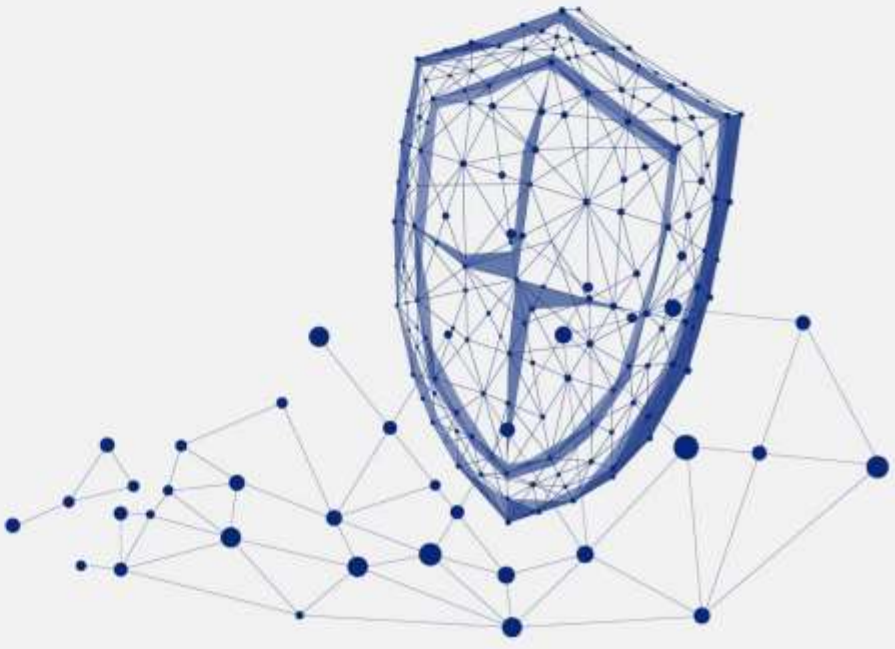
AiLPHA 大数据智能安全分析平台

V3.5.3

用户手册

文档版本： **02**

发布日期： **2021-03-26**



文档说明

产品名称		AiLPHA 大数据智能安全分析平台	
适用平台/版本		V3.5.3	
拟制人	AH1171（AiLPHA-测试）	**评审组**	AH5888（远程技术支持-标准文档）
发布人	AH5888（远程技术支持-标准文档）	**备注**	受控文档

修订记录

日期	修订版本	修改记录	修改人
2021-03-05	01	初次发布。	AH5888（远程技术支持-标准文档）
2021-03-26	02	第二次发布。 替换 2.3.4 关于截图。	AH5888（远程技术支持-标准文档）

目 录

前言

感谢您选择安恒信息的网络安全产品。本手册对安恒信息 AiLPHA 大数据智能安全平台（以下简称“大数据平台”、或“AiLPHA 大数据平台”）进行了简单介绍，并对平台的使用方法进行了详细描述。主要包括产品简介、首页、统一门户、态势感知、威胁感知、安全分析、安全运营、资产管理、系统管理和用户权限管理。

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

本文档主要适用于使用平台的人员，包括系统管理员、权限管理员、操作管理员等。本文假设读者对以下领域的知识有一定了解：

- TCP/IP、SNMP、Syslog、HTTP、FTP、NFS、Samba 等基础网络通讯协议
- 数据库、服务器、网络安全设备、路由器、交换机等常见设备（系统）的基本工作原理和配置
- 虚拟机、容器技术等常见的 IT 技术原理
- Syslog 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 界面上的各类控件名称以及内容。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。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”。

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. 产品简介

1.1 产品概述

AiLPHA 大数据智能安全分析平台采用大数据分析技术架构，结合专业的安全经验，依托雄厚的研发实力，兼顾未来业务的发展， 以“数据驱动安全分析， 形成安全闭环， 解决安全事件遗漏”为产品理念。为企业用户提供全局安全态势感知能力和业务不间断稳定运行提供安全保障， 为用户信息安全决策提供数据支撑。广泛适用于政府、金融、运营商、公安、电力能源、税务、工商、社保、交通、卫生、教育、电子商务及各企事业单位等。

