安全报告分析生成项目

—业务需求说明书

杭州安恒信息技术有限公司

二〇二〇年八月

文档修改记录

日期	修改说明	版本号	修改人
2020/8/13	1. 分析报告各元素说明 2. 原型图表的绘制以及替换 3. 攻击者地图细节分析图表字段修改 4. 受害者地图细节分析图表字段修改	V1.0	姜婧
2020/8/14	1. 攻击者细节分析表需求添加 2. 受害者细节分析表需求添加 3. 界面菜单布局需求原型图及描述表添加	V1.1	姜婧

目录

1 功能简介

通过在本平台创建安全报告生成任务并审核通过后可以导出报告以及查看数据渲染出的网页，报告中会主要从整体数据时序趋势分布、风险资产分布、受害者、攻击者、TOPN 攻击行为这几点进行模块分析，并总体分析说明以及给出处置建议，帮助用户从资产、受害对象、攻击手段等信息多维度分析资产的风险值趋势、风险状况分布等信息，并提供反馈建议提供对方修复使用。

2 名词约定

1. 受害者

a) 被攻陷的设备
b) 受到安全威胁的设备
c) 受到安全警告的设备

2. 攻击者

网络攻击是指针对网络设备，任何类型的进攻动作，攻击者可以是外部设备或内部设备。一般以 IP 地址来标识一个攻击。

3. 攻击链

攻击链是攻击者发动攻击的一些过程，如侦察、投递、内部渗透等。

4. 攻击行为风险等级

表示我们遭受的网络攻击的攻击威胁严重程度，由安全日志提供的信息字段安全告警威胁等级（threatSeverity）来衡量。风险等级分为高风险、中风险、低风险。

5. 资产风险等级

表示一个资产的安全风险，主要根据提供给我们平台的风险资产记录中的风险评级来呈现。风险评级分为三种：已失陷、高风险、低风险。

6. 有效攻击次数

表示攻击成功的攻击事件数量。

7. 热点告警事件

发生次数最多的告警事件

2.2 界面菜单布局需求

2.2.1 业务需求功能列表

用户登录平台默认显示【首页/总览】页面，如图 2-1 界面菜单布局所示。

图 2-1 界面菜单布局

界面菜单布局见表 2-1 菜单布局。

表 2-1 菜单布局

菜单布局	说明
一级菜单	**【基本流程】** 1) 有报告模块一个一级菜单 **【扩展流程】** 1) 点击菜单【报告模块】，显示报告总览页面
二级菜单	**【基本流程】** 2) 有整体数据时序趋势分布、风险资产分布、受害者分析、攻击者分析、TOPN 分析、分析处置及建议六个二级菜单 **【扩展流程】** 2) 点击菜单【数据时序趋势分布】，显示报告数据时序趋势分布页面

	3) 点击菜单【风险资产分布】，显示报告风险资产分布页面 4) 点击菜单【受害者分析】，显示报告受害者分析页面 5) 点击菜单【攻击者分析】，显示报告攻击者分析页面 6) 点击菜单【TOPN分析】，显示报告TOPN分析页面 7) 点击菜单【分析处置及建议】，显示报告分析处置及建议页面
按钮区	**【基本流程】** 1) 点击<导出>按钮，导出当前报告

2.2.2 需求优先级

高

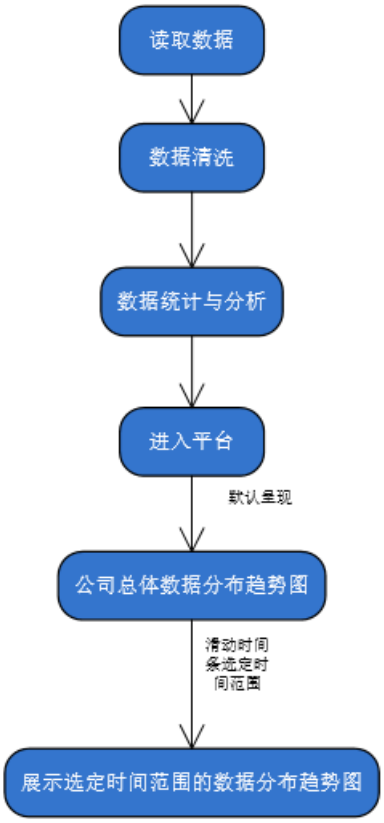
2.3 整体数据时序趋势分布业务需求

2.3.1 整体数据时序趋势分布描述

根据告警引擎等设备提供给我们平台的安全日志分析，提取出利用有效字段：安全告警威胁等级（threatSeverity），事件数量（eventCount），呈现出整体安全状况分布图。

2.3.2 业务流程

图 2-2 整体数据时序趋势分布流程图



2.3.3 业务需求功能列表

用户进入平台点击菜单的【首页/总览】，显示公司全部安全域的数据时序分布图分布。任务页面暂时还没有。

1. 数据时序分布趋势图

图表的横坐标显示时间，纵坐标是网络攻击攻击成功的攻击次数，三条曲线分别呈现攻击威胁严重程度高风险、中风险、低风险三种级别的网络攻击攻击成功的次数随着时间变化的变化；图表底下是可以选择指定时间间隔，用以查看对应的安全状况分布图。

