安恒信息
DAS-security 安全中国

明御®APT 攻击预警平台

用户手册

目 录

前言

概述

感谢您选择安恒信息的网络安全产品。明御®APT 攻击预警平台（简称“APT”或“平台”）通过对网络中的流量进行解析，发现其中的攻击事件。利用网络流量分析技术、异常访问定位技术、基于 Web 的攻击检测技术、恶意文件分析技术及云端的高级分析技术来综合分析检测发现 APT 攻击，大大提高了 APT 攻击的成功检测率和减少了误报情况。

本手册描述明御®APT 攻击预警平台产品用户使用过程中常用的操作和配置。

手册所提供的内容仅具备一般性的指导意义，并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号、配置文件不同等原因，手册中所提供的内容与用户使用的实际设备界面可能不一致，请以用户设备界面的实际信息为准，手册中不再针对前述情况造成的差异一一说明。

出于功能介绍及配置示例的需要，手册中可能会使用 IP 地址、网址、域名等。如无特殊说明上述内容均为示意，不指代任何实际意义。

预期读者

本文档主要适用于期望了解明御®APT 攻击预警平台的读者，包括服务工程师、系统管理员、网络管理员等。本文假设读者对以下领域的知识有一定了解：

- 网络安全相关知识，包括 APT、DDoS、SQL 注入、目录遍历、暴力破解等常见攻击原理及防护手段。
- 安全防护策略、NAT 地址转换、VPN、各类路由协议的基本工作原理和配置。

格式约定

本手册内容格式约定如下。

内容	说明
粗体字	Web 界面上的菜单、页签、页面名称、窗口名称、对话框名称，例如：“在菜单栏中选择**系统状态**进入**系统状态**页面，选择**接口状态**页签。”
< >	Web 界面上的按钮名称、复选框名称、文本框名称、选项名称等。例如：“微信认证失败，点击<**我要上网**>不弹出微信认证界面”。
➤	介绍 Web 界面的操作步骤时，用于隔离点击对象（菜单项、子菜单、按钮以及链接等），例如：“在菜单栏选择‘**策略配置➤认证管理➤认证策略**’查看是否开启了认证策略”。
斜体字	可变参数，必须使用实际值进行替代。例如：“在浏览器地址中输入‘http://*管理 IP*’，回车后进入系统 Web 管理平台登录页面”。

本手册图标格式约定如下。

图标	说明
	提示，操作小窍门，方便用户解决问题。
	说明，对正文内容的补充和说明。
	注意，提醒操作中的注意事项，不当的操作可能会导致设备损坏或者数据丢失。
	警告，该图标后的内容需引起格外重视，否则可能导致人身伤害。

获得帮助

使用过程中如遇任何问题，请致电服务热线 400-6059-110。

请访问安恒社区 https://bbs.dbappsecurity.com.cn/获取更多文档。

联系信息

地址：浙江省杭州市滨江区西兴街道联慧街 188 号安恒大厦

邮编：310052

电话：0571-88380999

传真：0571-28863666

官网：http://www.dbappsecurity.com.cn

邮箱：400-doc@dbappsecurity.com.cn

1. 快速入门

APT 攻击（Advanced Persistent Threat），即高级可持续威胁攻击，其危害及隐蔽性越来越高，一些涉密部门是被攻击的重点目标。当前的检测工具如杀毒软件、防毒墙、IPS、IDS、防火墙等设备的检测大多基于已知安全漏洞及恶意代码特征的部分攻击行为，无法检测利用 0day 漏洞进行渗透的攻击。

明御®APT 攻击预警平台通过对网络中的流量进行解析，发现其中的攻击事件。利用网络流量分析技术，异常访问定位技术、基于 Web 的攻击检测技术、恶意文件分析技术及云端的高级分析技术来综合分析检测发现 APT 攻击，提高 APT 攻击的检测成功率并减少误报。

1.1 产品特点

1.1.1 部署特点

- 系统使用旁路部署方式，不影响被检测网络的和服务器的正常运行。
- 可进行集群部署，方便系统性能提升。
- B/S 管理架构，使用简单。

1.1.2 检测功能

- 使用包括沙箱、智能分析引擎、威胁情报等检测技术多维度预警 APT 攻击。
- 使用综合行为分析关联并呈现更深层次的攻击行为。
- 支持 Web 等协议的快速解析。
- 内置大量安全检测策略，全方位满足不同用户的使用需求，安装调试简单便捷。
- 云端大数据分析，基于机器学习和深度挖掘等技术，实时共享最新安全威胁情报，快速预警新型恶意威胁。

1.2 产品功能

明御®APT 攻击预警平台具有以下八大功能模块。

一、导航

分为导航、失陷主机、攻击溯源三个页面，用于展示各类告警信息。

- 导航包括：攻击展示图、紧急事件总数、24 小时紧急事件、各阶段风险等级的统计、攻击源区域排名、高危风险类别和恶意文件总量。
- 失陷主机是对失陷主机事件、回连区域进行统计、最新事件等，并且通过图形化界面展示。
- 攻击溯源对攻击主机个数最多的情报事件、情报事件类型分布、威胁活动、情报事件攻击进行展示。

二、分析

主要包括分析（紧急事件分析、主机威胁分析、失陷主机分析、情报事件分析、攻击者视角分析、受害者视角分析、脆弱性分析、流量统计、统计分析、登录行为分析、抓包分析、PCAP 文件上传、威胁情报检索）、文件分析（文件威胁分析、回连域名/IP、文件审计、文件上传）、域名分析（受感染主机、C&C 服务器、高频访问同一域名）等功能以及文件审计和规则配置功能。

三、风险

对不同类型、级别的风险进行查询和处理。

四、资产

通过对流量中的 IP 地址、端口等进行统计，对网络资产进行主动发现 并快速识别未登记资产，可基于特定应用或服务对内部资产进行梳理（系统类型、IP、域名、端口等），查看资产端口暴露情况，特别是以非标端口提供的服务情况。

五、报表

提供综合威胁分析报告、主机威胁分析报告、文件威胁分析报告和外部威胁分析报告四种类型的报表，支持报表导出功能（导出格式分为 HTML、PDF、Word 三种），可定时发送天、周、月报表。

六、探测器

探测器主要用于监听各种类型的业务操作，完成数据采集和分析任务。

数据中心可以对子探测器进行同步验证。

七、配置

配置功能包括常规配置（设备自身运行相关的基本配置）、检测配置、联动配置、数据外送（NTP 模式）等功能。

八、系统

系统菜单功能主要包括权限管理（用户安全设置、IP 访问控制等）、数据维护（出厂设置）、系统资源、升级管理（手动升级、云端配置等）、许可证、日志管理及其他功能配置（SNMP 配置、网络配置等）。

1.3 角色与权限说明

系统缺省的四种角色和用户如下所示。

用户	角色	对应菜单权限	初始密码
admin	超级管理员	系统所有权限	Dbapp@2014
analyzer	风险查看员	具有首页、分析、风险、报表等菜单权限	Dbapp@2014
config	配置管理员	具有探测器和配置等菜单权限，包括配置引擎、策略、探测器、风险通知等	Dbapp@2014
system	系统管理员	具有系统菜单权限，拥有系统级别的配置、权	Dbapp@2014

用户	角色	对应菜单权限	初始密码
		限管理等操作权限	

1.4 登录系统

操作前提

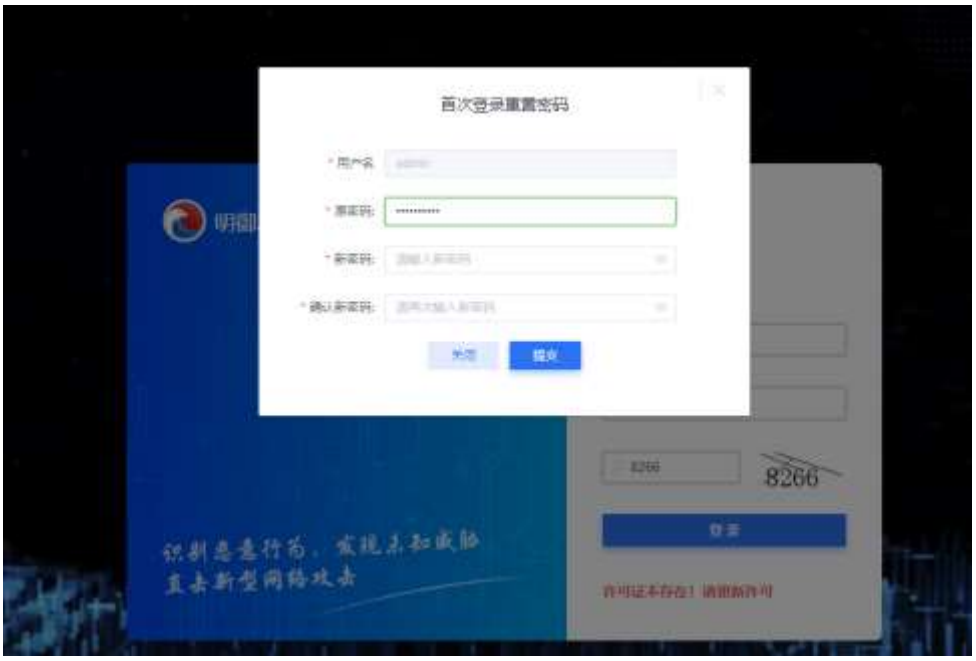
- 用户已经获取 APT 的访问网址。
- 用户已经获取系统登录账号以及账号密码。系统默认的用户名和密码为 **admin** 和 **Dbapp@2014**。

操作步骤

步骤1. 打开浏览器，输入 APT 访问地址（APT 设备的网络主机 IP）并回车。

为实现最佳浏览效果，建议使用最新版 Chrome 浏览器或者火狐浏览器。

步骤2. 进入登录页面，输入用户名、密码、验证码进行登录。



初次登录后参考界面提示进行修改密码操作，且密码不能设置为初始密码。

步骤3.　配置当前位置所在城市，添加方式请参考地理位置设置。

1.5 产品形态

APT 有三种产品形态：APT 模式、独立沙箱模式和 PTS 模式。独立沙箱模式和 PTS 模式产品形态见对应产品的*用户手册*。

登录成功后，默认进入导航页面，显示 APT 检测到攻击事件的统计和大致分布情况，如下图所示。

1.6 设备身份

部署单台 APT 设备，系统默认设备身份是数据中心（探测器）。

分布式部署场景下，需要用户使用串口方式设置设备身份。具体操作请参考《明御®APT 攻击预警平台 V2.0.67 快速部署手册》。

设备身份主要有三类：

- 数据中心：在新增探测器时，会把对应的探测器进行出厂设置，然后将数据中心全局配置同步到探测器上。
- 探测器：负责采集数据信息，采集到数据信息后，会把对应的风险信息、报表信息等都上传到数据中心。
- 数据中心（探测器）：具有数据中心和探测器的双重功能。

用户在不同身份的设备上可见的功能页面及操作权限不同，请参考下表。

设备身份	权限说明	菜单功能分配
数据中心（探测器）	拥有所有系统的操作权限且自身会采集数据	导航、分析、风险、资产、报表、探测器、配置、系统
数据中心	拥有所有系统的操作权限但自身不采集数据	导航、分析、风险、资产、报表、探测器、配置、系统
探测器	仅有采集数据权限	导航、分析、风险、资产、报表、探测器(仅查看)、系统

查看当前设备身份

点击 APT Web 界面右上角“**admin**”图标，在弹出的菜单中选择“**当前设备身份**”查看当前设备的身份信息。


明御APT攻击
预警平台

2. 导航

2.1 导航页面

用户登录系统后，默认进入导航页面。该页面主要对各种类型的告警数据进行统计分析，并通过图形化方式展现。

导航页面主要分为以下 8 个区域：1.统计信息、2.风险趋势、3.流量分析、4.攻击展示、5.高危风险识别、6.攻击源区域排名、7.紧急事件/高危事件、8.语音告警。

2.1.1 统计信息

导航页面左侧的**统计信息**（区域 1）显示统计周期内发现的紧急事件数，包括紧急事件总数和未处理事件总数；以及恶意文件数，包括恶意文件总数和已扫描文件总数。

统计周期默认为 24 小时，鼠标移到“最近 24 小时”可切换不同的统计周期。

如果统计信息中显示的紧急事件数或恶意文件数不为 0，表示用户网络环境中存在紧急安全事件或恶意文件，应尽快对感染主机进行安全防护。

- 点击**紧急事件数/总数**下方数据列出全部紧急事件，或点击**恶意文件数/扫描总数**下方数据列出全部恶意文件。
- 点击单条紧急事件或恶意文件查看详情。
- 如果确认已经处理完毕，在弹出窗口中点击<**处理**>关闭选中的紧急事件或恶意文件，如下图所示。

2.1.2 风险趋势

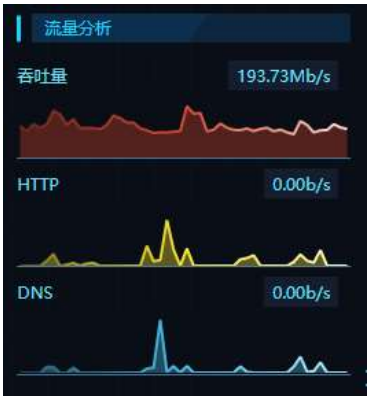
导航页面左边**风险趋势**（区域 2）显示统计周期内各阶段风险的总数和走势图，方便用户了解风险告警的走势情况。

折线图中蓝色表示低风险，橙色表示中风险、红色表示高风险，如下图所示。

点击各阶段风险下方的数据可以展示全部风险信息，点击单条风险信息查看详情并进行处理。

2.1.3 流量分析

流量分析（区域 3）从吞吐量、HTTP、DNS 三方面显示当前实时流量情况。



2.1.4 攻击展示

攻击展示（区域 4）通过分析 APT 捕获到的攻击行为，结合相关坐标信息，以图形化方式展示最新的攻击行为，包括攻击源与攻击目标等信息。点击攻击路线可展示统计周期内该攻击路线发生的高风险事件。

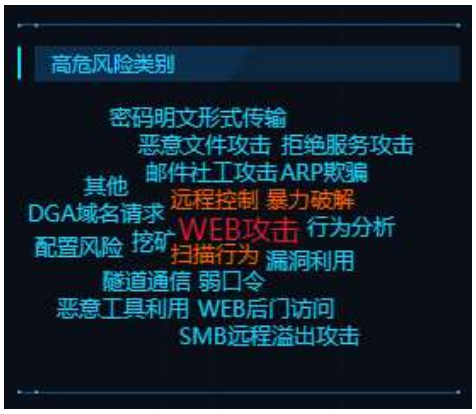
攻击展示图每隔 5 分钟刷新一次，只显示高风险的攻击行为。

点击单条风险事件查看详情并进行处理。

2.1.5 高危风险类别

高危风险类别（区域 5）展示统计周期内的高危风险攻击的所有类别，点击风险类别名称展示统计周期内

该风险类别的所有统计事件。



点击单条事件查看详情并进行处理。

2.1.6 攻击源区域排名

攻击源区域排名（区域 6）展示统计周期内风险事件最多的 6 个攻击源区域（国外数据大于 3 条时会显示国内 3 条+国外 3 条）。点击攻击源区域名称会显示指定攻击源区域在统计周期内的全部风险数据。

点击单条事件查看详情并进行处理。

2.1.7 紧急事件/高危事件

如果在统计周期内没有发生紧急事件，**紧急事件/高危事件窗**（区域 7）会显示最新 12 条聚合高危事件数据，手动刷新页面更新数据。

点击单条紧急事件或高危事件查看详情并进行处理。

2.1.8 语音告警

默认关闭，可在配置页面 语音告警打开。

语音播报在导航页面中心处，实时展示符合语音告警的信息。点击语音告警实时列表，可查看该风险的原始风险数据。

点击  关闭按钮可在导航处不展示实时播报的情况，点击右下角的  可恢复展示语音实时播报情况。

点击右下角的告警播报  ，显示统计周期内所产生的语音告警，展示了语音告警的发生时间、风险类型及风险等级、探测器名称、播报状态。点击风险名称可查看该风险的详细信息

2.2 失陷主机页面

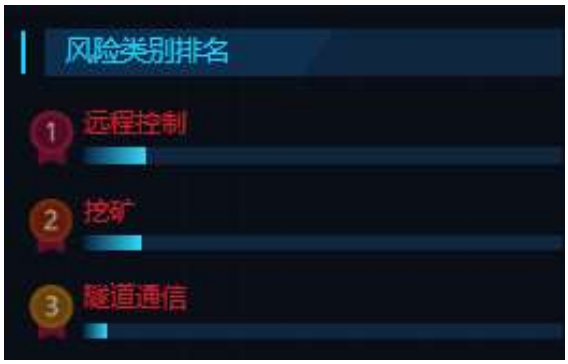
在系统菜单栏点击“**导航**”菜单下拉框，选择”**失陷主机**”切换到失陷主机页面。

失陷主机页面对失陷主机事件、回连区域进行统计，通过图形化界面展现最新安全事件。页面默认 5 分钟刷新一次。

失陷主机页面主要分为以下 7 个区域：1.风险类别排名、2.回连区域排名、3.风险事件、4.失陷主机 IP/黑客组织、5.失陷主机事件、6.最新事件、7.失陷主机数。

2.2.1 风险类别排名

风险类别排名（区域 1）展示统计周期内失陷主机相关的风险类别排名。



点击各类风险排名柱状图展示统计周期内指定类别风险的事件总数、趋势图以及最新的 8 条事件信息。

点击单条风险事件查看详情并进行处理。

2.2.2 回连区域排名

回连区域排名（区域 2）统计 DNS 流量下对恶意域名进行回连的区域排名。

点击回连地区可展示统计周期内该地区发生的回连事件列表，点击单条回连事件查看详情并进行处理。

2.2.3 **风险事件**

左侧圆环（区域 3）外环以**失陷主机**为视角，展示以失陷主机为事件类型的**风险事件**，其中外圈展示威胁情报事件，内圈展示非威胁情报事件。

失陷主机分布在亚洲、美洲、非洲、欧洲四个大洲对应的 1/4 圆环中。如果一个失陷主机多次受同一大洲地区（如日本、韩国）的攻击，默认展示最后一次发起攻击地区；如果一个失陷主机多次受不同大洲地区（如韩国、法国）的攻击，则分别在亚洲、欧洲两个地区中展示对应的信息。

圆环内每个矩形方块代表一个事件，鼠标悬停在矩形方块上会显示失陷主机的 IP 和攻击源区域。

左侧圆环（区域 3）内环以**横向攻击**为视角，展示以横向威胁为事件类型的风险事件。横向攻击视角外圈展示攻击状态为“**尝试**”的 IP，内圈展示攻击状态为“**成功/失陷**”的 IP；圆环中心的数字表示统计周期内横向攻击事件的攻击者 IP 总数。

圆环内每个矩形方块代表一个事件，鼠标悬停在矩形方块上会显示攻击状态和攻击者 IP。该 IP 在攻击状态相同时默认只展示 1 次。

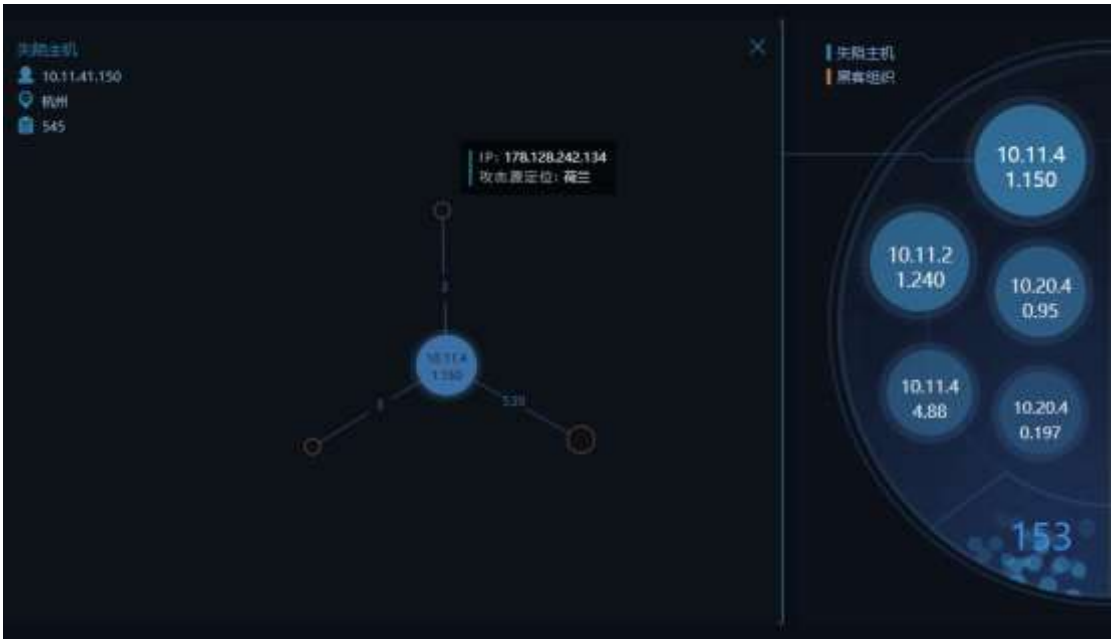
2.2.4 失陷主机 IP/黑客组织

右侧圆环（区域 4）左半部分默认展示遭受攻击最多前五位的失陷主机 IP，IP 地址下面的数字表示统计周期内失陷主机 IP 数量。

右侧圆环（区域 4）右半部分展示失陷主机事件的名称，默认展示攻击事件前五位的黑客组织名称。名称下面的数字表示统计周期内失陷主机事件原始数据的总数。

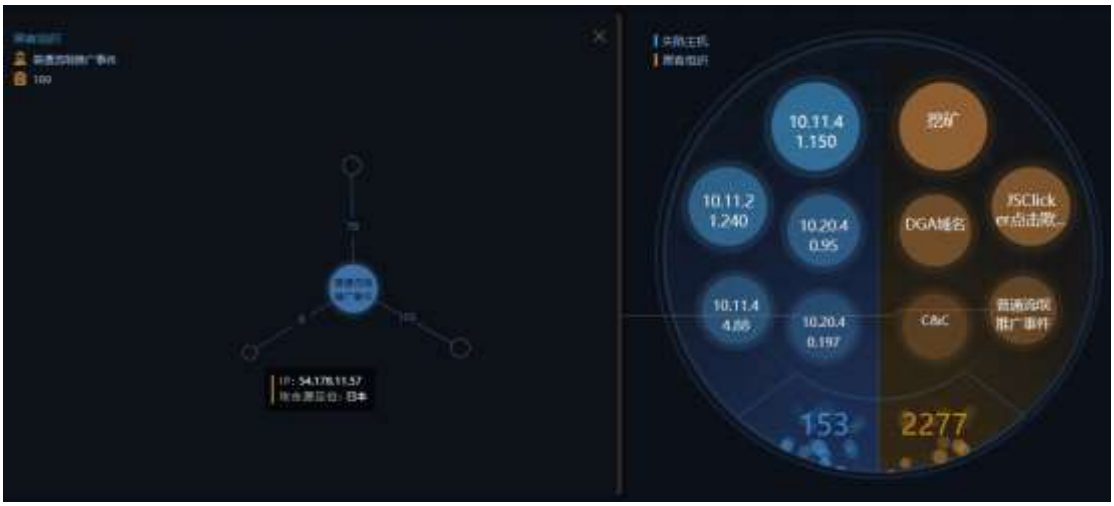
鼠标点击左半部分的 IP，在滑出窗口展示以下信息：

- 左上角展示失陷主机的 IP、被攻击源地区、被攻击总次数等。
- 下方展示失陷主机的被攻击关系图，关系图上的节点表示攻击者，节点之间的数字表示攻击次数。
- 鼠标悬浮在攻击源的节点上显示攻击源的 IP、地区，如下图所示。



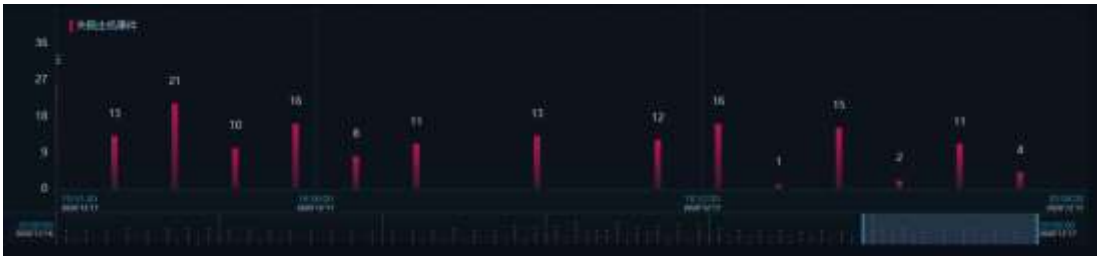
鼠标点击右部分的黑客组织事件，在滑出窗口展示以下信息：

- 左上角展示失陷主机的黑客组织/病毒家族名称、攻击事件总数。
- 下方展示失陷主机事件的攻击关系图，关系图上的节点表示被攻击者，节点之间的数字表示攻击次数。
- 鼠标悬浮在节点上显示攻击源的 IP、地区，如下图所示。



2.2.5 失陷主机事件

失陷主机事件（区域 5）以柱状图形式展示统计周期内各阶段失陷主机聚合事件的次数。



点击柱状图或柱状图上的数字展示该时间段的所有失陷主机事件列表，点击单条事件查看详情并进行处理。

2.2.6 **最新事件**

最新事件（区域 6）展示最近 9 条失陷主机事件。左侧的竖线表示风险等级：蓝色表示低危，黄色表示中危，红色表示高危。

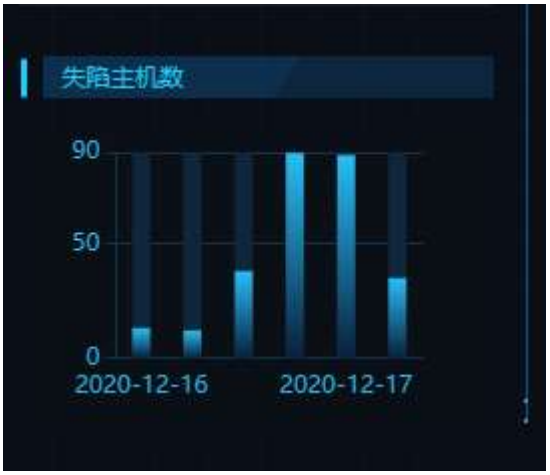
事件部分展示风险详情、事件名称、发生时间。

点击单条事件展示风险名称、域名、攻击者 IP、攻击源地区、受攻击者 IP、发生时间等详细信息。

2.2.7 失陷主机数

失陷主机数（区域 7）以柱状图形式展示统计周期内各时间段的失陷主机数量。

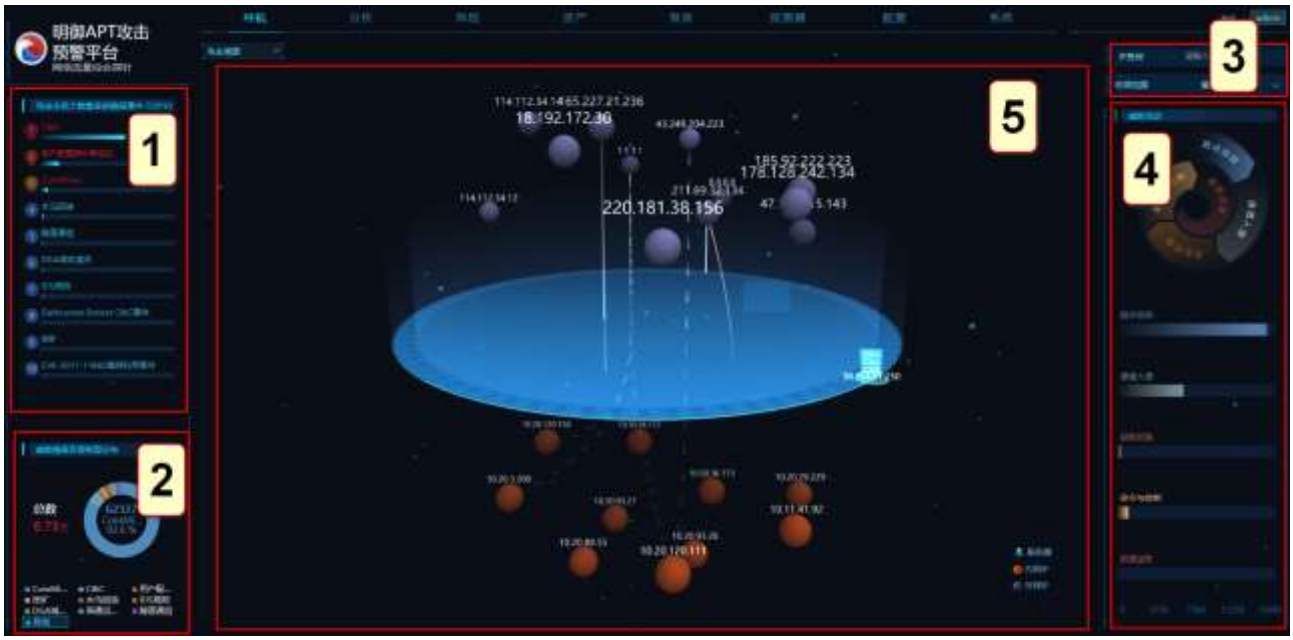
鼠标悬浮在柱状图上显示具体时间段和该时间段内的失陷主机数量。



2.3 攻击溯源页面

在系统菜单栏点击“**导航**”菜单下拉框，选择“**攻击溯源**”切换到攻击溯源页面。

攻击溯源界面展示 APT 攻击的溯源信息，主要分为以下 5 个区域：1.攻击主机个数最多的情报事件 TOP10、2.威胁情报告警类型分布、3.IP 查询、4.威胁活动、5.3D 展示。



2.3.1 攻击主机个数最多的情报事件 TOP10

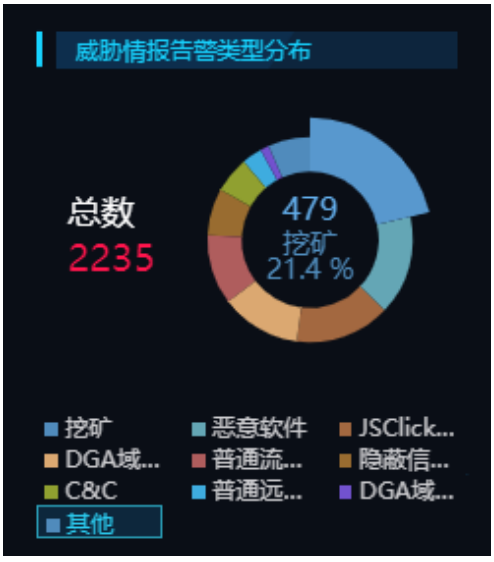
攻击溯源页面左上角（区域 1）展示统计周期内发起攻击次数最多的情报事件，最多展示 10 条。

