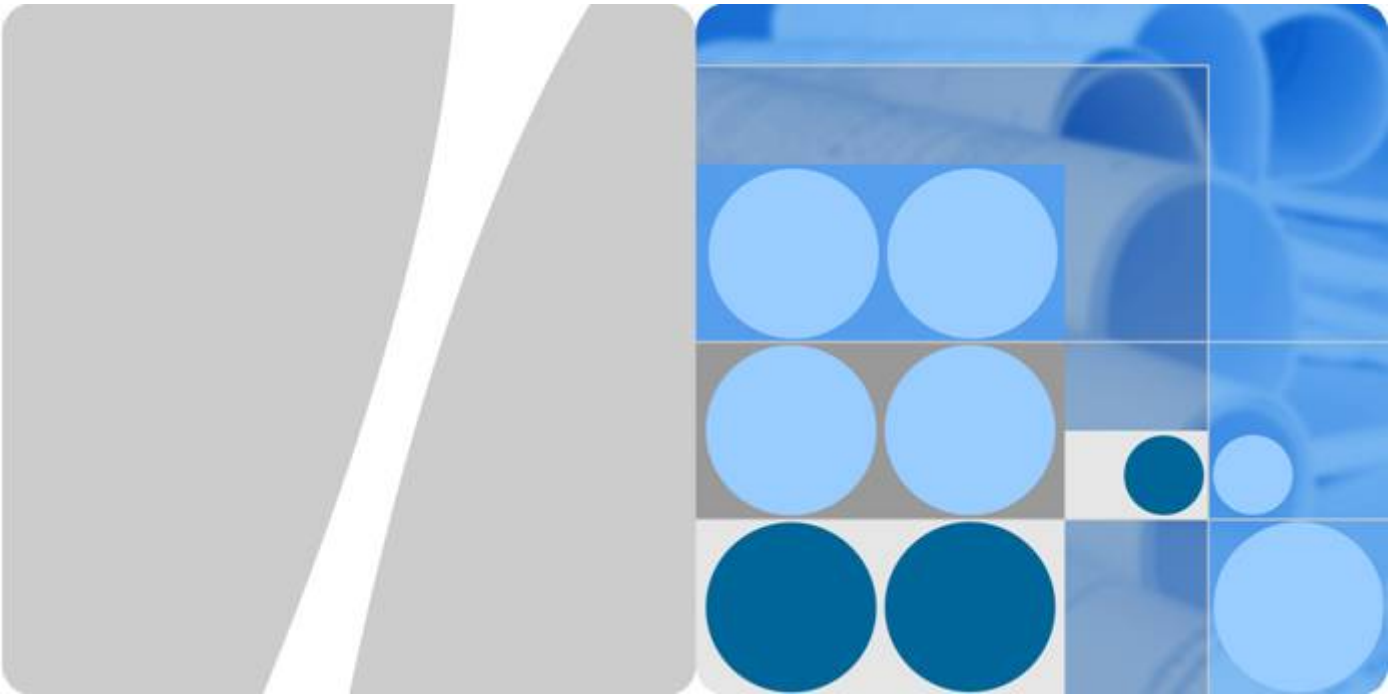


数据可视化

最佳实践

文档版本　01

发布日期　2019-04-19

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 使用 DLV 查看某企业安全态势

本文档介绍某企业安全态势监控大屏的创建过程，为云上企业的安全事件处置提供可视化的决策依据。

特点如下：

- 使用实时业务态势，可以实时检测，有效防范每一起安全事件。
- 使用地理化访问轨迹，通过2D、3D地图组件使安全威胁来源一目了然。
- 使用表格组件的条件样式，对风险等级做出明显区分，可以快速捕获高风险攻击源。

方案设计

列举展示内容：根据内容选择组件，该项目需要展示企业网站的访问情况与网站受攻击情况。内容主要包括两大类：访问信息与攻击信息。

访问状态下的访问信息与使用的组件类型如下表所示：

访问信息	组件类型
访问区域排行	区域排行
网站访问区域	中国地图
访问趋势	线状图
实时攻击信息	轮播表格

攻击状态下的攻击信息与使用的组件类型如下表所示：

攻击信息	组件类型
攻击区域排行	区域排行
攻击类型排行	轮播表格
攻击趋势	线状图

攻击信息	组件类型
攻击源	地球

准备工作

- 已开通关系型数据库RDS，并创建“数据库引擎”为“MySQL”的实例“rds-secure0”。
- 已购买云数据迁移CDM，新建集群“cdm-secure”。

