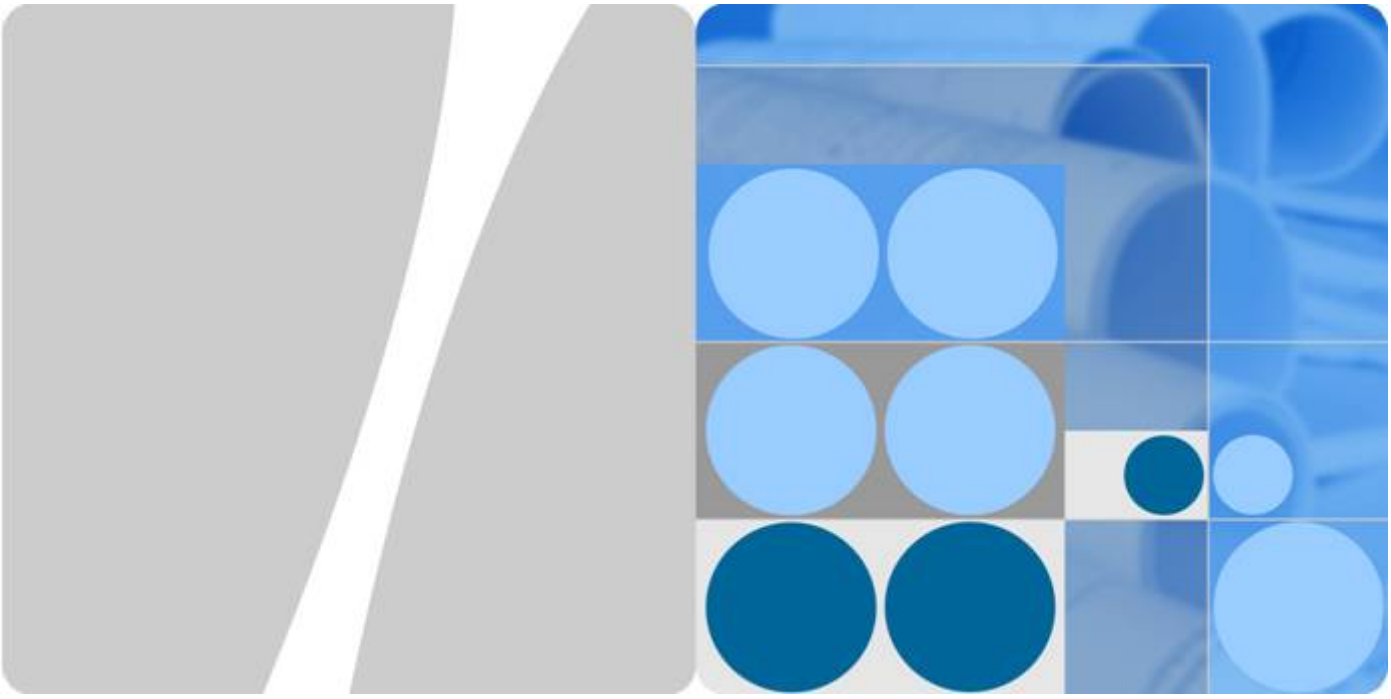


Data Lake Visualization

Best Practices

Issue 01

Date 2019-04-26

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Copyright © Huawei Technologies Co., Ltd. 2019. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

Contents

1 Viewing Enterprise Security Situations on DLV.....1

 Copyright © Huawei Technologies Co., Ltd.

1 Viewing Enterprise Security Situations on DLV

This document describes how to create a screen for monitoring enterprise security situations. The created screen will provide visualized decision-making basis for processing enterprise security events.

DLV has the following characteristics:

- Real-time security awareness: real-time security detection, effectively preventing security incidents
- Access source tracking: 2D and 3D map components, intuitively tracking security threat sources
- High-risk attack source capturing: table components available to list risk levels and help quickly capture high-risk attack sources

Solution Design

When designing a solution, determine the content to be displayed and select components based on the content. The content to be displayed is classified into the following types: access information and attack information.

The following table lists the access information and the required component types:

Access Information	Component Type
Access region ranking	Region ranking
Website access region	China map
Access trend	Line chart
Real-time attack information	Rotation table

The following table lists the attack information and the required component types:

 Copyright © Huawei Technologies Co., Ltd.

Attack Information	Component Type
Attack region ranking	Region ranking
Attack type ranking	Rotation table
Attack trend	Line chart
Attack source	Globe

Preparations

- Relational Database Service (RDS) has been enabled and instance **rds-secure0** for which **DB Engine** is set to **MySQL** has been created.
- Cloud Data Migration (CDM) has been enabled and cluster **cdm-secure** has been created.

  NOTE

  When you create cluster **cdm-secure** on the **Buy CDM** page, ensure that information about the VPC, subnet, and intranet security group information must be the same as that configured on the page for buying instance **rds-secure0**.

Preparing Data

Download data from **https://dlv-public-image.obs.cn-north-1.myhuaweicloud.com/demo1.zip** to the local host.