1.2 产品功能

1. 实时预警

   支持安全威胁实时分析、秒级预警、安全事件取证。

2. 亿级存查

   万亿级别的超大规模数据管理和快速查询。

3. 异常检测

   侦测越权行为、账户盗用等用户异常行为。

4. 智能学习

   基于机器学习， 为用户提供安全态势感知能力。

5. 深度关联

   支持深度联动分析识别影响范围有效安全事件。

6. 追踪溯源

   支持安全事件溯源， 还原攻击轨迹。

1.3 产品特点

1、 性能可靠稳定

采用多核处理技术、多线程应用系统，处理能力可达 10 万条/秒，节省用户成本； 支持分布式部署、并行处理， 兼顾未来扩容及发展的需求。

2、 超大存储查询

解决万亿级别的数据存储难题， 满足客户长时间的日志存储需求， 采用高效的压缩存储技术， 节省用户大量存储资源； 具备高效的查询能力， 能够在秒级内从数万亿条规模的结构化和非结构化大数据中查询出客户所需的数据， 提高工作效率。

3、 完善的数据可视化

数据大屏直观展示丰富易用的安全数据， 解决客户的整体安全态势感知需求； 表报系统支持定期自动生成丰富的行业安全报告和报表，解决客户的安全运营分析报表需求。

4、深度智能分析

采用大数据和机器学习技术， 对多维度的信息和多源数据进行整合、关联、智能分析和预测， 辅助安全人员做出精准判断和调查。

5、 模块化功能扩展及开放兼容

基于模块动态扩展技术， 能够为用户实现高度可扩展能力； 高度兼容多种主流安全设备， 采用专利技术提高协议解析的精准性，并提供丰富的第三方系统对接 API。

1.4 角色和权限说明

AiLPHA 大数据智能安全分析平台默认设置有三个账号， 分别是权限管理员（useradmin）、日志审计管理员（opadmin）和系统管理员（admin）。

用户角色	缺省用户名称	权限说明
权限管理员	useradmin	新增用户和角色。
日志审计管理员	opadmin	查看操作日志。
系统管理员	admin	除了新增用户角色以及查看操作日志外的所有权限。