  说明

  新建CDM集群“cdm-secure”时，在“购买云数据迁移集群”页面中的“虚拟私有云”、“子网”、“内网安全组”信息配置需要和RDS实例“rds-secure0”一致。

数据准备

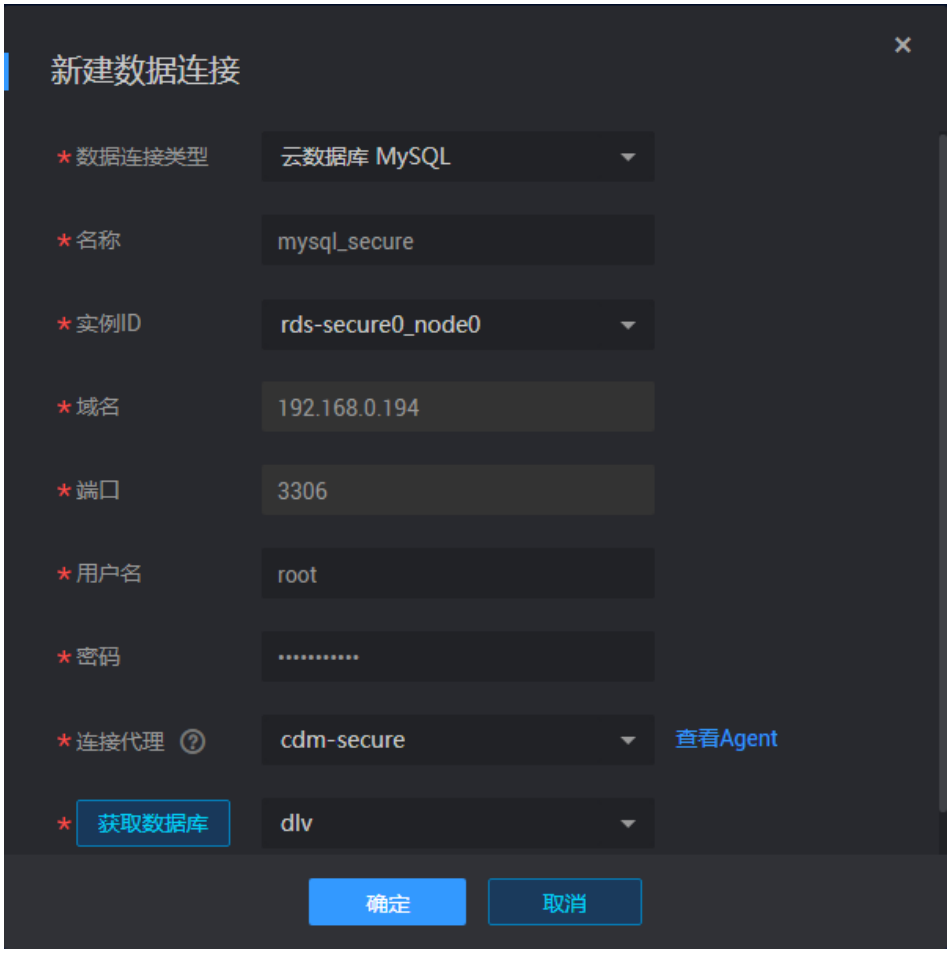
从**https://dlv-public-image.obs.cn-north-1.myhuaweicloud.com/demo1.zip**路径下载数据至本地。

选择创建好的RDS实例“rds-secure0”，输入用户名和密码登录到云上数据库MySQL，在“rds-secure0”根目录创建数据库“dlv”，选择“导入 · 导出 > 快速导入”将下载的sql数据导入到数据库中。

创建云数据库MySQL连接

1. 登录DLV控制台。
2. 选择“我的数据 > 新建数据连接”。
3. 在“新建数据连接”页面，选择建立“云数据库MySQL”的连接。
4. 设置云数据库MySQL名称为“mysql_secure”，配置“mysql_secure”的域名、端口、用户名、密码、连接代理集群。点击“获取数据库”，选择数据库“dlv”，单击“确定”，数据源“mysql_secure”创建成功。如**图1-1**所示。