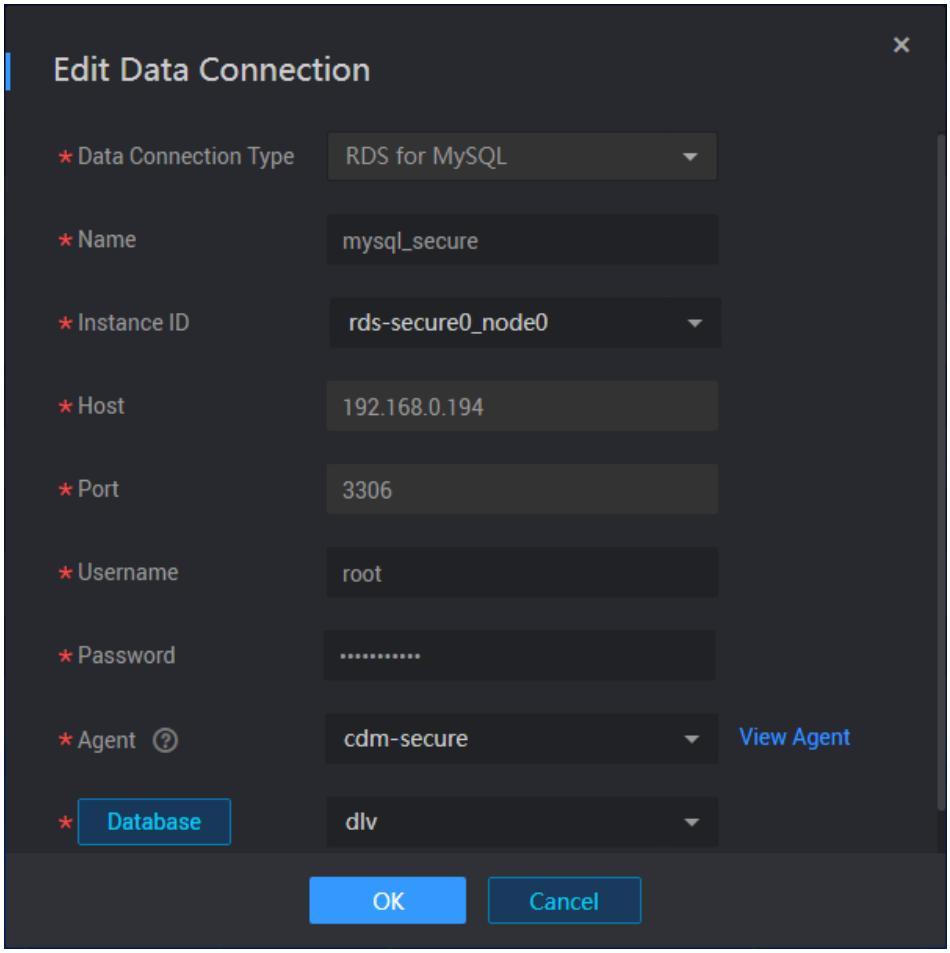
Select **rds-secure0** and enter the username and password to log in to RDS for MySQL. In the root directory of **rds-secure0**, create database **dlv**, and choose **Import·Export** > **Export**.

Creating an RDS for MySQL Data Connection

1. Log in to the DLV console.
2. Choose **Data** > **New Data Connection**.
3. In the **Data Connection Type** drop-down list, select **RDS for MySQL**.
4. Set the name, port, username, password, and agent of RDS for MySQL. Click **Database**, select **dlv**, and click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-1 Creating an RDS for MySQL data connection



Creating a Screen

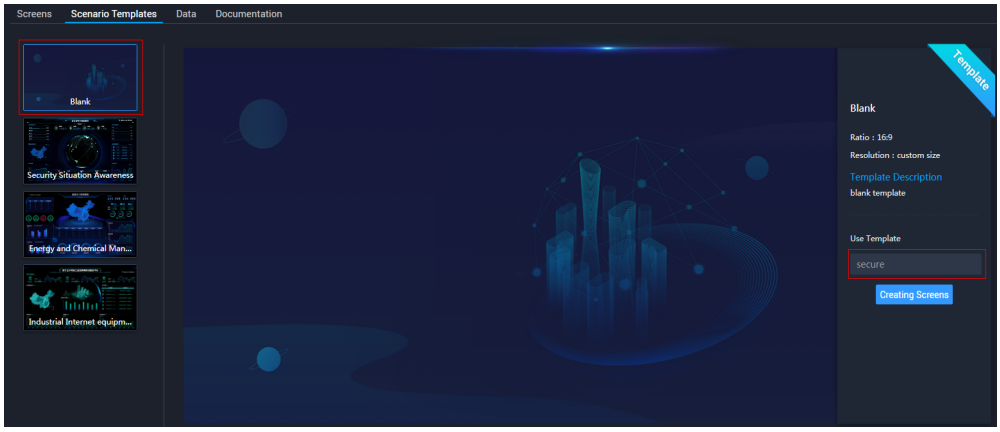
Step 1 Log in to the DLV console.

Step 2 **Screens** > **New Screen**.