点击柱状图展示统计周期内该情报事件聚合的 IP 风险信息，点击 IP 展示该 IP 相关的风险详情列表，点击单条风险查看详细信息并进行处理。

2.3.2 威胁情报告警类型分布

威胁情报告警类型分布（区域 2）从事件角度展示失陷主机各情报事件的占比。左侧数字为统计周期内各类情报事件的总数，圆环中间展示各类情报事件在统计周期内发生的总数、名称、占比。

默认展示情报事件统计周期内发生次数前 9 位情报事件类型，低于前 9 位的事件类型将全部统计为“其他”。



点击情报事件对应的圆环展示统计周期内该类型情报事件的风险信息列表（基于 IP 地址），点击 IP 展示该 IP 在统计周期内的情报事件信息，点击单条事件查看风险详情并进行处理。

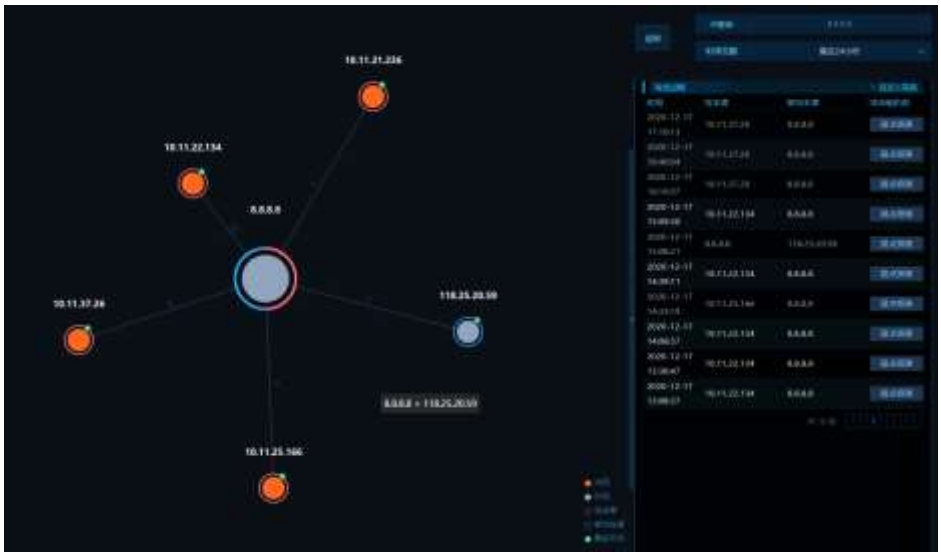
如果统计周期内记录的情报事件类型超过 9 类，点击饼图下方<**其他**>展示统计周期内所有情报事件的名称、发生次数以及占比，默认保留 1 位小数。

2.3.3 IP 查询

攻击溯源页面右上角（区域 3）展示 IP 查询框和时间范围。查询时间范围默认为最近 24 小时，可选择最

近 7 天、最近 1 个月、最近 2 个月。

在 IP 搜索栏输入 IP 或者在下拉框中选择 IP 进行搜索。左侧搜索结果关系拓扑图中蓝色外圈表示被攻击者，红色外圈表示攻击者，半蓝半红表示既是攻击者又是被攻击者，IP 之间的数字表示攻击次数。

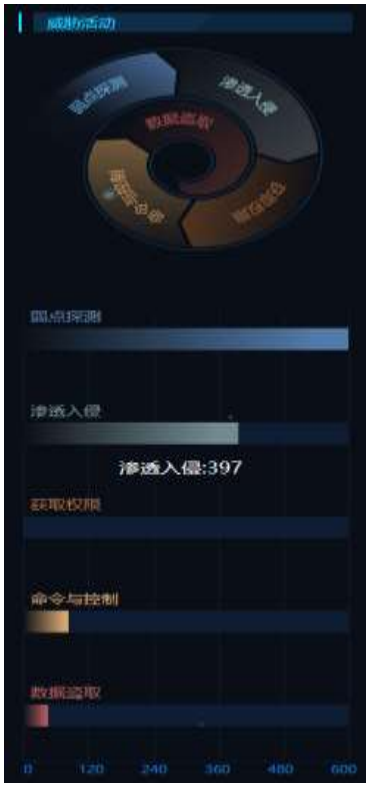


右侧列表显示所有匹配的搜索结果 (基于攻击过程的时间倒序) , 点击查看每个攻击过程的相关风险列表，点击单条风险查看风险详情并进行处理。

2.3.4 威胁活动

威胁活动（区域 4）以攻击链的形式，基于弱点探测、渗透入侵、获取权限、命令与控制、数据盗取 5 个节点对攻击事件进行归纳汇总。

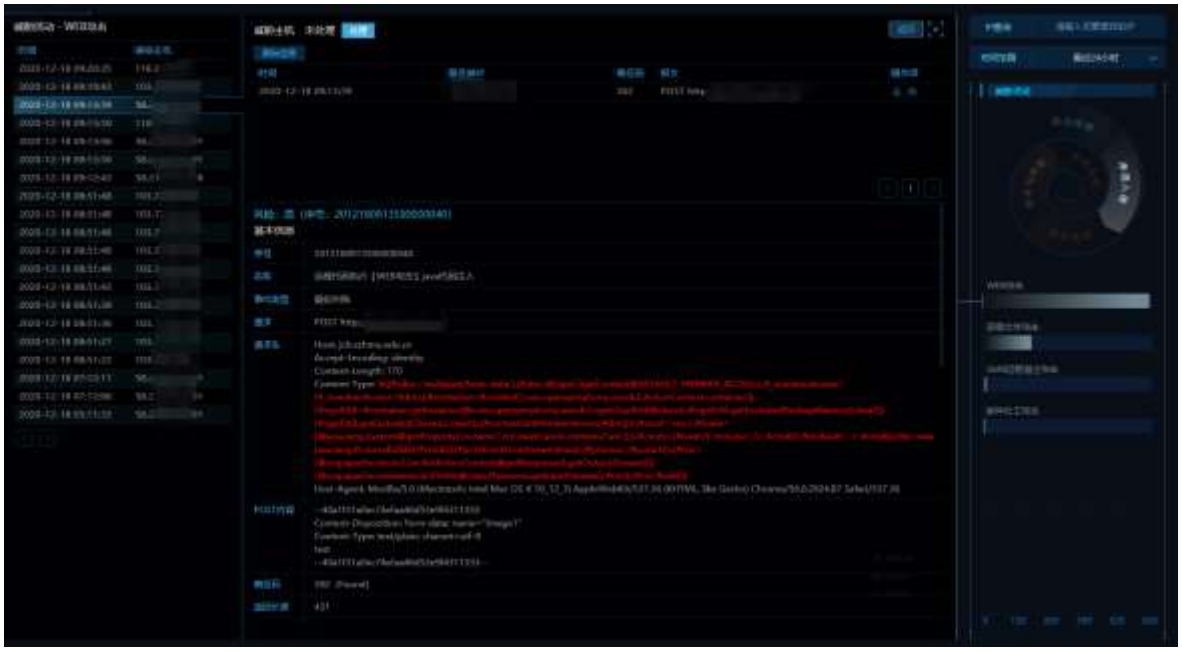
鼠标悬浮在威胁活动的柱状图上，显示不同攻击阶段名称和该阶段在统计周期范围内发生的告警总数。



鼠标点击威胁活动的柱状图，显示选中攻击阶段的所有风险类别名称；鼠标悬停在风险类别名称柱状图上，

显示该风险类别名称和统计周期范围内该风险类别下发生的告警总数。

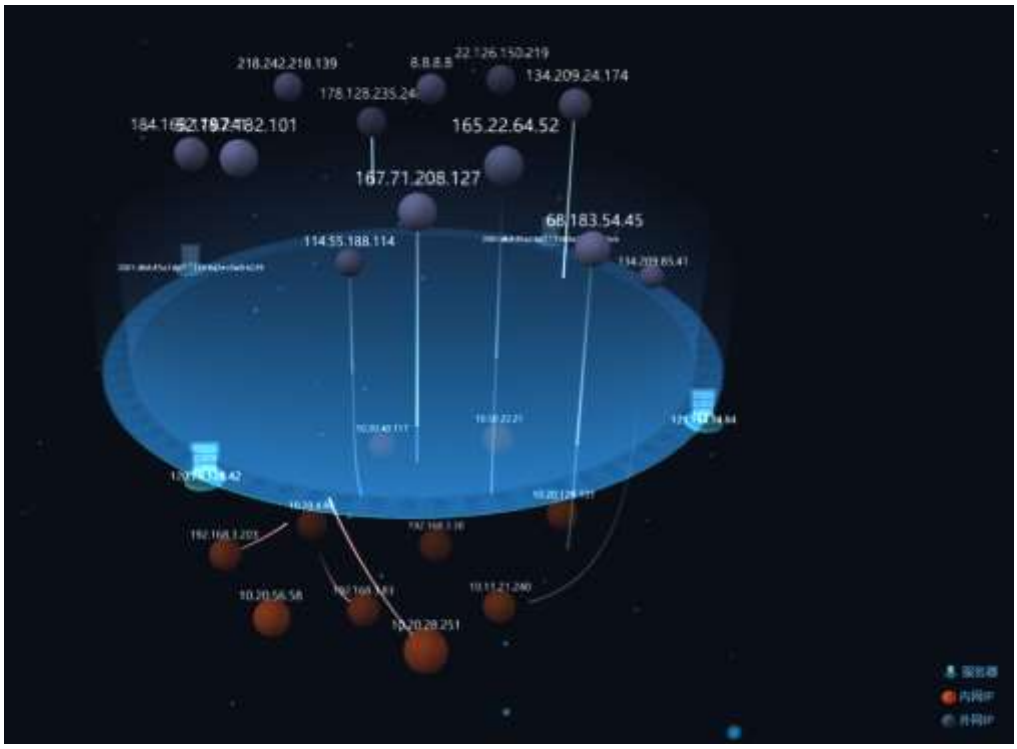
点击风险类别名称的柱状图显示统计周期范围内该风险类别下产生的所有风险信息列表，点击单条风险信息查看详情并进行处理。



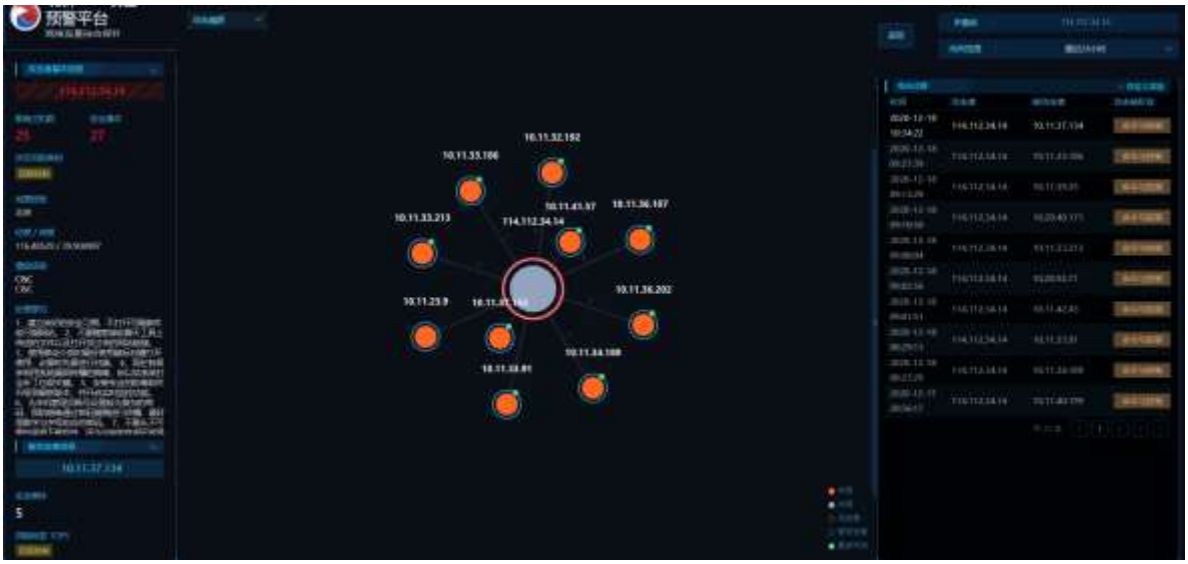
2.3.5 3D 展示

失陷主机页面中间的 3D 图形（区域 5）展示统计周期内 IP 间的攻击关系。上方紫黑色小球表示外网 IP，中间的图形表示服务器 IP、下方橙色小球表示内网 IP。默认展示攻击/被攻击次数最多、攻击方式最多或威胁等级最高的 IP 地址。外网 IP 最多展示 12 个，服务器 IP 最多展示 6 个，内网 IP 最多展示 10 个。

IP 之间的连线表示攻击者与被攻击者的关系，实线表示直接攻击，虚线表示间接攻击。



点击 IP 图标展示该 IP 相关攻击事件详情，包括攻击/被攻击事件关系拓展图、攻击者/被攻击者信息、攻击过程等。



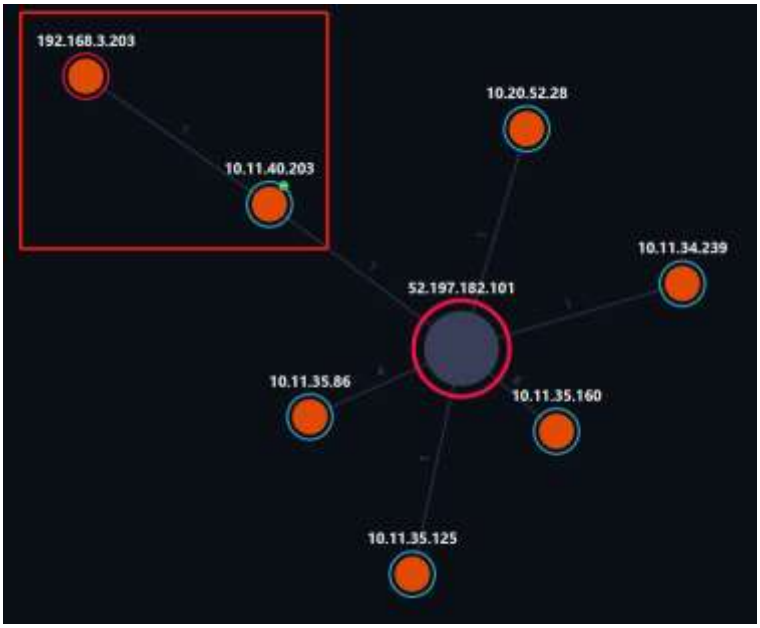
2.3.5.1 攻击/被攻击关系拓扑图

拓扑图展示攻击者和被攻击的基本信息，图中蓝色外圈表示被攻击者，红色外圈表示攻击者，半蓝半红表

示既是攻击者又是被攻击者，IP 之间的数字表示攻击次数。

点击攻击路线显示“**攻击者 IP➤被攻击者 IP**”，同时左侧展示对应攻击者和被攻击者基本信息，右侧展示这两个 IP 间的攻击事件。

IP 存在扩展攻击行为时，IP 外圈的右上角会编辑有图标。双击可向下扩展一层，同时图标变为，最多可以扩展两层；点击图标隐藏扩展的攻击路线，同时右上角变成展示之前的拓扑图。



2.3.5.2 攻击者基本信息

攻击者基本信息展示攻击者 IP、影响的内网主机数、攻击产生的风险事件、风险类别、地理位置、经纬度、匹配到的情报信息、处理建议等。内容超长时，会显示为下拉框形式，如下图展示。

点击右上角的图标展示统计周期内攻击者 IP 相关的攻击事件列表。

点击单条事件查看详情并进行处理。

2.3.5.3 被攻击者信息

被攻击者基本信息展示被攻击者的 IP、被攻击的事件数、被攻击产生的风险类型等。

点击右上角的展示统计周期内被攻击者 IP 相关的攻击事件列表。

点击单条事件查看详情并进行处理。

2.3.5.4 攻击过程

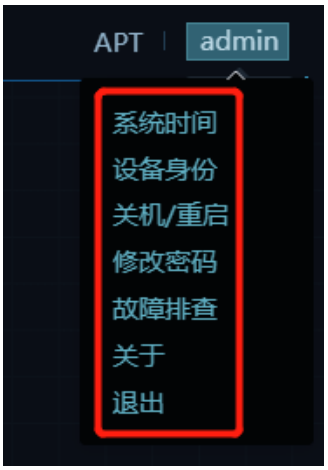
右侧默认展示攻击全过程，包括事件发生时间、攻击者 IP、被攻击者 IP、攻击链阶段。

点击左侧扩展攻击过程展示区，展示风险标签、攻击次数、攻击状态等更多详细风险信息。

点击右上角的<**自定义筛选**>筛选在攻击过程中显示的攻击链阶段。

2.4 主页 admin 菜单介绍

点击 APT Web 界面右上角<**admin**>（或其他登录用户名），弹出对应的功能菜单，如下图所示。



将鼠标悬停在“系统时间”、“设备身份”上显示相关信息，或点击“关机/重启”、“修改密码”、“故障排查”“关于”、“退出”执行相关操作。支持点击“故障排查”前往拍错页面。

菜单	功能描述
系统时间	可查看 NTA 服务器的系统时间。
设备身份	显示当前设备的身份。
关机/重启	关机或重启设备。
修改密码	修改当前用户的密码。
故障排除	进入故障排查登录页面。
关于	查看当前版本信息。
退出	退出系统。

3. 探测器

3.1 查看管理口 IP

管理口配置一般在 APT 快速部署的时候，通过串口程序 **1->1** 菜单完成，选择管理口设备及修改管理口 IP 地址。详细配置信息请参考对应版本的*快速部署手册*。

此外，可以通过 Web 界面配置管理口，详细请参考 Web 界面配置管理口。

在主菜单选择“**探测器**”，可以查看管理口 IP。

如下图所示，管理口为 *eth0*，管理口 IP 为 *192.168.33.236*。

3.2 探测器配置

探测器配置功能用于管理属于该数据中心的探测器，包括新增探测器、修改探测器及删除探测器。

3.2.1 新增探测器

在**探测器**页面，点击<**新增**>，在弹出的页面输入探测器名称、IP、端口，点击<**确定**>进行保存。

参数说明

参数	参数解释	是否必选
名称	输入探测器的名称。	是
探测器 IP	输入探测器设备的 IP。	是
探测器端口	输入探测器的端口。	是
发送最大速率	配置探测器的发送最大速率。一般使用缺省值。	是
发送主目录	配置探测器的发送主目录。一般使用缺省值。	是
发送时间段	配置探测器的发送时间段。一般使用缺省值。	是

新增探测器必须保证探测器的 sensor 版本和数据中心的 server 版本一致，否则会添加失败。

3.2.2 修改/删除探测器

在**探测器**页面，点击新增探测器右边的 图标编辑探测器配置项；点击新增探测器右边的 图标删除探测器。

3.2.3 升级探测器

在**探测器**页面，点击新增探测器右边的 图标，可以升级探测器，即升级版本升级包、策略升级包、排错升级包。

若不进行手动升级，版本升级包和策略升级包会隔 10 分钟从数据中心自动同步版本和策略升级包，排错升级包不会自动升级。

3.2.4 同步验证

在**探测器**页面，点击新增探测器右边的 图标，将数据中心设备配置同步到各个子探测器，实现分布式部署。

3.2.5 配置同步

在**探测器**页面，点击<**配置同步**>按钮，可以查看探测器使用的模板；点击 按钮，可以切换探测器使用的同步模板，探测器会按照模板勾选的内容同步相关配置。

点击<**同步模板**>，进入模板管理页面，可以新增、编辑模板，用户可以根据自己的实际使用需要，勾选需要同步的配置项。

3.3 流量代理（Agent 代理模式支持）

当 APT 使用 Agent 代理部署方式的时候，请参考本章配置。

3.3.1 打开 Agent 配置开关

Agent 配置开关在 APT 设备界面“**探测器➤流量代理**”上，默认不会打开，需要登录 APT 排错平台修改数据库配置才能打开。

操作步骤

步骤1.　使用 root 账户登录排错平台，登录方法参考登录故障排查平台。

步骤2. 在左侧导航树选择“**服务设置➤数据库管理**”，在该页面下方“**执行 SQL**”区域输入执行下方语句。

UPDATE wdd_sysconfig SET val = 2 WHERE FIELD='system' AND item = 'EngVirtualRecvWork';

步骤3. 在左侧导航树选择“**检测项目➤**3：**服务器状态检查**”。

步骤4. 点击“**探测器主引擎**”操作列的<**重启**>。

步骤5. 在弹出的提示框点击<**确定**>，完成探测器主引擎重启。

3.3.2 配置其他端口

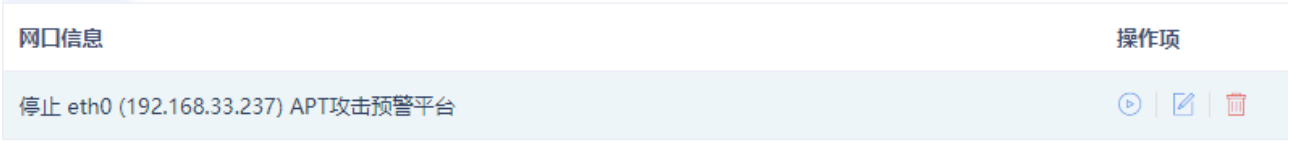
点击操作项的编辑图标，配置探测器接收端口。

默认 Agent 发送流量端口与探测器接收端口为 54321，修改端口后会重启 Agent 抓取流量任务以及探测器接收流量引擎。

3.3.3 测试链路

编辑网口信息，其中 IP 地址必须填写跟管理口非同网段的业务口 IP 地址。点击<**测试链路**>，测试 Agent 与探测器之间是否连通。

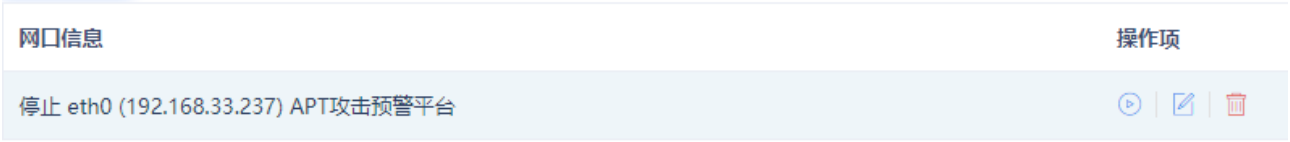
3.3.4 启动/停止/删除网口



- 启动：添加完成后默认停止，如需开启则点击对应的 <**启动**>。
- 停止：如需停止网口则点击 <**停止**>即可。
- 删除：删除网口会停止 Agent 上相应网口的获取流量任务。

3.3.5 编辑网口

修改网口将停止原网口的流量获取任务以及启动新网口的流量获取任务。



3.3.6 端口修改

默认 Agent 过滤端口为 APT 设备配置的端口。

点击 APT Web 界面“**配置➤常规配置➤基本配置**”菜单，下拉到“**当前配置 Web 端口**”区域可以查看并且新增或者删除相关端口。


明御APT攻击预警平台
导航
分析
风险
资产
报表
探测器
配置
系统
admin
常规配置
基本配置
检测配置
联动配置
风险通知
当前配置WEB端口
当前配置POP3端口
当前配置SMTP端口
当前配置IMAP端口

4. 配置

配置部分由**常规配置**、**检测配置**、**联动配置**、**数据外送**四部分组成。

4.1 常规配置

4.1.1 基本配置

在主菜单选择“**配置➤常规配置➤基本配置**”菜单，进入基本配置页面。

4.1.1.1 风险查询参数

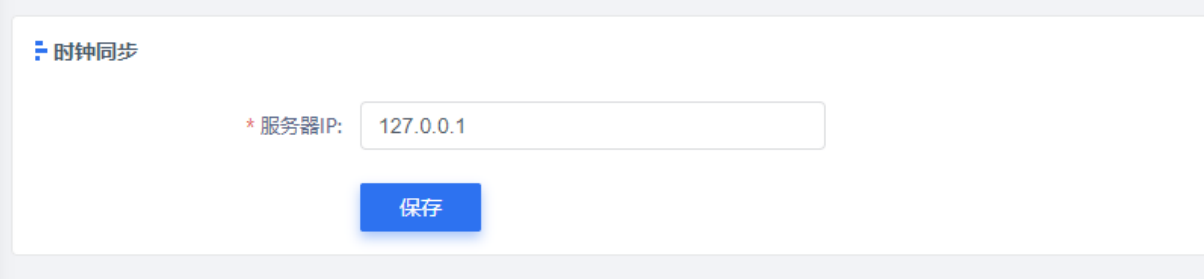
风险查询参数用来配置风险查询信息，配置界面如下。

配置完成后，在主菜单选择“**风险**”将按照上述配置显示风险查询结果。

4.1.1.2 时钟同步

配置 NTP 时钟同步服务器，此后 APT 设备就可以通过配置的 NTP 服务器进行时钟同步，包括 APT 设备的系统时间和硬件时间。

分布式部署场景下，数据中心从时钟同步服务器同步时钟，探测器则从数据中心同步时钟。



4.1.1.3 连网设置

选择<**是**>或<**否**>，允许或禁止 APT 设备访问互联网。

4.1.1.4 Web 规则配置

针对不同的网络部署环境，APT 提供两套 Web 规则供用户选择。

- 当 APT 部署在 Web 服务器或邮件服务器等，可选择<**外网规则**>。
- 当 APT 部署在企业或单位出口交换机时，会有大量内网 IP 访问外网，这些访问容易产生包括 XSS 在内的一些误报，为减少误报可选择<**内网规则**>。

Web 规则配置的界面如下所示，默认为内网规则，切换实时生效。

4.1.1.5 会话释放策略配置

配置会话的 DNS 策略，包括超时释放和实时释放两种。选择实时释放时，系统收到响应后立即释放会话，会导致会话应用流量统计信息日志量增多，外送时建议关闭 DNS 协议的会话应用流量统计信息。

DNS 超时释放需要等待 30s 会释放会话。

4.1.1.6 Web/邮件端口配置

根据自身的网络环境配置审计端口。系统支持 Web 端口、POP3 端口、SMTP 端口、IMAP 端口等配置。

一般情况下，系统会审计这些协议默认的端口。如果用到非默认端口，需要手动增加或者开启对应的协议自动识别。增加非默认端口或开启协议自动识别后，系统才会对这些非默认端口进行审计。

APT 设备默认会对 Web 非标端口（如 8899 端口）进行审计，但默认不审计邮件协议的非标端口。

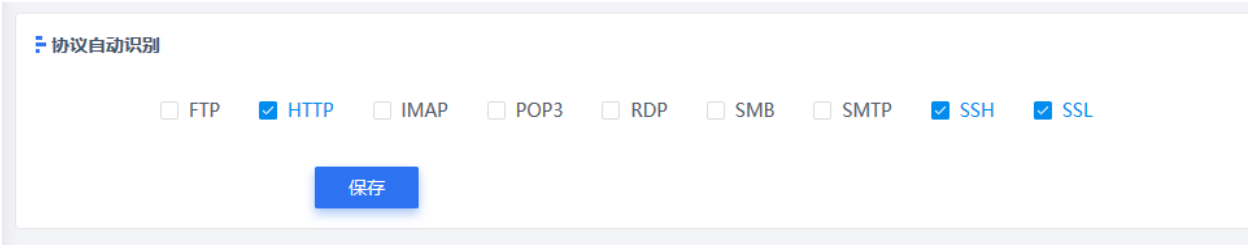
Web/邮件端口配置界面如下。

默认端口不能删除，其中 Web 类型默认端口是 80，POP3 类型默认端口是 110，SMTP 类型的默认端口是 25。

对于加密传输端口，需要在 SSL 流量检测菜单上传证书，并配置端口才能生效。例如：Web 的 443 端口，POP3 的 995 端口以及 SMTP 的 465 端口，具体请参考 SSL 流量检测。

4.1.1.7 协议自动识别

对 FTP、HTTP、IMAP、POP3 等 9 种协议进行自动识别，可识别这 9 种协议的非标端口并进行审计检测。默认开启 HTTP、SSH、SSL 协议。



4.1.1.8 功能配置开关

配置登录行为分析的开关，默认关闭状态。

登录行为分析主要针对流量中登录行为进行分析。若关闭登录行为分析，不会对流量中的登录行为进行分析；开启登录行为分析，可在“**分析➤分析➤登录行为分析**”中查看具体的登录信息。

4.1.2 地理位置

4.1.2.1 配置地理位置

第一次登录系统后，需要设置地理位置，如未设置，用户登录成功时会重新提示，默认添加内网 IP（例如 192.168.0.0/16 等 IP），如下图所示。

设备部署位置为**单位出口或内网**时，需在**地理位置设置**中完整配置内网 IP 地址，以保证检测功能正常运行，且需要确认内网地址已经完整配置，否则该弹窗提示将一直会显示，如下图所示。

如需对此配置做出调整，选择“**配置➤常规配置➤地理位置**”菜单，点击<**新增**>，如下图所示。

配置完成后，新增地理信息将添加到地理位置设置列表中。勾选当前所在城市所在行，点击 按钮可以修改当前城市。

4.1.2.2 导入/导出地理位置信息

系统支持增量导入和全量导入两种方法导入地理位置。

- 增量导入是导入与当前列表 IP 地址不同的信息。
- 全量导入会将系统原有的数据清除，导入表格内的 IP 地址信息，请谨慎操作。

  如果需要导入地理位置配置信息，建议先点击<**下载模板**>，按照模板内容填写完成后保存，点击<**导入**>。
- 点击<**全部导出**>，以 xlsx 格式导出全部数据。

当城市对应的 IP 地址为局域网地址时，国家一栏填写“局域网”即可。

4.1.3 客户网络

对客户网络进行网段划分，标注网络等级、所属区域、责任人、描述配置等，便于用户细化客户网络等级、区域等。

操作入口

选择“**配置➤常规配置➤客户网络**”菜单，点击<**新增**>，填写名称、IP/IP 段、网络等级、所属区域、责任人、描述等信息，然后点击<**确定**>，完成客户网络添加。

- ◆ 网络等级有 1~10 级，数值越大表示重要性越高。
- ◆ IP/IP 段的地址格式需按照右侧的要求填写。

相关操作

- ◆ 选中多个添加的客户网络，点击<**删除**>按钮可以批量删除已经添加的客户网络。
- ◆ 选中单个添加的客户网络，点击该客户网络对应的 可以删除已经添加的客户网络。

4.1.4 语音告警

用来控制**导航-语音告警**的开启和关闭，可配置语音告警的风险级别、风险类别、攻击状态、客户网络。开启语音告警后，可在导航页面查看实时语音告警和历史语音告警。默认语音告警关闭状态。

数据中心可以对探测器进行配置管理，如图所示。

- **APT 攻击预警平台**这一行是数据中心和探测器对自身的语音告警配置；对探测器的语音告警进行配置，语音告警会上传到数据中心进行语音告警。

  点击 按钮，可以进行配置修改。

- 探测器语音告警页面只能对自身进行配置管理，如图所示。

4.1.5 NAT 地址解析

针对通过 HTTP 代理或负载均衡方式连接到 Web 服务器的客户端最原始的 IP 地址的 HTTP 请求头字段，可进行配置字段名读取首次或末次的 IP 地址从而获取真实的 IP 地址。