图 2-4 数据时序分布图

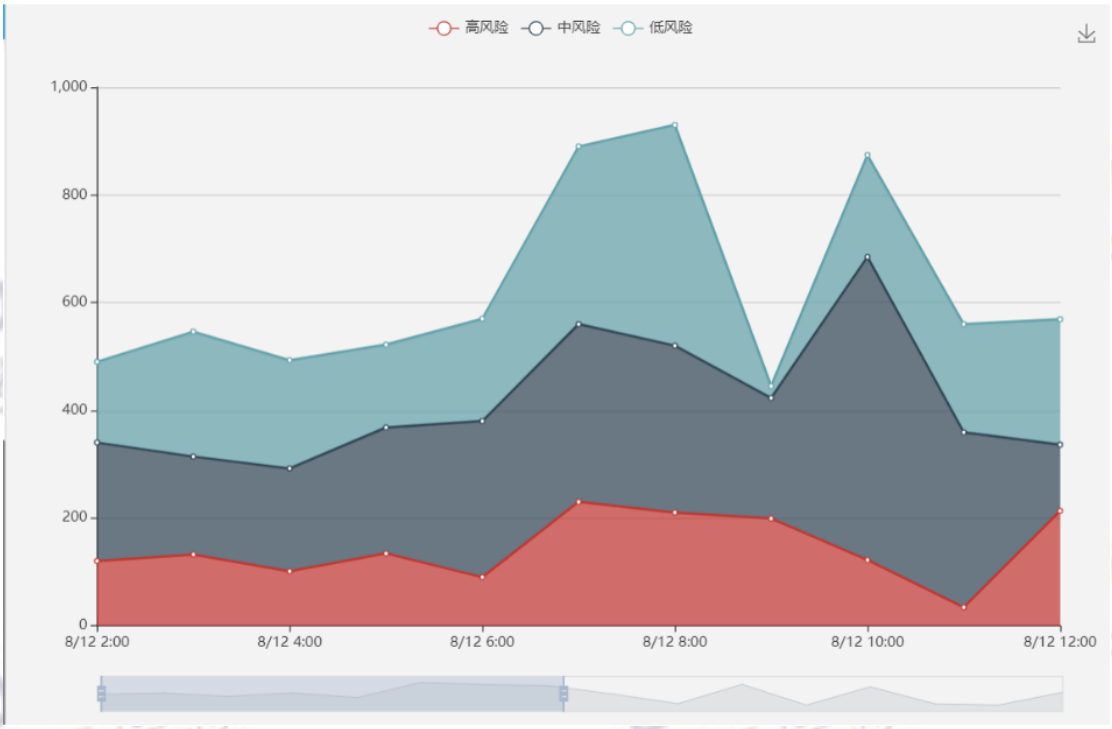


表 2-4 图表总体元素说明

类型	描述
曲线	三条曲线表示不同安全告警威胁等级，即攻击威胁严重程度；红色表示高风险，黑色表示中风险，蓝色表示低风险
横坐标	时间
纵坐标	攻击次数（累计还是当前）

2. 菜单栏

在页面的左侧，有一个菜单栏，如下表说明：

表 2-5 菜单栏总体元素说明

菜单	描述	内容
攻击类型	该菜单下拉可以选择不同攻击类型的数据分布时序趋势图，也可以选择全部；通过该功能，使用户能更加详细地了解自己的安全状况。	可供选项13种告警类型，如DDOS、探针扫描、漏洞利用、web攻击、账号异常、配置风险、行为审计等

3. 时间范围

在趋势图下有一个滑动选择框，可以拖动两边选择自己想要了解的时间间隔的时序趋势图。

2.3.4 需求优先级

高

2.4 风险资产分布及表格展示业务需求

2.4.1 扫描总览描述

该业务展示了客户的风险资产分布，根据风险资产记录数据进行数据处理，展示客户的高风险、中风险、低风险甚至是已失陷的资产分布，采用饼图等图表形式更直观的展示。

2.4.2 业务流程

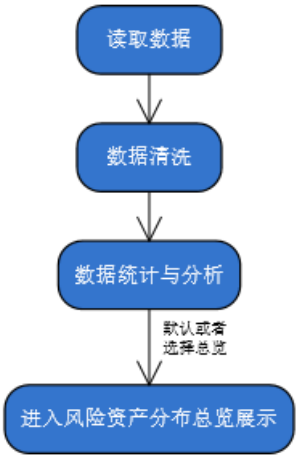


图 2-2 风险资产分布流程图

2.4.3 业务需求功能列表

下面分别对这几块区域进行说明：

1. 具体页面呈现

1、 饼图呈现

类似于下图，饼图呈现更直观的风险资产分布，不同颜色呈现不同风险评级的风险资产数量，已失陷的、高风险的、低风险的。

图 2-6 风险资产分布原型图

处理方式	事件数量	所占比例
已失陷	13	0.18%
低风险	162	2.24%
高风险	7059	97.58%

2、 表格呈现

在饼图右边呈现更为详细的表格化风险资产分布，如下表范例描述所示。

图 2-7 风险资产展示表

安全域	资产名称	风险评级
风暴中心（机房）	WEB服务器-10.20.82.92	已失陷
风暴中心（机房）	WEB服务器-10.20.82.92	已失陷
服务中心（机房）	WEB服务器-10.20.82.92	已失陷
服务中心（机房）	WEB服务器-storm-node-10	已失陷
AiLPHA-SOC（机房）	WEB服务器-storm-node-10	已失陷