Step 3 Select a blank template and create a screen.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-2 Creating a screen

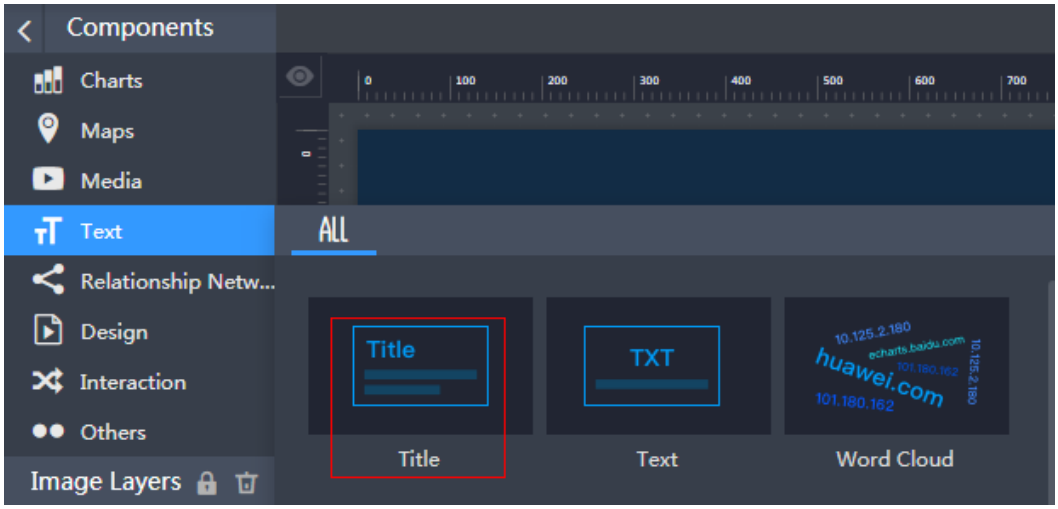


----End

Adding a Title Component

Step 1 In the **Text** component library, select a **Title** component.

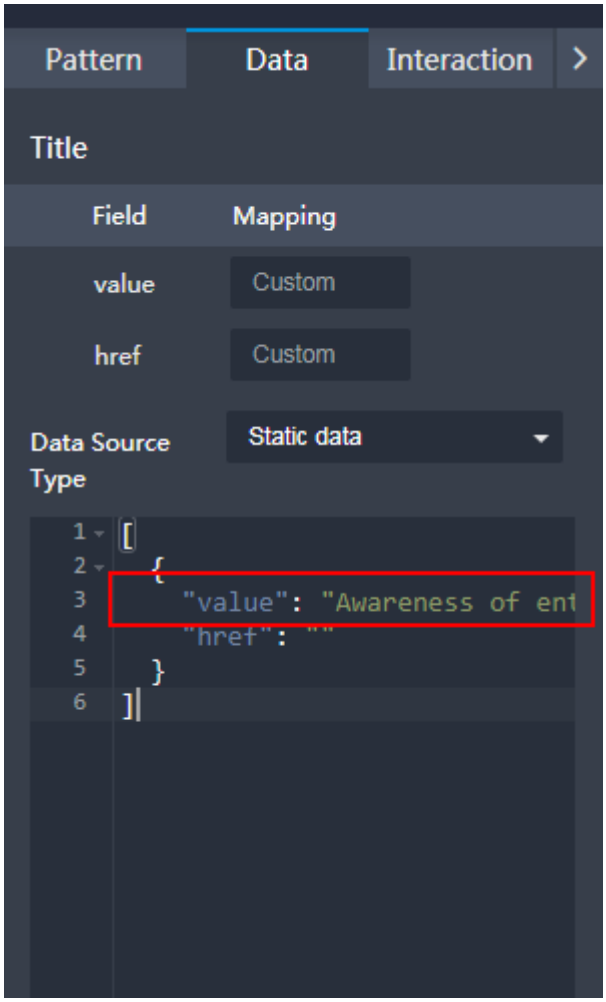
Figure 1-3 Adding a title component



Step 2 On the **Data** panel, set **value** to **Awareness of enterprise security situations**.

 Copyright © Huawei Technologies Co., Ltd.