操作入口

在菜单栏选择“**配置➤常规配置➤NAT 地址解析**”进入 NAT 地址解析配置页面。

点击<**新增**>可以增加 NAT 地址解析配置。

4.1.6 资产识别配置

资产识别配置主要用于资产识别，勾选完成该类资产，将在资产概况中展示该类资产数据。

4.2 检测配置

4.2.1 引擎管理

用来控制各种风险检测机制的停止和运行。

操作入口

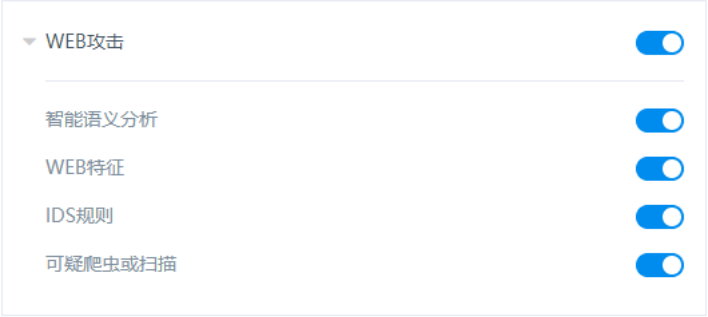
选择“**配置➤检测配置➤引擎管理**”菜单进入**引擎管理**页面。

默认**行为分析**、**ARP 欺骗**、**扫描行为**和**邮件社工攻击**这 5 个引擎为禁用，其他引擎默认开启。

点击 **Web 攻击**下的 图标，展示**智能语义分析、WEB 特征、IDS 规则、可疑爬虫或扫描 4 个**子引擎。

智能语义分析是把人类自然语言，转化为机器能读懂的代码。即对检测内容进行语法分析，提高规则模型的适用性。

WEB 特征、IDS 规则是通过内部规则进行匹配产生告警的。



4.2.2 文件检测

文件检测包含了安全文件大小、沙箱检测配置、压缩文件中子文件真实格式识别、沙箱操作系统设置、分

离文件后缀、恶意文件 MD5 等。

4.2.2.1 检测配置

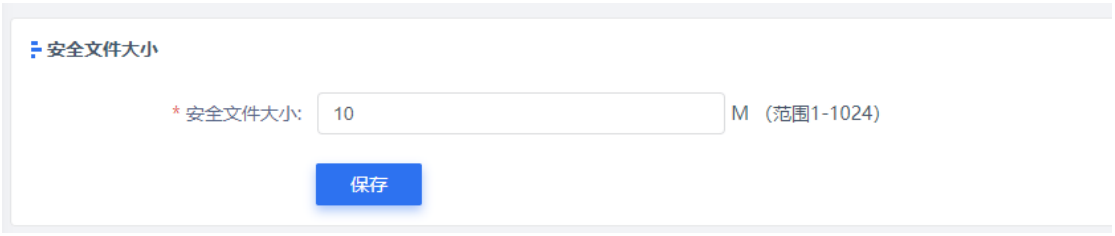
设置文件检测的相关配置。

操作入口

选择“**配置**”主菜单，在左侧导航树选择“**检测配置➢文件检测➢检测配置**”。

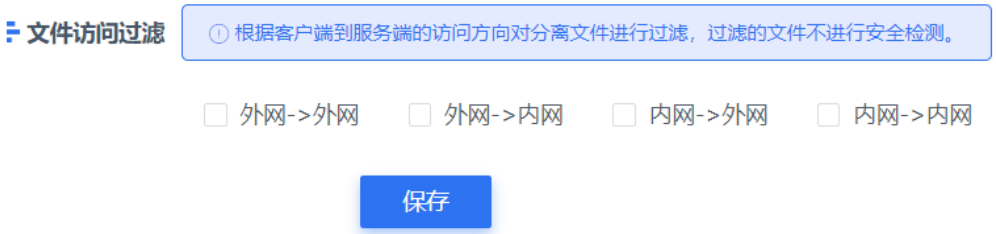
1) 安全文件大小

安全文件大小设置用来设定系统对用户发送或接收文件大小检测的门限。假如文件大小超过设定的门限大小，系统将不检测该文件。配置界面如下。



2) 文件访问过滤

文件访问过滤，是根据客户端到服务端的访问方向对分离文件进行过滤，过滤掉文件不进行安全检测。



3) 文件威胁情报

设置文件威胁情报是否开启。开启文件威胁情报之后可以在情报事件分析界面查询到相关的文件威胁情报数据。

4) 沙箱检测配置

沙箱检测配置有两种选项：**“检测所有文件”**和“**仅检测恶意文件**”。两种配置的不同导致检测效率不同。

检测所有文件，会对流量中识别到的所有文件进行检测，检测结果更具全面性，但是这样会花费大量的系统资源；仅检测恶意文件，只检测流量中病毒木马扫描和静态分析结果判定为为恶意文件的文件，可提升沙箱检测性能。如果性能不足，建议选择“仅检测恶意文件”。

5) 监测结果复用

设置是否复用监测结果。

6) 压缩文件中子文件真实格式识别

开启之后，可以检测压缩包中文件格式非真实，或无后缀的情况。

7) 沙箱网络行为

沙箱检测文件时的沙箱行为，包含“API 解析”和“数据包保存”两种。用户选择“数据包保存”时，会在风险查询界面提供保存的数据包下载链接。

8) 沙箱操作系统配置

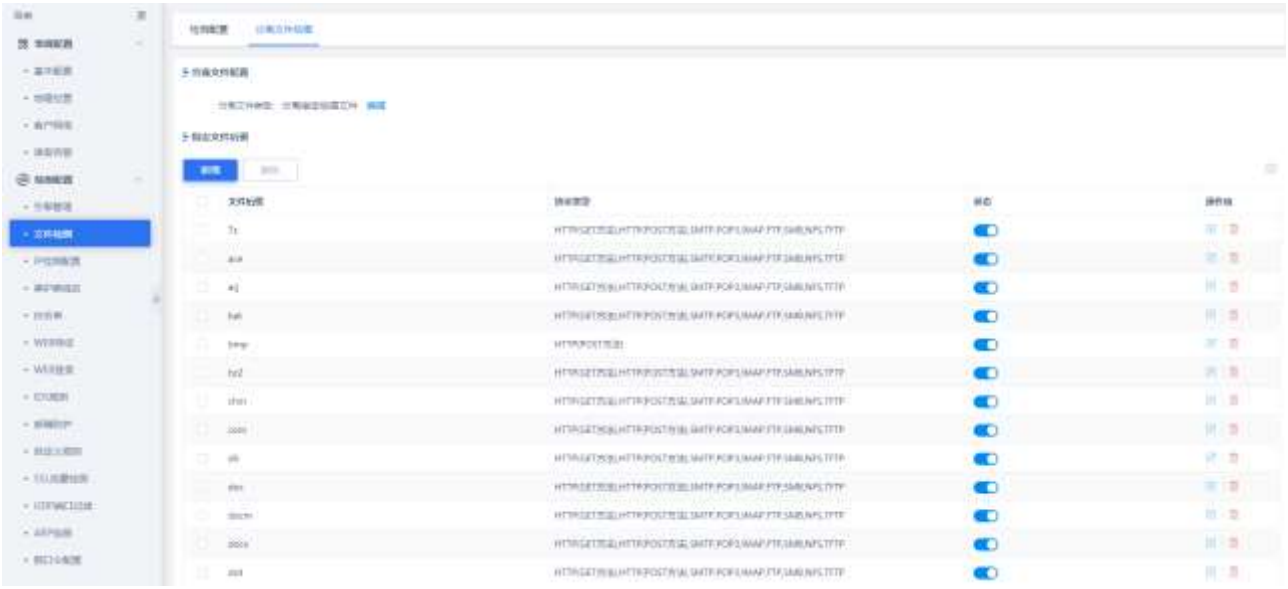
当沙箱有多种操作系统时，用户可以选择使用某种操作系统镜像类型沙箱。

4.2.2.2 分离文件后缀

分离文件后缀功能用来配置系统对哪些后缀类型的文件以及哪些协议类型中包含的文件后缀进行分离操作。协议类型主要有 HTTP(GET、POST)、SMTP、POP3、IMAP、FTP、SMB、NFS、TFTP。

操作入口

选择“配置”主菜单，在左侧导航树选择“**检测配置➤文件检测➤分离文件后缀**”。



配置选项包括<**分离所有文件**>和<**分离指定后缀文件**>两种。在**分离文件后缀**页面点击<**编辑**>选择分离文件类型。

- 分离所有文件会对所有的文件后缀报文进行分离，包括没有后缀的文件。
- 如果选择了<**分离指定后缀文件**>，在下方列表查看文件后缀列表并确保需要启用条目**状态**列下的 开关处于打开状态。如需要新增待处理文件的后缀类型，点击<**新增**>增加文件后缀。

输入文件后缀，选择协议类型，点击<**确定**>即可添加成功。保存成功后会在列表中显示新增的后缀类型以及协议类型。

4.2.2.3 恶意文件 MD5

恶意文件 MD5 支持自定义恶意文件信息、新增导入恶意文件信息以及根据 MD5 查询对应的 MD5 文件，可以让设置的样本经过系统检测产生恶意文件风险告警。

操作入口

选择“**配置**”主菜单，在左侧导航树选择“**检测配置➤文件检测➤恶意文件 MD5**”。

点击<**新增**>按钮，输入文件 MD5 值、恶意信息描述，添加恶意文件 MD5。

支持增量导入、全量导入两种导入方式。

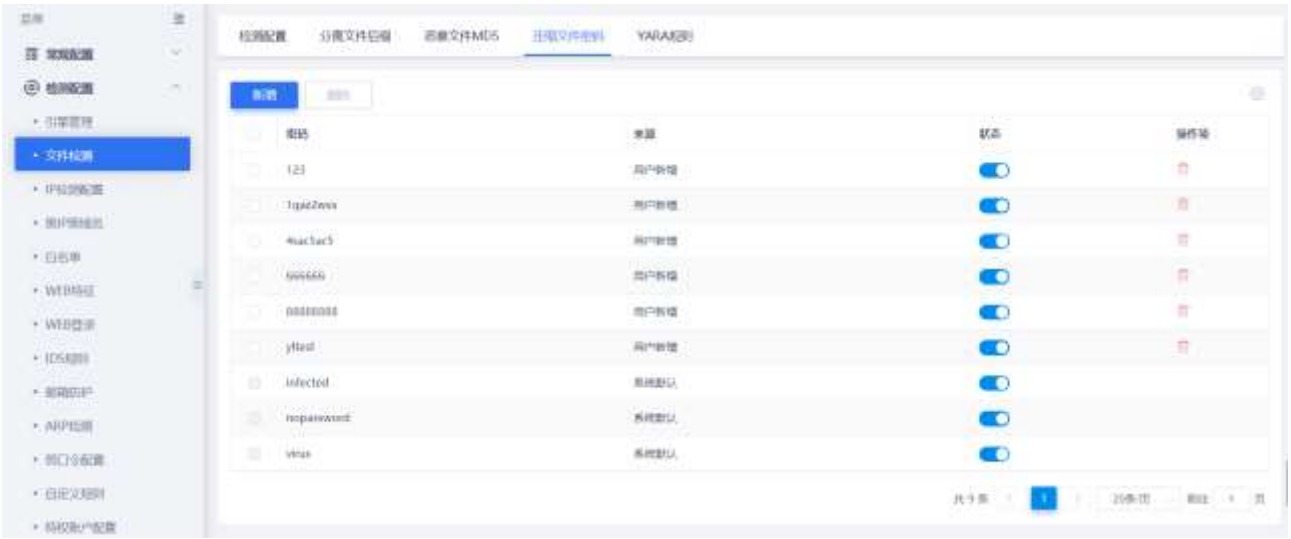
全量导入会覆盖原有数据，请谨慎操作！

4.2.2.4 压缩文件密码

可自定义设置加密压缩文件的解压密码（若 APT 设备分离出加密压缩文件后没有在本功能中匹配到相应解压密码，则设备对该文件会解压失败而导致沙箱无法进行检测）。

操作入口

选择“**配置**”主菜单，在左侧导航树选择“**检测配置➤文件检测➤压缩文件密码**”。



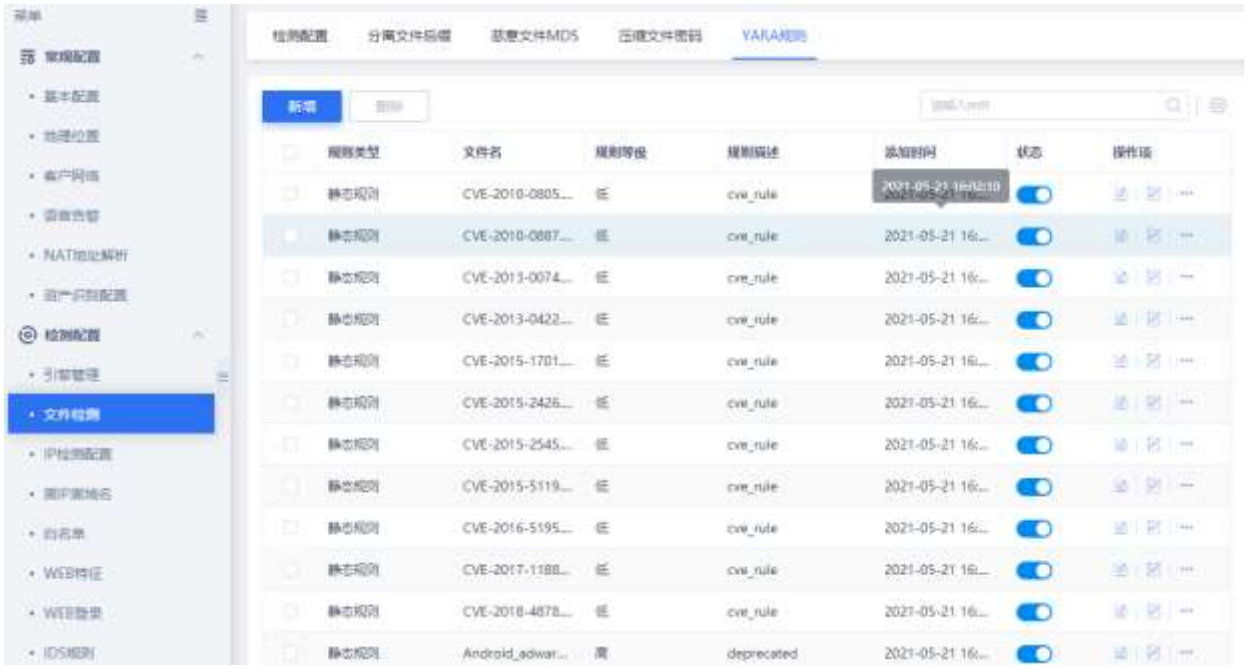
- 点击<**新增**>按钮，输入密码添加解压密码，最多允许十个有效密码，如果想继续添加，需删除或手动关闭某条密码，系统默认三条密码不可删除。

4.2.2.5 YARA 规则

YARA 的每一条描述或规则都由一系列字符串和一个布尔型表达式构成。YARA 规则可以提交给文件或正在运行的进程，帮助用户识别其是否属于某个已进行规则描述的恶意软件。

操作入口

选择“**配置**”主菜单，在左侧导航树选择“**检测配置➤文件检测➤YARA 规则**”进入 **YARA 规则配置**页面。



点击<**新增**>，在弹出的新增对话框设置相关参数，可以新增 YARA 规则。

4.2.3 IP 检测配置

IP 检测配置包含 IP 过滤和指定 IP 检测，对应页签括号内数字表示启用该规则的数目。

4.2.3.1 IP 过滤

IP 过滤的作用是不审计在 IP 过滤表中配置的相应 IP 报文。可以通过新增和导入两种方式添加 IP 过滤。

操作步骤

步骤1. 登录系统 Web 界面，选择“**配置➢检测配置➢IP 检测配置**”菜单。

步骤2. 点击“**IP 过滤**”页签。

步骤3. 点击<**新增**>，添加 IP 地址过滤；或者点击<**导入**>批量添加 IP 地址过滤。可选择<**按单个 IP 地址过滤**>或<**按一对 IP 地址过滤**>。

- **按单个 IP 地址过滤**：输入 IP 后，点击<**保存**>即可。当目的 IP 或源 IP 匹配该 IP 后，系统对其报文均不会产生审计行为。

- **按一对 IP 地址过滤**：添加的时候，IP1 必填（支持网段），IP2（不支持网段）和端口可以选填。

- 导入 IP 地址过滤

  点击<**导入**>，导入指定的 IP 过滤规则。导入的方式有增量导入、全量导入两种。建议点击<**下载模板**>，然后根据模板格式填写好后导入。

  增量导入是导入与列表 IP 地址不同的信息，全量导入是会将当前列表的所有 IP 地址的信息清除，导入表格内的 IP 地址信息。

- 点击<**全部导出**>，以 xlsx 格式导出列表所有内容。

4.2.3.2 指定 IP 检测

启用后，APT 只审计在指定 IP 检测中配置的相应 IP 的报文。

操作步骤

步骤1. 登录系统 Web 界面，选择“**配置➤检测配置➤IP 检测配置**“菜单。

步骤2. 点击“**指定 IP 检测**”页签。

步骤3. 点击<**新增**>，添加 IP。支持 IPv4 和 IPv6 格式的单个 IP 地址或 IP 地址段。

- 导入 IP 检测

  点击<**导入**>，导入指定的 IP 检测规则。导入方式有增量导入、全量导入两种。增量导入是导入与列表 IP 地址不同的信息，全量导入将列表的所有 IP 地址的信息清除，导入表格内的 IP 地址信息。

  建议下载模板根据模板格式填写完成后，点击<**导入**>。

- 点击<**全部导出**>，以 xlsx 格式导出列表中全部 IP 检测配置信息。

4.2.4 黑 IP 黑域名

手动添加黑 IP 黑域名后，当攻击者访问用户配置的黑 IP 黑域名时，系统就会产生远程控制（用户配置数据）告警。

操作步骤

步骤1. 登录系统 Web 界面，选择“**配置➤检测配置➤黑 IP 黑域名**”菜单。

步骤2. 点击“**黑 IP**”或“**黑域名**”页签，点击<**新增**>手动添加黑 IP 或黑域名。

或点击<**导入**>批量导入黑 IP 或黑域名。目前只支持增量导入，即导入与列表 IP 地址或域名不同的信息。

导入支持明文或密文方式，密文方式采用的是 MD5 加密，导入的界面如下。

目前仅支持导出明文数据，即未加密的数据。

步骤3. 点击<**导入记录**>，可按导入批次查看导入数据的导入类型、导入数量和加密类型等信息。

4.2.5 白名单

添加和启用/禁用白名单，包括文件白名单、域名白名单、黑 IP 白名单、黑域名白名单、客户端 IP 白名单、服务端 IP 白名单、IDS 规则白名单、Web 特征风险白名单、发件人邮箱白名单和发件人域名白名单等。

操作入口

选择“**配置**”主菜单，在左侧导航树选择“**检测配置➤白名单**”，进入白名单相关界面。

除了 WEB 特征白名单，其他类型的白名单都支持导入、导出操作。

4.2.5.1 文件白名单

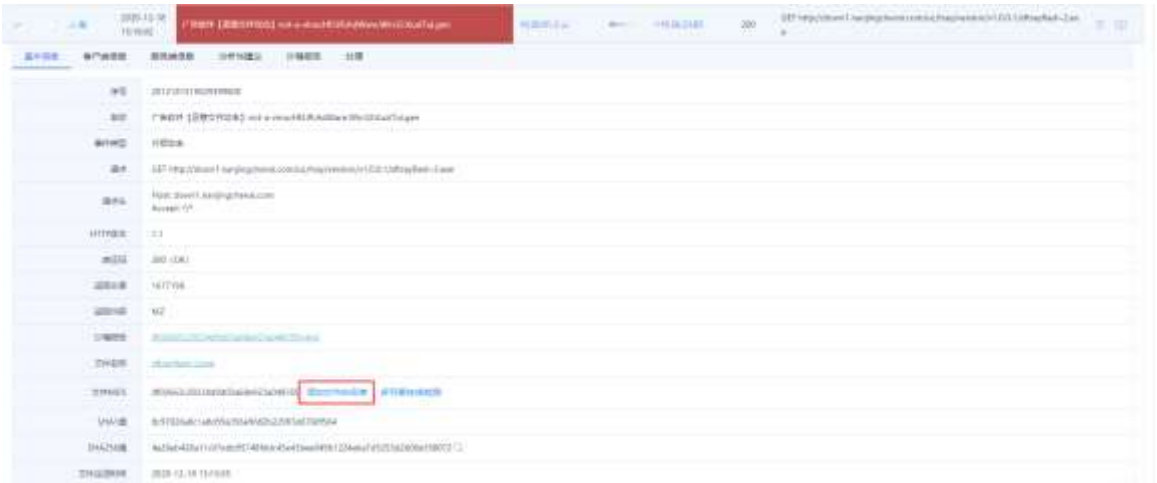
文件白名单启用后，该文件在非手动上传场景下检测结果为安全。

添加方式有两种。

◆ 在“**文件白名单**”页面，点击<**新增**>，输入文件 MD5 值，界面如下。

或点击<**导入**>批量导入白名单。目前支持增量导入和全量导入两种类型，导入的界面如下。

◆ 在主菜单选择“**风险**”进入风险查询页面，在列表中点击单条风险展开详情，在风险详情的**文件 MD5** 部分（如果有）点击<**添加文件白名单**>，如下图所示。



4.2.5.2 域名白名单

配置域名白名单后，不再产生该域名的审计和告警。域名白名单的添加方式有两种：

◆ 在“**域名白名单**”界面，点击<**新增**>，输入域名手动添加，如下图所示。

◆ 在主菜单选择“**风险**”进入风险查询页面，查询可能涉及域名访问的风险告警（例如恶意文件攻击），在风险列表的**操作项**列下点击 按钮添加，如下图所示。

4.2.5.3 黑 IP 白名单

配置黑 IP 白名单后，IP 地址为该 IP 的攻击事件不再产生远程控制告警。黑 IP 白名单的添加方式有两种：

◆ 在“**黑 IP 白名单**”界面，点击<**新增**>，输入 IPv4 或 IPv6 地址手动添加，如下图所示。

◆ 在主菜单选择“**风险**”进入风险查询页面，查询远程控制告警（例如 IDS 规则告警）。如果用户想把某个黑 IP 列为白名单（即之后不对访问该 IP 的行为产生“**远程控制**”告警），可以通过风险查询页面风险列表**操作项**列下的按钮 添加黑 IP 白名单，如下图所示。

4.2.5.4 黑域名白名单

配置黑域名白名单后，该域名不再产生远程控制告警。黑域名白名单的添加方式有两种：

◆ 在“**黑域名白名单**”界面，点击<**新增**>，输入域名手动添加，如下图所示。

◆ 用户可以通过风险页面查询远程控制告警（例如威胁情报告警）。如果用户需要把某个黑域名列为白名单（即之后不对访问该域名的行为产生远程控制告警），可以通过风险查询页面风险列表**操作项**列

下的按钮 来添加黑域名白名单，如下图所示。

4.2.5.5 客户端 IP 白名单

配置客户端 IP 白名单后，该客户端 IP 不再产生的审计和告警。仅支持单个 IP，添加方式有两种：

- 在“**客户端 IP 白名单**”界面，点击<**新增**>，输入 IPv4 或 IPv6 地址手动添加，如下图所示。

- 用户可以通过风险页面查询可能涉及到客户端操作的告警（例如 Web 攻击告警）。如果用户需要把某个客户端 IP 列为白名单（即之后不对来自该客户端 IP 的行为产生告警），可以通过风险查询页面风险列表**操作项**列下的 按钮来添加客户端 IP 白名单，如下图所示。

4.2.5.6 服务端 IP 白名单

配置服务端 IP 白名单后，该“服务端 IP+端口”不再产生审计和告警。服务端 IP 白名单添加方式有两种：

◆ 在“**服务端 IP 白名单**”界面，点击<**新增**>，输入 IPv4 或 IPv6 地址手动添加，如下图所示。

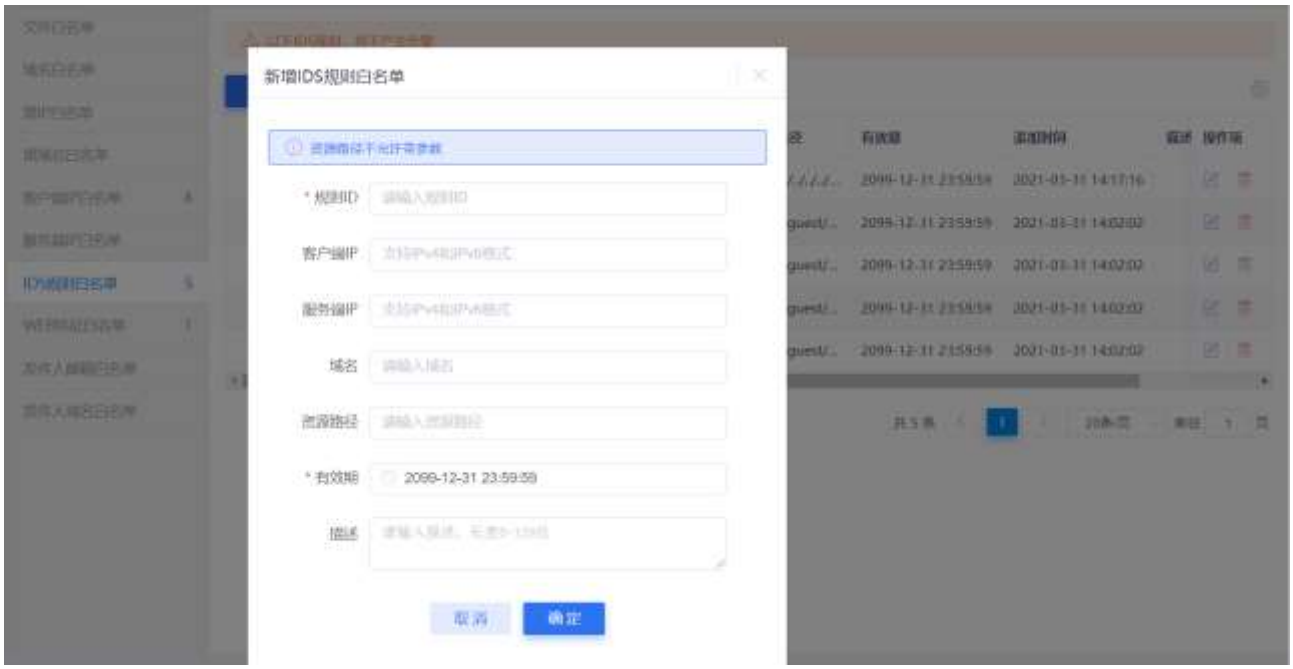
◆ 用户可以通过风险页面查询可能涉及到服务端操作的告警（例如 Web 攻击告警）。如果用户需要把某个服务端 IP 列为白名单（即之后不对来自该服务端 IP+端口的行为产生告警），可以通过风险查询页面风险列表**操作项**列下的 按钮来添加服务端 IP 白名单，如下图所示。

4.2.5.7 IDS 规则白名单

配置 IDS 规则白名单后，满足配置的“规则 ID+客户端 IP+服务端 IP+资源路径+有效期”的风险数据将不再产生 IDS 规则告警。

添加方式有两种：

◆ 在“**IDS 规则白名单**”页面，点击<**新增**>，在界面上输入规则 ID、客户端 IP、服务端 IP、该条规则的资源路径、IDS 规则白名单有效日期，如下图所示。



◆ 在主菜单选择“**风险**”进入风险查询页面，查询可能涉及 IDS 检测的风险（例如策略来源选择“**IDS 规则**”），在风险列表的**操作项**列下点击 按钮添加。风险查询界面添加 IDS 规则白名单有四种组合类型，分别是为规则名称、规则名称+客户端 IP、规则名称+服务端 IP 和规则名称+客户端 IP+服务端 IP 等，如下图所示。

在风险查询页面，可通过设置 Web 攻击的 IDS 规则来源、远程控制（IDS 规则）、隧道通信（IDS 规则）、挖矿、恶意工具利用、其他等风险条件过滤出涉及到 IDS 检测的风险。

4.2.5.8 Web 特征白名单

配置 Web 特征风险白名单后，满足配置的“客户端 IP+域名+Web 特征类别+Web 特征规则+HTTP 方法”

条件的风险数据将不再产生 Web 特征风险告警。

添加方式有两种：

- 在“**Web 特征白名单**”页面，点击<**新增**>，输入客户端 IP+域名+Web 特征类别+Web 特征规则+HTTP，如下图所示。

- 在主菜单选择“**风险**”进入风险查询页面，查询可能涉及 Web 特征的风险（如策略来源选择“**Web 特征规则**”），在风险列表的**操作项**列下点击 按钮添加。Web 特征风险白名单有三种组合类型，分别是为客户端 IP+域名、客户端 IP+域名+规则名称、域名+规则名称，如下图 所示。