有关角色和权限配置的更多详细信息，请参考用户权限管理。

如无特别说明， 本文仅从 admin 视角进行描述，配置内容以 admin 用户操作举例说明。

2. 首页

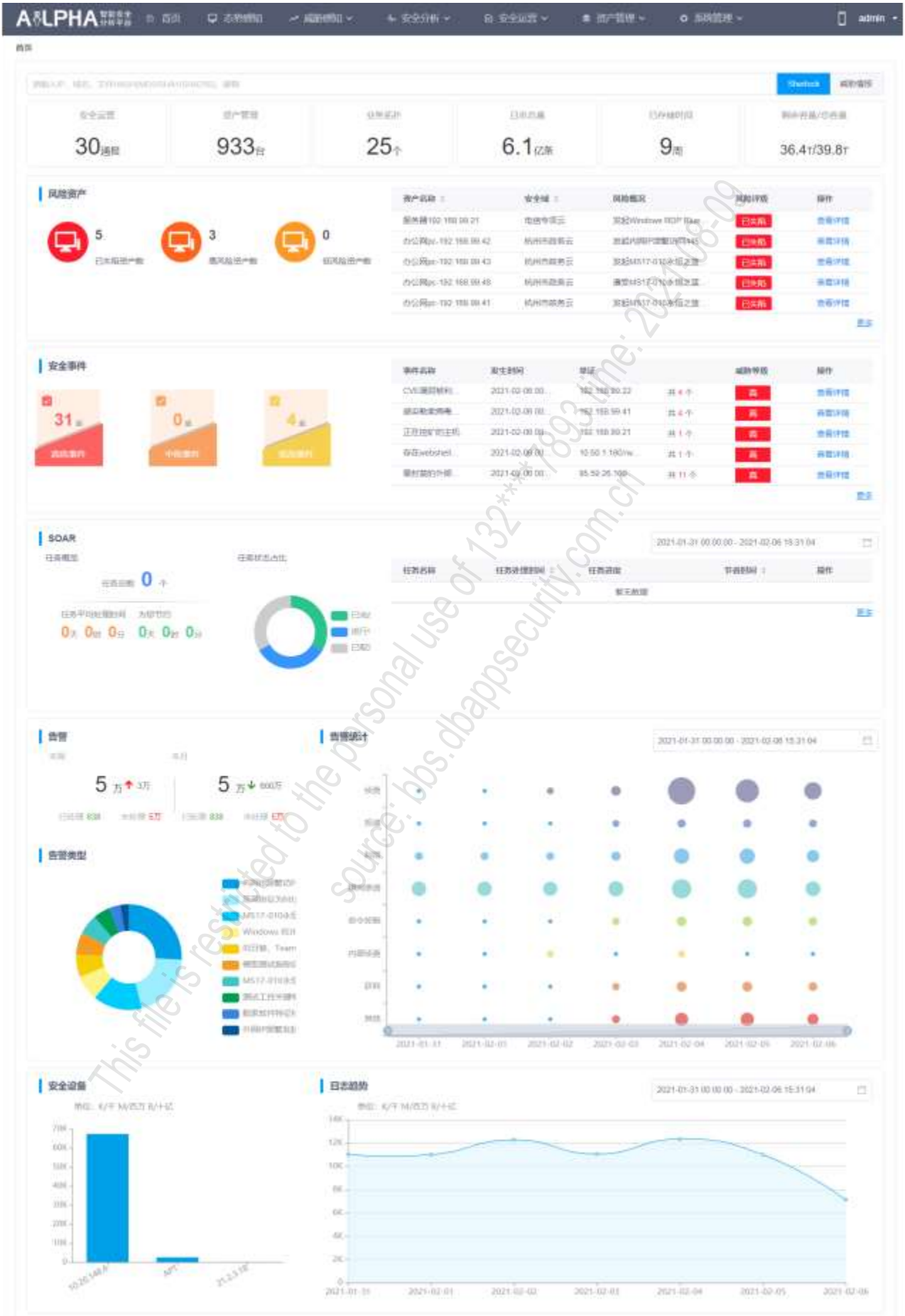
2.1 登录首页

设备安装上架并连接网线、电源后， 用户可通过 Web 方式登录及管理 AiLPHA 大数据智能安全分析平台。在浏览器中输入https://AiLPHA 大数据智能安全分析平台 IP，进入登录窗口。

在登录窗口中输入用户名、密码， 点击<**登录**>进入 AiLPHA大数据智能安全分析平台。

- 目前只支持 Chrome 浏览器。
- 出厂默认管理 IP 请查看设备面板，默认用户名/密码为： admin/iS%4Rh37g3。
- 现场部署并且对接 AiCSO 系统后，支持使用 AiCSO 账号登录。

管理员及拥有所有功能模块访问权限的用户登录后进入的默认页面如下。



页面布局分为功能菜单、 用户信息和信息展示区三部分。

序号	名称	说明
1	功能菜单	以不同的角度提供各类管理功能的配置入口， 方便用户根据实际需要进行切换，如下图所示。 
2	用户信息	显示当前登录用户， 可在此区域进行修改用户信息、查看入门引导（仅限 admin)、查看小工具、 查看平台版本、退出登录等操作，如下图所示。 
3	信息展示区	该区域主要用于展示各类风险、告警信息展示， 以及执行相关的功能操作。详细操作请参考首页信息展示区概要。

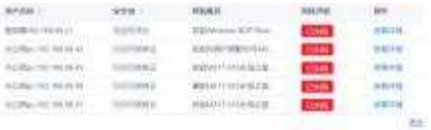
租户用户（即只拥有部分权限的账号）登录后进入的默认页面如下，具体因 useradmin 所分配的权限和可用功能模块而异。

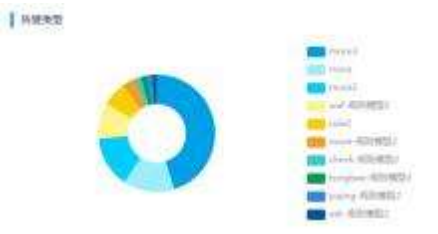
- 直接关闭浏览器标签的方式无法使已登录到设备上的用户退出。
- 在 AiLPHA 大数据智能安全分析平台页面右上角上单击用户， 在弹出的下拉框菜单选择 “**退出**” ，可以退出Web 登录。