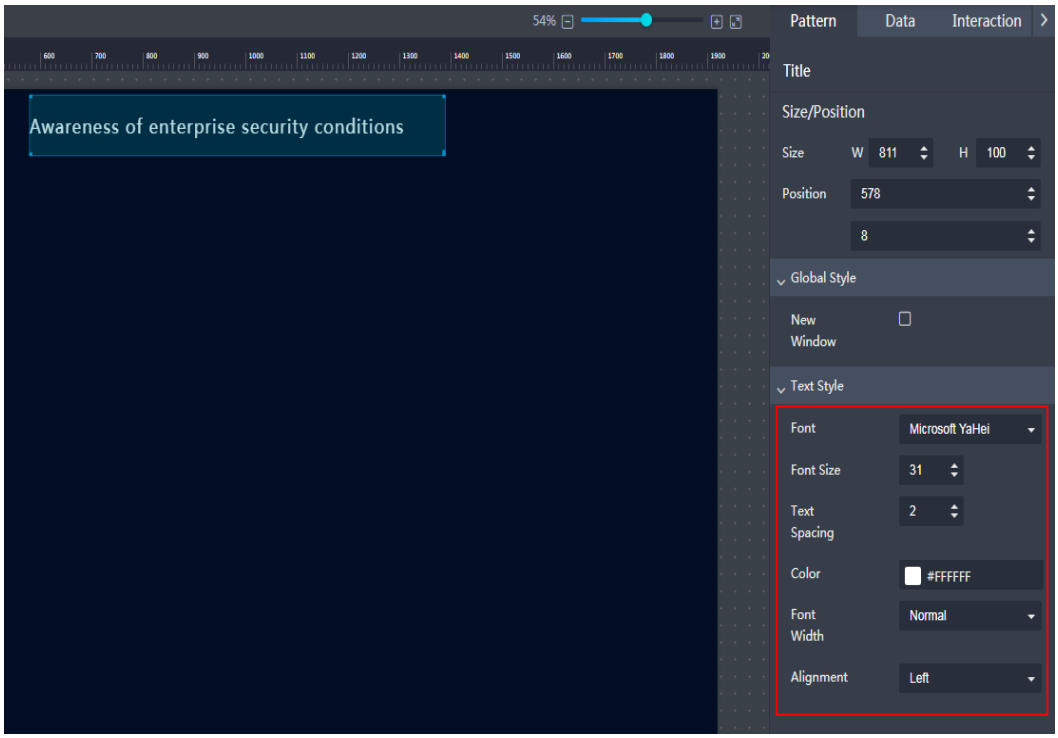
Figure 1-4 Data display



Step 3 Click the **Pattern** panel and configure the text style of the title.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-5 Configuring the title pattern

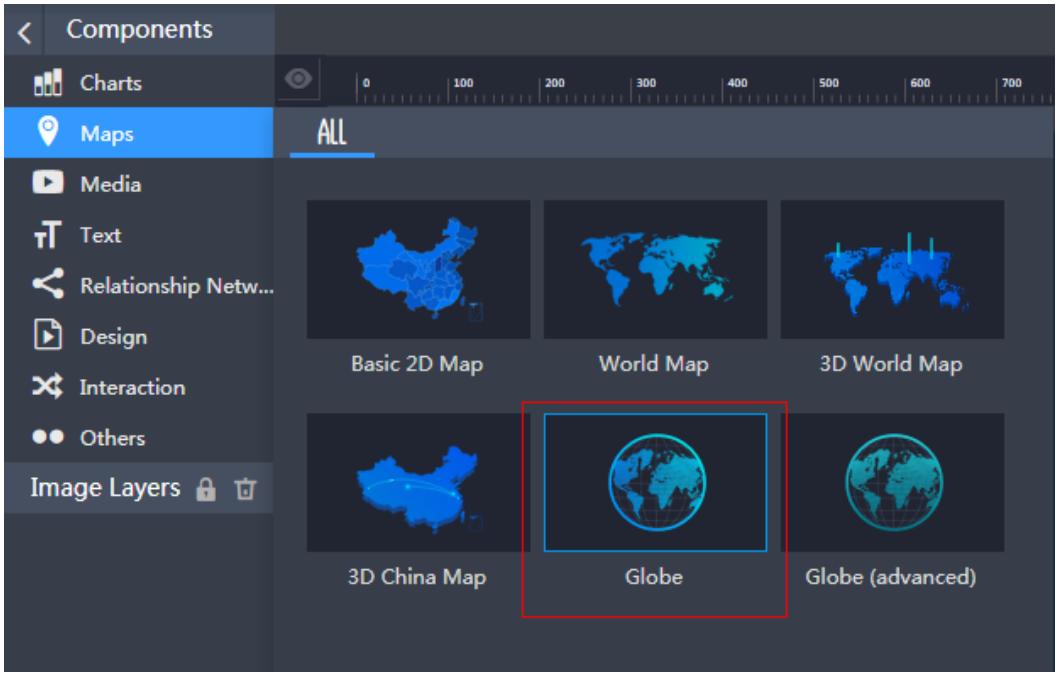


----End

Adding a Globe Component

Step 1 In the **Globe** component library, select a **Globe** component.