表 2-7 图表总体元素说明

安全域（IP 可选）	资产名称	风险评价
各个部门机房区域	安全域的资产（服务器）的名称，可以IP地址呈现	呈现一个安全域的资产的安全状况

2.4.4 需求优先级

高

2.5 受害者分析业务需求

2.5.1 受害者分析业务描述

通过对安全日志的分析，我们可以从中分析出受害者的地理位置分布，受害者资产名称，被攻击次数等各种信息，对这些信息进行整合，输出到安全报告中，给客户一个直观的展示。同时也可以生成一个 h5 页面，给用户更好的体验。

2.5.2 业务流程

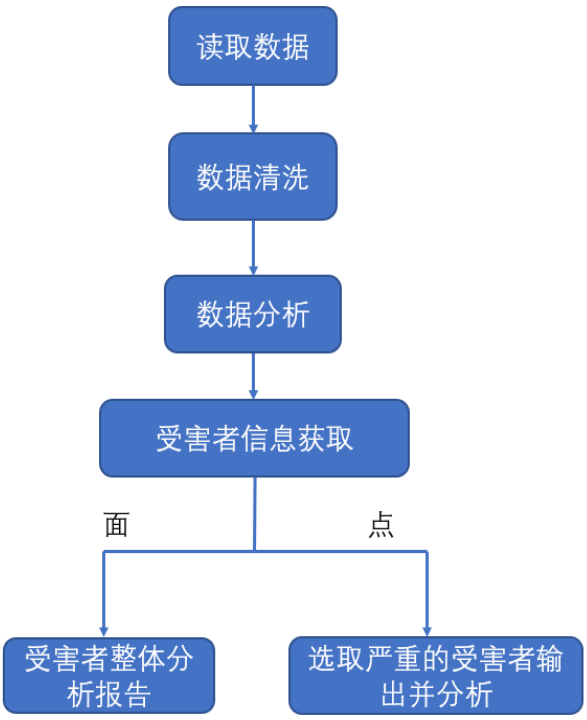
后端通过对 log 日志进行读取、清洗、分析，生成受害者受害区域分布以及被攻击次数等信息，分成点与面两个部分：

点（详细分析）：针对受攻击情况比较严重的 topN 受害者，输出详细的受害者信息，例如受害者 ip，受攻击的资产信息，受害者详细地理，受攻击次数，所占比例等。下方还可以生成一个详细信息的表格。

