**企业网络资产及安全事件分析与可视化**

**解决方案**

1. **赛题分析**

在企业的高速发展过程中，信息化建设起着非常重要的支撑作用，网络是任何信息化建设的基础，必须要保证企业网络的安全与稳定。然而随着互联网的飞速发展，企业的网络系统正面临着越来越多的威胁。企业的重要文件、数据库中的重要数据等信息都存在着安全隐患，一旦丢失、损坏或泄露，都会给企业造成很大的损失。如果是商业机密信息，给企业造成的损失会更大，甚至会影响到企业的生存和发展。

A企业，成立于2010年，国家级高新技术企业，全球领先的智能终端解决方案提供商，产品包括智能家居、智能穿戴、物联网、卫星通信移动终端等消费电子产品。近期A企业的网络安全部门发现一起网络安全事件，公司重要系统被攻击，导致重要数据发生泄漏。

1. **初赛**

请基于该企业内部正常网络日志数据，给出可视分析方案，对企业内部的网络资产进行发现和分类，并给出资产之间的通信模式。

1. **复赛**

该企业重要数据发生泄露，请根据该期间内的公司网络日志数据，给出可视分析方案，找出可能的资产异常通信模式，并对该网络安全事件的攻击过程进行描述。

1. **解题思路**

2.1 出题背景

在奇安信的产品矩阵中，其中一个功能叫做“互联网资产发现”，其定义为：基于网络扫描、搜索引擎、互联网基础数据引擎主动探测用户在互联网上暴露的资产，可以形成明确的资产清单。帮助用户发现自己的未知资产。（出处：<https://www.qianxin.com/service/IntAsset_discovery>）

互联网资产发现是利用奇安信自身的安全大数据进行企业互联网资产梳理与暴露面筛查的服务。该服务通过数据挖掘和调研的方式确定企业资产范围，之后进行主动精准探测深度发现企业暴露在外的IT设备、端口以及应用服务，并由奇安信安全专家对每个业务梳理分析，结合业务特点对资产重要程度、业务安全需求进行归纳，最终针对性的形成客户的资产画像，精准探测企业互联网暴露面。

**通过该服务，可以获得：**

* 掌控：全面掌握互联网资产暴露范围和攻击面，形成自己的互联网资产地图。
* 敏捷：快速周期性排查未知互联网边界资产，实时发现企业IT资产与业务变更。

**该服务主要满足如下安全需求：**

* 解决大型甲方单位无法掌控自身安全边界的问题。
* 快速周期性排查业务部门对外开放的业务系统，一站式解决业务部门私自上线无法监管的问题。

另一方面，奇安信跟北京大学合作，获得了数据可视化顶级会议IEEE VIS 2018的2018 VAST MC3最高奖项。同时，奇安信还赞助了2019 ChinaVis可视化比赛，其下属的雷尔平台实验室多次获得可视化比赛奖项和赞助ChinaVis等可视化大赛，并研发了胶囊全景体验平台(Capsule [VR](http://www.qudong.com/vr))，如下图所示：