图 1-1 创建 mysql_secure



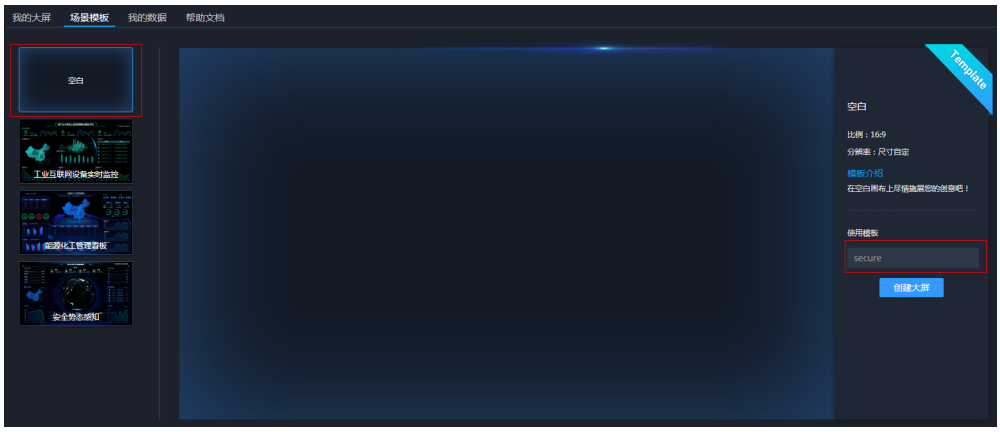
创建大屏项目

步骤1 登录DLV控制台。

步骤2 单击“我的大屏 > 新建大屏”，

步骤3 选择空白模板，新建一个大屏名称为“secure”的大屏。

图 1-2 新建大屏

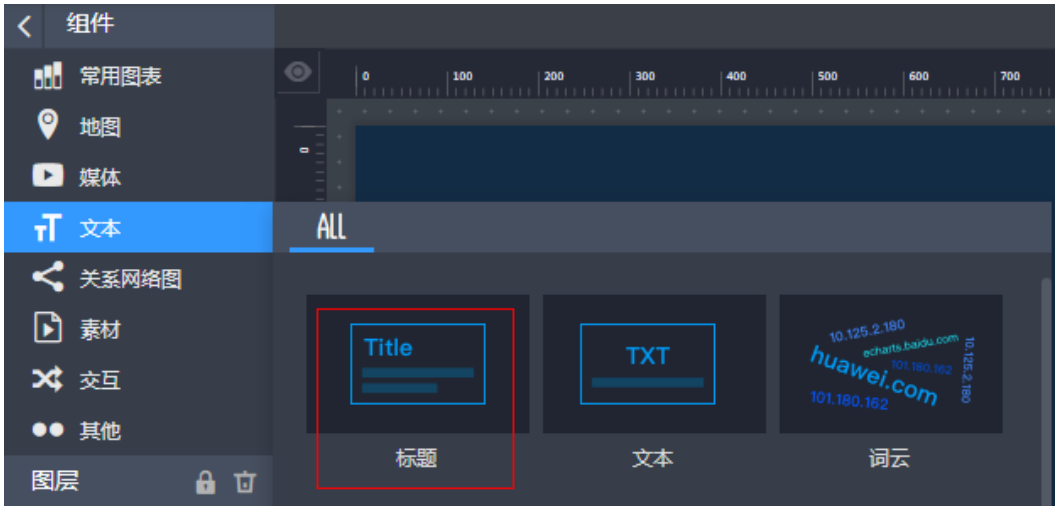


----结束

添加标题组件

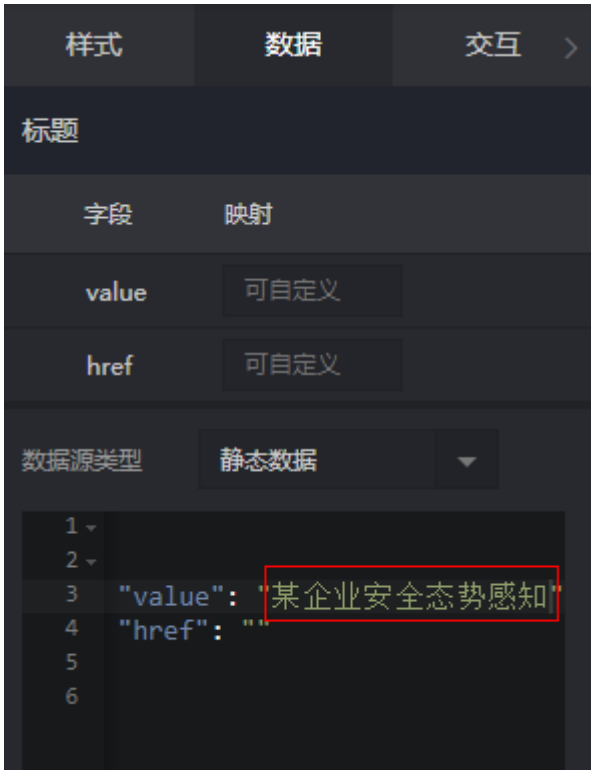
步骤1 在组件列表下的“文本”组件库中选择“标题”组件。

图 1-3 插入标题组件



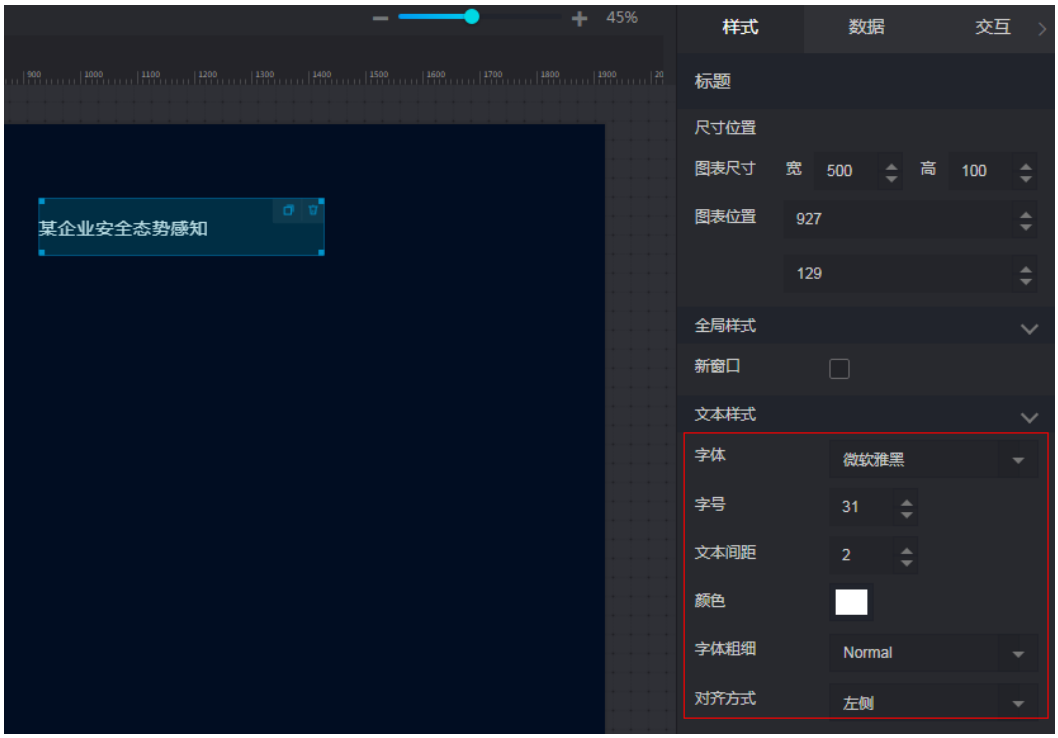
步骤2 单击“标题”组件的“数据”面板，设置value值为“某企业安全态势感知”。

图 1-4 某企业安全态势感知



步骤3 单击“样式”面板，配置标题的文本样式。如图1-5所示。

图 1-5 配置标题组件



----结束

添加地球组件

步骤1 在组件列表下的“地图”组件库中选择“地球”组件。

图 1-6 插入地球组件

步骤2 在“样式”面板中配置飞线颜色样式。如图1-7所示。

图 1-7 飞线样式配置

步骤3 单击“数据”面板，在字段映射处配置“from”映射为“attack_source”，“to”映射为“attack_dest”。在“数据源类型”的下拉选项中选择“数据库”，“选择已有数据连接”的下拉选项中选择“mysql_secure”，通过sql语句查询攻击数据，单击“查看数据响应结果”。执行不同的sql语句，数据响应的结果不同，您可以根据不同的攻击类型输入不同的sql语句。

- 查询攻击类型XSS的sql语句：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
- 查询攻击类型CSRF的sql语句：SELECT CONCAT(t.src_lng , ',', t.src_lat) as attack_source, CONCAT(t.target_lng, ',', t.target_lat) as attack_dest, COUNT(1)