面（整体分析）：对所有受害者进行归纳总结，生成一个综合的报告，最终以图表的形式展现出来。

在前端生成一个直观的展示页面，产生一个地图，并在地图下方生成一个 TopN 的表格，同时可以在前端选择导出一个 word 或者 pdf 文档，下载到本地。

图 2-8 受害者分析流程图



2.5.3 业务需求功能列表

用户导入数据，执行程序，后端分析处理生成安全报告，并将数据传入前端，前端接受收到数据生成对应的前端页面，直观地显示出安全报告的详细内容，给用户更好的体验。

页面中会产生受害者地域分布图

在地域分布中包含着详细的信息

同时在分布图下方会有一张图表展示 TopN 的详细信息，表格中包含受害者 ip，国家以及受害时间等信息。

下面分别对这几块区域进行说明。

1. 地图总体分析

可以根据扫描任务、分析对象、扫描时间进行查询，页面默认显示如图 2-所示。

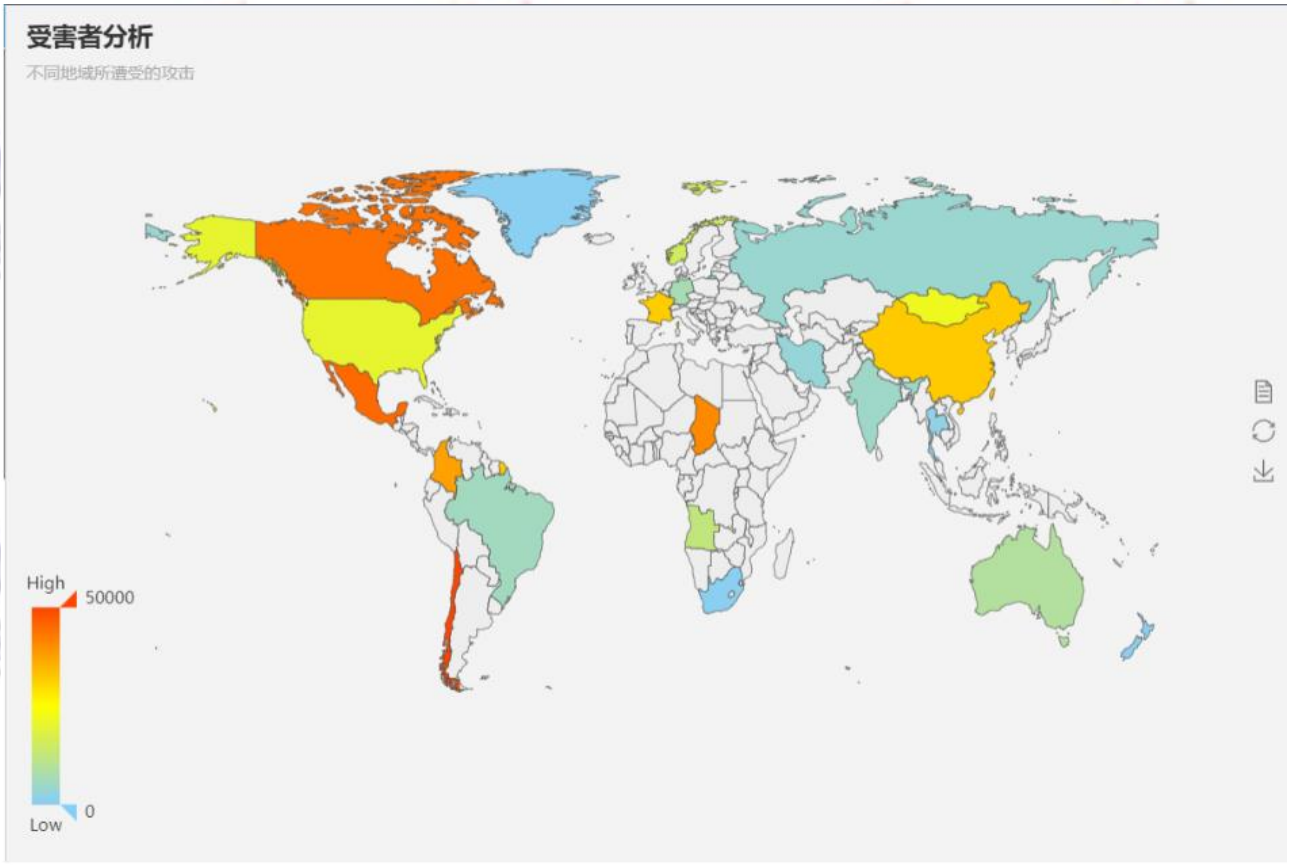


图 2-9 总体展示图

查询条件	说明
受害者整体展示	**【基本流程】** 获取数据并作出分析 将受害者总体信息与详细信息整合并生成图形展示 以颜色区分受害程度 **【规格及限制】** 1) 每次只能生成一个图表

	【非功能需求】 1) 初始状态不显示

表 2- 10 图表详细元素说明

2. 地图详细分析

将鼠标移动至遭受攻击较为严重的地区（红色部分），即可获取其详细信息。

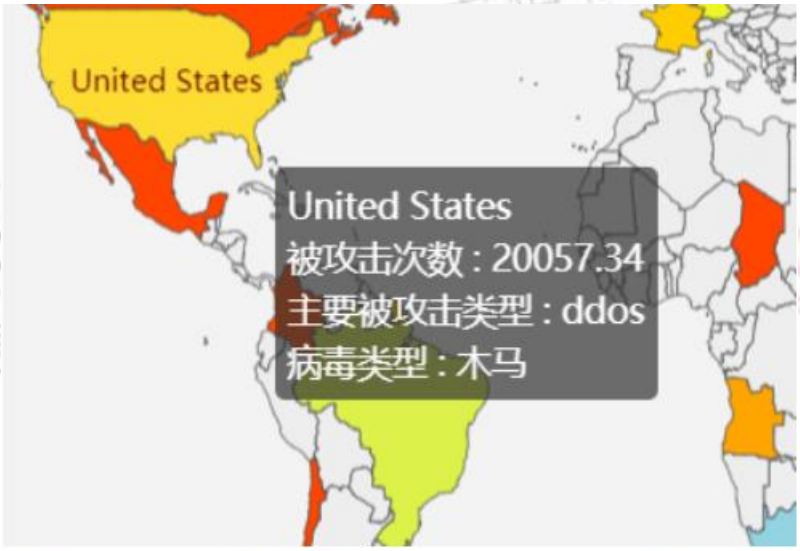


图 2-10 总体展示图表

查询条件	说明
受害者详细展示	**【基本流程】** 1) 查看受害者分析 2) 将鼠标移动至受攻击严重的地区（红色部分） 3) 弹出该地区的详细信息 **【规格及限制】** 1) 鼠标移开后信息消失 **【非功能需求】** 1) 初始状态为空

表 2-11 图表详细元素说明

3. 受害者详细分析

被害者	IP地址	所在国家	时间
a	123.123.123.1	美国	2020-08-14 11:06
b	125.20.22.23	美国	2020-08-14 11:06
c	100.55.62.31.25	美国	2020-08-14 11:06
d	101.25.30.100	美国	2020-08-14 11:06