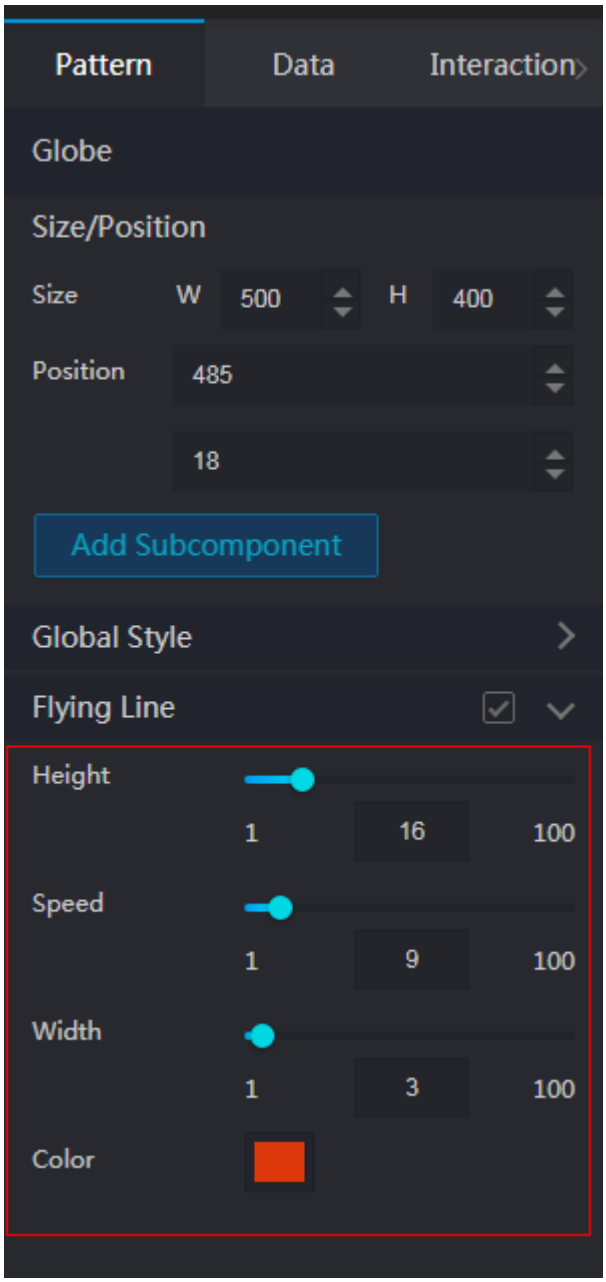
Figure 1-6 Adding a globe component



 Copyright © Huawei Technologies Co., Ltd.

Step 2 In the **Pattern** panel, configure the color style of the flying lines.

Figure 1-7 Configuring flying lines



Step 3 On the **Data** panel, set **from** to **attack_source** and **to** to **attack_dest**. Select **Database** from the **Data Source Type** drop-down list and select an existing data connection from the **Data Connection** drop-down list. Query the attack data using SQL statements, and click **View Response Result**. Different SQL statements lead to different data response results. You can enter different SQL statements based on specific attack types.

- SQL statement for querying XSS attacks: SELECT CONCAT(t.src_lng , ',', t.src_lat) as attack_source, CONCAT(t.target_lng, ',', t.target_lat) as attack_dest, COUNT(1) AS attack_num FROM dlv.ods_attack_log t where t.attack_type="XSS" GROUP BY t.src_lng , t.src_lat , t.target_lng , t.target_lat

 Copyright © Huawei Technologies Co., Ltd.

- SQL statement for querying CSRF attacks: SELECT CONCAT(t.src_lng , ',', t.src_lat) as attack_source, CONCAT(t.target_lng, ',', t.target_lat) as attack_dest, COUNT(1) AS attack_num FROM dlv.ods_attack_log t where t.attack_type="CSRF" GROUP BY t.src_lng , t.src_lat , t.target_lng , t.target_lat
- SQL statement for querying sensitive_file attacks: SELECT CONCAT(t.src_lng , ',', t.src_lat) as attack_source, CONCAT(t.target_lng, ',', t.target_lat) as attack_dest, COUNT(1) AS attack_num FROM dlv.ods_attack_log t where t.attack_type="sensitive_file" GROUP BY t.src_lng , t.src_lat , t.target_lng , t.target_lat

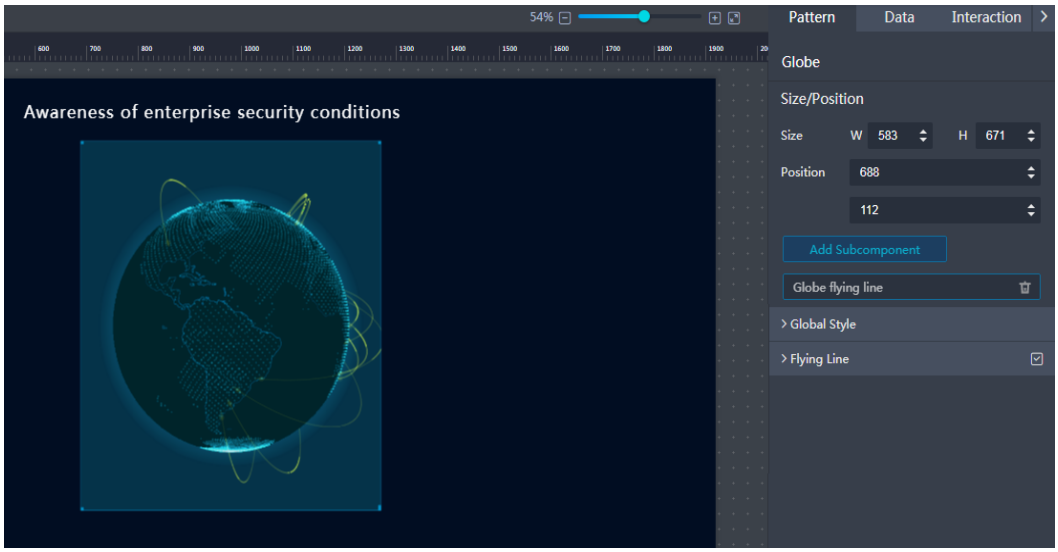
Figure 1-8 XSS data response results



Step 4 On the **Pattern** panel, click **Add Subcomponent** and select **Globe flying line** from the drop-down list.