4.2.5.9 发件人邮箱白名单

配置发件人邮箱白名单后，此发件人发出的邮件不再产生审计和告警。

添加方式有两种：

- 在“**发件人邮箱白名单**”界面，点击<**新增**>，输入发件人邮箱，界面如下。

- 在主菜单选择“**风险**”进入风险查询页面，查询可能涉及邮件发送的风险（如邮件社工攻击），在风险列表的**操作项**列下点击 按钮添加，如下图所示。

4.2.5.10 发件人域名白名单

配置发件人域名白名单后，在该列表中的发件人域名不再产生审计和告警。添加方式有两种：

- 在“**发件人域名白名单**”界面，点击<**新增**>，输入发件人邮箱域名来手动添加，界面如下。

◆ 在主菜单选择“**风险**”进入风险查询页面，查询可能涉及邮件发送的风险（如邮件社工攻击），在风险列表的**操作项**列下点击 按钮添加，如下图所示。

4.2.6 Web 特征

对 Web 特征规则进行启用和禁用管理，特征管理的攻击类型有：SQL 注入、命令注入、跨站脚本、远程代码执行、文件上传、路径遍历、信息泄露、越权访问及其他。

操作入口

选择“**配置**”主菜单，在左侧导航树选择“**检测配置➤Web 特征**”。点击页签进入不同类型的 Web 特征管理页面。

◆ 在 Web 特征列表下，点击**状态**列下 图标可以切换禁用、启用状态；点击<**全部禁用**>或<**全部开启**>禁用或开启全部规则，如下图所示。

4.2.7 Web 登录

设置 Web 登录相关的配置，包括用户名、密码和用户名来源、登录状态码及返回值内容等配置。

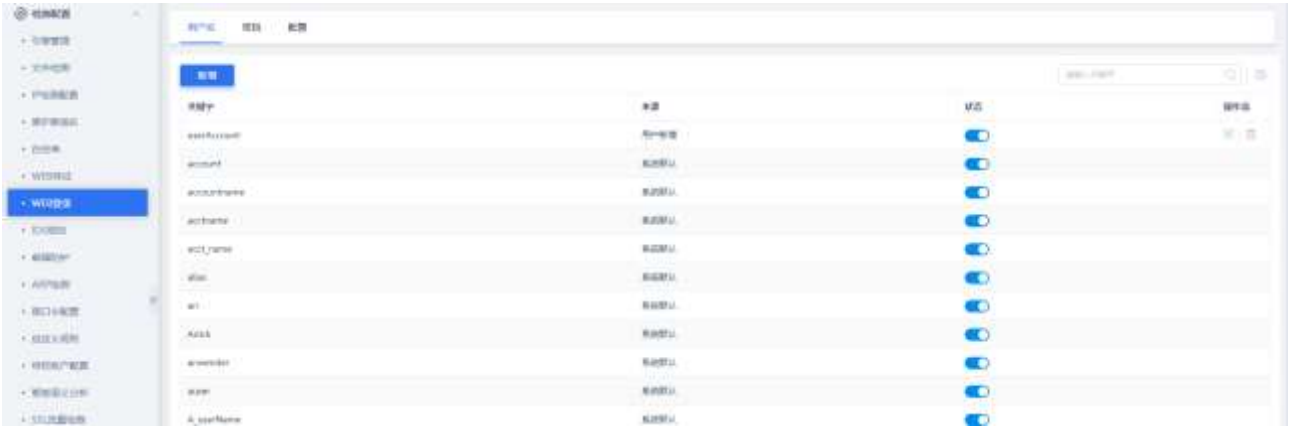
操作入口

选择“**配置**”主菜单，在左侧导航树选择“**检测配置➤Web 登录**”。点击页签进入不同类型的 Web 登录配置页面。

4.2.7.1 用户名密码管理

新增用户名/密码关键字，提高对 WEB 登录行为，弱口令、弱密码进行精确匹配。

可以单击状态栏按钮启用/禁用该关键字。

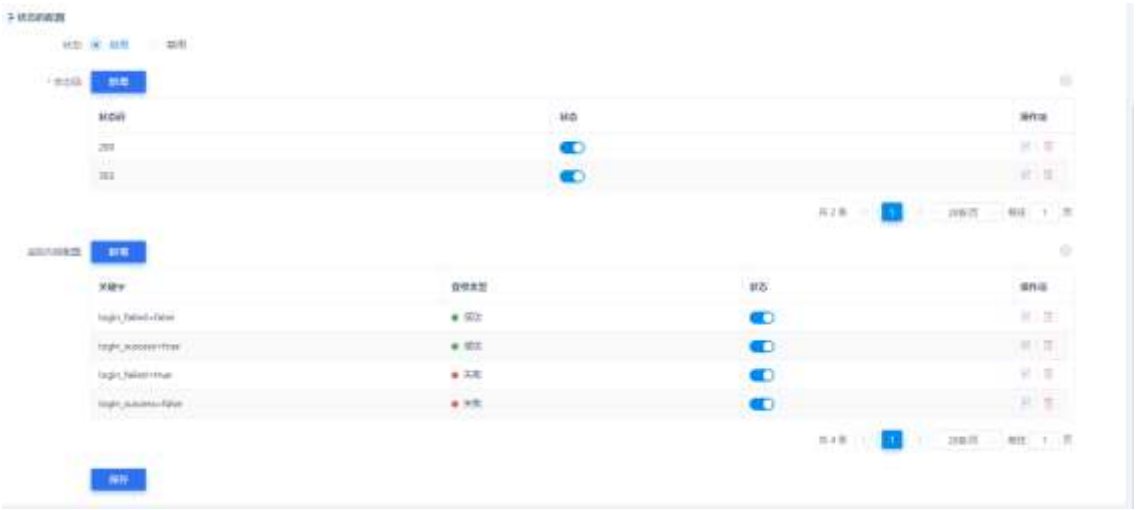


4.2.7.2 配置

用户名来源用于配置用户登录行为用户名获取方式，例如请求 url 状态开启，用户名可以从请求 URL 中去解析获取。

系统默认请求头认证、请求 URL、postbody 普通格式均开启，postbody -JOSN 格式、请求头 cookie 需手动开启。

状态码配置主要用于配置用户登录行为登录状态的判断，用户登录行为满足配置的状态码，则该次登录状态即为成功；用户登录行为返回内容中满足返回内容配置，即可判断该登录行为成功或者失败。



4.2.8 IDS 规则

IDS 规则管理可通过页面对 IDS 规则进行启用、禁用的管理，IDS 规则主要有 WEB 攻击、远程控制、WEB 后门访问、拒绝服务攻击、隧道通信、挖矿、恶意工具利用、漏洞利用、其他等 9 个风险。

操作入口

在菜单栏选择“**配置➤检测配置➤IDS 规则**”进入 **IDS 规则**页面。

- 点击**状态**列图标来切换禁用、启用状态来对规则进行管理。也可以点击<**全部禁用**>来禁用全部规则，点击<**全部开启**>开启全部规则。还可以通过勾选“只看紧急事件”来筛选紧急事件。

- IDS 规则配置，目前系统支持精简规则和全量规则两种规则模式。

- 精简规则：是经过安恒威胁分析团队筛选的，比较常见且重要的规则。
- 全量规则：为了提高检出率，加入了更加复杂多样的规则库，匹配性增多，系统资源占用率高，建议在设备流量吞吐相对较大的场合慎重开启。

◆ 系统支持精简、平衡、增强三种置信度，置信度是基于规则的匹配内容是否可信，危害范围进行综合评判。

- 精准：该模式规则数量较少，但告警准确度高、误报可能性较低。
- 平衡：模式在保证告警准确度的前提下，选择适当重要的规则。
- 增强：该模式规则数量较多、检测范围广，但出现误报的可能性增大。

◆ 支持导出 IDS 规则管理的规则 ID、IDS 规则名称、启用/禁用状态、风险名称等内容。

4.2.9 邮箱防护

在邮箱防护模块，可以点击<**新增**>，添加域名及邮箱服务器 IP 地址，添加后的邮箱才会有发件人欺骗检测，及在引擎管理下邮件社工检测中的针对发件人欺骗的检测才会生效。

操作入口

在菜单栏选择“**配置➤检测配置➤邮箱防护**”进入**邮箱防护**页面。

4.2.10 ARP 检测

ARP 检测功能可将 IP 地址与 MAC 地址绑定，便于识别解析 ARP 欺骗，提高检测精度。

操作入口

在菜单栏选择“**配置➤检测配置➤ARP 检测**”进入 ARP 检测配置页面。

◆ 点击<**新增**>可以进行单个 IP 地址与 MAC 地址的绑定。

◆ 点击<**导入**>可以进行批量增加数据，点击<**导出**>可以进行批量导出数据。

◆ 支持增量导入、全量导入两种导入方式。

全量导入会覆盖原有数据，请谨慎操作！

4.2.11 弱口令配置

通过对常见应用的用户名、口令进行提取，并进行复杂度判断，以识别应用中存在的弱口令的 情况，减除

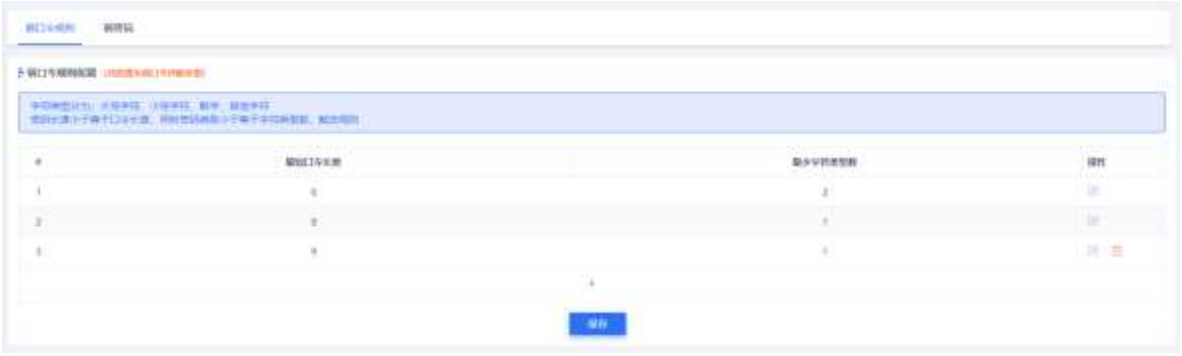
企业应用中潜在的风险隐患。

操作入口

在菜单栏选择“**配置➤检测配置➤弱口令配置**”进入**弱口令配置**页面。

- 点击**弱口令规则**进行规则配置，本项是弱口令判定依据，凡是符合设定条件的即为弱口令。满足规则字符类型≤2，口令长度≤6 或者 字符类型≤1，口令长度≤8 即被判断为弱口令。
- 可以点击 + 进行增添规则或者点击 进行删除规则，单击 进行规则修改。

系统最多保存 4 条弱口令规则。



- 点击**弱密码**，可以增添自定义明文密码以及 MD5 密码，支持单个增添以及批量导入。关闭状态则禁用该条密码检测。

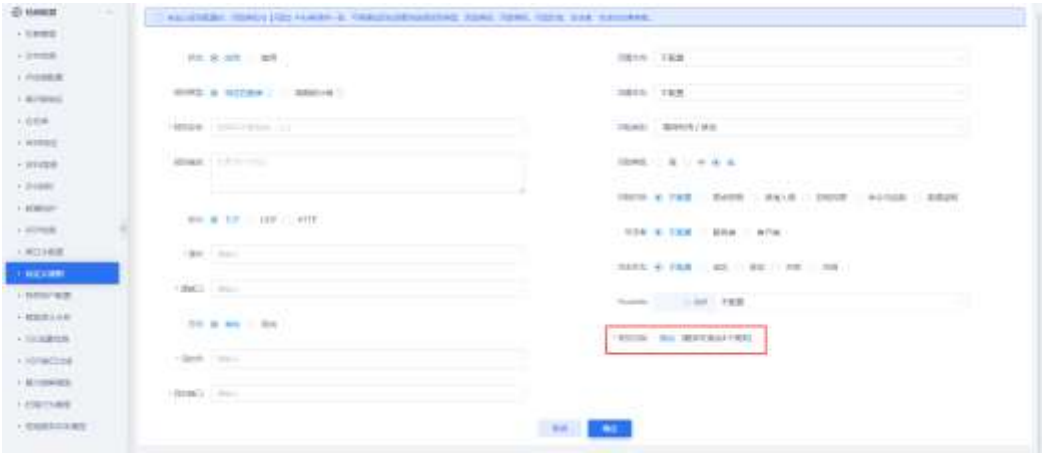
4.2.12 自定义规则

根据用户需要，自定义特征检测规则。当规则状态为<**启用**>时，如果流量中有满足配置的内容，风险页面就会产生自定义特征检测告警。

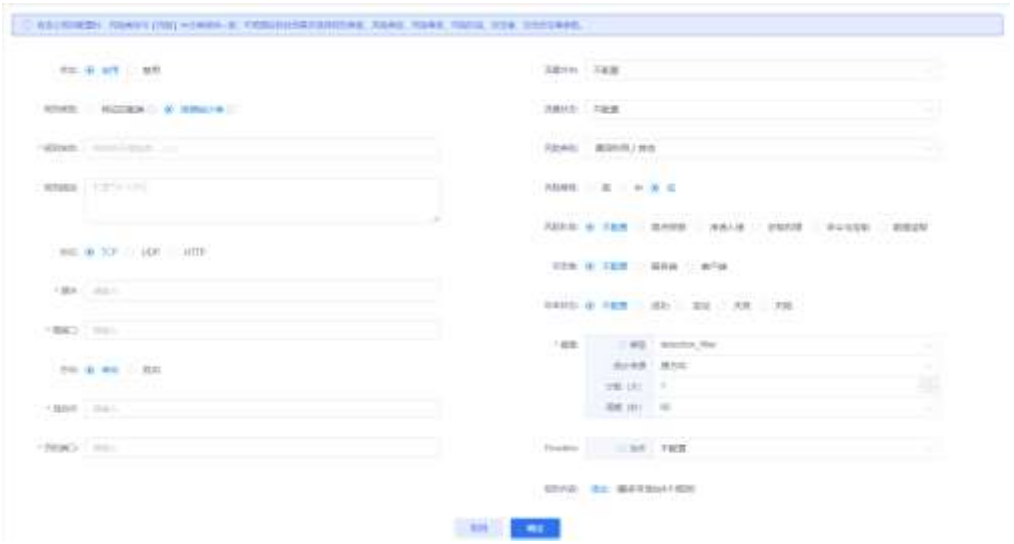
操作入口

选择“**配置**”主菜单，在左侧导航树选择“**检测配置➤自定义规则➤新增**”，根据规则类型选择特征匹配类或周期统计类 填写各项规则匹配条件，如下图所示。

- 默认选择特征匹配类，根据规则内容和 Flowbits 进行匹配。Flowbits 会进行标记流，匹配时告警更加的精准。



- 选择**规则类型**为“周期统计类”时需要设置阈值，在周期内统计来源满足次数要求并符合规则内容和 Flowbits 才会触发告警。



◆ 点击<**添加**>添加规则内容，即特征中需具体匹配的流量内容。

添加规则界面参数说明如下。

参数名称	参数说明	默认值
内容源	设置规则内容来源。 可以选择不配置或者来自文件。	◆ 不配置 ◆ 文件
内容	设置规则内容。	手动输入。
距离	距离是一个配合规则内容使用的参数。距离参数设置了内容模式匹配函数从它搜索的区域的起始位置后的某一距离开始搜索。	手动输入。 距离参数和范围参数一般配合使用。
范围	范围是一个配合规则内容使用的参数。范围参数设置了内容模式匹配函数从它搜索的区域的起始位置开始的搜索最大范围。范围要比规则内容包含的字符数目多，才能进行匹配。	手动输入。 距离参数和范围参数一般配合使用。
深度	深度是一个配合规则内容使用的参数。深度参数设置了内容模式匹配函数从他搜索的区域的起始位置开始搜索多少个字符。深度要比规则内容包含的字符数目多，才能进行匹配。	手动输入。 深度参数和偏移量参数一般配合使用。
偏移量	偏移量是一个配合规则内容使用的参数。偏移量参数设置了内容模式匹配函数从他搜索的区域的起始位置偏移多少个字节开始搜索。	手动输入 深度参数和偏移量参数一般配合使用。
大小写敏感性	配置搜索时内容规则中的字符是否需要严格匹配大小写字母。	◆ 忽略 ◆ 不忽略
区域	设置搜索区域，即规则匹配搜索的范围。	不配置、URL、请求方法、Cookie、请求头、请求报文

4.2.13 特权账户配置

涉及登录行为相关的应用场景，例如特权账号登录、弱口令、脆弱性分析等，需要对特权账户进行标识，因此需对应增加配置界面进行区分。

操作入口

选择“**配置**”主菜单，在左侧导航树选择“**检测配置➤特权账户配置**”，当有登录的账号满足状态开启的账号名称和登录协议，即可被标注为特权账号。

◆ 点击<**新增**>按钮，新增特权账户，输入特权账号，选择登录协议，界面如下。

4.2.14 智能语义分析

智能语义分析是把人类自然语言转化为机器能读懂的代码。即对检测内容进行语法分析，提高规则模型的适用性。

为了防止现场智能语义分析误报过多，该模块可以针对单个智能语义分析（例如：智能语义分析 XSS 攻击等）进行引擎的关闭。

操作入口

选择“**配置**”主菜单，在左侧导航树选择“**检测配置➤智能语义分析**”，主要控制智能语义分析功能的开启状态。

4.2.15 SSL 流量检测

SSL 流量检测是对当前用户网络环境中出现的加密协议流量（HTTPS、SMTP、POP、IMAP）进行检测。该检测需要上传相对应证书，即该加密协议流量中网站的私钥（目前只支持 RSA 私钥解密）。

证书上传操作方法

步骤1. 登录系统 Web 界面，选择“**配置**”页签。

步骤2. 在左侧导航树选择“**检测配置➤SSL 流量检测**”。

步骤3. 点击<**上传证书**>，在弹出的界面上配置私钥别名、私钥密码、服务器 IP 地址、对应的协议以及加密端口、上传服务器私钥文件。完成后，满足该配置的加密协议流量就能被审计并检测。

- 点击左侧的⊕增加协议及对应端口，一个 IP 地址最多输入 4 个端口。

- 点击右侧的⊕新增 IP 地址记录，IP 地址只允许输入单个 IP。

- 证书编码格式为 PEM 文件格式，如 PKCS#8 加密格式、PKCS#8 非加密格式、Openssl ASN 格式等。
- 证书名称由数字、字母、-、_、.组成，长度：1~255。
- 此处配置不需要再在端口配置中新增 ssl 加密端口

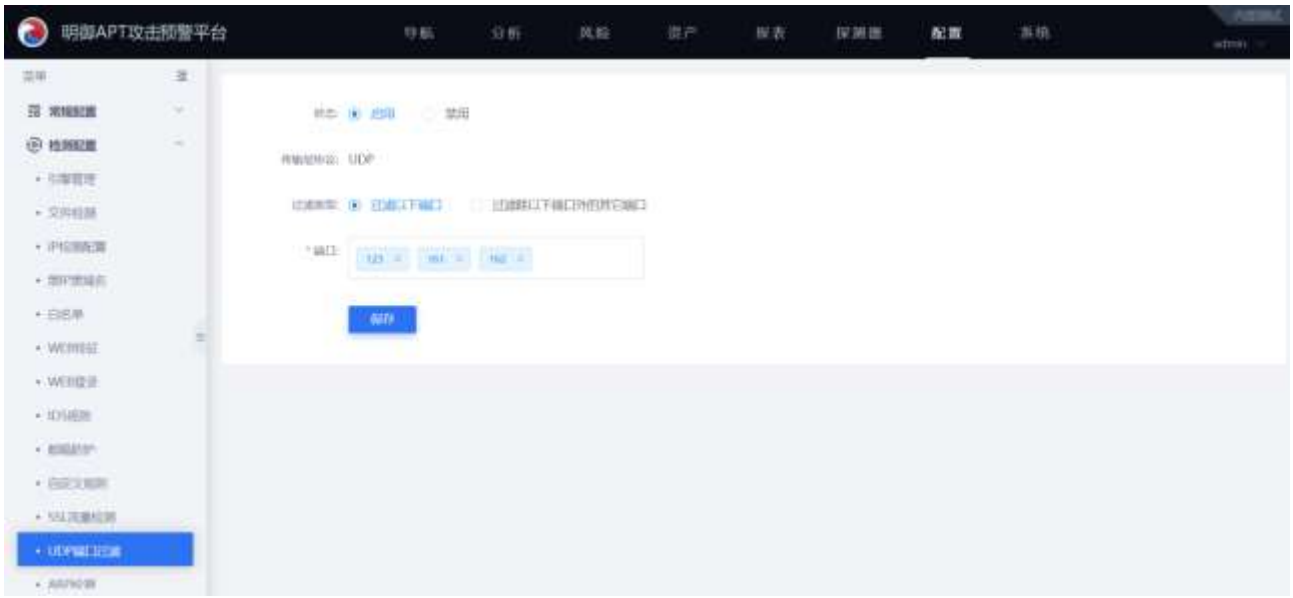
4.2.16 UDP 端口过滤

自定义对 UDP 协议（传输层）进行端口过滤，过滤掉无需检测的协议端口。

操作入口

选择“**配置➤检测配置➤**UDP **端口过滤配置**”菜单进入 UDP **端口过滤配置**页面。

- **过滤类型**可选择“过滤以下端口”（即端口黑名单形式）或“过滤以下端口外的其他端口”（即端口白名单形式）。
- 如果不需要过滤 UDP 协议端口，选择<**禁用**>。



4.2.17 暴力破解模型

对暴力破解模型的触发机制进行设置，适应用户的实际使用环境，主要涉及**时间范围、登录次数、检测机制**等关键指标进行配置，满足设置的触发机制的风险才会产生告警信息

操作入口

在菜单栏选择“配置➤检测配置➤暴力破解模型”进入暴力破解模型页面。

点击开启该类型风险检测（启用模型需要在“**配置➤检测配置➤引擎管理**”页面确认**暴力破解**及其子模型开关已开启）；点击可以编辑该模型，更改配置内容。

4.2.18 扫描行为模型

对扫描行为模型、爬虫扫描模型的触发机制进行设置，适应用户的实际使用环境，主要涉及**统计周期、访问 IP、访问端口、访问次数**等关键指标进行配置，满足设置的触发机制的风险才会产生告警信息

操作入口

在菜单栏选择“**配置➤检测配置➤扫描行为模型**”进入**扫描行为模型**页面。

点击开启该类型风险检测（启用模型需要在“**配置➤检测配置➤引擎管理**”页面确认**扫描行为**及其子模型开关已开启）；点击可以编辑该模型，更改配置内容。

4.2.19 拒绝服务攻击模型

对拒绝服务攻击模型的触发机制进行配置，适应用户的实际使用环境，主要涉及**统计周期、单包长度阈值、统计周期内访问阈值、统计周期内总流量阈值**等关键指标进行配置，满足设置的触发机制的风险才会产生告警信息

操作入口

在菜单栏选择“**配置➤检测配置➤拒绝服务攻击模型**”进入**拒绝服务攻击模型**页面。

点击开启该类型风险检测（启用模型需要在“**配置➤检测配置➤引擎管理**”页面确认**拒绝服务攻击**及其子模型开关已开启）；点击可以编辑该模型，更改配置内容。

4.3 联动配置

4.3.1 EDR 联动

APT 检测到恶意文件投递行为，且接收恶意文件的主机 IP 为内网 IP 时，同步该恶意文件 MD5 值和内网 IP 地址给 EDR 管控平台，由 EDR 管控平台返回该 MD5 值对应恶意文件的执行状态，如果样本还在该 IP 主机上，也返回该样本的路径。同时 EDR 会扫描该内网主机近期活跃文件，检测是否存在其他恶意文件。

操作入口

在左侧导航树选择“**配置➤联动配置➤EDR 联动**”进入 **EDR 联动配置**页面，选择 **EDR 管控中心**页签添加联动 EDR 设备信息。

- 选择**联动信息**页签可以查看样本投递时间、被投递病毒的 IP、样本文件 MD5、联动状态、样本执行结果、样本路径、EDR 病毒木马扫描结果。在操作项列下点击图标查看选中样本的详细信息。

4.3.2 WAF 联动

APT 支持与 Web 应用防火墙进行联动，阻断针对 Web 服务器的恶意攻击，从而达到更好的安全防护效果。

实现原理

WAF 联动的阻断类别分为两种，一种是基于源 IP 的阻断，一种是基于服务端 URL 的阻断。

当 APT 检测到流量中有上传 Webshell 且攻击状态为成功的行为、下载 Webshell 行为或某个源 IP 上传了恶意文件，会生成联动策略并通知 WAF 对 Webshell 页面或该 IP 的任何访问进行阻断。其中对于 Webshell 页面永久阻断，对上传恶意文件的源 IP 的阻断时间为 1 小时，阻断时间过后如再次上传恶意文件，则再次阻断 1 小时。

操作步骤

步骤1. 在菜单栏选择“**配置➤联动配置➤WAF 联动**”进入 **WAF 联动**配置页面。

步骤2. 选择 **WAF 设备**页签，点击<**新增**>，添加待联动的 WAF 设备。

步骤3. 选择**联动策略**页签，查看该策略相关联的阻断事件。

点击**策略溯源事件次数**列的数字，查看策略溯源详细信息，也可对策略进行启用和禁止操作。

步骤4. 选择**阻断事件**页签，查看阻断事件详情。

页面展示所有 WAF 回送的阻断事件，包括发生时间、源 IP、目的 IP、域名、报文和触发策略等，如下图所示。点击列表中的触发策略，可查看关联的原始风险。

- 对于 Webshell 攻击，WAF 阻断这个 Webshell 页面，所有 IP 都不能访问。返回给客户端的阻断页面如下所示。

- 对于恶意文件攻击，WAF 阻断客户端 IP 的访问，上传恶意文件的客户端 IP 对保护站点的所有 URL 都不能访问，其他 IP 对保护站点的访问正常。返回给客户端的阻断页面如下所所示。

4.3.3 防火墙联动

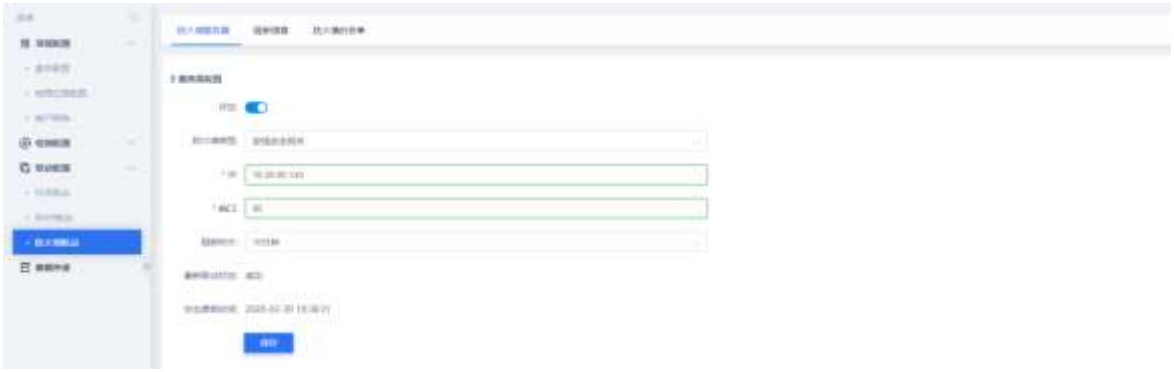
APT 支持与明御®安全网关（DAS-Gateway）进行联动。检测到风险信息后，触发 DAS-Gateway 对指定源 IP 列表进行阻断。其中阻断时长可统一在 APT 产品的防火墙联动页面中进行设定，默认为 10 分钟。

当攻击者（符合 APT 所定义的 Web 特征检测、扫描行为、web 后门访问、隐蔽信道、暴力破解、挖矿、远控工具利用等风险）是外网 IP 时，APT 会生成联动策略并通知 DAS-Gateway 对该攻击者进行阻断。

操作步骤

步骤1. 在菜单栏选择“**配置➤联动配置➤防火墙联动**”进入**防火墙联动**页面。

步骤2. 选择**防火墙服务器**页签配置联动防火墙，输入服务器 IP、端口（默认 80 端口）、阻断时长等。



步骤3. 点击**阻断信息**页签可查看阻断 IP、阻断开始时间、阻断结束时间、阻断状态。如果阻断过程中又有对应新的风险产生，会重新计算阻断结束时间，如下图所示：

- 点击<**阻断 IP**>可跳转页面展示该阻断 IP 的风险列表。

- 点击**操作项**下的 图标，可查看该阻断 IP 的风险详情信息。

- 点击**操作项**下的图标加入防火墙白名单，加入防火墙白名单后防火墙不再对该 IP 进行阻断，该 IP 仍能正常产生告警。

步骤4. 点击**防火墙白名单**页签，可以新增、启用、禁用和删除防火墙白名单。点击**状态**栏下的图标切换阻断 IP 的状态，灰色时表示不会阻断该 IP。

4.4 数据外送

数据外送指 APT 以网络流量综合探针形态运行时，采集到数据信息后把对应的风险信息、审计信息等上传到数据中心（如安恒信息的 AiLPHA 大数据平台），或以邮件、钉钉等方式发出通知。

使用须知

- 当 APT 平台从 V2.0.62 版本升级到 V2.0.63 及以上版本时，禁用的配置会被删掉，如需继续用此配置，请在升级前启用该配置。
- 服务器类型有 7 种：分别为 SYSLOG、KAFKA、邮件、FTP、短信、钉钉、上传恶意文件。

4.4.1 服务器配置

用户首先需完成服务器配置才能够开始数据外送。

操作步骤

步骤1. 登录 APT Web 系统，在菜单栏选择“**配置➤数据外送**”进入**数据外送**页面，选择**服务器信息**页签，点击<**新增**>，选择服务器类型、发送格式、数据加密等，点击<**下一步**>，直到完成配置。

相关配置项请参照下表：

参数名称	参数说明	参数取值
服务器类型	数据外送服务器类型。	SYSLOG\KAFKA\邮件\FTP\短信\钉钉\上传恶意文件共 7 种。
发送格式	服务器发送的格式。	默认选择 APT 风险通知。 KAFKA 服务器对接大数据产品可选择“**安恒 AILPHA 大数据平台 3.4 及以下版本接口规范(JSON 格式)或者安恒 AILPHA 大数据平台 3.5 及以上版本接口规范(JSON 格式)**”。
数据加密	数据是否加密。	是、否。
加密方式	选择数据加密方式	AES、SM4 当“**数据加密**”参数选择“**是**”的时候，该参数可配。
密钥	加密密钥。	默认或者自定义。 当“**数据加密**”参数选择“**是**”的时候，该参数可配。

步骤2. 点击<**下一步**>，在弹出的界面完成服务器配置。根据上一步勾选的服务器类型不同，界面参数也不同。详细参数配置可以参考下表。

参数名称	参数说明	参数取值
SYSLOG 服务器配置		

参数名称	参数说明	参数取值
服务协议	配置 SYSLOG 服务器传输协议。	UDP、TCP。
编码格式	配置SYSLOG服务器使用的编码格式。	◆ GBK：汉字编码字符集。 ◆ UTF-8：针对 Unicode 的可变长度字符编码。
IP	配置 SYSLOG 服务器 IP 地址。	输入 IP 地址。
发送者	配置风险消息发送者。	缺省值：dbapp。
端口	配置服务器使用端口。	缺省值：514。
接收设置（当 SYSLOG 服务器的“发送格式”选择“APT 风险通知”时，该参数可配）		
发送类型	配置风险通知消息的发送类型。	◆ 发送统计消息 ◆ 发送单条
类型	配置接收风险消息的类型。	点击下拉框选择。
等级	配置接收风险消息的级别。	点击下拉框选择。
KAFKA 服务器配置		
主题	设置 KAFKA 服务器的发送消息主题。	手动输入。
服务器版本	设置 KAFKA 服务器版本。	◆ 0.8.0 ◆ 0.9.0 及以上
服务器列表	设置 KAFKA 服务器列表。可以输入多个服务器，以 **IP:HOST 端口**方式填写。	例如：192.168.1.1:9092。

参数名称	参数说明	参数取值
是否需要压缩	配置 KAFKA 消息是否压缩传输。	是、否。
发送者	配置风险消息发送者。	缺省值：dbapp。
编码格式	配置服务器使用的编码格式。	◆ GBK：汉字编码字符集。 ◆ UTF-8：针对 Unicode 的可变长度字符编码。
服务器响应	配置是否需要等待 KAFKA 服务器响应再发送数据。	◆ 不等待：发送方不等待 KAFKA 服务器接收响应，直接发送数据。延迟最低，数据仅仅发送一次，可靠性低。 ◆ 等待 leader 应答：发送方等待 KAFKA 服务器写入 leader 消息后发送数据。延迟较低，可靠性稍高，但仍然有丢失数据可能。 ◆ 等待所有应答：发送方等待 KAFKA 服务器写入全部消息后发送数据。延迟较高，可靠性高，发送效率最低。
协议类型	选择协议类型	◆ 明文 ◆ SSL ◆ SASL 认证+明文 ◆ SASL 认证+SSL
邮件服务器配置		
发送邮件服务器	配置发送邮件服务器的域名或者 IP 地址。	手动输入。
发送者	配置风险消息发送者。	缺省值：dbapp。
DNS 服务器配置	配置邮件服务器的 DNS 服务器 IP。	缺省值为 114.114.114.114，可以更改。

