

知 CSAP网络安全态势感知的可视化大屏界面显示的是什么数据

IPS防攻击

卯静

2020-09-23 发表

问题描述

CSAP网络安全态势感知的可视化大屏界面显示的是什么数据

解决方法

外网攻击趋势 ----- 显示的是安全日志，源IP是外网，目的IP是内网，不需要生成安全事件

整网威胁态势 -----显示的安全事件，不是安全日志。根据安全事件里面的源和目的IP情况进行展示

脆弱性态势 ----- 通常都是导入漏扫报告，要求漏扫报告里面的IP都是平台上的“资产”,如果IP是属于配置了用户地址段，需要对应的删除用户地址，再导入。另外，我司的FW和IPS设备也可以上报脆弱性相关的安全日志，平台也会生成对应的安全事件，生成的安全事件和导入漏扫报告的效果基本相同。FW和IPS上报脆弱性相关的安全日志，主要是弱口令、配置风险的日志