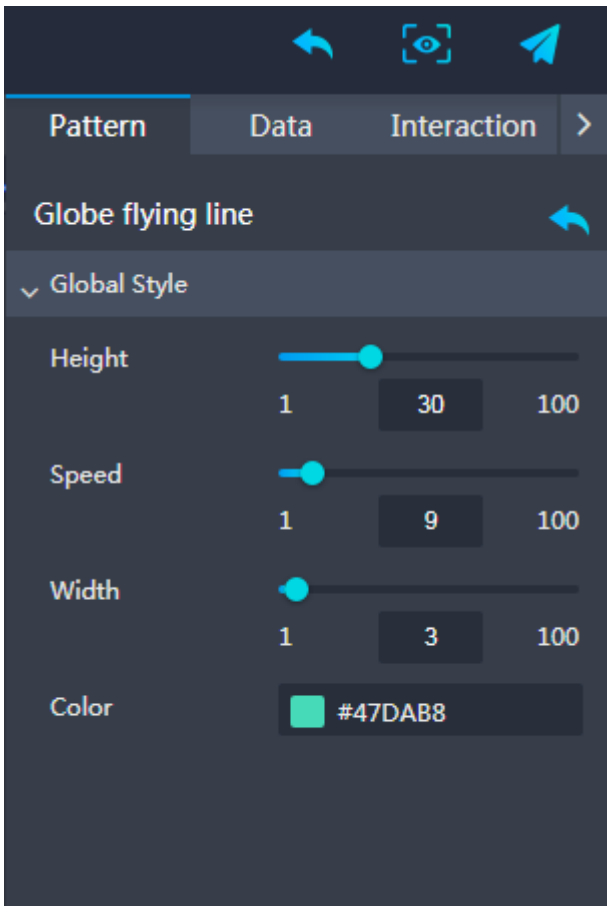
 Copyright © Huawei Technologies Co., Ltd.

Figure 1-9 Adding a flying line



Step 5 Click **Flying line**. The **Flying line** panel is displayed. In the **Pattern** panel, configure the color style of the flying lines.

Figure 1-10 Configuring flying lines



Step 6 Repeat Step 3 to configure the flying line data on the **Data** panel, enter the SQL statement for querying CSRF attacks, and click **View Response Result**.

 Copyright © Huawei Technologies Co., Ltd.

Step 7 Repeat **Step 4**, **Step 5**, and **Step 6** to configure the pattern and data of another flying line, enter the SQL statement for querying sensitive_file attacks, and click **View Response Result**.

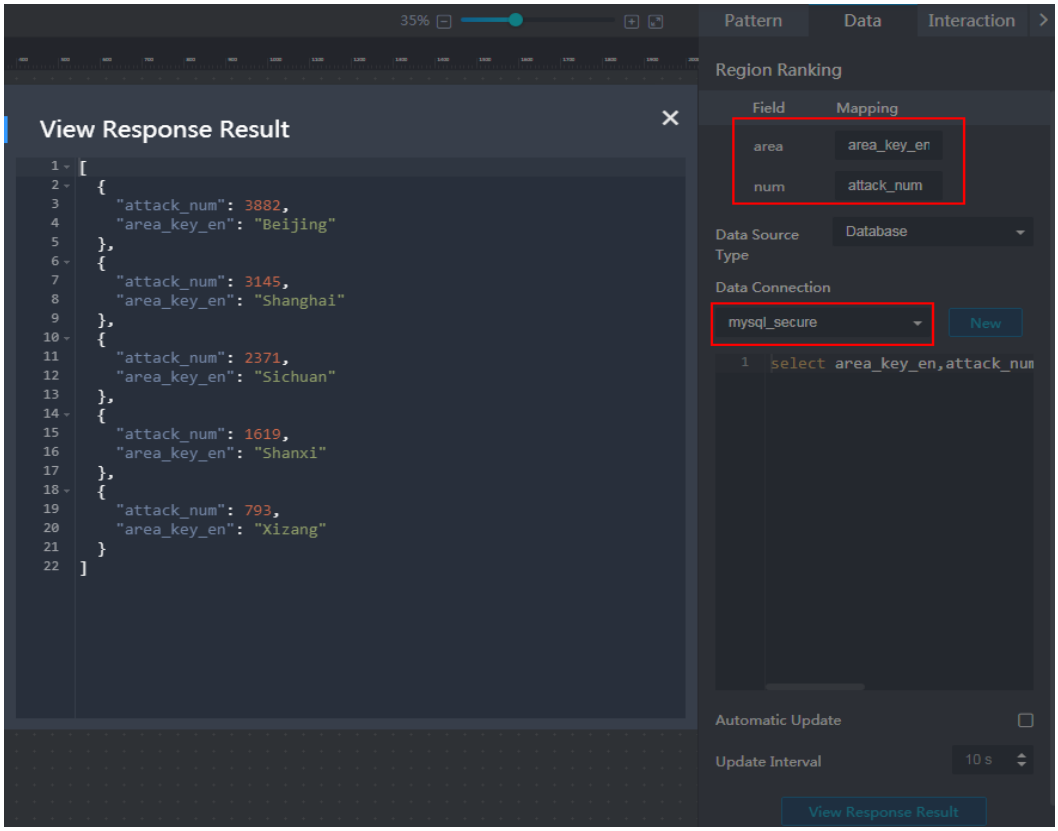
----End

Adding a Region Ranking Component

Step 1 In the **Charts** component library, select a **Region Ranking** component.