参数名称	参数说明	参数取值
发送者邮箱	配置发送者邮箱。	手动输入。
SMTP 验证	配置是否使用邮件服务验证。	◆ 不需要验证：默认配置。 ◆ 需要验证：选择该参数，需要配置验证密码和加密类型（不加密、TLS 或 SSL 加密）。
端口	配置邮件传输服务使用的端口。	默认端口 25。
接收设置（邮件服务器）		
每类事件显示前	配置接收邮件的显示数目。	默认 100 条。可以手动输入。
接收邮箱地址	配置接收邮箱地址。	手动输入。可以配置多个接收邮箱。
FTP 服务器配置		
IP	配置 FTP 服务器的 IP 地址。	手动输入。
上传目录	配置 FTP 主目录的相对路径。	手动输入。默认主目录则填写“/”
端口	配置 FTP 服务器端口。	默认端口 21。
用户名/密码	配置 FTP 服务器登录用户名和密码。	手动输入。
编码格式	配置服务器使用的编码格式。	◆ GBK：汉字编码字符集。 ◆ UTF-8：针对 Unicode 的可变长度字符编码。
接收设置（FTP 服务器）		
单个文件最多显示前	配置单个接收文件最多显示的数目。	默认前 100 条。可以手动输入。

参数名称	参数说明	参数取值
接收统计信息	配置是否接收邮件统计信息。	是、否。
短信服务器配置		
服务器 IP	配置短信服务器 IP 地址。	手动输入，支持 IPv4 和 IPv6。
格式	短信服务器格式。	默认。
端口	配置短信服务器使用的端口。	手动输入。
编码格式	配置服务器使用的编码格式。	◆ GBK：汉字编码字符集。 ◆ UTF-8：针对 Unicode 的可变长度字符编码。
请求参数	配置短信服务器的请求参数。包括手机号码和短信，其中手机号码可配置。	手动输入手机号码。 短信不需要配置，默认为告警信息。
请求方式	配置短信服务器请求方式。	◆ GET：从服务器获取数据，安全性低。 ◆ POST：向服务器传送数据，安全性高。
URL	配置短信服务器的 URL 地址。	手动输入。
钉钉群机器人服务器设置		
机器人 URL	配置钉钉群机器人服务器URL地址。	手动输入。
上传恶意文件配置		
上传恶意文件的服务器 IP	配置上传恶意文件的服务器 IP。	手动输入。
上传风险相关恶意文件	配置是否上传风险相关恶意文件。	◆ 上传。 ◆ 不上传，默认值。

参数名称	参数说明	参数取值
上传风险相关沙箱报告	配置是否上传风险相关沙箱报告。	◆ 上传。 ◆ 不上传，默认值。
发送风险内容（当服务器类型选择“发送格式”选择“APT 风险通知”时，该参数需单独配）		
风险级别	配置发送特定级别的风险消息。	全部、高、中、低。
攻击状态	配置发送特定攻击状态的风险消息。	全部、成功、尝试、失陷。
风险类别	配置发送特定类型的风险消息。	点击下拉框选择。
客户网络	配置发送消息到特定的客户网络。	点击下拉框选择。 点击<**编辑**>，可跳转到“**配置➢客户网络**”页面进行配置。
数据发送配置（**当服务器类型选择“发送格式”选择“安恒 AILPHA 大数据平台”时，该参数可配**）		
审计信息	勾选是否发送审计信息及选择相关协议类型。	根据实际需要进行勾选。
风险信息	请参考“发送风险内容”。	请参考“**发送风险内容**”。
会话应用识别信息	勾选是否发送会话应用识别信息。	根据实际需要进行勾选。
会话应用流量统计信息	勾选是否发送会话应用流量统计信息及选择相关协议类型。	根据实际需要进行勾选。

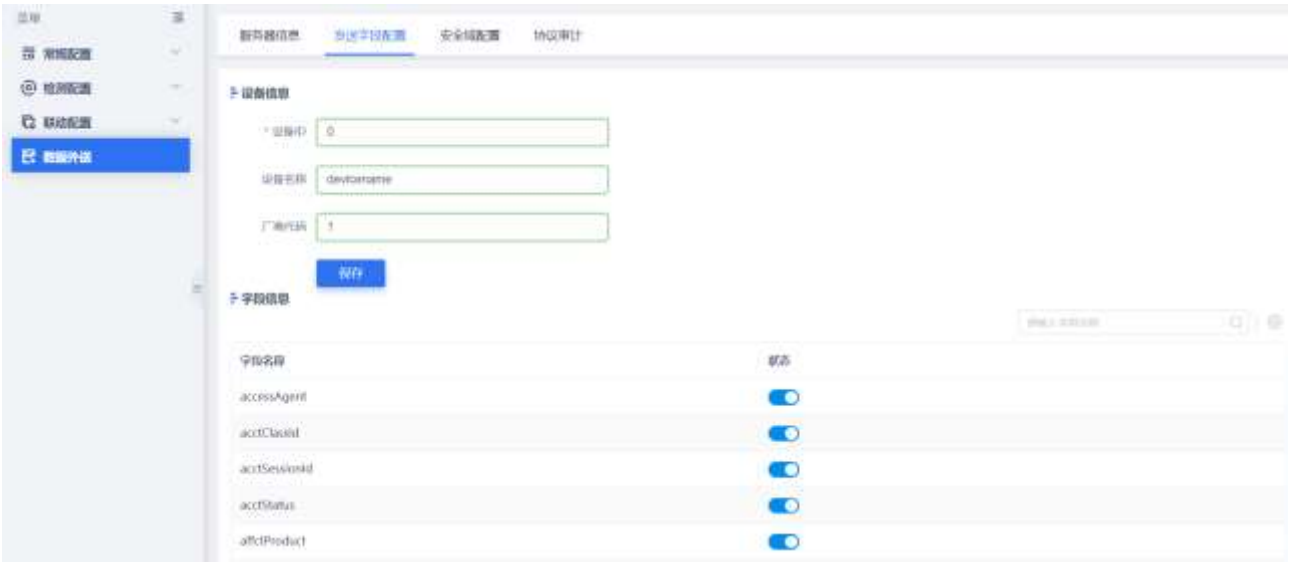
参数名称	参数说明	参数取值
传输层流量统计	勾选是否发送传输层流量统计。	根据实际需要进行勾选。
应用层统计信息	勾选是否发送应用层统计信息。	根据实际需要进行勾选。
登陆行为统计信息	勾选是否发送登陆行为统计信息。	根据实际需要进行勾选。
文件安全检测信息	勾选是否发送文件安全监测信息。	根据实际需要进行勾选。

- 发送数据时默认数据不加密，当发送数据时选择数据加密，密钥可以选择默认或者自定义，密钥加密方式是“**base64**”。
- 对于 KAFKA 服务器，系统支持安恒 AiLPHA 大数据平台 3.5 及以上版本接口规范(JSON 格式)，并且支持审计信息配置白名单时是否外送、告警时是否外送、非告警时是否外送。
- 勾选白名单时外送：支持 HTTP 协议的客户端白名单、服务端白名单、HTTP 的 IDS 规则。
- 勾选（非）告警时外送：支持 HTTP 协议和 DNS 协议的 IDS 规则。

4.4.2 发送字段配置

在主菜单选择“**配置**”，然后在左侧导航树选择“**数据外送➢发送字段配置**”，配置发送服务器的设备 ID、设备名称和厂商代码。

字段信息的字段适只适用于自定义 json 格式（对接安恒信息的 AiLPHA 大数据平台），默认发送开启的字段（**状态**栏下开关设置为 ）。



4.4.3 安全域配置

安全域配置用于从 AiLPHA 大数据平台上更新安全域、内网 IP、规则等，该功能默认关闭。

在主菜单选择“**配置**”，然后在左侧导航树选择“**数据外送➢安全域配置**”，配置 AiLPHA 大数据平台的 IP 以及端口并且启用该功能后，就可以从该平台上更新信息。

4.4.4 协议审计

协议审计用于控制服务器信息-审计信息部分，ICMP、NETFLOW 协议外送勾选按钮显示，默认关闭。

在主菜单选择“**配置**”，然后在左侧导航树选择“**数据外送➢协议审计**”，选择开启按钮，点击保存，就

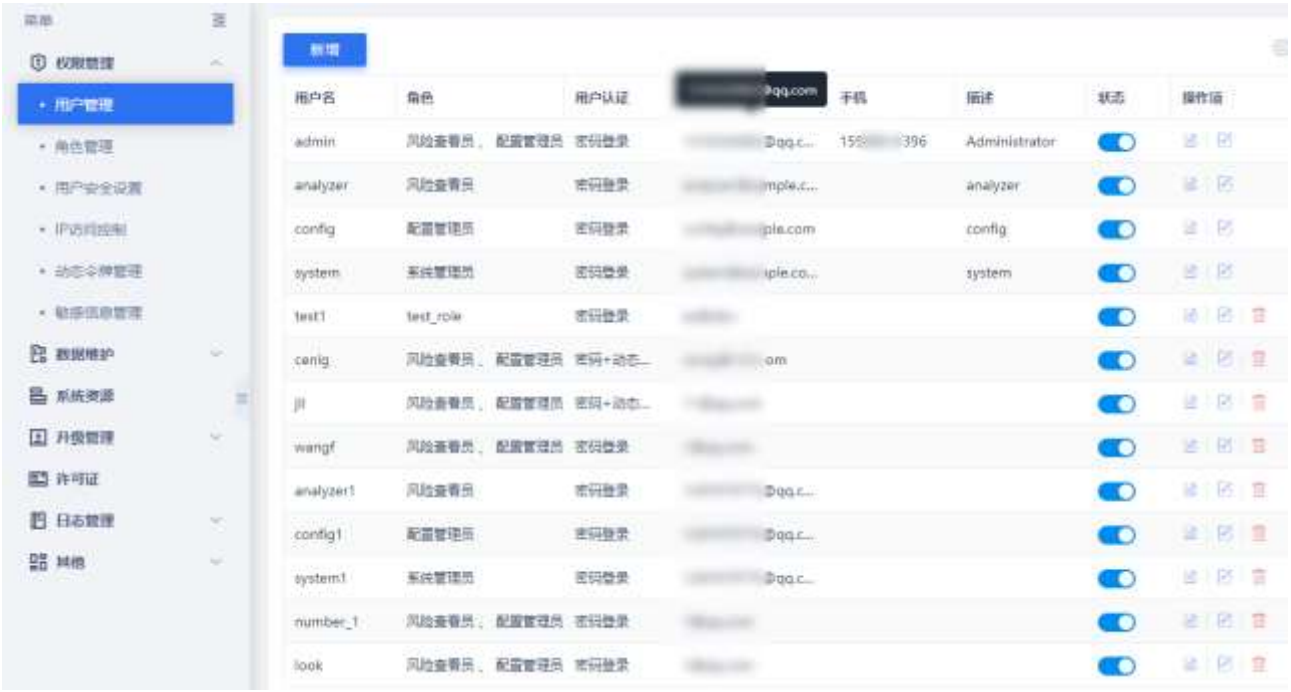
可以在配置服务器信息-审计信息部分勾选这两个协议。

5. 系统

登录数据中心（探测器）Web 界面可以看到“**系统**”选项卡下所有菜单。

分布式部署场景下，登录单个探测器 Web 界面，进入“**系统**”选项卡只能看到部分菜单，不能对“**系统**”配置进行修改。

系统菜单主要功能有**权限管理**、**数据维护**、**系统资源**、**升级管理**、**许可证**、**日志管理**和**其他**。系统配置功能可以让管理员用户更好的管理系统权限、数据、资源、许可、升级和日志等重要系统功能，让设备更加安全高效的运行。



5.1 权限管理

5.1.1 角色管理

系统内置四个角色为风险查看员、配置管理员、系统管理员和超级管理员。详细情况请参考系统自带用户和角色。

操作入口

在菜单栏选择“**系统➤权限管理➤角色管理**”进入**角色管理**页面。

点击<**新增**>添加角色并且赋予新角色对应权限。

5.1.2 用户管理

系统自带四个用户。对应系统缺省的四种角色，支持编辑但无法删除。

用户	角色	对应权限	初始密码
analyzer	风险查看员	查看导航、分析、风险记录、报表等	Dbapp@2014
config	配置管理员	配置引擎、策略、探测器、告警外送等	Dbapp@2014
system	系统管理员	拥有系统级别的配置、权限管理权限	Dbapp@2014
admin	超级管理员	系统所有权限	Dbapp@2014

操作入口

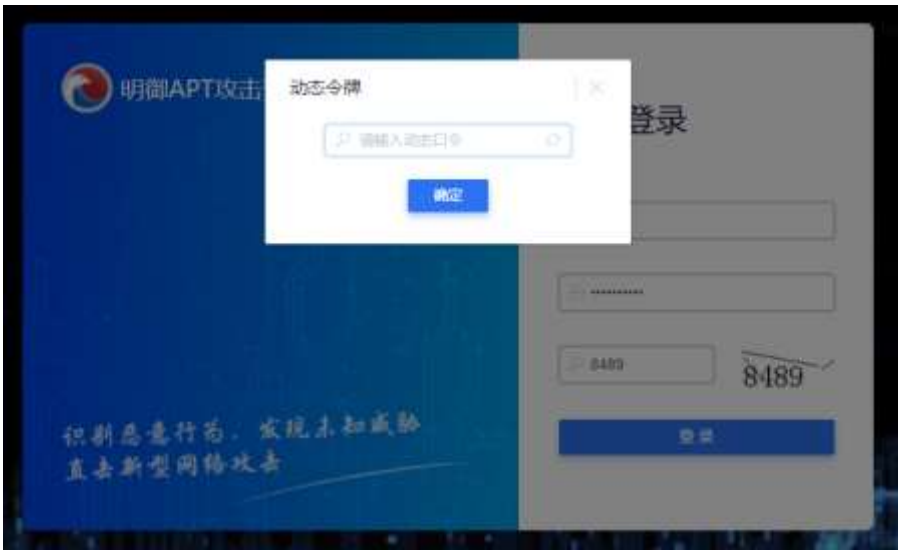
在菜单栏选择“**系统➤权限管理➤用户管理**”进入**用户管理**页面，点击<**新增**>创建新用户。支持对非系统

自带用户进行编辑和删除操作。

新建用户界面包括基本信息、联系方式、角色类型等，根据界面提示信息直接填写即可。点击状态启用或禁用该用户名。

登录认证方式可选择密码登录、密码+动态口令登录。动态令牌需要在“**系统➤权限管理➤动态令牌管理**”中导入对应的 xml 文件，具体配置请参考动 态 令 牌 管 理 。

认证方式为**密码+动态口令登录**的用户登录系统输入正确的用户名密码后还需要输入动态口令方可登录成功。



如果时间不一致，导致口令校验错误，可点击输入框中的同步按钮 进行同步，同步完成后输入当前口令即可。当前动态口令输入当前显示的口令，下一条动态口令输入当前口令改变后的下一条口令。

新增用户或修改用户密码后，系统暂不做强制性退出，需单独退出重新登录才能生效。

5.1.3 用户安全设置

在菜单栏选择“**系统➤权限管理➤用户安全设置**”进入**用户安全设置**页面。

配置安全相关选项，包括登录安全设置、密码长度设置、密码过期设置、超时设置等。

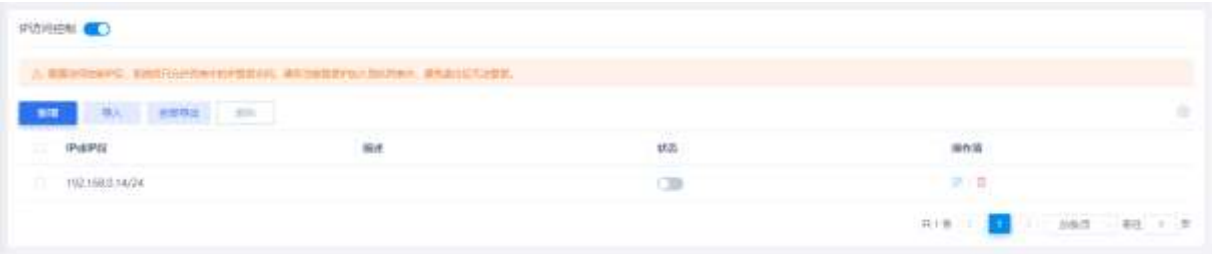
5.1.4 IP 访问控制

在菜单栏选择“**系统➤权限管理➤IP 访问控制**”进入 **IP 访问控制**页面。

- 启用该功能时，可以新增、修改、删除、导入访问该设备的 IP 地址或者 IP 地址段。开启后，只有当前列表中的 IP 地址可以访问 APT 设备。

  若列表中无数据或所有 IP 都被禁用，IP 访问控制无效，所有 IP 都可以访问。

- 禁用该功能时，不容许新增、导入、全部导出、删除 IP 访问控制列表等操作。所有 IP 都可以访问 APT 设备。



5.1.5 动态令牌管理

导入对应的 xml 文件，列表上会显示动态口令的序列号、生产时间、失效时间。

5.1.6 敏感信息管理

操作入口

在菜单栏选择“**系统➤权限管理➤敏感信息管理**”进**入敏感信息管理**页面。

系统用户查**弱密码、暴力破解、密码明文传输**类型风险详情时，需输入**敏感信息管理密码**才能够查看告警中含有的密码信息、下载或者在线预览数据包。

系统分为三类用户：**无权限用户、需要验证密码用户、无需验证密码用户。**

管理密码可以默认同 admin 账号密码，也可以新建管理密码。

无需验证用户，密码直接显示，数据包可以下载和在线预览；

无权限用户查看相应风险详情时，密码隐藏，无查看按钮，无法下载预览数据包，如图所示。

需要验证密码用户查看相应风险详情时，密码隐藏，查看按钮显示；点击弹出敏感信息密码输入弹框，如图所示。

5.2 数据维护

数据维护配置包括备份与恢复、自动清理和出厂设置等相关配置。

备份和恢复只能在每台机器上面单独完成，数据中心不能控制探测器的备份和恢复。

5.2.1 自动备份

自动备份采用备份前一天的告警数据方式完成，并且提供 FTP 自定义时间点外送到备份服务器上以及上传备份文件的功能。

无论是否配置 FTP 服务器及发送配置，数据都会在本地自动备份。为了确保备份数据安全性，建议配置 FTP 服务器并且开启备份数据自动外送功能。

备份选项卡配置功能点包括：备份文件存放目录、占用所属分区最大比例、FTP 服务器及发送配置以及历史备份记录等。

应用举例

使用场景：每天 0 点时开始备份，上传到备份服务器 192.168.33.196 的目录为/data/recv/backup。

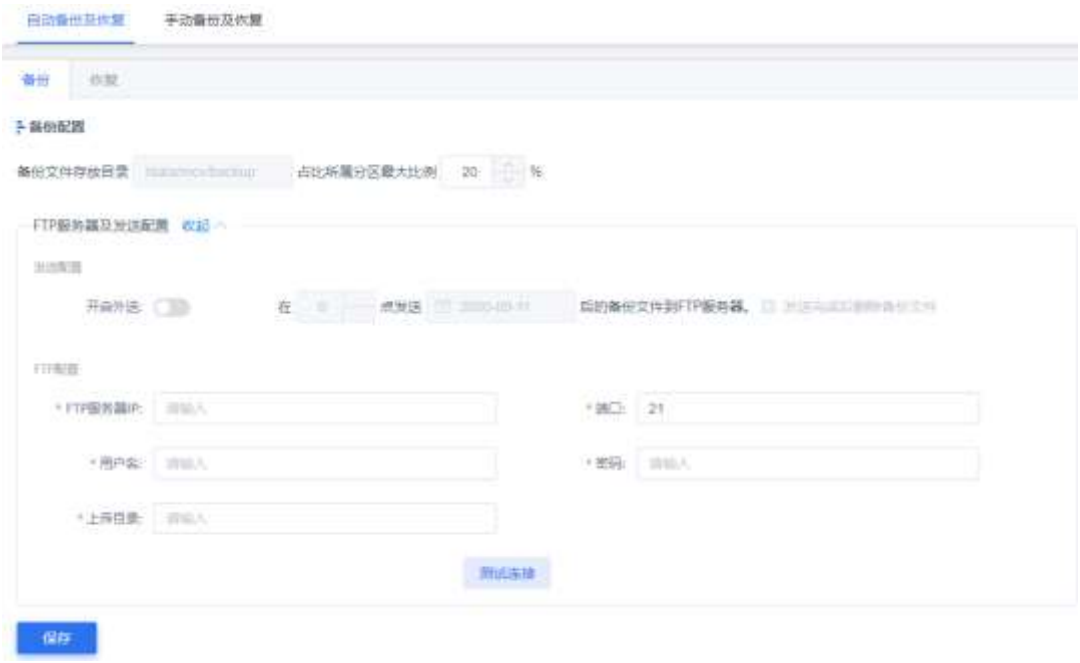
操作步骤

步骤1. 登录 APT Web 界面，在菜单栏选择“**系统➢数据维护➢备份和恢复**”进入**备份与恢复**页面，选择**自动备份及恢复**页签。

步骤2. 选择“**备份**”页签，设置自动备份参数。

1) 设置备份占用所属分区最大比例为 20%。

2) 配置 FTP 服务器，备份文件产生后将自动上传到 FTP 服务器。需要确保 FTP 服务器可用，配置完成后，点击<**测试连接**>测试 FTP 服务器是否可用。



步骤3. 点击<**保存**>。

步骤4. 当时间到次日 0 点时，备份文件生成后，可以在历史备份记录列表中查看备份文件。备份文件会自动上传到 FTP 服务器。

5.2.2 自动恢复

点击<**恢复向导**>进行数据恢复操作。

操作步骤

步骤1. 在菜单栏选择“**系统➤数据维护➤备份和恢复**”进入**备份与恢复**页面，选择**自动备份及恢复**页签。

步骤2. 选择**恢复**页签。

步骤3. 点击<**恢复向导**>，选择备份文件存在的位置。

有两个位置供选择：一个是本地目录：/data/recv/backup，一个是 FTP 服务器。本地目录为必选，

如选择 FTP 服务器，系统会通过 FTP 服务器上的备份文件进行恢复。

步骤4. 点击<**下一步**>，选择数据的发生时间段进行恢复。

1) 选择要恢复的探测器。

2) 选择要还原的时间范围和数据类型，然后点击<**完成**>。

步骤5. 在弹出的提示框点击<**确定**>，提交自动恢复任务。

步骤6. 等待几分钟，在恢复列表中查数据恢复情况。

5.2.3 手工备份

操作步骤

步骤1. 在菜单栏选择“**系统➤数据维护➤备份和恢复**”进入**备份与恢复**页面，选择**手动备份及恢复**页签。

步骤2. 选择**备份**页签。

步骤3. 点击<**备份当前配置**>，备份系统当前的配置信息。

备份完成后，在备份文件列表点击该备份文件可以下载到本地。

5.2.4 手工恢复

操作步骤

步骤1. 登录系统 Web 管理界面，点击“**系统**”主菜单，在**备份和恢复**页面，选择**手动备份及恢复**页签。

步骤2. 选择**恢复**页签，上传备份文件进行手动恢复数据。

该操作会导致原有配置被覆盖，使用时请谨慎操作。

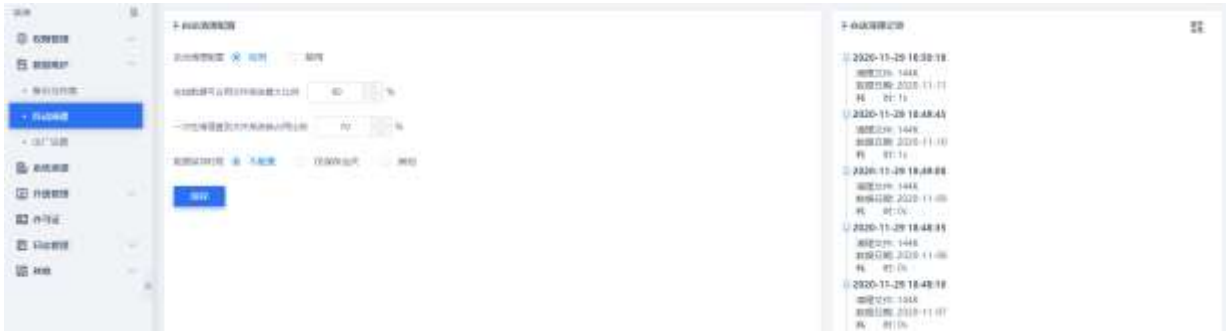
5.2.5 自动清理

开启自动清理配置后，可以防止在线数据占满系统存储空间。

在菜单栏选择“**系统➤数据维护➤自动清理**”进入**自动清理配置**页面，启用或禁用该功能。

当存储空间达到系统配置阈值上限（如下图配置的 80%）就会清理业务数据及文件系统中的部分文件，直到占用空间低于配置阈值下限(如下图中配置的 70%)。

系统默认不配置数据保存时限，用户可以根据自己需要进行配置，界面如下所示。



- 清理动作门限可配置。默认 80%，即当数据分区的磁盘空间被占用超过 80%后，系统会自动清理数据直到空间占用小于 70%（默认值，可配置），由最老的数据开始清理。
- 在线数据文件保存目录默认使用数据分区“/data”。
- 清理数据前会先进行数据备份，除非备份目录也达到清理上限。

5.2.6 出厂设置

出厂设置包含两个功能，一个是**清理业务数据**，一个是**恢复出厂设置。**

第一次设备出厂时做清空测试业务数据。此功能会清空系统内部数据，请谨慎操作。

在主菜单选择“**系统**”，然后在左侧导航树选择“**数据维护➢出厂设置**”。

清理业务数据

删除全系统所有业务相关的数据，包括风险、审计、报表、日志信息等（配置信息不会删除）。

请慎重执行！

恢复出厂设置

删除系统所有数据及配置信息，恢复到出厂状态，请慎重执行！

恢复出厂设置后，**admin** 密码会恢复为初始密码 **Dbapp@2014**。

5.3 系统资源

在菜单栏选择选择“**系统➢系统资源**”查看系统自身或各个探测器运行状态，包括 CPU 使用率、内存使用率等。

5.4 升级管理

5.4.1 手动升级

5.4.1.1 系统版本/排错版本升级

前提条件

已经获取版本升级包文件且文件版本比系统当前版本新。

- 系统版本升级包示例：
  GoldenEyeIPv6_B9A2C_sen2.0.66.22621.201216_ser2.0.66.22620.201216_r23146.encrypt.tar.gz
- 排错版本升级包示例：
  GoldenEyeIPv6_1F350_maintain2.0.66.22457.201210_r23158.encrypt.tar.gz

---

系统版本升级和排错版本升级操作方法相同。

升级步骤

步骤1. 在菜单栏选择“**系统➢升级管理➢手动升级**”进入**手动升级**页面，选择**版本升级**页签。

步骤2. 点击<**选择文件**>，选择版本升级文件点击上传。

步骤3. 确认升级成功。

1) 上传成功后，等待一段时间完成升级。

- 对于系统版本升级，一般需要等待 10~20 分钟左右的时间。若升级版本跨度较大，需多等待一段时间。
- 对于排错版本升级，一般等待 5 分钟左右就可以。

2) 点击上图的<**刷新**>按钮。

3) 重新登录 APT 系统，再次进入上图页面查看右下方的升级信息。如果升级时间信息和升级结果信息显示与本次升级操作时间以及版本号一致，则表明本次升级成功。

相关操作

当有添加探测器的情况下，可以在数据中心设备的“**探测器**”菜单下点击 按钮对探测器进行手动升级，若不进行手动升级，探测器也能从数据中心自动同步版本并升级。

5.4.1.2 策略版本升级

完成系统版本升级和排错版本升级后，检查策略库版本信息，如果获取的策略包比当前系统显示的版本新，则执行策略库版本升级操作。否则无需升级策略库版本。

前提条件

已经获取策略库升级包文件且文件版本比系统当前版本新。

策略版本升级包示例：**GoldenEyeIPv6_17DEC_strategy2.0.22505.201212.1.encrypt.tar.gz**

升级步骤

步骤1. 在**手动升级**页面，选择**策略库升级**页签。

步骤2. 点击<**选择文件**>按钮，选择版本升级文件点击上传。

步骤3. 确认升级成功。

1) 上传成功后，等待 5 分钟左右的时间。若升级版本软件包较大，需多等待一段时间。

2) 点击上图的<**刷新**>按钮。

3) 重新登录 APT 系统，再次进入上图页面查看右下方的升级信息。如果升级时间信息和升级结果信息显示与本次升级操作时间以及版本号一致，则表明本次升级成功。

5.4.2 在线升级

除了本地手动升级外，还可以通过在线升级方式对产品进行升级。

操作前提

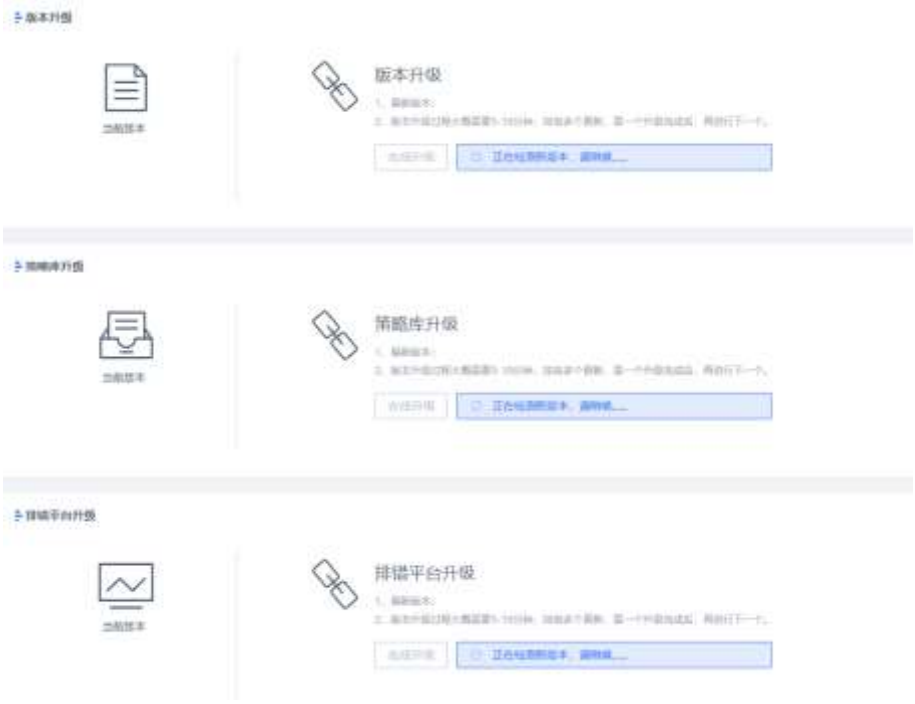
- APT 设备具有外网访问权限，可以连接 APT 云端服务器。
- 当云端服务器的版本升级包、排错升级包、策略升级包比当前设备的版本要新的时候，在线升级界面就会显示有最新版本可以更新，点击实时升级按钮即可升级。