图 2-12 总体展示图表

查询条件	说明
受害者详细表格展示	**【基本流程】** 4) 在地图下方生成TopN受害者表格 5) 白哦个中有其地域分布，ip，国家等详细信息 **【规格及限制】** 2) 只显示部分数据 **【非功能需求】** 2) 初始状态为空

2.5.4 需求优先级

高

2.6 攻击者分析业务需求

2.6.1 攻击者分析描述

用户可以直观的在前端页面看出攻击者的区域分布以及攻击热度等信息，同时有攻击详细信息的展示功能，后端生成的报告与前端页面组件类似，攻击者分析的详细信息以文字方式总结。

2.6.2 业务流程

后端通过对 log 日志字段例如攻击链(killChain)、安全告警威胁等级(threatSeverity)、来源IP(srcAddress)、来源国家 (srcGeoCountry)、进行读取、清洗、分析，生成攻击区域分布以及热度等信息，在后端渲染出 word 文档，同时提供接口给前端进行调用。

前端在页面渲染一个类似地图的组件，选取攻击活动强的前 10 俄国区域进行展示，通过攻击区域的颜色来展示攻击的热度，颜色越深，攻击的强度越强。同时在地图组件下端有攻击者的最新攻击信息，以表格形式展示。

当用户的点击焦点在前端组件上停留，则会详细显示，如攻击者 IP、攻击设备(deviceCat)、攻击链(killChain)、攻击方法（attackMethod)等信息。

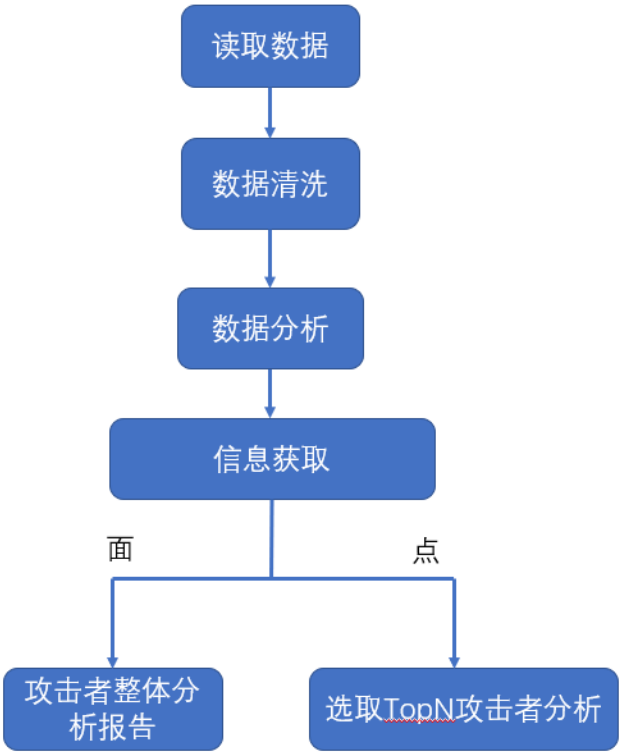


图 2-13 攻击者分析流程图

2.6.3 业务需求功能列表

后端将攻击者分析的结果在后端生成一份 word 报告，同时提供接口给前端进行渲染，前端以类似地图的组件进行结果展示，前后端尽量风格一致，图表简洁明了，分析内容精准直接，前端提供下载分析报告的按钮。