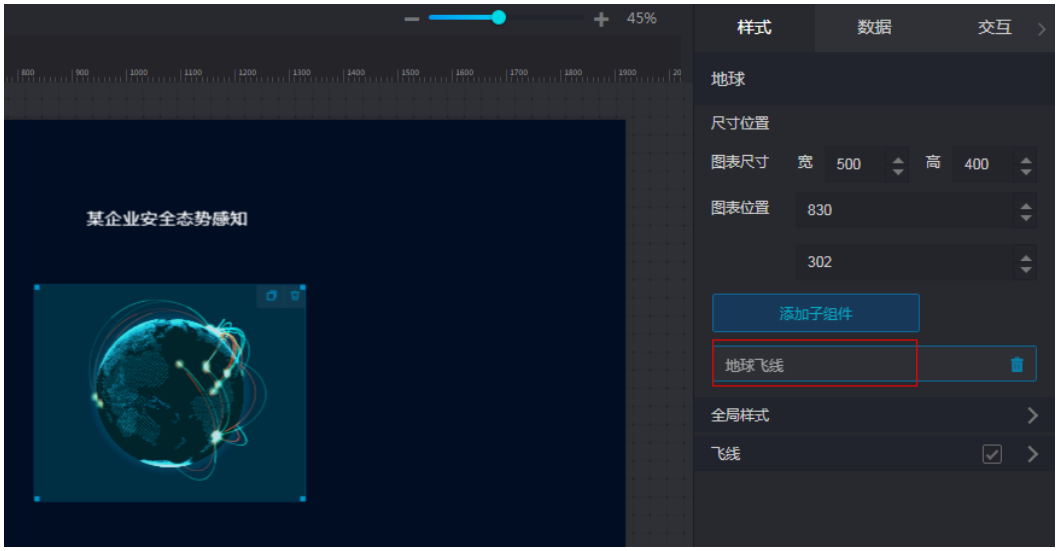
AS attack_num FROM dlv.ods_attack_log t where t.attack_type="CSRF" GROUP BY t.src_lng , t.src_lat , t.target_lng , t.target_lat

- 查询攻击类型sensitive_file的sql语句：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