操作方法

步骤1. 登录 APT Web 管理页面，在菜单栏选择“**系统>升级管理>在线升级**”进入**在线升级**页面。

步骤2. 点击<**在线升级**>按钮进行升级。

- 有多个更新时，需要一个升级完成后再进行下一个升级。
- 策略升级需要在版本升级完成后进行。



步骤3.　升级验证。

等待升级完成后，重新进入“**在线升级**“页面，查看当前版本是否为最新版本。

5.4.3 云端配置

开启云端配置后，APT 可以引入安恒信息的云端威胁情报等资源，提升检测能力及对新发安全事件的响应速度。云端配置功能包括云端配置和云端功能配置。

使用前提

APT 设备可以访问云端服务器。

操作入口

在菜单栏选择“**系统>升级管理>云端配置**”进入**云端配置**页面，点击**云端配置**开关 开启或关闭云端配置功能。可使用默认的云端地址或者手动配置云端地址和端口。

可使用默认的云端地址或者手动配置云端地址和端口。

编辑云端地址时可选择<**代理服务**>，需填写代理服务地址、端口、认证用户名和认证密码。

代理服务器（Proxy Server）可以代理网络用户访问网络信息。增加代理服务功能，便于内网用户通过代理服务访问云端内容，进行云端功能配置。

配置完成后点击<**保存**>。点击<**在线验证**>查看云端配置是否可以正常使用。

云端功能配置

配置是否使用各种云端功能。包括策略库自动更新、上传恶意样本到云端、紧急事件云端同步、威胁情报更新、版本自动更新、排错平台自动更新等。

5.4.4 托管配置

托管配置是将本地设备托管到大数据平台，可以由大数据平台进行统一管理，对设备版本升级、许可证更新进行同步等操作，本地设备无法再对这些功能进行操作。

配置成功后，APT 产品可以从大数据平台同步关闭 IDS 规则，对 IDS 规则进行管理；独立沙箱产品可以从大数据平台同步文件检测配置。

操作入口

在 APT 管理界面选择“**系统➤升级管理➤托管配置**”菜单，点击**服务器配置**区域的状态开关按钮开启或关闭服务器托管功能。

- 当状态开关打开时，可以编辑托管服务器地址，须填写 **IP 域名**和**端口**号，点击<**保存**>即刻生效。

- 点击<**取消托管**>，可关闭该功能。

5.5 许可证

查看当前系统许可证的使用期及维护期。

操作入口

在菜单栏选择“**系统➤许可证**”进入**许可证**页面。

点击<**上传许可**>上传并更新许可证。

申请许可时需注意产品形态，请选择用户需要的”许可类型”。

5.6 日志管理

5.6.1 系统日志

记录系统运行相关日志信息，包括异常日志、通讯日志和其他日志等。

操作入口

在菜单栏选择“**系统➤日志管理➤系统日志**”进入**系统日志**页面。

查看所有系统日志，点击 输入筛选条件查询日志；点击日志对应的 查看日志详细信息、处理日志。

系统支持系统日志的导出。

5.6.2 操作日志

记录用户对系统的操作信息，包括登录系统、退出系统及各种新增、修改、删除等信息。

操作入口

在菜单栏选择“**系统➤日志管理➤操作日志**”进入**操作日志**页面。

查看所有操作日志，点击 输入筛选条件查询日志；点击日志对应的 查看日志详细信息。

系统支持操作系统日志的导出。

5.6.3 升级日志

记录设备升级信息，便于用户查看版本、策略等升级记录和升级结果。

操作入口

在菜单栏选择“**系统>日志管理>升级日志**”进入**升级日志**页面。

查看所有升级日志，点击日志对应的 查看日志详细信息。系统支持升级日志的导出。

5.7 其他

5.7.1 SNMP 配置

简单网络管理协议（SNMP）是用于 IP 网络管理（服务器、工作站、路由器、交换机等）的一种标准协议，属于应用层协议。

启用 SNMP 配置后，APT 设备作为 SNMP 服务器，客户端可以通过 oid 向 APT 发送请求并建立联系。

操作入口

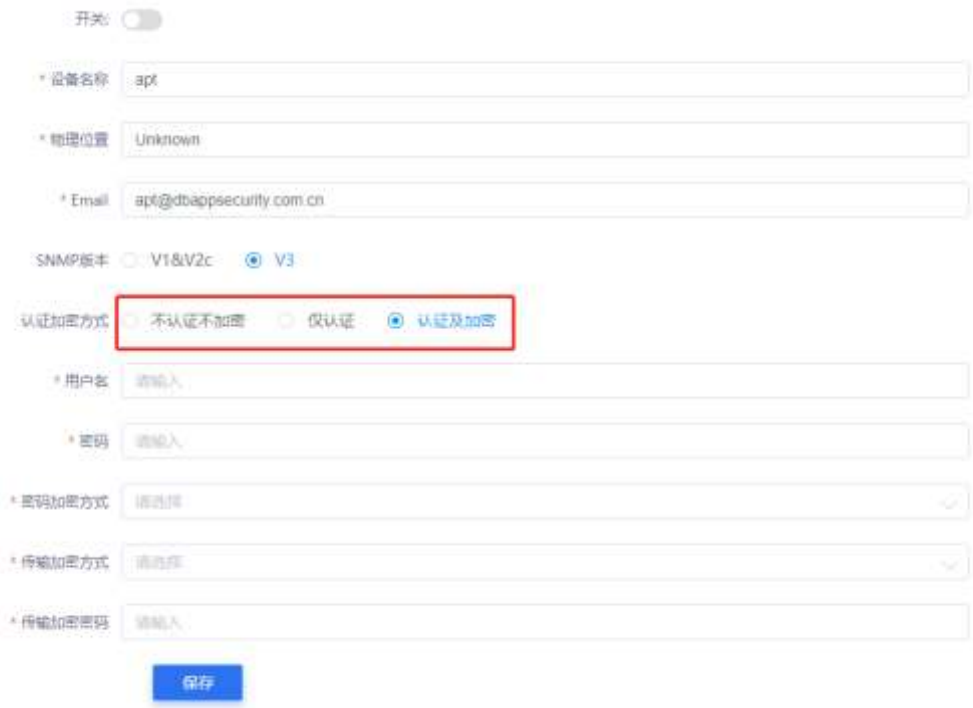
在菜单栏选择“**系统➤其他➤SNMP 配置**”进入 **SNMP 配置**页面。

滑动开关开启或关闭 SNMP 功能。

开启 SNMP 配置之前需要确认 APT 设备的防火墙中是否开启 SNMP 服务，可以在“**系统➤系统资源**”菜单下按“Shift+I”组合键查看 SNMP 服务是否开启。

- SNMP 版本为 V1&V2C 时，配置 Community string 值。配置界面如下。

- SNMP 版本为 V3 时，认证方式有不认证不加密（noAuthNoPriv）、仅认证（authNoPriv）、认证及加密（authPriv）这 3 种，需要配置用户名、密码、密码加密方式（MD5、SHA1）、传输加密方式(DES、AES)、传输加密密码等，配置界面如下。



5.7.2 网络配置

网络配置包括管理口配置（包括 IP 版本、管理口 IP、子网掩码、网关等）、DNS 配置以及业务口配置等。

操作入口

在菜单栏选择“**系统➤其他➤网络配置**”进入**网络配置**页面。

业务口配置功能可以自定义选择不需采集流量的网口，配置界面如下所示。


业务口配置
业务口选择:
待选择
0/10
eth0
eth1
eth11
eth2
eth4
eth5
eth6
eth7
已选择
0/1
eth3
保存

6. 分析

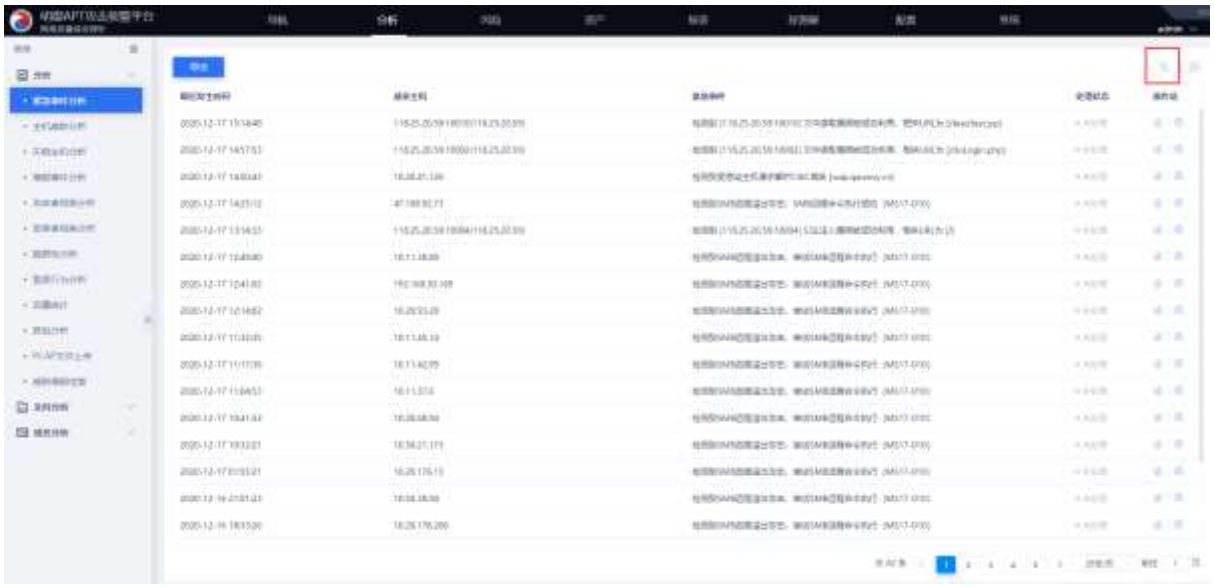
6.1 分析

6.1.1 紧急事件分析

以列表形式展现当前用户网络环境中出现的必须紧急处理的安全事件（**默认显示未处理的紧急事件**），让用户更直观、更客观、更准确地感知紧急事件，处理紧急事件。

操作入口

在菜单栏选择“**分析>分析>紧急事件分析**”进入**紧急事件分析**页面。



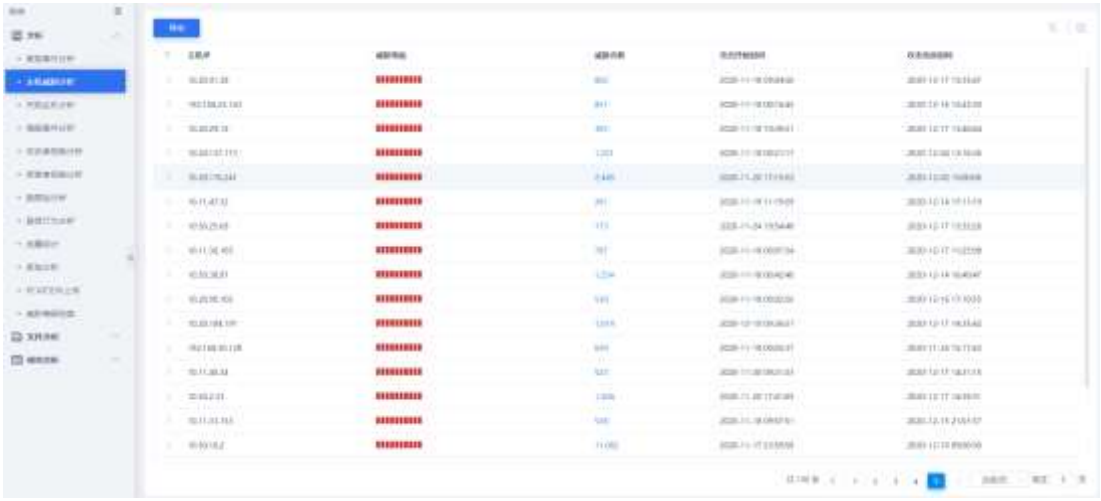
- 点击页面右上角的 ，输入筛选条件查询紧急事件；点击 查看紧急事件详细信息，可以在跳转页面点击<**处理**>确认紧急事件；点击 直接确认紧急事件。
- 点击<**导出**>以表格形式导出当前紧急事件。

6.1.2 主机威胁分析

主机威胁分析基于不同风险事件对网络安全的威胁程度换算成一个可直观显示的数值，以便让用户更直观、更客观、更准确地感知一个风险事件的威胁程度或者某个 IP 可能产生的风险影响范围。

操作入口

在菜单栏选择“**分析➤分析➤主机威胁分析**”进入**主机威胁分析**页面。



查看主机威胁详细信息

点击主机威胁分析任意一条记录或者点击列表中 > 图标，可以展开查看主机 IP 的威胁指数、攻击溯源、攻击过程、攻击溯源可视化选项卡等详细信息。

6.1.2.1 主机威胁指数

主机威胁指数选项卡展示主机IP在最近30天内的威胁活动和威胁性指数。如果主机存在相关的威胁活动，包括被攻击行为或者主动攻击行为，则对应的威胁活动阶段会有一个绿色小图标。

例如，如果主机被渗透入侵或入侵他人，则威胁活动中的“**渗透入侵**”阶段会有一个绿色小图标 

，图标上面的数字表示渗透入侵活动的次数。点击图标查看威胁详情。

6.1.2.2 攻击溯源、攻击过程和攻击溯源

- 选择**攻击溯源**选项卡，页面展示攻击溯源时间轴，包括攻击类型、攻击次数和攻击状态等。如下图所示，点击**攻击次数**可查看具体攻击行为。

- 选择**攻击过程**选项卡，页面展示攻击过程图形化攻击阶段图。如下图所示，点击**攻击次数**可查看具体攻击行为。

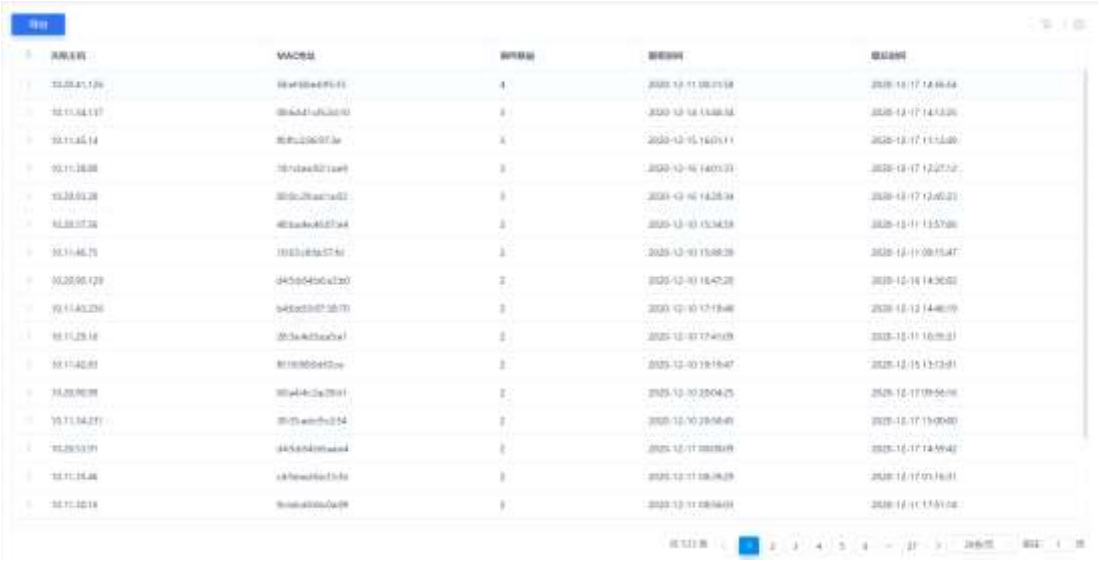
- 选择**攻击溯源可视化**选项卡，页面展示攻击溯源图形化攻击阶段图。

6.1.3 失陷主机分析

展示失陷主机被攻击情况，包括失陷主机 IP、MAC 地址、事件数量、最初时间、最后时间等。可快速发现所有失陷主机及相关取证信息。

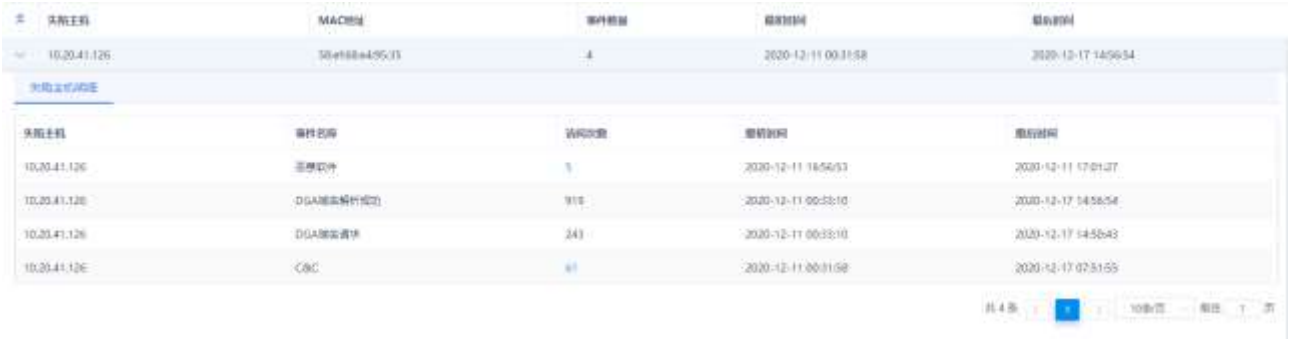
操作入口

在菜单栏选择“**分析>分析>失陷主机分析**”进入**失陷主机分析**页面。



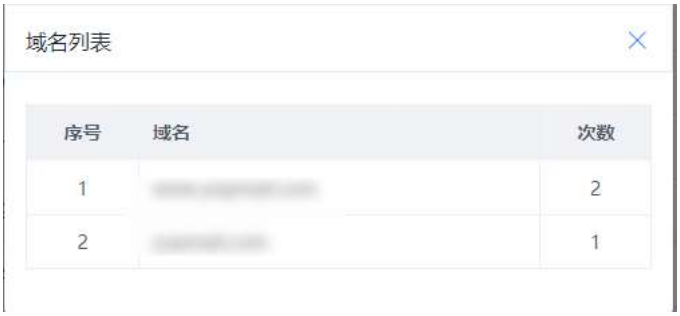
查看失陷主机详细信息

- 选择任意一条数据，点击 > 图标查看失陷主机事件名称和访问次数等信息。



- 点击**失陷主机明细**列表中任一条数据 IP 位置可以跳转链接至**风险**页面查看详情。

- 当事件名称为**远程控制（威胁情报）**类型的风险数据时，点击**访问次数**列对应的数字可以展示域名列表。



查询失陷主机

点击页面右上方的 ，根据风险类型、失陷主机名称、事件名称、时间范围等参数进行查询。

其中，事件名称可以输入部分内容进行模糊查询。

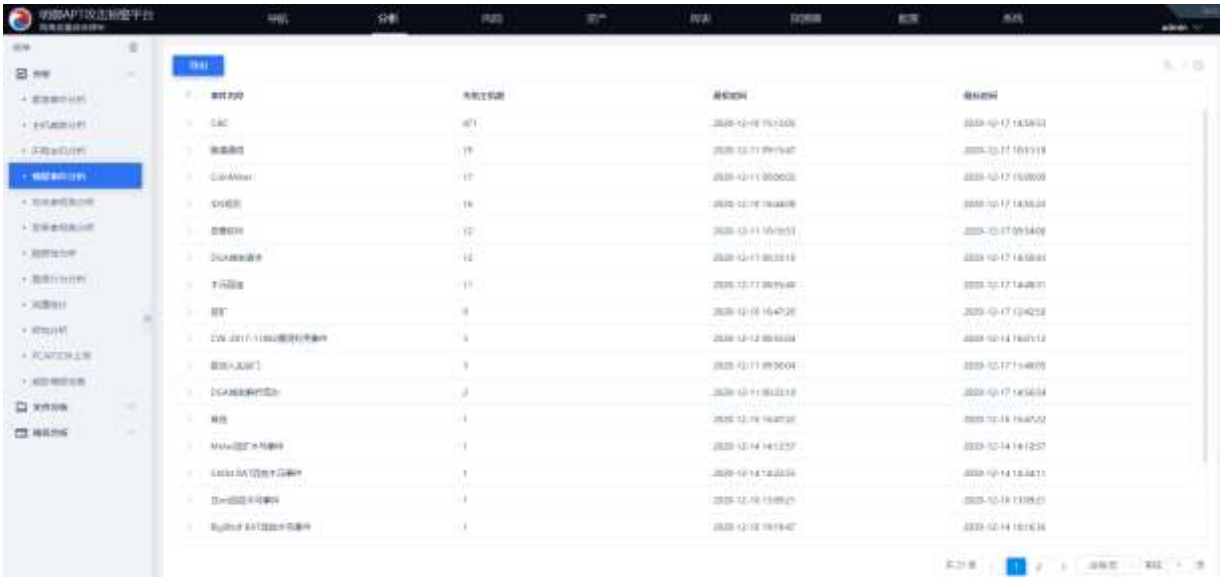
6.1.4 情报事件分析

情报事件分析是以事件角度查看失陷主机，将同一类事件合并展示，显示事件名称、失陷主机数，最初时

间、最后时间等。通过查看情报分析，可快速掌握同一风险事件有哪些失陷主机、访问次数以及最早发生时间和最晚发生时间。

操作入口

在菜单栏选择“**分析>分析>情报事件分析**”进入**情报事件分析**页面。



查看情报事件明细

- 选择任意一条数据，点击 > 图标查看失陷主机事件名称和访问次数等信息。

- 点击**情报事件明细**列表中任一条数据可以跳转链接至**风险**页面查看详情。
- 当事件名称为**远程控制 (威胁情报)** 类型的风险数据时，点击**访问次数**列对应的数字会展示域名列表。

查询情报事件

点击页面右上方的 ，根据风险类型、事件名称、时间范围查询参数进行查询。事件名称可以输入部分内容进行模糊查询。

6.1.5 攻击者视角分析

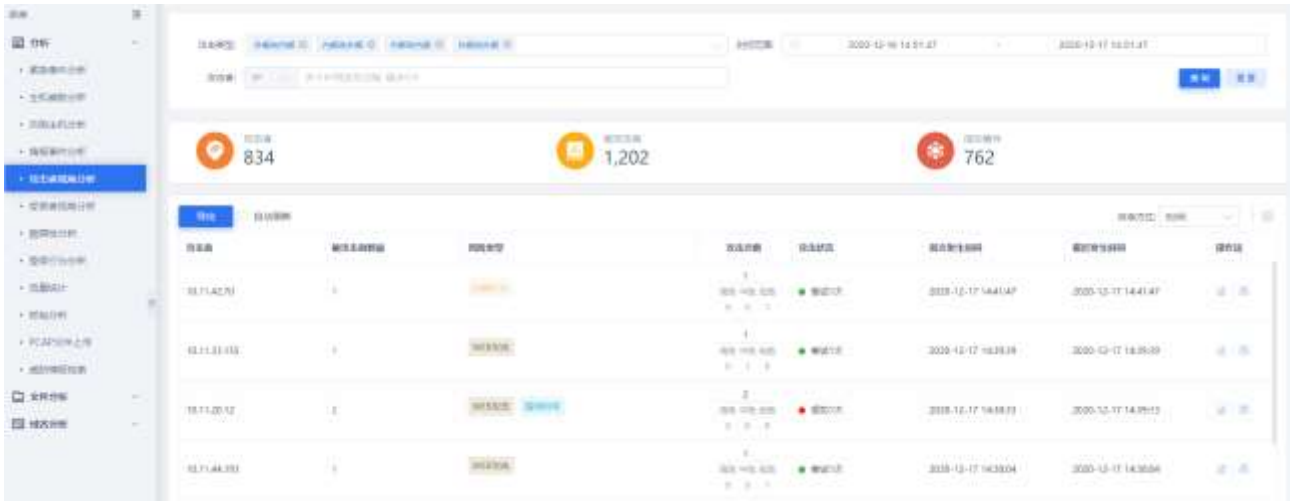
攻击者视角分析从多方面展现攻击事件，包括攻击方向、攻击者 IP 数、被攻击者 IP 数和攻击成功事件数目，便于用户清晰了解网络攻击情况，快速处理风险。

用户可以通过攻击方向、时间范围及攻击者 IP 查找相关攻击事件，快速获悉攻击者 IP、攻击手段、攻击资源等信息。

攻击者视角分析列表展示当前时间范围内的攻击者事件，包括攻击者 IP、被攻击者数量、风险类型、攻击方向、攻击次数、攻击状态、发生时间等。

操作入口

在菜单栏选择“**分析>分析>攻击者视角分析**”进入**攻击者视角分析**页面。



- 点击<**导出**>导出所有的攻击者 IP，方便用户进行排查。
- 在攻击者列表的**操作项**列下，点击 或列表中被攻击者数量列的数字可以展示该攻击者 IP 详细信息。

- 继续在指定 IP 的风险详情页面点击 ，跳转到**风险**页面显示风险详情。

- 点击<**处理**>或 处理事件，完成对攻击事件的后续处理。确认处理后，此条攻击者 IP 将不会在界面显示。

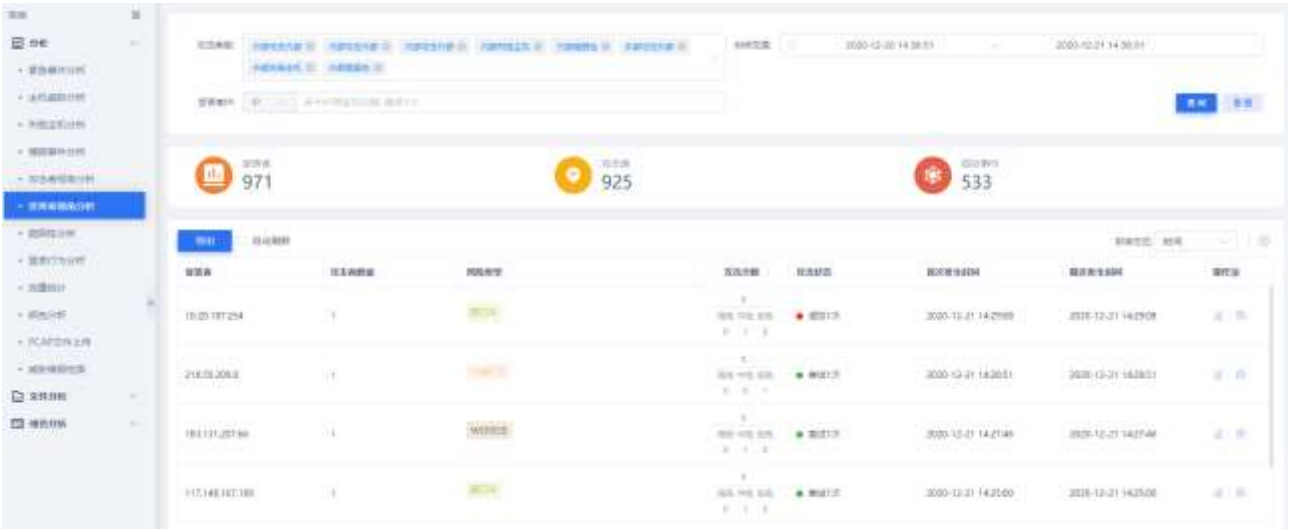
6.1.6 受害者视角分析

受害者视角分析从受害者视角展示内部资产受攻击情况，包括攻击方向、攻击者 IP 数、受害者 IP 数和攻击成功事件数目，便于用户清晰了解网络攻击情况，快速处理风险。

用户可以通过攻击类型、时间范围及受害者 IP 查找相关事件，快速获悉受害者 IP、受攻击手段、受攻击资源等信息。受害者视角分析列表展示当前时间范围内的事件，包括受害者 IP、攻击者数量、风险类型、攻击方向、受攻击次数、受攻击状态、发生时间等。

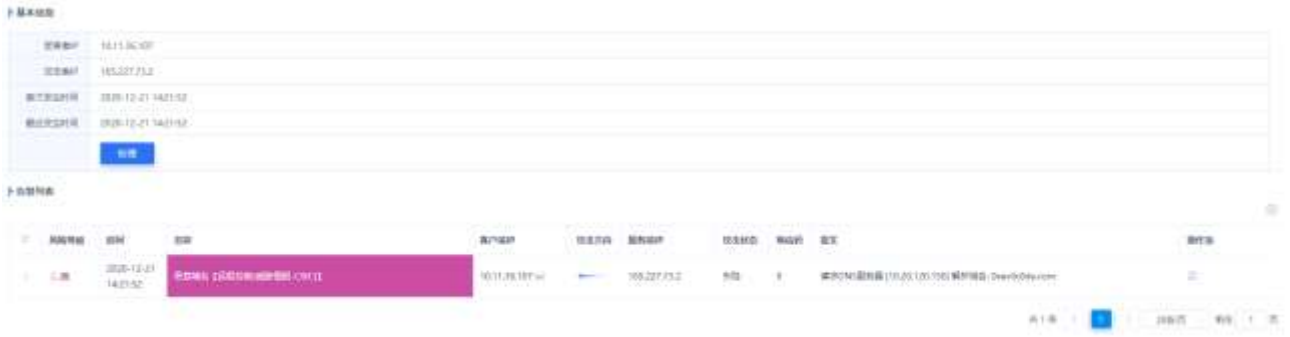
操作入口

在菜单栏选择“**分析>分析>受害者视角分析**”进入**受害者视角分析**页面。



- 点击<**导出**>导出所有的受害者 IP，方便用户进行排查。
- 在受害者列表的**操作项**列下，点击 或列表中攻击者数量列的数字可以展示该受害者 IP 详细信息。