Step 2 On the **Pattern** panel, configure the component pattern. On the **Data** panel, set **area** to **area_name_en** and **num** to **pv_num**. In the **Data Source Type** drop-down list, select **Database**. In the **Data Connection** drop-down list, select an existing data connection. Execute SQL statement **select area_name_en,pv_num,percent from dw_pv_country order by 2 desc** to query the access region ranking and then click **View Response Result**.

Figure 1-11 Viewing the response result

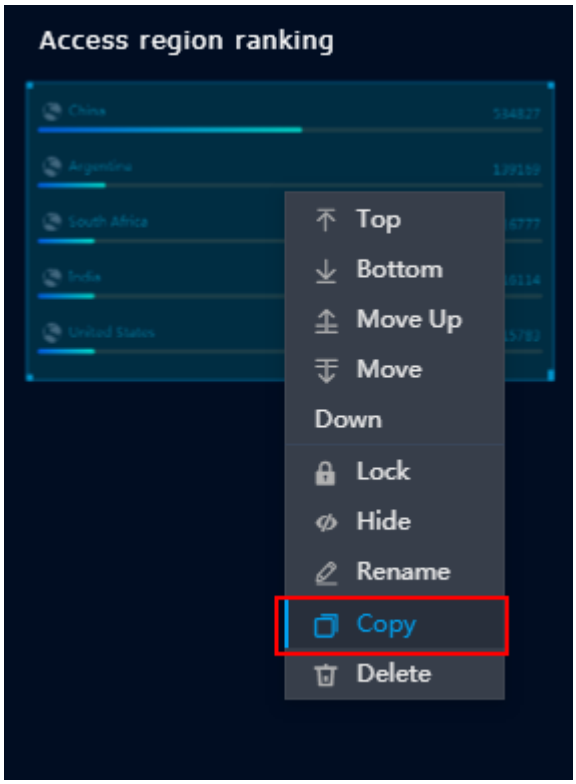


Step 3 Drag a **Title** component from the component library, place it above the **Region Ranking** component, and enter **Access Region Ranking** as a title.

Step 4 Right-click the **Region Ranking** component and select **Copy** from the shortcut menu to generate a new **Region Ranking** component.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-12 Copying a region ranking component



Step 5 Repeat Step 2 to configure the component pattern. On the **Data** panel, set **area** to **area_key_en** and **num** to **attack_num**. Execute the following SQL statement: **select area_key,attack_num from dw_attack_province order by 2 desc limit 5**

Step 6 Drag a **Title** component from the component library, place it above the new **Region Ranking** component, and enter **Attack Region Ranking** as a title.

Figure 1-13 Adding a Region Ranking Component



----End

Adding Other Components

Step 1 Add **Basic 2D Map** and **Title** components. Name the **Title** component **Website access region**. Configure **Pattern** and **Data** of the **Basic 2D Map** component.

 Copyright © Huawei Technologies Co., Ltd.

After configuring mapping on the **Data** panel of the basic 2D map, execute the following SQL statement: select area_key as name,pv_num as value from dw_pv_province

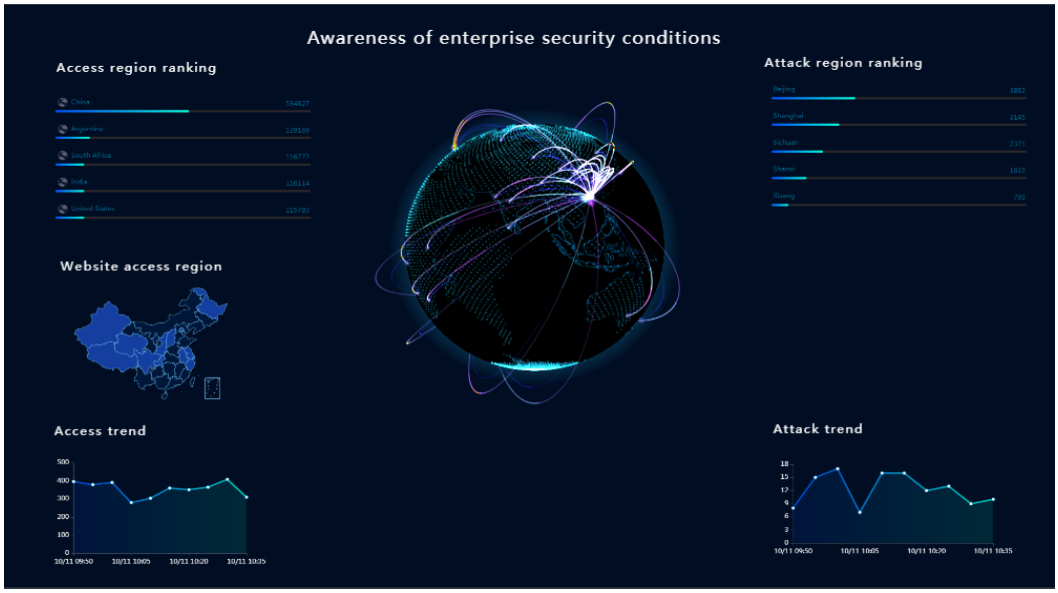
Step 2 Add **Line Chart** and **Title** components. Name the **Title** component **Access trend**. Configure **Pattern** and **Data** of the **Line Chart** component.