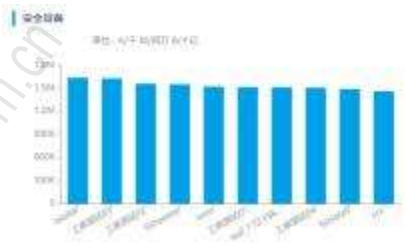
2.2 首页信息展示区概要

登录大数据平台后默认**首页**页面信息展示区展示数据及可执行操作请参见下表。

区块	说明	详细
搜索框	◆ 支持输入 IP、域名、文件 HASH、邮箱。 ◆ IP 支持 sherlock 溯源，跳转至“**威胁感知➤Sherlock**”页面。 ◆ IP、域名、文件 HASH、邮箱支持威胁情报查询，跳转至“**安全分析➤威胁情报➤情报查询**”页面。	
安全运营	◆ 展示平台当前开启状态的通报数据。 ◆ 点击跳转至“**安全运营➤工作台**”页面。	
资产管理	◆ 展示平台当前资产个数。 ◆ 点击跳转至“**资产管理➤资产管理**”页面。	
业务拓扑	◆ 展示平台当前业务拓扑个数。 ◆ 点击跳转至“**威胁感知➤业务全景**”页面。	
日志总量	◆ 展示当前设备上所有接入的日志总量（数据源为原始日志）。 ◆ 跳转至“**安全分析➤Investigation➤原始日志**”（跳转无带入时间，默认本日）。	

区块	说明	详细
已存储时间	◆ 显示当前设备上所有接入数据的已存储时间，单位 周（与索引状态无关）。 ◆ 点击跳转至“**系统管理➢配置管理➢数据配置**”界面。	
剩余容量/总容量	◆ 当前的数据磁盘使用情况。 ◆ 跳转至“**系统管理➢运维管理➢存储管理**”页面。	
风险资产	◆ 显示最近 7 天内风险资产数： 已失陷、高风险、低风险资产个数。 ◆ 支持跳转。	
风险资产列表	◆ 展示 Top5 风险资产信息（资产感知页面列表前 5 个）。 ◆ 点击<**更多**>，跳转至“**威胁感知➢资产感知**”页面。	
安全事件	◆ 显示最近 7 天内安全事件： 高危事件、中危事件、低危事件个数。 ◆ 支持跳转。	
安全事件列表	◆ 展示 Top5 安全事件信息（安全事件页面列表前 5 个）。 ◆ 点击<**更多**>，跳转至“**威胁感知➢安全事件**”页面。	

区块	说明	详细
SOAR （任务看板）	显示最近 7 天内任务状态占比和任务趋势。 不支持跳转。	
任务列表	展示 Top5 任务信息（任务看板页面列表前 5 个） 点击<**更多**>， 跳转至 “**安全分析➤SOAR➤任务看板**” 页面。	
告警	◆ 告警显示： ● 本周/本月的所有告警数(所有安全告警（包括误报）)。 ● 显示本周与上周， 本月与上月对比的告警数， 红色是上升， 绿色是下降。 ● 点击<**带入时间条件**>（本周/本月）跳转至 “**安全分析➤Investigation➤安全告警**” 页面。 ◆ 已处理、未处理告警数量（已处理是处于处理中、处理完成、误报的告警），点击<**带入条件**>跳转至 “**安全分析➤Investigation➤安全告警**” 页面。	
告警类型	告警类型Top10。	

区块	说明	详细
告警统计	◆ 显示查询时间范围内的告警统计。 ◆ 圆点图中： ● 从上至下显示： 探查、 投递、利用、横向渗透、命令控制、 内部侦察等告警情况。 ● 以圆点大小显示告警数趋势。 ● 当鼠标移到圆点上， 圆点具有光环。显示时间、攻击链名称、具体告警数量；若无告警显示无数据。 ● 单击圆点， 进入**安全告警**页面。	
安全设备	平台安全设备日志量 Top10 排行。	
日志趋势	查询时间范围内日志趋势图。	