◆ 继续在指定 IP 的风险详情页面点击 ，跳转到**风险**页面显示风险详情。



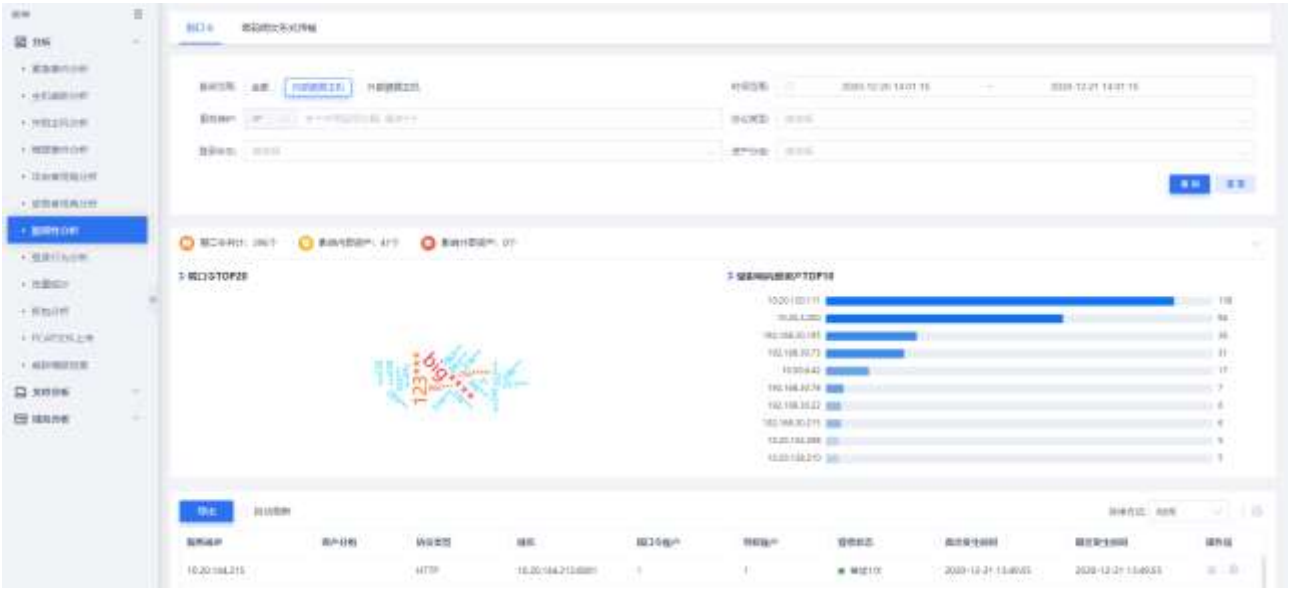
◆ 点击<**处理**>或 处理事件，完成对事件的后续处理。确认处理后，此条受害者 IP 将不会在界面显示。

6.1.7 脆弱性分析

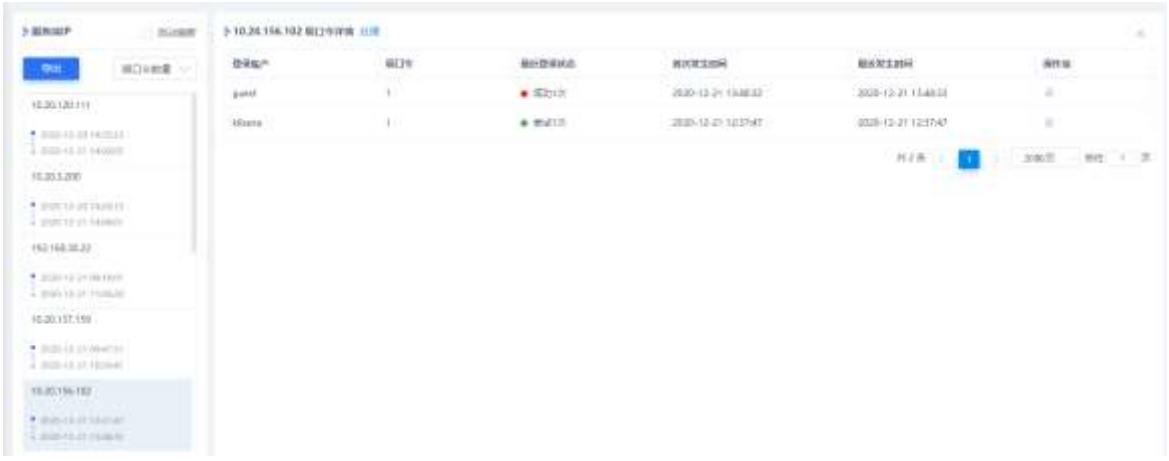
脆弱性分析统计**弱口令、密码明文传输**类型风险受到影响的主机、账号信息，展示弱口令 TOP20、受影响内部资产 TOP10，便于用户清晰了解自身密码相关的风险信息，快速处理风险

操作入口

在菜单栏选择“**分析➤分析➤脆弱性分析**”进入**脆弱性分析**页面。



- 点击<**导出**>导出主机信息，方便用户进行排查
- 在弱口令列表的**操作项**列下，点击 可以展示 IP 下弱口令的详细信息。



- 继续在指定 IP 的风险详情页面点击 ，跳转到**风险**页面显示风险详情。

6.1.8 流量统计

流量统计页面展示统计时间内 APT 采集的网络流量，并且实时更新，方便用户了解统计时间内 APT 流量

采集情况。

操作入口

在菜单栏选择“**分析>分析>流量统计**”进入**流量统计**页面。

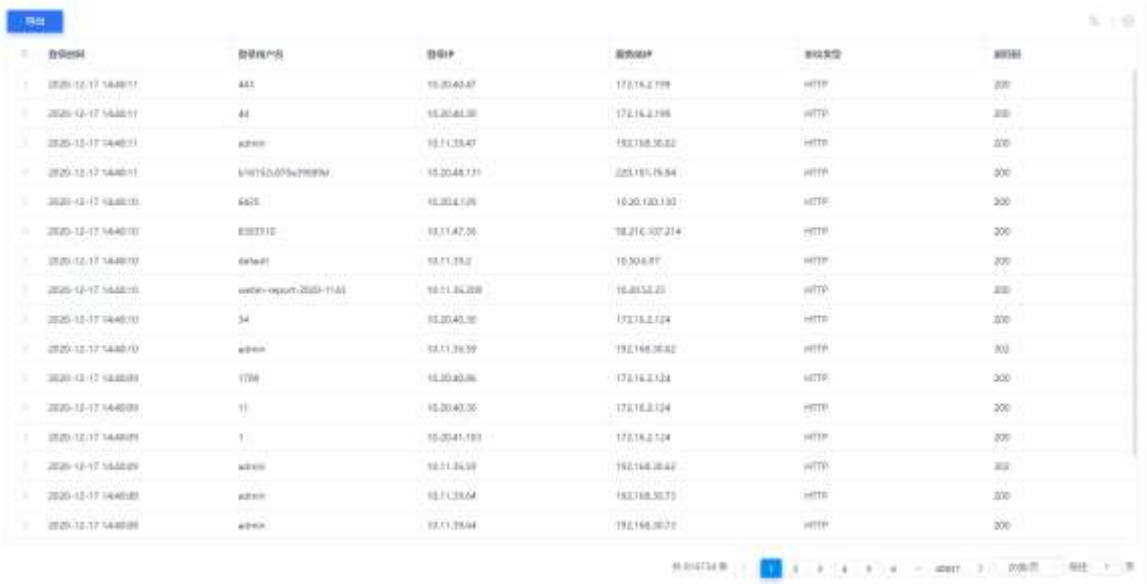
点击**流量统计折线图**右上方的时间按钮可以选择统计时间段；数据中心可以查看探测器的流量曲线，左上方下拉框可以选择需要展示的探测器流量曲线。

6.1.9 登录行为分析

登录行为分析用于业务口流量的登录行为进行统计分析。当基本配置中的登录行为分析开关打开，此模块才会显示，具体配置见功能配置开关。

操作入口

在菜单栏选择“**分析>分析>登录行为分析**”进入**登录行为分析**页面。



- 登录行为分析支持的协议类型如下所示。

  Telnet、FTP、Radmin、SMB、IMAP、POP、HTTP、Oracle、Mssql、Sybase、MySQL、DB2、PostgreSQL、LDAP、QQ 等。

- 不支持加密数据库。
- HTTP、SMTP、IMAP、POP3 这 4 种加密协议默认不解析。（如果需要审计，请先在 SSL 配置里上传对应的证书，具体操作请参考 SSL 流量检测）。

- **查看登录行为详细信息**

  选择登录行为分析列表中的任意一条数据，点击 > 图标展示登录行为的详细信息，包括基本信息、客户端信息以及服务端信息，如下图所示。

- **查询登录行为信息**

  点击页面右上方的 ，根据登录 IP、协议类型、时间范围排查用户登录行为。

6.1.10 抓包分析

抓包是对业务口产生的流量进行抓包。

操作入口

在菜单栏选择“**分析➤分析➤抓包分析**”进入**抓包分析**页面。

点击<**新增**>，可以根据客户需求进行流量抓包。

新增抓包分析参数设置主要包括：协议类型、抓包时长、文件大小、IP1、IP1 端口、IP2、IP2 端口等。

当抓包时长和文件大小其中任意一项满足抓包分析参数设置，都会结束抓包。

在抓包过程中，点击对应的抓包分析项目操作列的 手动停止抓包。

抓包结束后，在界面上会显示文件名称、文件大小、状态、任务开始时间、任务结束时间、协议类型、IP1、IP1 端口、IP2、IP2 端口、操作项（重新抓包、删除）。

点击已经抓取数据包的**文件名称**可以下载数据包；点击操作项 按钮可以重新抓包；点击操作项 按钮删除已抓到的数据包。

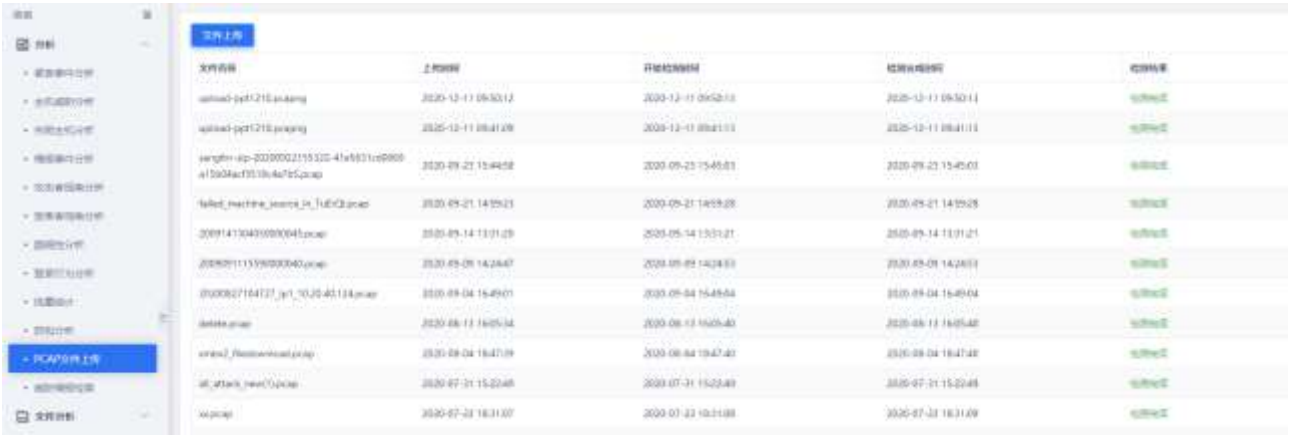
6.1.11 PCAP 文件上传

上传 PCAP 格式文件，系统会对该文件进行回放，如果含有风险事件，系统检测完成会产生相应的告警信息，可在**风险**页面搜索查看。

操作入口

在菜单栏选择“**分析➢分析➢PCAP 文件上传**”进入 **PCAP 文件上传**页面。

支持本地 PCAP 包上传分析，点击<**文件上传**>，选择本地文件上传，即可对上传的 PCAP 转包文件检测并且给出检测结果。



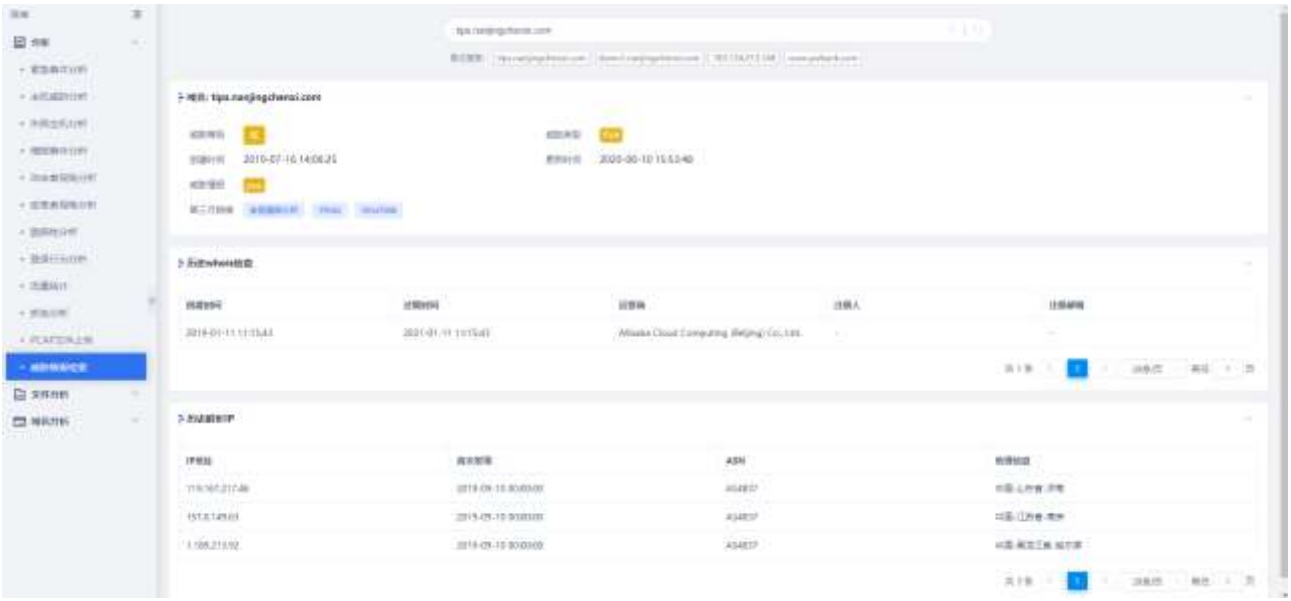
点击<**选择文件**>，上传文件进行检测。如下图所示。

6.1.12 威胁情报检索

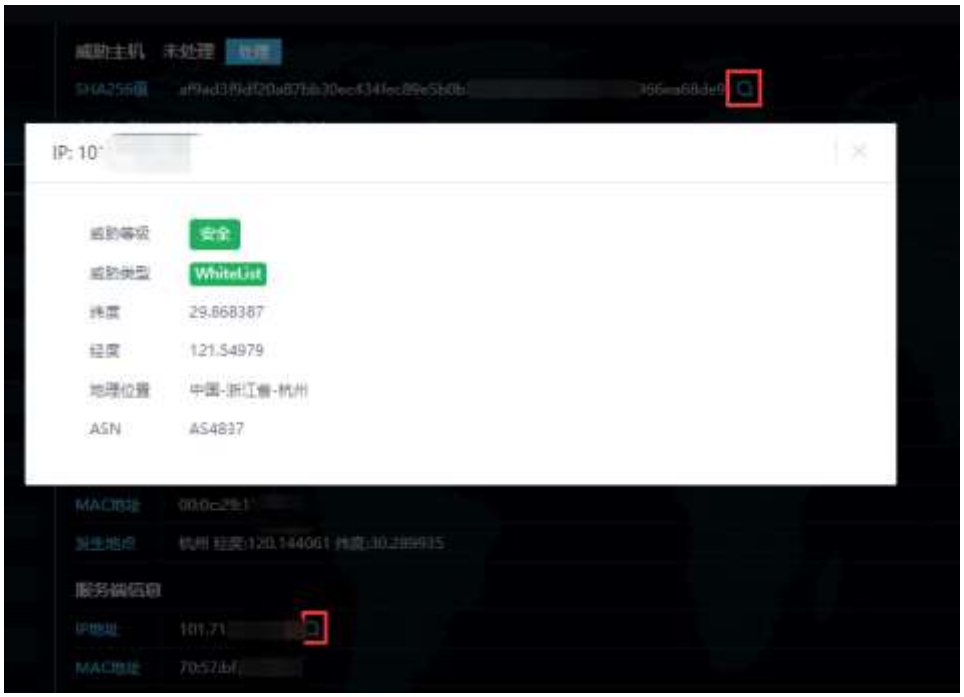
威胁情报检索提供域名、IP 地址、SHA256 值向云端查询展示相关的威胁情报，用户需在“系统➤**升级管理➤云端配置**”配置好云端信息，方可查询。

操作入口

在菜单栏选择“**分析➤分析➤威胁情报检索**”进入**威胁情报检索**页面。



风险详情页面，含有 IP 地址、域名、SHA256 值的地方点击搜索按钮，查看云端情报。



6.2 文件分析

6.2.1 文件威胁分析

文件威胁分析展示当前所有恶意文件信息，包括文件 MD5、威胁指数、传播次数、病毒检测、静态检测、动态检测等信息。

操作入口

在菜单栏选择“**分析➤文件分析➤文件威胁分析**”进入**文件威胁分析**页面。

查看文件威胁详细信息

点击某个文件样本信息，或点击左侧 > 图标，进一步展现该文件的详细信息：

- 受感染主机：展示所有接收该文件的主机 IP。若该 IP 是接收邮箱所对应的，则括号内显示接收邮箱。

  点击**传播次数**列下数字查看该文件所感染其他主机的风险详情。

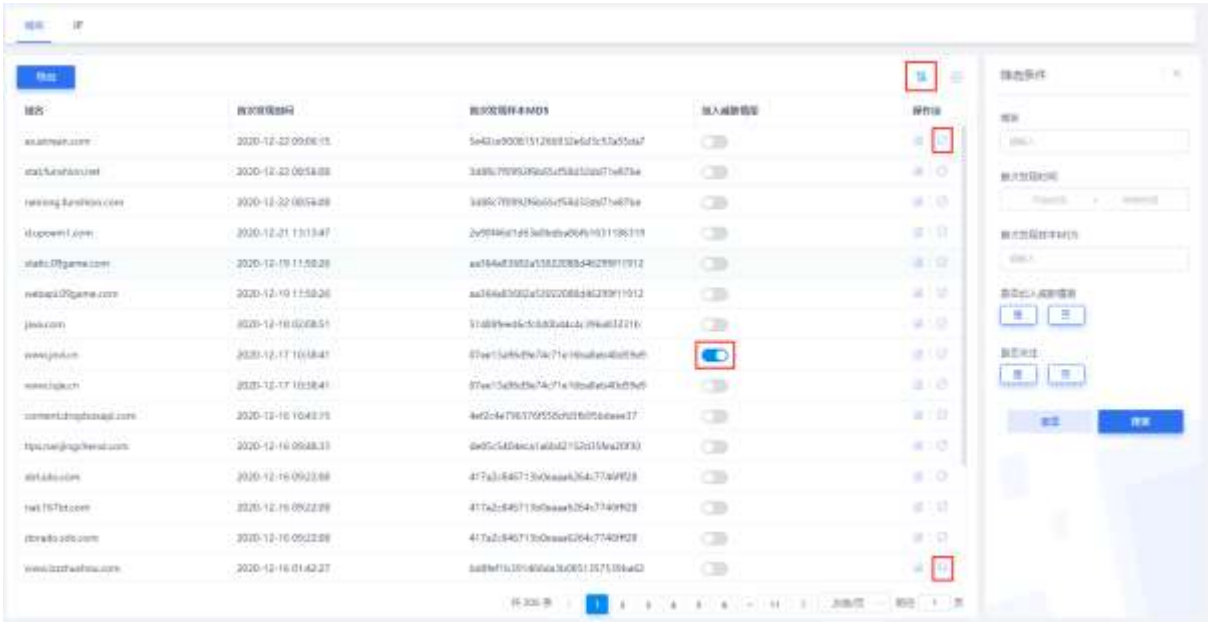
- 威胁情报：显示文件 MD5、文件名称、沙箱报告、云端确认、威胁指数、传播协议（HTTP、SMTP）、传播次数、病毒检测、静态检测、动态检测等内容。

◆ 可视化分析：沙箱报告中的动态运行图。

◆ 沙箱报告：威胁文件的沙箱报告。

6.2.2 回连域名/IP

回连域名/IP 取自【沙箱报告—软件环境—尝试与 N 个域名/IP 通信】部分。目的是将恶意文件回连的域名和 IP 列表展示，并提供加入威胁情报功能。便于用户检测访问该部分域名/IP 的行为。



相关操作

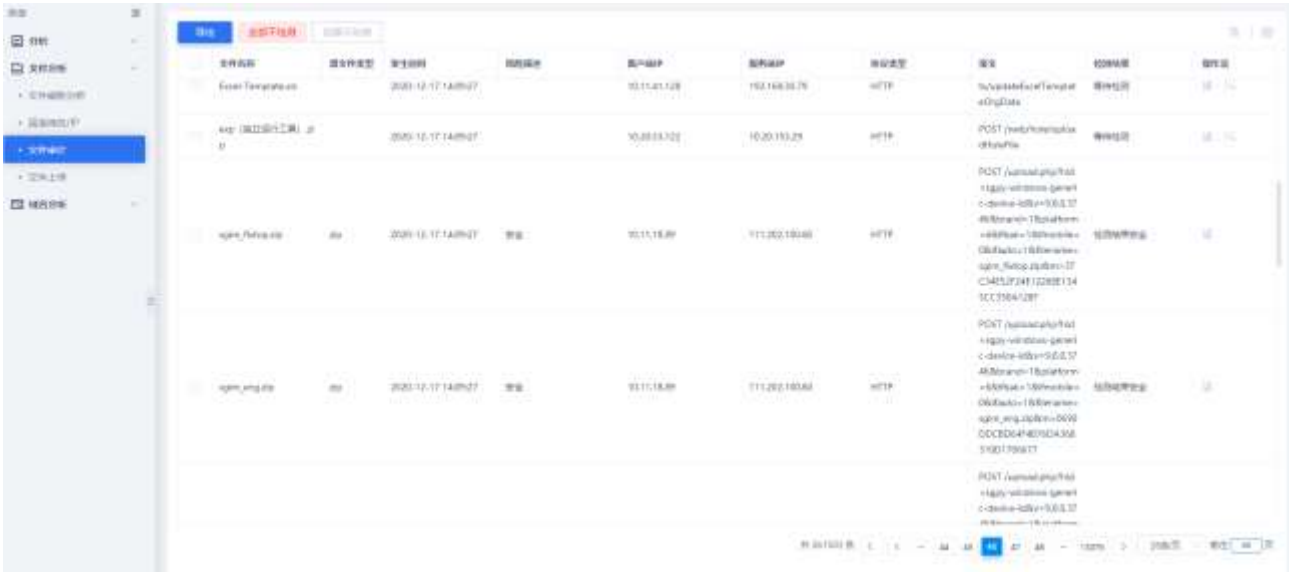
- **加入威胁情报**功能启用时，该域名/IP 加入威胁情报库；按钮禁用时，根据该域名/IP 不加入威胁情报，匹配的告警不生效。
- 点击操作栏中的 <**查看**>按钮，跳转风险页面、展示产生该域名的恶意文件告警。
- 点击 <**不再关注**>按钮，该域名归类为不再关注，列表中默认不展示；但启用的威胁情报生效，即修改域名/IP 是否关注并不影响该域名/IP 的启用/禁用状态。
- 点击 <**筛选**>按钮，弹出筛选页面，搜索不关注的数据，可以点击 <**重新关注**>按钮，该域名归类为关注，列表中默认展示。
- 沙箱报告中新产生回连域名/IP 时，数据更新到列表中，默认关注，威胁情报默认不启用。

6.2.3 文件审计

文件审计显示当前被系统审计的所有文件列表。

操作入口

在菜单栏选择“**分析➢文件分析➢文件审计**”进入**文件审计**页面。



相关操作

- 点击 通过检测结果、文件类型、时间范围等过滤出符合相应检测结果的文件信息。
- 当用户确认某个文件或某些文件是绝对安全的，并且这些文件状态尚未检测处理，可以勾选文件，点击<**批量不检测**>进行手动处理。
- 手动处理过的文件系统会提示检测结束安全，点击操作项列的 可以查看被审计文件详细信息。
- 检测结果确认安全的文件默认不保存沙箱报告。

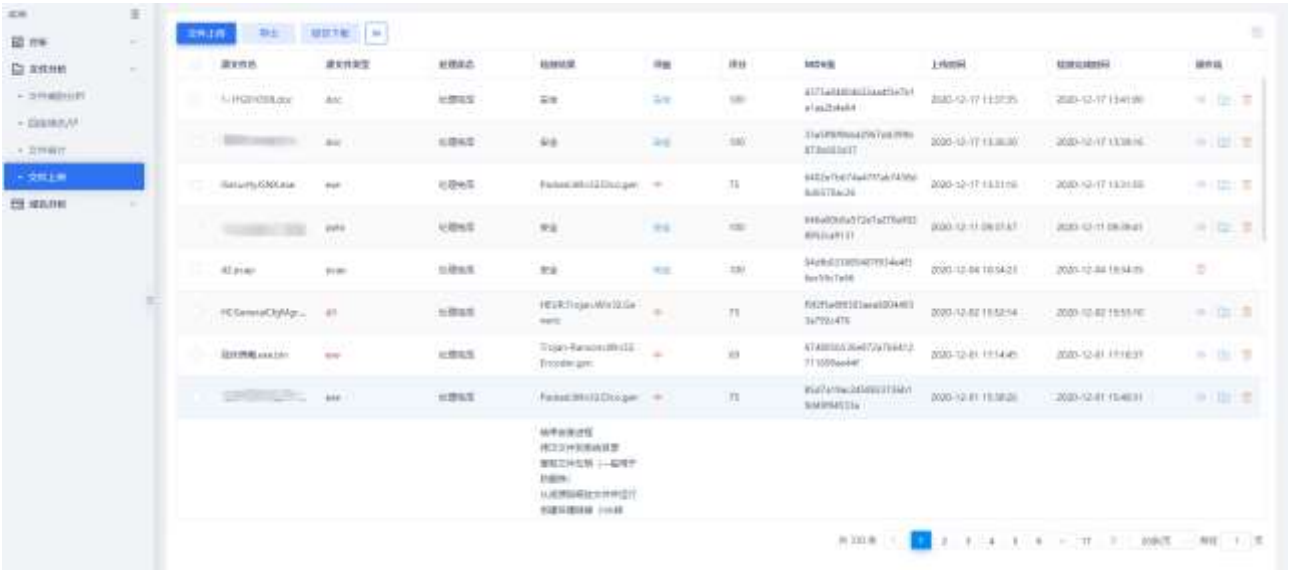
6.2.4 文件上传

对上传文件进行检测。目前检测方法有三种：病毒木马扫描、静态分析、动态模拟分析。

文件上传检测优先级高于文件审计检测。

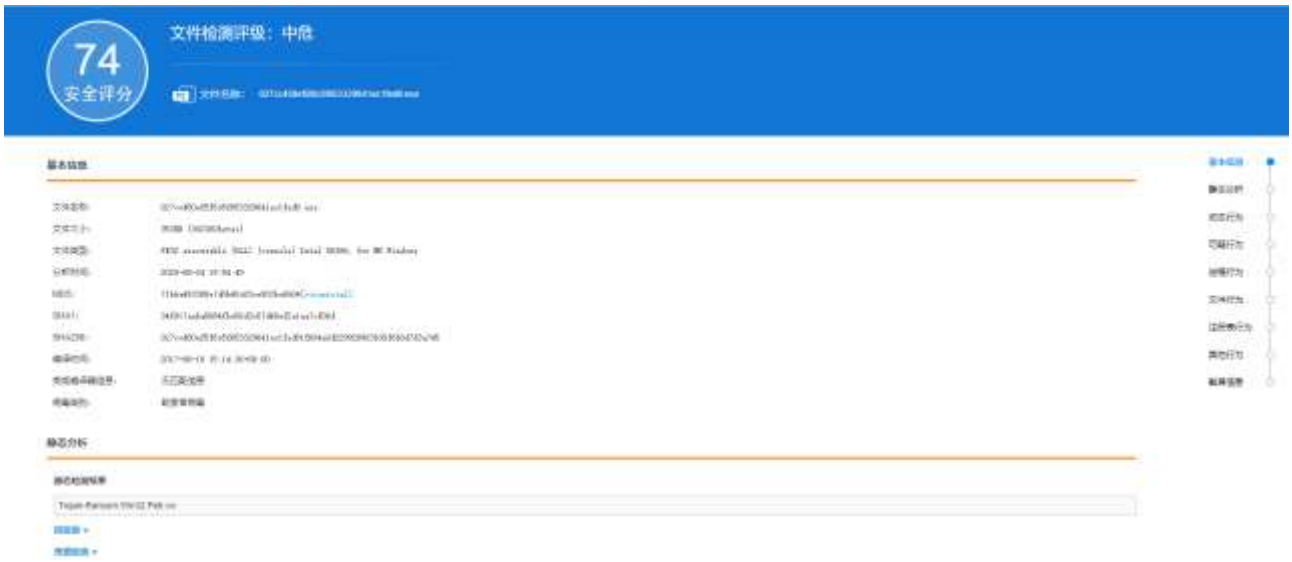
操作入口

在菜单栏选择“**分析➢文件分析➢文件上传**”进入**文件上传**页面。



◆ 点击<**文件上传**>，上传文件进行检测。如下图所示。

◆ 当文件检测以动态模拟分析方式进行时，如果文件被检测出存在可疑的攻击行为，就会生成报告。点击该文件操作项列下的 按钮预览检测报告，点击 按钮下载检测报告。报告截图如下所示：



◆ **相关操作**

在**文件上传**页面点击<**导出**>导出设定时间范围的上传文件结果，点击<**报告下载**>下载设定时间范围的检测报告。

6.3 域名分析

6.3.1 受感染主机

通过 DNS 流量检测 DGA 域名请求功能，自动识别流量中的 DGA 域名请求，从中发现受感染主机，确认僵尸主机受感染的病毒木马类型。

操作入口

在菜单栏选择“**分析➤域名分析➤受感染主机**”进入**受感染主机**页面。

受感染主机菜单将捕获到的受感染主机 IP、MAC 地址、受感染的病毒木马类型以及触发时间等直观展现出来。如下图所示。

查看受感染主机详细信息

在受感染主机列表左侧，点击 > 图标查看受感染主机详细信息。

选择**受感染主机明细**页签，查看受感染主机 IP、佐证、DGA 家族、病毒类型及触发时间等。如下图所示：

选择**回连 C&C 域名**页签查看回连 C&C 域名详细信息。

6.3.2 C&C 服务器

C&C 服务器指的是远程命令和控制服务器。目标机器可以接收来自服务器的命令，从而达到服务器控制目标机器的目的。该方法常用于病毒木马控制被感染的机器。

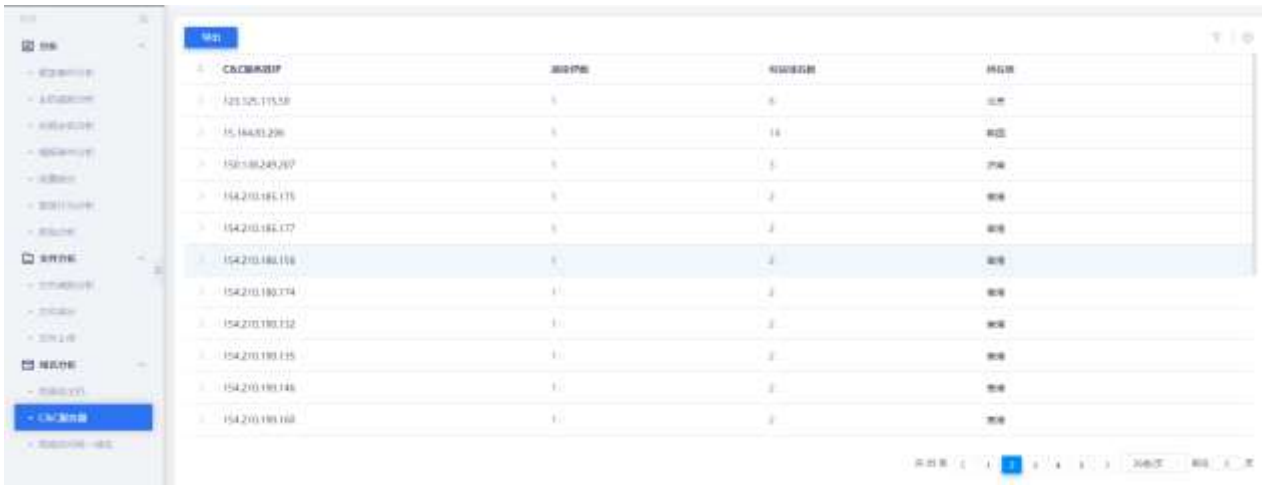
APT 通过 DNS 流量检测 DGA 域名请求功能，发现受感染主机后，并进一步通过 DGA 域名请求中成功解析的 C&C 服务器的 IP 地址，结合 bot 受感染的病毒木马类型，最终确认被同一 C&C 服务器受控的僵尸

