一、设备信息总览和网络拓扑图由接口8规定

接口8中包含两张图，分别为all和sub，sub图是all图的子集，页面上应有一个开关键控制展示的是全图还是子图，页面上的设备类型对应device\_type，标识对应network\_ip，网络流量对应net\_traffic，设备状态对应status，0为正常、1为异常。



二、检测数据由接口10规定

Detection\_info 为检测时间，trace\_info为溯源时间，detection\_accuracy\_info

为检测成功率。每种类型的数据里有id（30001、40001、50001）用于表示使用yzn和不使用yzn的同一组数据。



三、攻击检测与溯源事件由接口11规定

接口数据和页面上的数据一一对应，接口中包含唯一标识id，与接口6\_7和接口9中的唯一标识对应。



四、溯源分析中的拓扑图和节点列表由接口6\_7规定

接口6\_7对应的是溯源分析里的拓扑图，一条溯源分析对应一张拓扑图，拓扑图由graph\_id唯一标识。

nodes中的id对应页面中的节点名称，label对应页面中的节点描述，shape对应页面中的节点类型，其中ellipse对应文件、diamond对应网络、box对应进程。示例如下：



结合接口6\_7中的边关系，构成溯源分析中的拓扑图形成该页面红色矩形框中的拓扑。



五、溯源分析中的时间轴由接口9规定

接口9中的数据用于生成溯源分析中的时间轴，分为三个阶段，数据处理，攻击检测，一条溯源分析对应一张时间轴，时间轴graph\_id唯一标识，对应接口6\_7的唯一标识。