图 1-8 XSS 的数据响应结果

步骤4 在地球“样式”面板单击“添加子组件”，下拉列表中选择“地球飞线”。如图1-9所示。

图 1-9 添加地球飞线组件



步骤5 单击“地球飞线”，进入“地球飞线”配置面板。在“样式”面板中配置飞线颜色样式。如图1-10所示。

图 1-10 地球飞线样式配置

步骤6 重复步骤3在“数据”面板中配置地球飞线数据，输入查询CSRF攻击类型的sql语句，单击“查看数据响应结果”。

步骤7 重复步骤4，步骤5，步骤6配置另外一组地球飞线样式和数据，输入查询sensitive_file攻击类型的sql语句，单击“查看数据响应结果”。

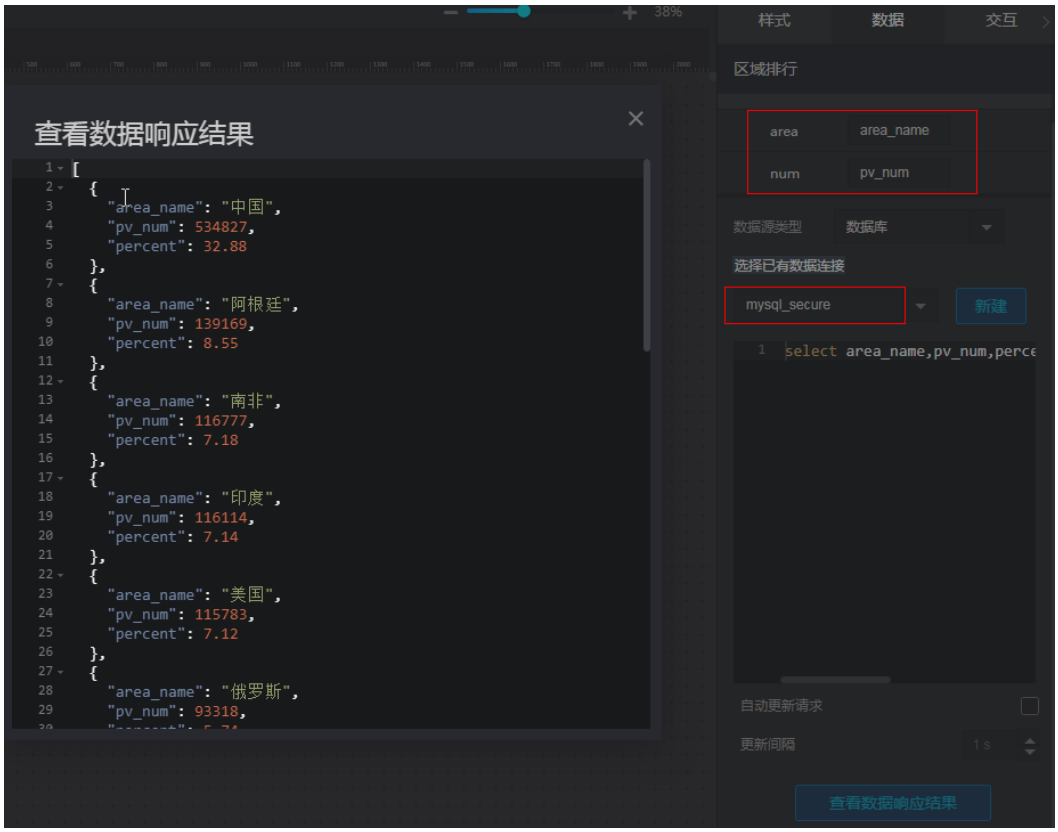
----结束

添加区域排行组件

步骤1 在组件列表下的“常用图表”组件库中选择“区域排行”组件。

步骤2 在组件右侧的“样式”中配置组件样式，“数据”面板中字段映射处配置“area”映射为“area_name”，“num”映射为“pv_num”，“数据源类型”的下拉选项中选择“数据库”，“选择已有数据连接”的下拉选项中选择“mysql_secure”，通过sql语句“select area_name,pv_num,percent from dw_pv_country order by 2 desc”查询访问区域排行，单击“查看数据响应结果”。

图 1-11 访问区域排行



步骤3 在左侧组件库中拖动一个“标题”组件至“区域排行”组件的上方，并给标题组件命名为“访问区域排行”。

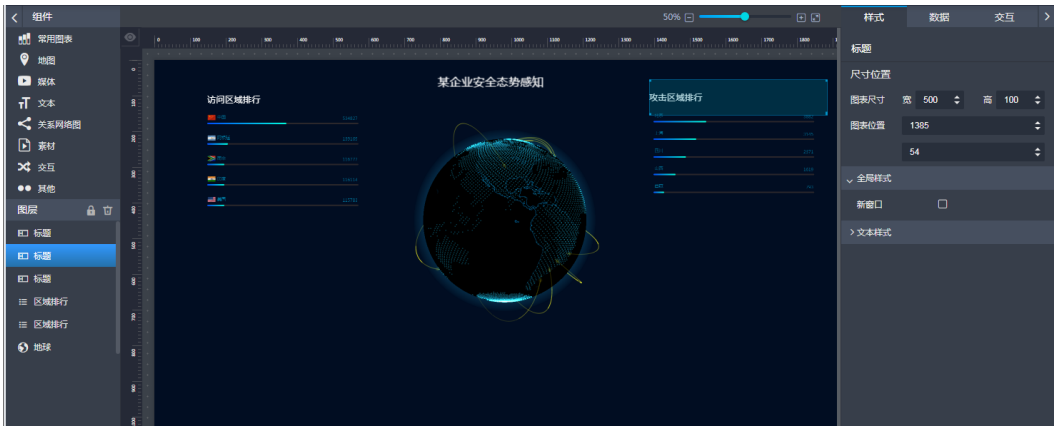
步骤4 右键单击“区域排行”，选择“拷贝”，复制一份新的区域排行组件。

图 1-12 拷贝区域排行组件

步骤5 重复步骤2配置组件样式，“数据”面板中字段映射处配置“area”映射为“area_key”，“num”映射为“attack_num”，执行sql语句“select area_key,attack_num from dw_attack_province order by 2 desc limit 5” 访问攻击区域排行。

步骤6 在“新的区域排行”组件上方配置一个名称为“攻击区域排行”的“标题”组件。

图 1-13 添加区域排行组件



----结束

添加其他组件

步骤1 添加“基础平面地图”和“标题”组件，标题组件命名为“网站访问区域”，配置“基础平面地图”的组件“样式”与“数据”。

基础平面地图在“数据”面板中配置字段映射后，执行sql语句：select area_key as name,pv_num as value from dw_pv_province;