2.3 用户信息区域介绍

登录系统后， 在页面右上角的用户信息区域显示当前登录用户， 可在此区域进行修改用户信息、查看入门引导 (仅限 admin)、 查看小工具、 查看平台版本、退出登录等操作。

2.3.1 个人中心

点击页面右上角的用户名称，在弹出的下拉菜单选择“**个人中心**”可以查看或者编辑当前用户的个人信息。

点击**登录密码**处的<**修改密码**>， 在弹出的修改密码对话框可以修改用户密码。

2.3.2 入门指引

点击页面右上角的用户名称， 在弹出的下拉菜单选择“**入门指引**”可以查看系统入门指引， 点击对应的蓝色字体， 可以自动跳转到对应的功能界面进行配置。入门指引用于引导用户完成初始配置。 主要包括以下几个方面：

- 企业信息： 包括授权许可配置和组织架构配置。
- 网络环境： 配置内网 IP、划分安全域、查看原始日志。
- 资产梳理： 导入资产和Web 业务系统、将重点监控的资产拖拽到拓扑中。
- 安全建模： 使用模型管理和黑白名单对告警精准度和误报进行调优。
- 安全监测： 监测全网安全态势并处置风险资产、查看并且处理告警、使用 Sherlock 对安全事件溯源。

2.3.3 小工具

支持使用小工具对指定内容生成二维码、 Base64 编解码和 URL 编解码。

点击页面右上角的用户名称，在弹出的下拉菜单选择“**小工具**”可以使用二维码等小工具。

2.3.3.1 二维码

进入小工具页面后，选择**二维码**页签，左边输入框输入内容，点击<**生成二维码**>，右边展示生成二维码，扫描二维码可获取输入内容。输入框最多支持 2950 字节生成二维码。

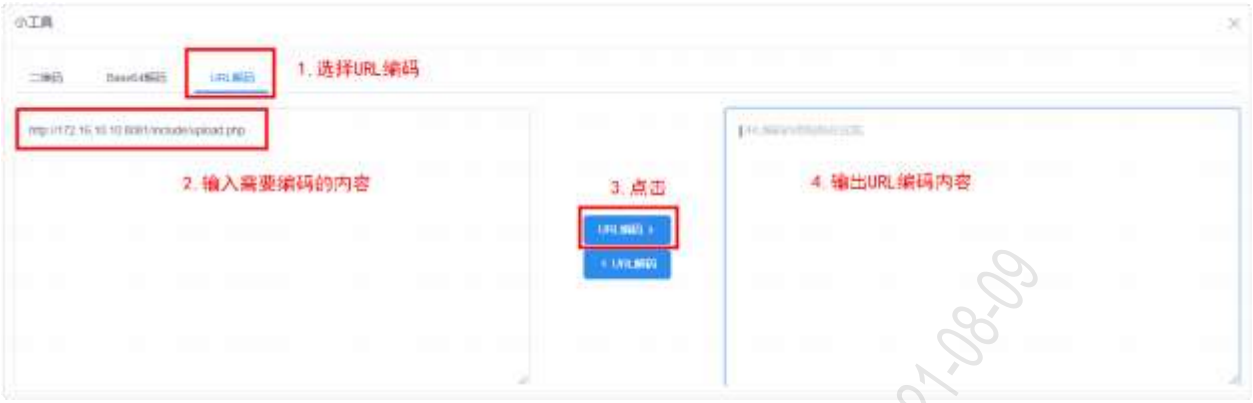
2.3.3.2 Base64 解码

进入小工具页面后， 选择 **Base64 解码**页签。 当左边输入框输入源内容， 点击<**Base64编码**>，右边输入框中将会输出 Base64 编码内容，如图所示。