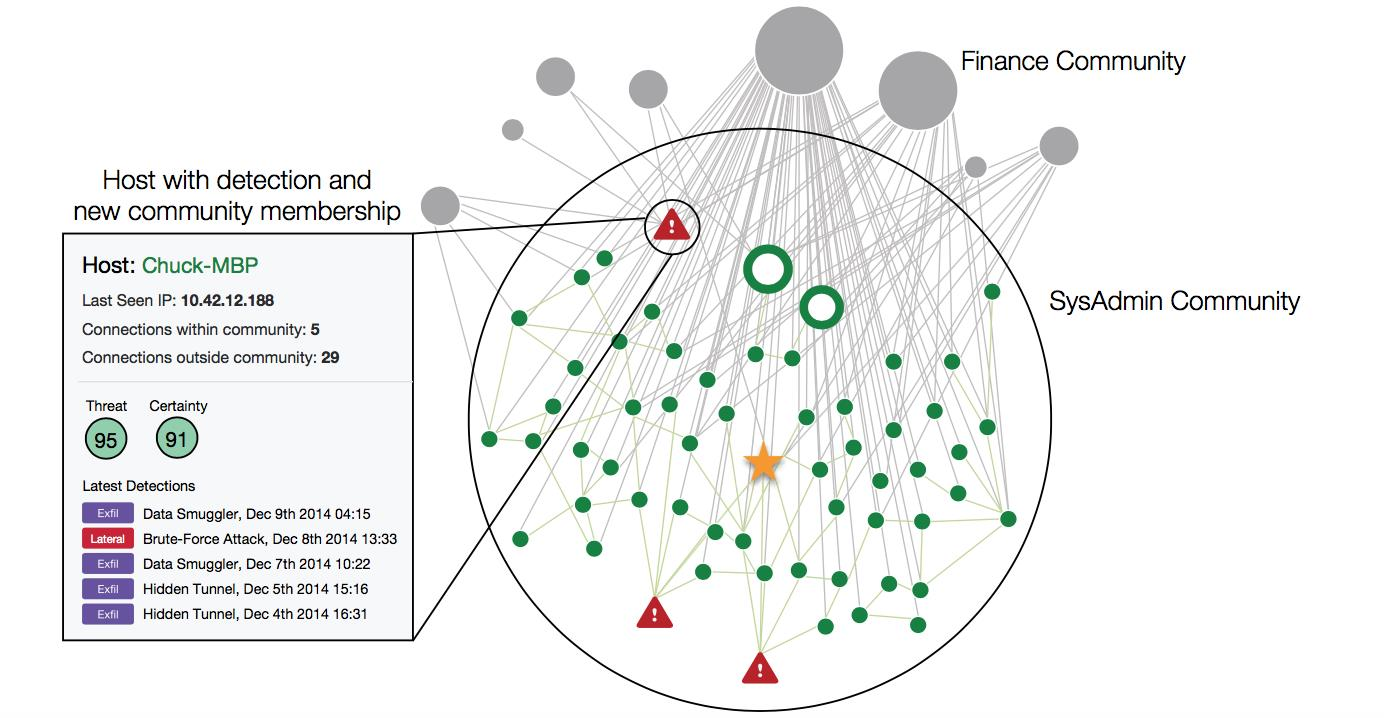
奇安信雷尔平台技术部门研发的Capsule VR 虚拟智慧城市场景

**2.2 核心要素**

本次可视化大赛的核心要素是两点：

* **发现互联网资产及其网络边界；**

发现**暴露在外的IT设备、端口以及应用服务**，并由奇安信安全专家**对每个业务梳理分析**，结合业务特点对**资产重要程度、业务安全需求**进行归纳，最终针对性的形成客户的**资产画像**，精准探测企业互联网暴露面。



奇安信的关键资产的流量模型

* **分析网络攻击事件（数据泄露）并描述其发生过程；**

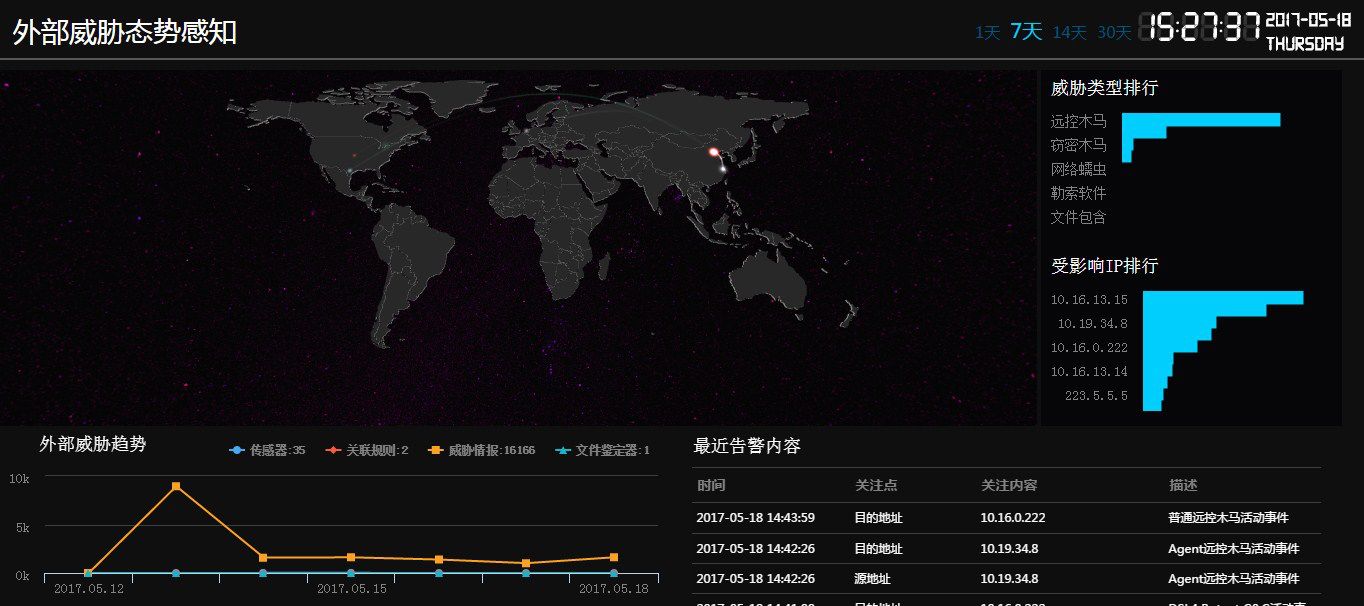
该企业重要数据发生泄露，请根据该期间内的公司网络日志数据，给出可视分析方案，找出可能的**资产异常通信模式**，并对该网络安全事件的**攻击过程进行描述**。

**2.3 解题思路**

**2.3.1 可视化思路**

* 提供大屏展示效果（dashboard，类似上图中的大屏效果）；
* 提供按层级或目录树检索来查看不同层级的可视化效果；
* 提供网络拓扑图（哪怕不精确或者是按功能区来画的整体拓扑结构图），并在拓扑图上做一些流量可视化效果；

奇安信的产品可视化界面参考图：



**2.3.2 数据分析算法**

**2.3.2.1 互联网资产发现算法**

从初步的分析来看，无法用简单的算法来区分外部服务器是企业自己的还是外部其他企业的，应该要结合手工分析和调研才能精准确定，因此这里只能使用一个推导出来的大概的网络拓扑来表示，比如某些网段划为办公区、某些作为服务器区等；

拓扑结构的效果图参考下图：



**2.3.2.2 网络安全事件发现算法**

需要根据复赛数据来分析设计；