在地图组件的下方有攻击者的最新攻击信息，以表格形式展示，有攻击者、攻击手段、攻击意图、攻击地址、攻击时间等信息。

下面分别对这几块区域进行说明。

1. 地图总体分析

图 2-14 总体展示图表

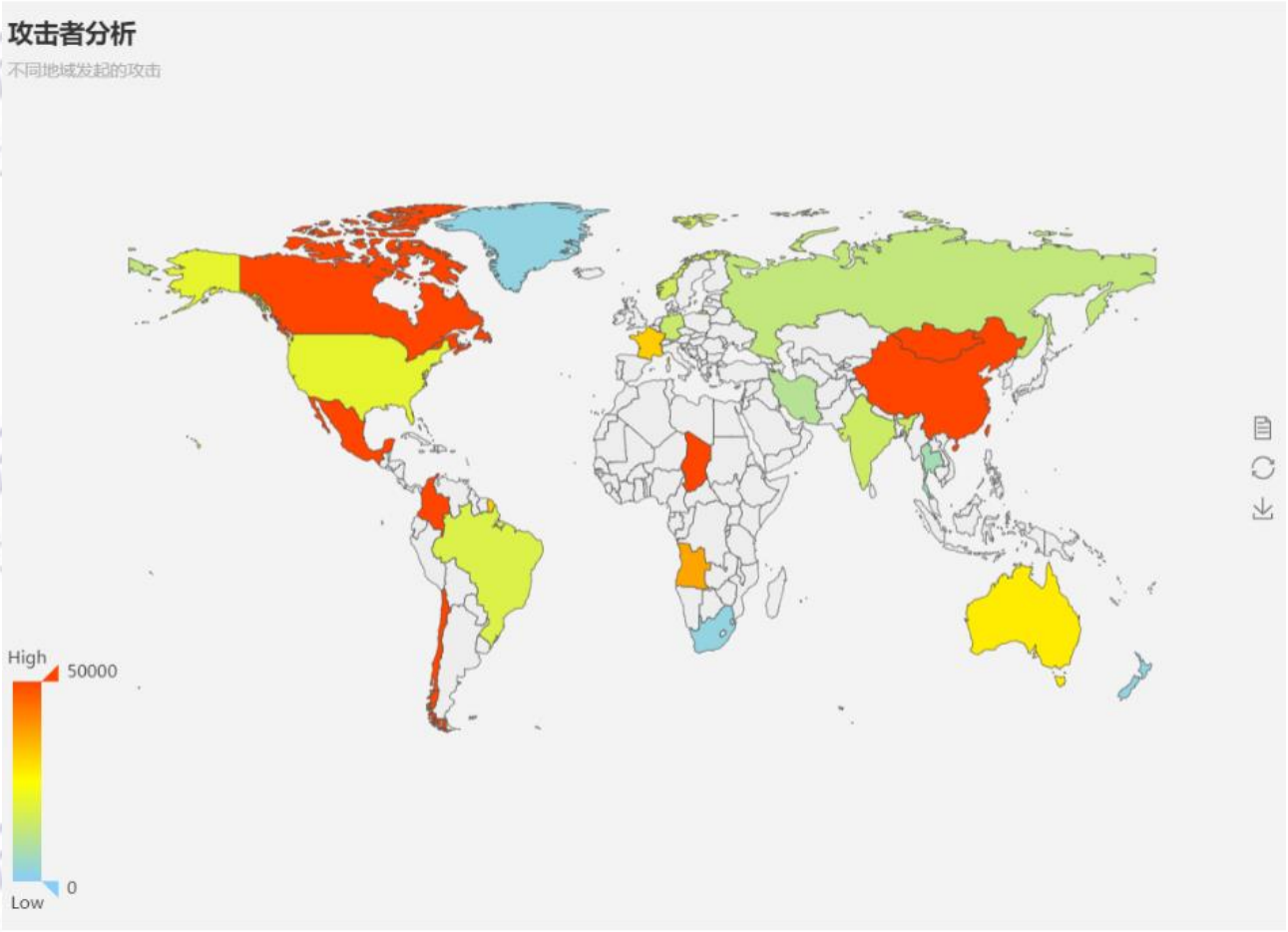


表 2-14 图表总体元素说明

板块名称	说明
攻击者整体展示	**【基本流程】** 1) 用户选择左侧攻击者分析板块的多选框 2) 板块以地图形式呈现，攻击者分布在不同的地域 3) 地图的热度图代表了该区域的攻击强度，色度越接近红色攻击的范围和强度越高 **【规格及限制】** 1) 地图默认显示攻击活动频繁的前10个地区 **【非功能需求】** 2) 初始状态实时显示

2. 地图细节分析

用户鼠标焦点在攻击区域内，弹出详细信息

图 2-15 地图细节展示原型

表 2-15 地图细节展示元素说明

板块名称	说明
攻击者具体显示	**【基本流程】** 1) 默认情况下隐藏 2) 用户鼠标焦点移动到地图区域内弹出详细信息气泡 3) 气泡框展示出该区域攻击者的详细信息如攻击者次数、攻击结果、攻击手段等信息 4) 用户鼠标焦点移出，气泡隐藏 **【非功能需求】** 1） 详细信息简洁精准，展示美观

3. 最新攻击者分析

图 2-16 攻击者详细分析原型表

攻击者	攻击手段	攻击意图	攻击地址	时间
a	DDOS	利用型攻击	美国	2020-08-14 1...
b	渗透	利用型攻击	美国	2020-08-14 1...
c	恶意邮件	利用型攻击	美国	2020-08-14 1...
d	跨站攻击	利用型攻击	美国	2020-08-14 1...

表 2-16 攻击者详细分析表元素说明

板块名称	说明
攻击者具体显示	**【基本流程】** 1) 随着攻击者分析板块出现 2) 当有新的攻击产生，表格信息实时更新 **【规格及限制】** **1)** 地图默认显示攻击活动频繁的前5个地区 **【非功能需求】** 1) 表格信息要求实时性

2.6.4 需求优先级

高

2.7 TOPN攻击行为分析业务需求

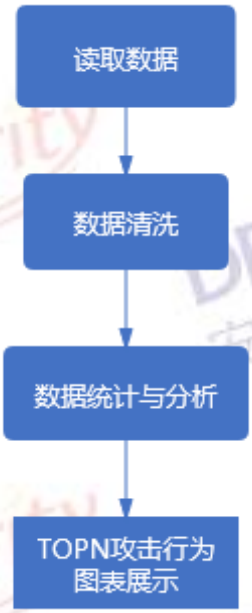
2.7.1 TOPN 攻击行为分析业务描述

用户导入数据，执行程序，后端进行数据处理，从中获取攻击事件的攻击来源、攻击方法、漏洞、安全告警威胁等级、攻击对象、受害对象地区分布等各种信息，经过统计分析，得到不同维度 TOPN 热点攻击事件，并将数据传入前端，前端接受数据生成对应的前端页面，且输出到安全报告中。

