IDC 安全监测分析平台

1、产品简介

以IDC机房用户为维度，对多源全量日志采集解析，流量关联分析为核心，实现IDC用户流量全生命周期的可视化；结合威胁情报分析，关联IDC用户流量，实现IDC机房用户的安全画像分析，同时针对威胁取证和溯源，提出安全解决方案和安全产品服务，针对IDCISP信息安全项目提供增值分析功能。

2、产品架构

功能架构图

3、核心功能

- **流量流向分析：**

支持按天、按周、按月统计所有用户整体的流量趋势，TOP10用户流量。也可以单独分析每个用户流量趋势和该用户的应用大类流量、应用小类详细统计信息。

支持按天、按周、按月统计所有应用大类流量趋势、TOP10应用大类和每个应用大类下的应用小类流量信息；支持按天、按周、按月统计所有应用小类流量趋势、TOP10应用小类和每个应用小类流量信息

- **信安系统事件分析**

支持接收 IDC/ISP 信息安全管理系统中 EU 执行单元上报的用户相关的信息安全管理日志、网络安全日志、数据安全日志日志，并进行汇总统计不同类型的安全事件数量及同比增减。支持按天、按周、按月统计三类安全事件趋势以及详细的安全事件名称分布、TOP5 安全事件。

- **威胁情报分析**

支持接收 IDC/ISP 信息安全管理系统中 EU 执行单元过滤白名单之后上报的用户全量上网日志，再根据分析系统内置的威胁情报规则进行匹配，发现威胁事件。可以根据威胁事件数量、威胁事件类型、攻击主机、受害主机、IOC 对象（域名、URL、IP）等维度统计，并且可以同比增减数量。

支持按威胁事件类型统计事件分布，也可以按 IOC 检测对象统计事件数量趋势。支持从事件视角、攻击视角、受害事件等三个维度详细统计威胁事件情况。支持对历史流量命中的威胁事件按照事件类型进行统计命中数量。

- **安全画像报告**

支持按客户生成报告预览，并支持导出，导出格式支持 PDF；客户安全画像报告支持以下内容：

(1)分析报告总结：本次报告统计的时间范围、风险情况和攻击次数、最危险客户、热门安全事件及客户情况、处置建议；

(2)整体安全评分：综合评分及评分说明；

(3)受害客户分析：统计失陷用户 IP、安全事件及等级、主动攻击次数及攻击时间等；

(4)攻击者分析：攻击成功事件、攻击 IP、攻击成功次数、失陷用户户 IP、攻击时间等；

(5)安全事件详情：安全事件风险分布、趋势分布、高危/中危/低危事件详情（安全事件名称、描述、处置建议、事件次数及详细攻击日志)

4、 产品价值

- **挖掘数据价值：**信息安全管理系统经过多年的建设记录了庞大的数据，IDC 安全监测平台可以有效的复用现有系统的数据进行二次分析，挖掘数据价值；
- **业网协同创新：**网络部门和 IDC 政企部门根据业务需求需要进行增值业务创新，提升收入，两者的协同可以从产品、业绩上都做出创新；
- **投资小回报高：**复用现有的 DPI EU 数据采集系统，只用建设上层数据分析平台即可，分析输出安全画像报告，提供安全产品及安全服务，增加收入；