After configuring mapping on the **Data** panel of the line chart, execute the following SQL statement: select date_hour,pv_num from (select date_hour,pv_num from dw_pv_hour order by 1 desc limit 10) pv_hour order by 1

Step 3 Copy the line chart and title components in **Step 2** to generate a new pair of line chart and title components. The new title component is named **Attack Trend**. Configure **Pattern** and **Data** of the new line chart.

After configuring mapping on the **Data** panel of the line chart, execute the following SQL statement: select date_hour,attack_num from (select date_hour,attack_num from dw_attack_hour order by 1 desc limit 10) attack_hour order by 1

Figure 1-14 Adding basic 2D map and line chart components



Step 4 Add two **Rotation Table** components to display attack details and attack type ranking.

After configuring mapping on the **Data** panel, execute the following SQL statement:

```
SELECT FROM_UNIXTIME(FLOOR(ROUND(date_time / 1000)),'%Y-%m-%d %H:%i:%S') as
date_time,province_key_en,CONCAT('***', SUBSTRING(url, 20, 30), '***')
url,t1.type_name_en,(case risk_level when '8' then 'High-risk' when '7' then
'Middle-risk'when '6' then 'Middle-risk'when '5' then 'Low-risk'when '4' then
'Low-risk' else 'Low-risk' end)as risk_levelFROMods_attack_log t,dim_attack_type
t1WHERERt.attack_type = t1.type_codeAND province_key IS NOT NULL ORDER BY 1
DESCLIMIT 10;
```

After configuring mapping on the **Data** panel, execute the following SQL statement:

```
select attack_type_name_en, (case risk_level when '8' then 'High-risk'
when '7' then 'Middle-risk
when '6' then 'Middle-risk'
when '5' then 'Low-risk'
when '4' then 'Low-risk' else 'Low-risk' end)
as risk_level,attack_num from dw_attack_type order by 3 desc;
```

 Copyright © Huawei Technologies Co., Ltd.

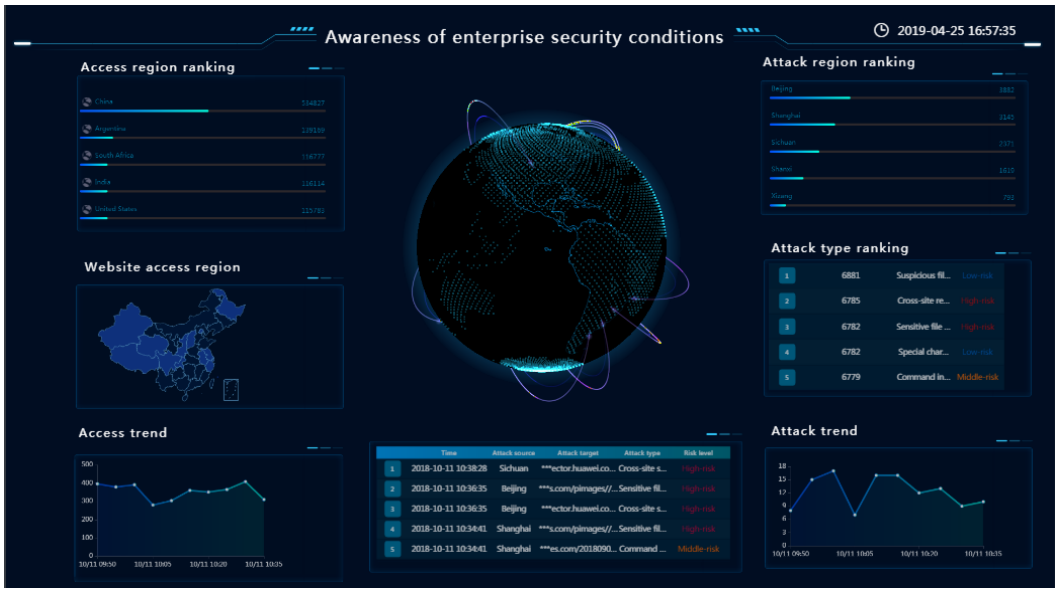
Step 5 To differentiate risk levels, set the red color to indicate the critical level in **Condition Style** on the **Data** panel.

Figure 1-15 Rotation table



Step 6 Add other components such as Custom Background, Border, and Timer Selector. The following figure shows the final display effect of the security situation awareness screen:

Figure 1-16 Security situation awareness screen



----End

 Copyright © Huawei Technologies Co., Ltd.