2.7.2 业务流程

后端通过对输入的安全日志进行数据读取、清洗，再根据不同维度对数据进行统计与分析，得到不同的 TOPN 攻击事件，并以图表形式展出。

图 2-17 TOPN 攻击行为分析流程图



2.7.3 业务需求功能列表

1. 总体分析

用户导入数据，执行程序，后端分析统计得到不同维度 TOPN 热点攻击事件与攻击事件次数的信息，并将其通过具体数值在安全报告中展示出来。

具体展示以下关系：

1. 不同攻击者(attacker)发起的有效攻击次数 TOPN
2. 不同威胁等级（threatSeverity)的有效攻击次数 TOPN
3. 不同攻击方法(attackMethod)的有效攻击次数 TOPN
4. 不同告警类型（category）的有效攻击次数 TOPN。

2. 详细分析

详细显示不同攻击者、威胁等级、攻击方法、攻击目的城市等有效攻击次数情况，如图 2-18 TOPN 攻击事件展示。

图 2-18 TOPN 攻击事件展示示例

攻击意图	攻击次数	攻击手段
僵木蠕	90	网站恶意链接
跨站攻击	90	恶意链接
灰色软件	83	代码注入
漏洞利用	81	数据库暴力破解
跨站攻击	76	SQL注入

页面各元素说明见表 2-17 任务元素详情。

表 2-17 任务元素详情

页面元素	说明
页面显示	**【内容说明】** 该功能展示： 1. 攻击意图（如漏洞、跨站攻击）的有效攻击次数TOPN； 2. 安全告警等级(高、中、低三级)的有效攻击次数TOPN； 3. 不同攻击方法（如网络钓鱼、邮件欺骗、web漏洞）的有效攻击次数TOPN； 4. 不同告警类型（如DDOS、探测扫描）的有效攻击次数TOPN；

2.7.4 需求优先级

高

2.8 分析说明和处置建议业务需求

2.8.1 分析说明和处置建议业务需求描述

通过对安全日志的分析，从中获取攻击事件的告警类型、攻击对象等信息，经过统计分析，输出对热点告警事件的处置建议，以文字的形式插入到安全报告中。

2.8.2 业务流程

用户导入数据，执行程序，后端分析处理生成安全报告，并将数据传入前端，前端接受数据生成对应的前端页面。通过匹配告警子类型，用户可看到对热点告警事件的分析说明和对应的处置建议。

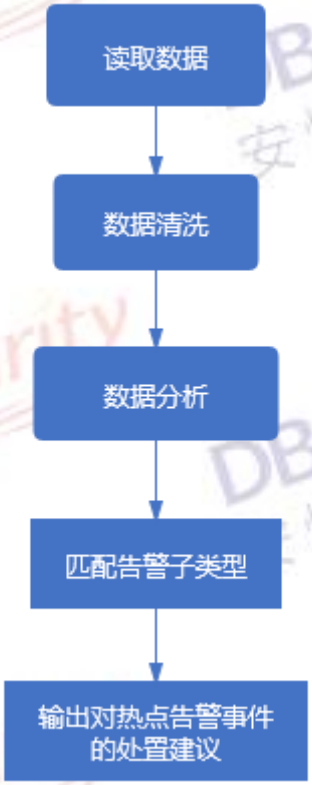


图 2-3 分析说明和处置建议业务流程图

2.8.3 业务需求功能列表

后端通过对安全日志进行读取、清洗、分析，得到关系数据，其中统计得到热点告警事件，匹配告警子类型，输出不同告警子类型对应的处置建议(suggestion)，并以文字形式在后端渲染出的安全报告中展示出来。同时后端提供接口给前端进行调用，在前端页面中也输出对应信息。