当右边输入框输入编码后内容， 点击<**Base64解码**>，左边输入框将会输出解码内容，如图所示。

2.3.3.3 URL 解码

进入小工具页面后， 选择 **URL 解码**页签； 当左边输入框输入源内容， 点击<**URL编码**>，右边输入框中将会输出 URL 编码内容， 如图所示；



当右边输入框输入编码后内容， 点击<**URL解码**>， 左边输入框将会输出解码内容， 如图所示。

2.3.4 关于

点击页面右上角的用户名称， 在弹出的下拉菜单选择“**关于**”可以查看系统版本信息， 包括软件版本和规则版本等。

2.3.5 退出

点击页面右上角的用户名称，在弹出的下拉菜单选择“**退出**”可以注销当前用户。

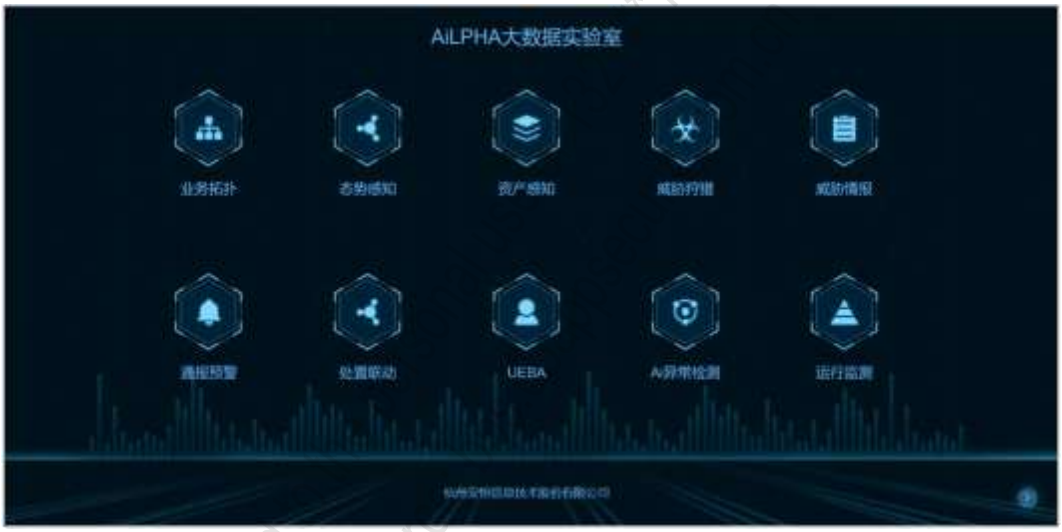
3. 统一门户

3.1 功能简介

点击平台左上角的 logo AiLPHA，进入**统一门户**页面。可以根据不同用户的喜好自定义统一门户信息，统一门户设置只和当前登录账号相关。

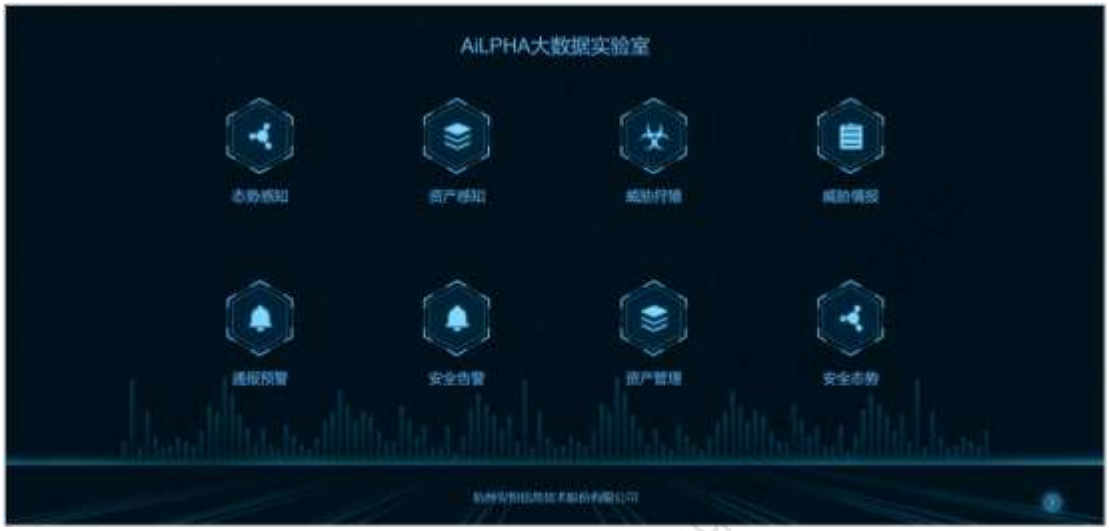
3.2 区块概要

非租户用户的统一门户菜单包含： 业务拓扑、态势感知、资产感知、威胁狩猎、威胁情报、通报预警、处置联动、 UEBA、 Ai 异常检测、运行监测，如下图所示。



租户用户的统一门户菜单包含： 态势感知（同 admin）、资产感知（同 admin）、威胁狩猎（同 admin）、威胁情报（同 admin）、通报预警（同 admin）、安全态势（新增大屏）、安全告警、资产管理，如下图所