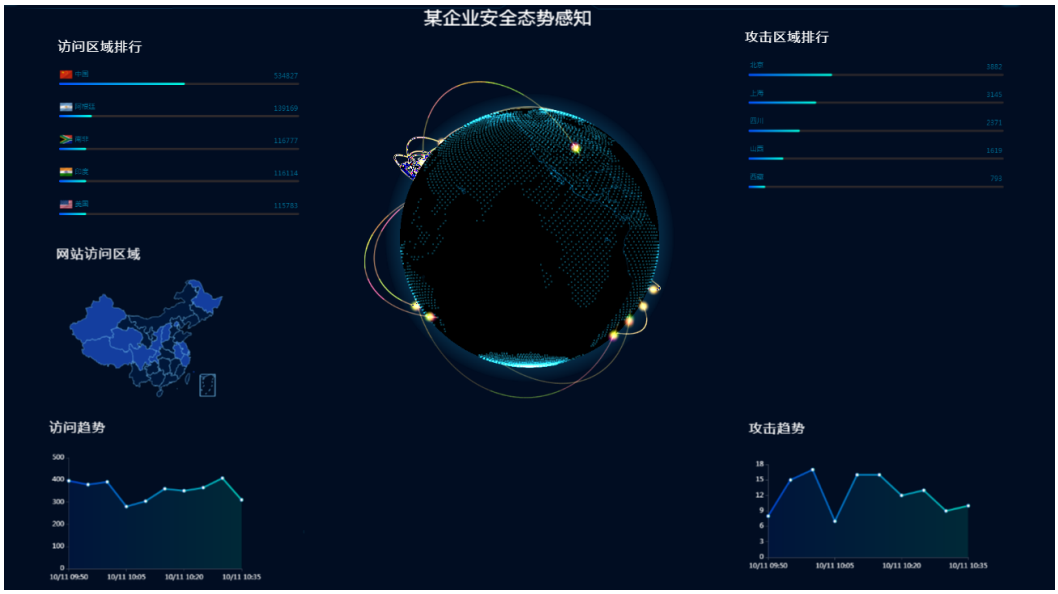
步骤2 添加“线状图”和“标题”组件，标题组件命名为“访问趋势”，配置“线状图”组件的“样式”与“数据”。

访问趋势的线状图在“数据”面板中配置字段映射后，执行sql语句：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;

步骤3 复制**步骤2**中的线状图和标题组件，生成一份新的线状图和标题组件。新的标题组件命名为“攻击趋势”。配置新的线状图组件的“样式”与“数据”。

攻击趋势的线状图在“数据”面板中配置字段映射后，执行sql语句：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;

图 1-14 添加基础平面地图、线状图组件



步骤4 添加两个“表格轮播”组件分别展示攻击详细信息和攻击类型排行。

在“数据”面板中配置字段映射后，执行攻击详细信息的sql语句：

```
SELECT FROM_UNIXTIME(FLOOR(ROUND(date_time / 1000)),                    '%Y-%m-%d %H:%i:
%S') as date_time,                province_key,                CONCAT('***', SUBSTRING(url, 20, 30), '***')
url,                t1.type_name_cn,(case risk_level when '8' then '高危'  when '7'  then  '紧急' when '6'
then '紧急' when '5' then '一般' when '4' then '一般' else '一般' end) as risk_level
FROM                ods_attack_log t,                dim_attack_type t1
WHERE                t.attack_type = t1.type_code                AND province_key IS NOT
NULL                ORDER BY 1 DESC                LIMIT 10;
```

在“数据”面板中配置字段映射后，执行攻击类型排行的sql语句：

```
select attack_type_name, (case risk_level when '8' then '高危'
when '7' then '紧急'
when '6' then '紧急'
when '5' then '一般'
when '4' then '一般' else '一般' end)
as risk_level,attack_num from dw_attack_type order by 3 desc;
```

步骤5 为了表示不同风险级别，在“数据”面板的“风险系数”参数下的“条件样式”页签中，设置红色为高危级别。

图 1-15 表格轮播

步骤6 最后添加背景图片、边框、时间器等素材。安全态势感知大屏最终展示效果如下图所示。

图 1-16 安全态势感知大屏

----结束

发布大屏

预览大屏请参考**预览大屏**进行操作。

发布大屏请参考**发布大屏**进行操作。