1. 分析及建议展示示例

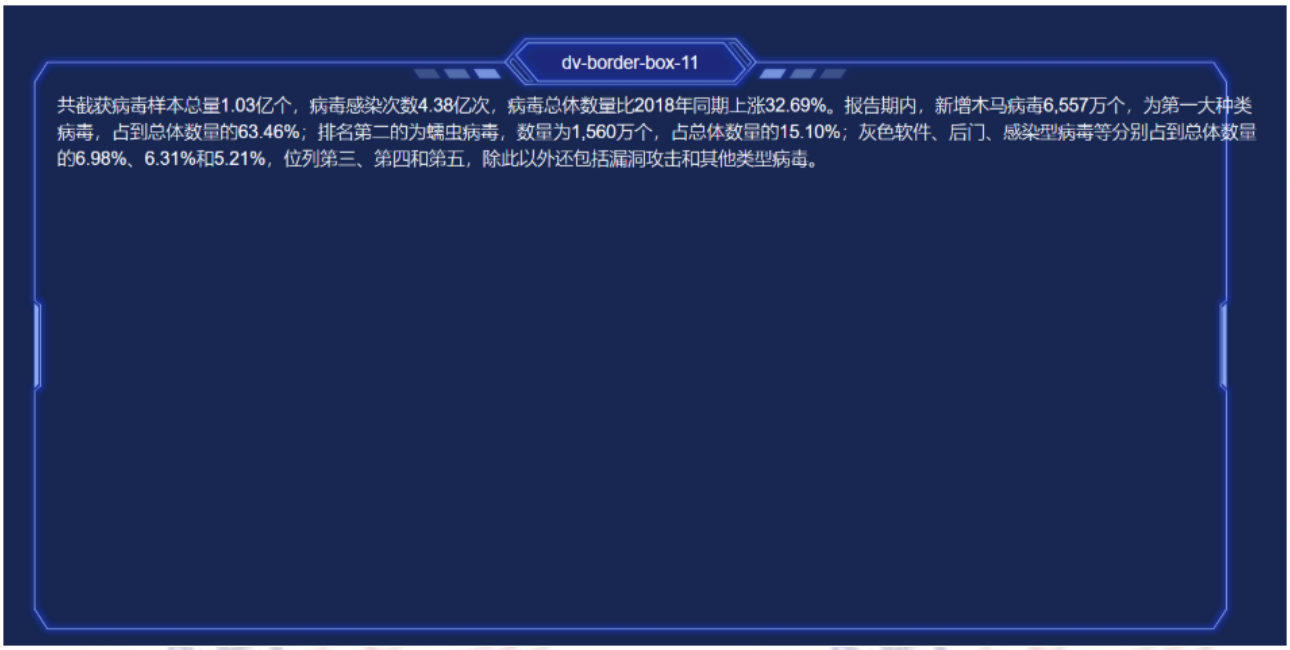


图 2-4 分析和建议结果展示

2.8.4 需求优先级

高

2.9 报告导出业务需求

2.9.1 报告导出业务描述

用户自行选择报告的分析时间范围，从时间范围内筛选信息，点击生成报表重新渲染页面，或者点击导出按钮生成对应的 word 文档。

2.9.2 业务流程

图 2-19 报告导出业务流程图示例

2.9.3 业务需求功能列表

图 2-20 报告导出页面原型图示例

1. 选择时间范围

表 2-18 任务元素详情

元素	说明
时间选择按钮	**【基本流程】** 1) 点击时间输入框，对起始时间进行选择 2) 点击时间输入框，对结束时间进行选择

2. 生成报表

表 2-19 任务元素详情

元素	说明
生成报表按钮	**【基本流程】** 3) 点击生成报表按钮，根据获取的数据重新渲染页面图表

3. 导出报告

表 2-20 任务元素详情

元素	说明
导出报告按钮	**【基本流程】** 4) 点击导出按钮，自动生成word报告文档

2.9.4 需求优先级

高

2.10 网页展示业务需求

2.10.1 网页展示描述

大屏页面实时显示系统当前的风险情况。

2.10.2 业务流程

页面显示当前系统中的整体数据时序分布、风险资产分布、受害者分析、攻击者分析、TOPN 攻击行为分析、分析说明以及处置建议数据。

2.10.3 业务需求功能列表

暂无整体展示页面图。

表 2-21 页面说明

页面元素	说明
页面显示	**【基本流程】** 5) 页面显示以下内容 a) 标题显示为：安全报告分析生成平台 b) 标题后面平台描述 c) 左侧从上而下数据时序分布趋势图、资产分布图、高风险资产陈列表、 d) 中间显示受害者或攻击者分析：包括被攻击次数、地理位置、被攻击来

	源等 e) 右侧从上而下显示TOPN排行表、分析以及处置建议 6) 按上图所示的布局显示 **【扩展流程】** 1) 页面中相关的数据每隔1小时到后台取1次，事件相关的数据每隔5分钟到后台取1次 2) 界面上所有轮播的地方每隔30秒切换显示

2.10.4 需求优先级

高

3 其他非业务需求

3.1 性能需求

所有页面响应时间不超过 3 秒。

程序运行过程中后台占用系统资源情况。

3.2 用户界面需求

界面要求用户导出数据方便、快捷、有较详细的操作说明和指导。

界面操作要求简单易用友好。

不同尺寸显示器、不同分辨率下要求显示友好。

同级菜单字体、大小统一。

相同功能的按钮名称、格式统一。

3.3 模块化需求

新需求数据需要模块化，需要与现有平台数据隔离，如果有数据共用通过接口实现。

3.4 浏览器兼容性需求

支持 IE11 及以上版本

支持 chrome48 及以上版本

支持 firefox44 及以上版本
支持 360 v8 及以上版本
支持 safari v8 及以上版本

3.5 数据库存储量要求

以一年时长存储为例：

表 3-21 数据库储存量说明

项目	说明
分析日志数量：1000000	按工作日平均每天分析10w条日志，一年250个工作日计算
任务执行次数（导出报告数量）：450000	按每个子任务平均执行20次计算
攻击者分析数量：2200000	按每个扫描报告中包含5个攻击者计算
受害者分析数量：1800000	按每个扫描报告中包含4个攻击者计算

3.6 其它

需要考虑后续版本在线升级。
自身操作日志记录，且每个模块的操作日志格式统一。