网络（botnet）。

操作入口

在菜单栏选择“**分析➤域名分析➤C&C 服务器**”进入 **C&C 服务器**页面。

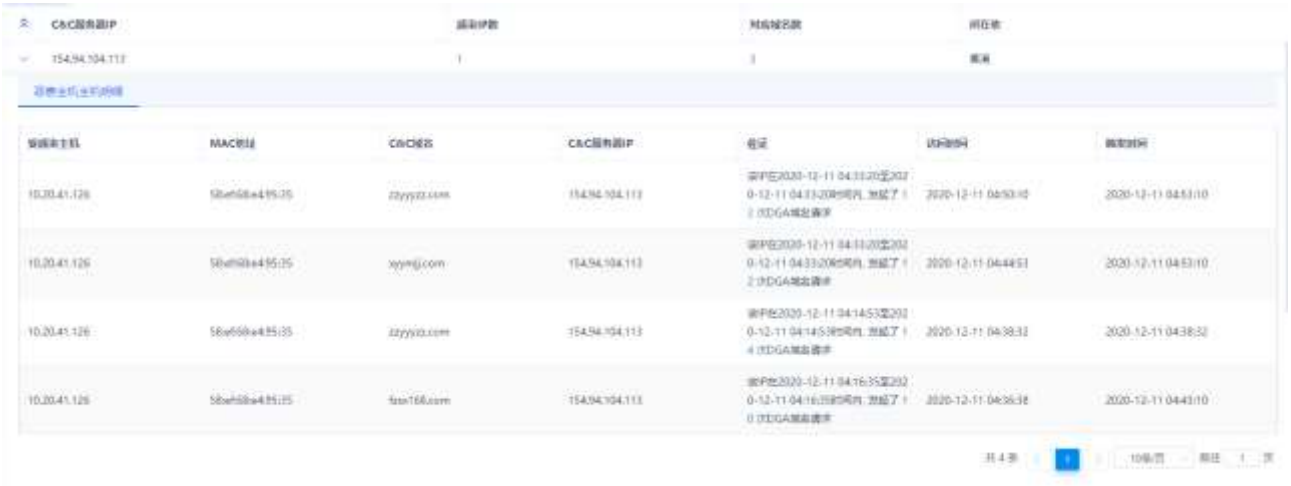
C&C 服务器菜单用来管理捕获的 C&C 服务器，并将 C&C 服务器 IP、感染 IP 数等展示出来。如下图所示。



点击<**导出**>将 C&C 服务器信息汇总导出，点击**感染 IP 数**对应的数字和**域名数**对应的数字可分别查看 IP 或域名详细数据。

查看 C&C 服务器详细信息

在 C&C 服务器列表左侧，点击 > 图标查看 C&C 服务器 IP 所对应的受感染主机 IP、MAC 地址、C&C 域名、C&C 服务器 IP、佐证、访问时间、触发时间等信息。如下图所示。



6.3.3 高频访问同一域名

高频访问同一域名菜单用于管理被捕获和检测到的同一域名频繁被访问信息。

操作入口

在菜单栏选择“**分析➤域名分析➤高频访问同一域名**”进入**高频访问同一域名**页面。

查看高频访问域名详细信息

在域名列表左侧，点击 > 图标查看 IP 在某个时间段内访问该域名以及子域名的明细，从而确认其威胁程度。

点击蓝色域名查看详细的域名及其子域名列表。如下图所示。


域名列表
域名
g.com
zzgvvg.com
gvvg.com
共 100 条
10条/页
1 2 3 4 5 6 … 10
前往 1 页

7. 风险

7.1 查询和处理风险

该功能用于查询特定风险类型告警，例如，通过勾选某一风险类别或其他一些附加条件(如：事件类型、风险类别、攻击状态等)来查询相关风险告警。其中风险级别、事件类型、风险类别等可多选。

操作入口

在菜单栏选择“**风险**”进入风险查询页面。

默认查询条件展示风险级别、数据类型、事件类型、风险类别、攻击状态、处理状态、时间范围等。

默认时间范围可以通过“**配置➤常规配置➤基本配置**”菜单的**风险查询参数**部分的**查询缺省时间范围**设定。

点击<**重置**>将查询条件重置成默认查询条件。查询界面如下。

查询结果

原始数据为单条风险记录；聚合数据将 30 分钟内相同源 IP、目的 IP 和相同规则的 Web 攻击风险、自定义特征检测风险、挖矿等风险的原始数据集合为一条。其它类别的风险也可通过聚合数据查询，但实际查询结果与原始数据相同。

风险类别选择<**全选**>，点击<**查询**>，列表默认展示风险等级、发生时间、风险名称、客户端 IP、攻击方向、服务端 IP、响应码、报文等。

点击右上角 图标可以对列表进行隐藏或显示，刷新页面后展示默认列。查询结果界面如下。

导出风险

点击<**导出**>，可以以 EXCEL 格式导出查询结果中的所有风险，包括时间、风险名称、IP、报文等信息。

处理风险

在风险列表中勾选多条记录，点击<**处理**>，可对风险进行批量处理。处理操作包括修改风险状态（**处理中**、**处理完成**、**延迟处理**、**拒绝处理**和**其他**）及添加描述，如下图所示。

风险关联信息查询

在风险查询结果界面，点击“**客户端 IP**”或“**服务端 IP**”进行风险关联信息查询。例如点击“**客户端 IP**”，

指定客户端 IP、服务器端 IP、风险类别及时间范围等过滤条件，查询出指定 IP 在选择的时间范围产生的攻击，如下图所示。

查看风险详细信息

在风险列表区域左侧，点击 > 图标查看风险详细信息，包括基本信息、客户端信息、服务端信息、关联信息、处理等，并可对该风险进行处理。

若关联查询前的数据是原始数据或聚合数据，那么关联查询出来的数据对应为原始数据或聚合数据，查看详细信息对应为原始数据或聚合数据的详细信息页面。

- Web 特征检测、远程控制、SMB 远程溢出攻击、挖矿、自定义特征检测产生的聚合风险的详细信息中除以上信息外，还包括原始信息列表。

- Web 行为分析风险的详细信息中除以上信息外，还包括关联信息列表。
- 动态检测产生的风险的详细信息中除以上信息外，还包括文件下载和沙箱报告。
- 隐蔽信道通信的聚合风险详细信息中除以上信息外，还包括 DNS 详细信息。

7.2 应用举例

本章分别以 Web 后门访问和恶意文件攻击-动态检测产生的风险为例，展现查看风险详细信息及如何处理风险。

应用举例一：Web 后门访问风险处理举例

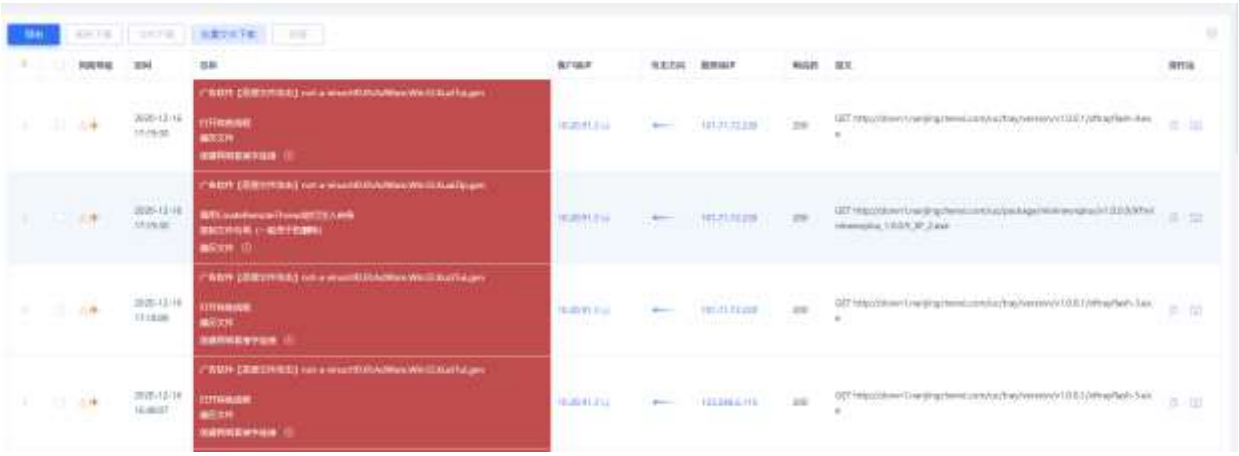
步骤1. 在风险查询结果页面中选择一条 Web 后门访问风险，点击该条风险，如下图所示，点击每个选项卡查看风险详细信息、参考分析与建议及对风险状态进行处理。

步骤2. 在风险查询结果页面中，还可以通过点击操作中的  按钮对该条 Web 后门访问记录进行**添加 IP/Host 白名单**的操作。添加 IP/Host 白名单后，符合刚刚添加的 IP 及 HOST 的数据将不再产生告警。

添加 IP/Host 白名单操作的界面如下。

应用举例二：恶意文件攻击-动态检测产生的风险处理举例

步骤1. 在风险查询界面，选择并且查看恶意文件攻击告警查询出来的界面。

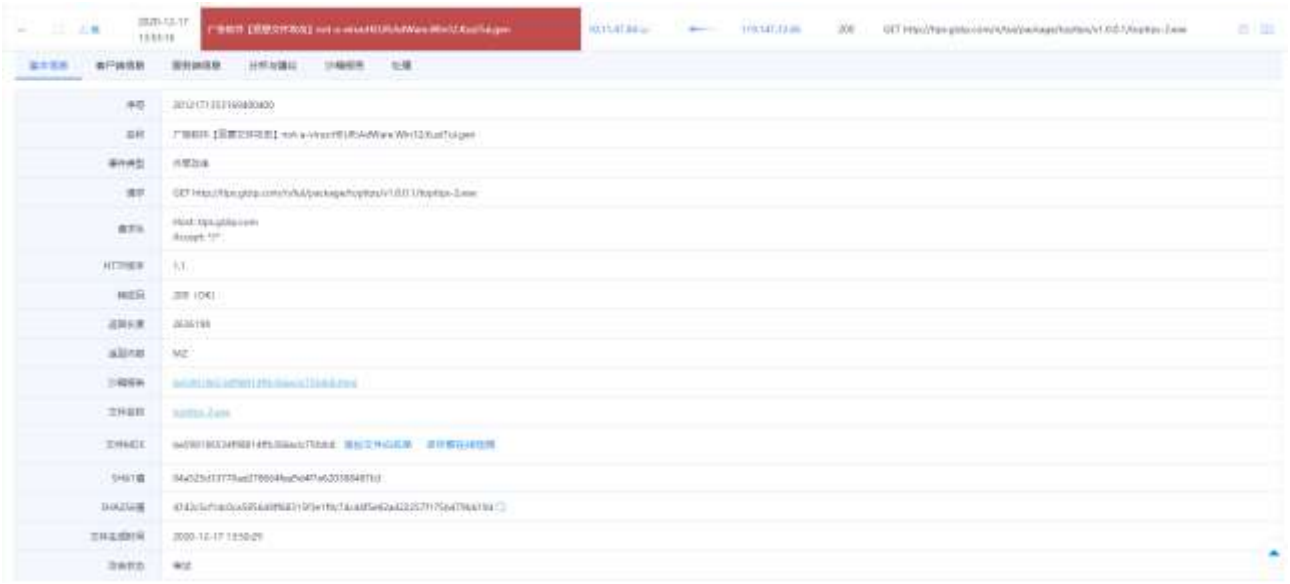


步骤2. 在上图中，勾选多条记录，批量下载沙箱报告和恶意文件，或者点击操作列 按钮下载单个恶意文件。

步骤3. 选择一条恶意文件攻击-动态检测风险，点击该条风险，处理风险。如下图所示。

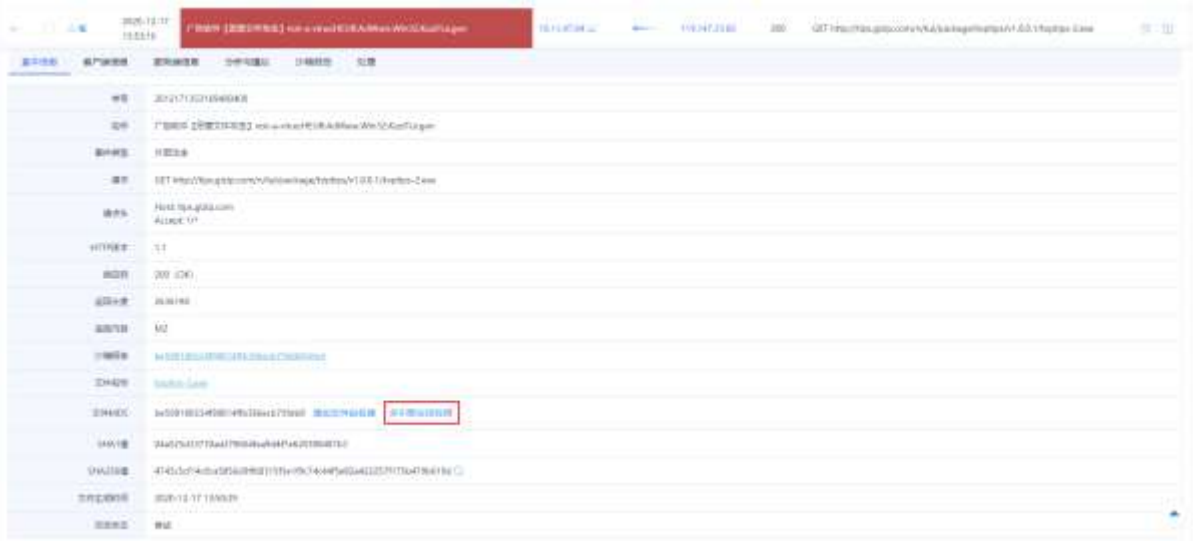
- 点击各选项卡查看风险基本信息、客户端信息、服务端信息、分析与建议、沙箱报告以及对风险状态进行处理。
- 点击文件下载和报告下载按钮，下载恶意文件和沙箱运行报告。

- 点击<**添加白名单**>，将此文件 MD5 设置为白名单。当下次再次审计该文件的 MD5，不再进行检测，直接报安全。

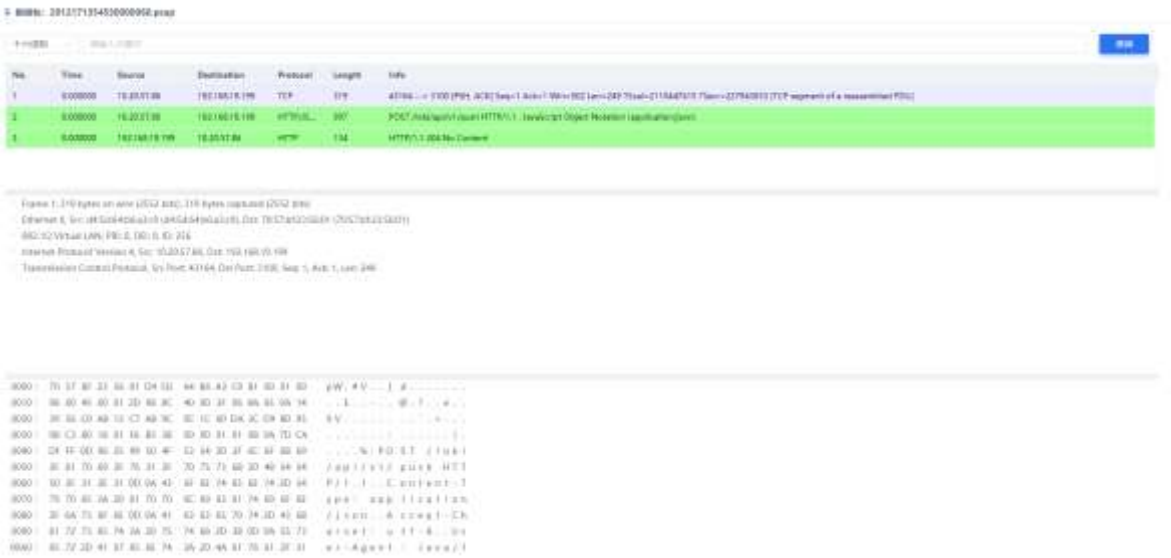


步骤4. （可选）当用户在“**系统➢升级管理➢云端配置**”菜单中开启云端配置的情况下，查询恶意文件攻击风险数据，除了以上信息外，增加**多 AV 引擎检测**结果功能。通过全球知名 AV 检测引擎的检测结果进行辅助判断。

点击<**多引擎在线检测**>，会连接到多 AV 引擎检测结果的页面，如下图所示。



点击**数据包名称**，可下载风险数据包，方便用户取证；点击**数据包名称**右边的按钮，可在线查看数据包。



8. 资产

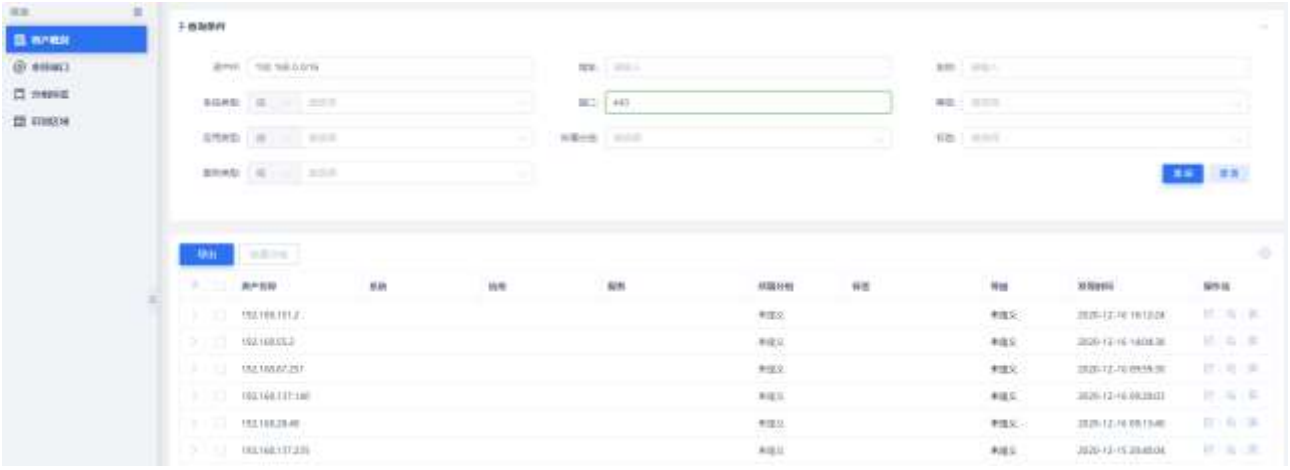
8.1 资产概况

在菜单栏选择“**资产➤资产概况**”进入**资产概况**页面。页面下方会列出用户已经扫描识别出的资产，更多信息请参考识别区域。

APT 支持 IPv4 与 IPv6 地址解析资产，、

概况模块可以通过输入 IP/IPv4 段、域名、资产名称、系统类型、端口号、等级、应用类型、所属分组、标签、服务类型等进行资产查询。

- 点击<**导出**>可以将所得信息导出为 Excel 格式。点击>键可以查看资产详情。



- 单击编辑按钮，可以对未定义的资产进行分配编辑。其中，**所属分组**和**标签**需要在主菜单选择“**资产➤分组标签**”进入对应页签设置。

◆ 单击攻击溯源按钮，跳转导航-攻击溯源页面，查询该 IP 地址的相关信息

◆ 单击主机威胁按钮，弹主机威胁详情页面，查看该资产的主机威胁详情。

包括主机威胁指数、攻击溯源、攻击过程和攻击溯源可视化等信息。

8.2 非标端口

操作入口

在菜单栏选择“**资产➤非标准口**”进入非标准口查询页面。

查询条件支持通过资产 IP/IP 段、协议类型、端口号等查询条件，方便用户对非标准口进行查询。

针对非标端口展示其端口、协议类型、资产名称（IP 地址）、所属分组、标签、等级、发现时间。可根据非标端口查看资产的异常情况。

8.3 分组标签

操作入口

在菜单栏选择“**资产➤分组标签**”进入分组和标签设置页面。

◆ 选择**分组**页签，可以自定义增加分组名，可以在**资产概况**处依据分组对查询到的资产进行分类。

◆ 选择**标签**页签，可以自定义增加标签，可以在**资产概况**处依据资产标签对查询到的资产进行分类。

8.4 识别区域

操作入口

在菜单栏选择“**资产➤识别区域**”进入识别区域设置界面。设置识别区域后，可以对满足条件的 IP/IP 地址段进行扫描并识别其中资产，否则不进行扫描和识别。

点击<**导入**>进行批量新增，点击<**全部导出**>可以导出全部数据。

可以新增内部 ip 地址，默认 ip 地址段由**配置➤常规配置➤地理位置**中的 ip 地址同步而来，更改地理位置中 ip 内容后，新增数据自动同步。

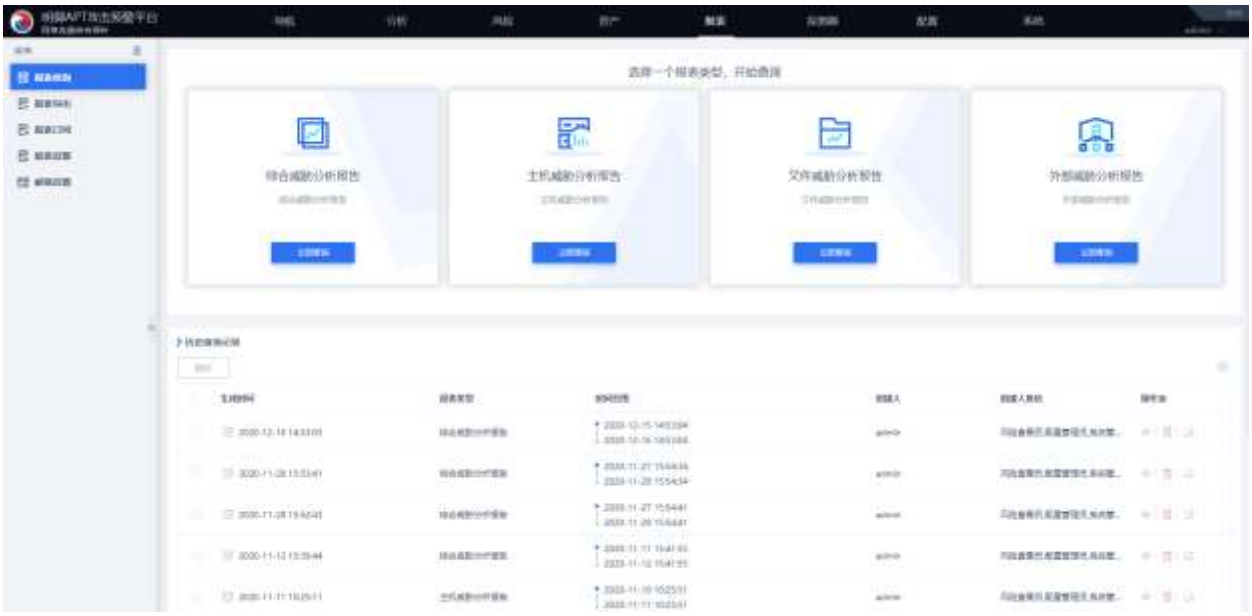

新增内部地址
* 国家:
中国
城市选择:
浙江 / 杭州
* IP地址:
单位地址:
内网地址:
取消
确定

9. 报表

9.1 报表分类

将报表类别归纳为综合威胁分析报告、主机威胁分析报告、文件威胁分析报告和外部威胁分析报告四种类型。

- 综合威胁分析报告主要是从整体风险情况来进行事件类型的分析，包括风险总览、安全事件分析、失陷主机、外部威胁、横向威胁、对外攻击威胁、脆弱性分析、文件威胁分析、风险类型说明和处理建议。
- 主机威胁分析报告主要是以主机视角来分析发生的风险情况，包括风险总览、失陷主机、横向威胁、对外攻击威胁、脆弱性、风险类型说明和处理建议。
- 文件威胁分析报告主要是根据恶意文件来从风险趋势、投递情况、恶意文件进行分析，包括风险总览、恶意文件风险趋势、恶意文件投递风险、APT 事件、恶意文件分析、恶意文件风险描述和处理建议。
- 外部威胁分析报告主要是以外部攻击视角根据攻击者和被攻击者来进行分析，包括风险总览、风险趋势、被攻击主机、外部攻击者、风险类型介绍和处理建议。



9.2 报表查询

报表查询可以查询综合威胁分析报告、主机威胁分析报告、文件威胁分析报告和外部威胁分析报告四种类型。

操作入口

在菜单栏选择“**报表➤报表查询**”进入**报表查询**页面，点击<**立即查询**>后选择时间范围进行报告预览。报告预览如下图所示。

历史查询记录记录历史报表详情，包括报表生成时间、报表类型、时间范围、创建人（登录用户）、创建人角色等。

在历史查询记录列表的**操作项**列下，点击 预览该时间范围内的报表，无需重新生成；点击 图标删除选中的报表记录；点击 将设定时间范围的报表以 **RAR** 压缩包格式导出。

如果报表预览时间过长可能会被清掉，页面上将不显示 预览、 导出图标。

9.3 报表导出

在菜单栏选择“**报表➤报表导出**”进入**报表导出**页面，可以选择时间范围、报表类型、报表格式（HTML、PDF、WORD）三个参数导出报表。

导出可选择全部报表类型，但格式只能选择一种。

在历史导出记录列表的**操作项**列下，点击 图标删除选中的报表记录；点击 将设定时间范围的报表以 RAR 压缩包格式导出。

9.4 报表订阅

报表订阅可按照用户需要定时自动生成并发送报表到配置好的邮箱。

在菜单栏选择“**报表➤报表订阅**”进入**报表订阅**页面，勾选启用状态、配置发送周期、报表类型、报表格式和收件人邮箱，点击<**保存**>完成报表订阅配置。

配置报表订阅前先点击“报表➤邮件服务器”配置邮件服务器。详细请参考邮件服务器设置。

◆ 用户可在**报表订阅历史**列表查看、编辑和删除历史订阅报表记录，如下图所示。

◆ 点击**历史发送记录**选项卡，展示发送报表的生成时间、报表类型、时间范围、报表格式、发送周期、发送结果等。用户可以重发或者删除历史报表订阅记录。

9.5 报表设置

在菜单栏选择“**报表➤报表设置**”进入**报表设置**页面，可自定义报表的组织 Logo 和产品名称，可自定义报

表的组织 Logo 和产品名称。

◆ 默认使用安恒信息的 Logo，产品名称为”**明御 APT 攻击预警平台**“ 。如下图所示。

PDF、HTML 格式报表中不展示产品名称。

◆ 产品名称是非必选项，若不选产品名称，导出报表中 Word 页面不显示产品名称，如下图所示。

9.6 邮箱设置

报表发送功能需配置邮件服务器。

操作入口

在菜单栏选择“**报表➤邮箱设置**”进入**邮箱设置**页面。

配置参数包括发送邮件服务器、发送者、DNS 服务器配置、发送者邮箱、端口、SMTP 验证等参数。其中密码为发送者邮箱 SMTP 服务的授权码。

参数配置完成后，点击<**发送测试邮件**>，输入**接收邮箱地址**，确保邮件服务器可以正常工作。

10. 登录故障排查平台

APT 故障排查平台，简称“排错平台”，有两种方式登录：

- 在任意 Web 管理页面按“Shift+p”组合键可弹出排错管理窗口，点击<**故障排查平台**>，输入账号密码进入。
- 在浏览器地址栏输入***:http://管理 IP:82/***，输入账号和密码进入。

APT 排错平台的登录账号分 **admin** 和 **root** 两个，**admin** 账户对产品进行普通管理，**root** 账户属于产品本身出现故障或者需要修改配置时才需要使用。

- admin 用户的密码是 Das@2014。
- root 密码每天变化，若需要 root 账户密码请联系产品组人员并说明问题情况，代理商请向区域渠道负责人联系获取。

11. 术语&缩略语

术语	解释
APT 攻击	APT 攻击（Advanced Persistent Threat），即高级可持续威胁攻击,也称为定向威胁攻击，指某组织对特定对象展开的持续有效的攻击活动。这种攻击活动具有极强的隐蔽性和针对性,通常会运用受感染的各种介质、供应链和社会工程学等多种手段实施先进的、持久的且有效的威胁和攻击。
DDoS	分布式拒绝服务攻击(Distributed Denial of Service Attack，简称 DDoS)是指处于不同位置的多个攻击者同时向一个或数个目标发动攻击，或者一个攻击者控制了位于不同位置的多台机器并利用这些机器对受害者同时实施攻击。由于攻击的发出点是分布在不同地方的，这类攻击称为分布式拒绝服务攻击，其中的攻击者可以有多个。
DHCP	动态主机配置协议（Dynamic Host ConfigurationProtocol）为网络中的主机动态分配 IP 地址、子网掩码、网关等信息。
NAT	网络地址转换（Network Address Translation），可以把局域网内的多台计算机通过 NAT 转换后共享一个或多个公网 IP 地址，接入 Internet，这种方式同时也可以屏蔽局域网用户，起到网络安全的作用。通常共享上网的宽带路由器都使用这个技术。
SaaS	SaaS 是 Software-as-a-Service 的缩写名称，意思为软件即服务，即通过网络提供软件服务。SAAS 是云计算的一种服务模式。
认证	是一种信用保证形式。按照国际标准化组织（ISO）和国际电工委员会（IEC）的定义，是指由

	国家认可的认证机构证明一个组织的产品、服务、管理体系符合相关标准、技术规范（TS）或其强制性要求的合格评定活动。
虚拟机	虚拟机（Virtual Machine）指通过软件模拟的具有完整硬件系统功能的、运行在一个完全隔离环境中的完整计算机系统。在实体计算机中能够完成的工作在虚拟机中都能够实现。在计算机中创建虚拟机时，需要将实体机的部分硬盘和内存容量作为虚拟机的硬盘和内存容量。每个虚拟机都有独立的 CMOS、硬盘和操作系统，可以像使用实体机一样对虚拟机进行操作。