示。



各模块详细说明见下表。

区块	说明	详细
菜单跳转	点击大屏上的图标可以快速跳转至相应菜单页面。当某用户不具备某菜单权限，菜单变灰不可点击跳转。	
图标	点击页面右下方的  ，可以显示相关图标。 ◆ 编辑菜单图标  ：点击后， 可对大屏名称和菜单进行编辑， 也可对菜单进行顺序调整。 ◆ 首页图标  ：点击后， 跳转至首页，若无首页权限， 跳转至用户登录后显示的页面。 ◆ 重置图标  ：点击确认后， 统一门户大屏恢复出厂状态（不包括大屏名称）。 ◆ 确认图标  ：点击后， 保存编辑后的内容， 大屏变成不可编辑状态。 点击编辑图标后才会出现确认图标。	 

区块	说明	详细
添加菜单	点击业务图标右上角编辑按钮时， 可以进行添加菜单操作。 菜单总数不得超过 10 个。 ◆ 图标： 默认图标，点击可进行修改。 ◆ 对应名称： 可自定义， 可重复， 必填。 ◆ 对应菜单： 选择后不可重复选择。 ◆ 对应路径： 可选择， 可自定义， 必填。 ◆ 主菜单栏和子菜单栏： 最多可添加两个子菜单栏。	

4. 态势感知

4.1 概述

以缩略图的形式展示态势感知解决方案。

- 当用户为非租户时， 包括： 外部攻击态势、 横向威胁感知、 资产失陷态势、 Web 业务系统态势、 数据中心态势、 AI 异常分析、 Sherlock 网络星空、 资产态势感知、 攻击者追踪溯源、 资产威胁溯源、 平台运行状态监测、 启用状态的重保方案、 Aiview 和仪表盘。
- 当用户为租户时，包括： 安全态势、 Sherlock 网络星空、 资产态势感知、 攻击者追踪溯源、 资产威胁溯源。

4.2 外部攻击态势

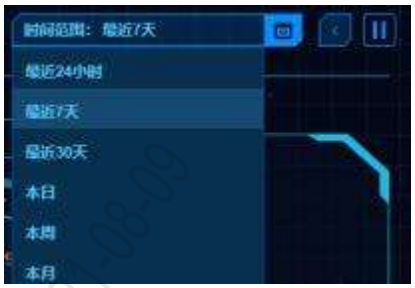
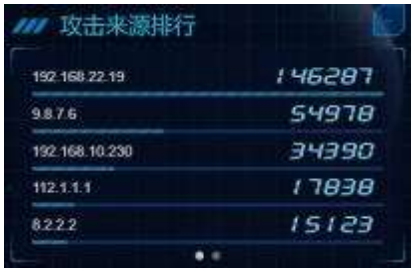
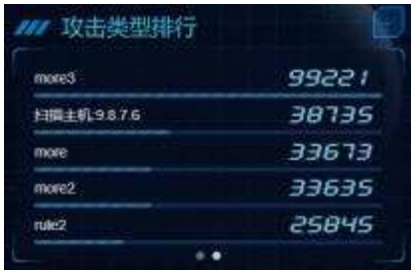
4.2.1 功能简介

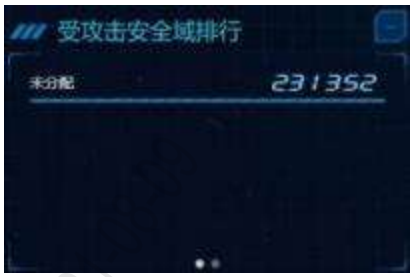
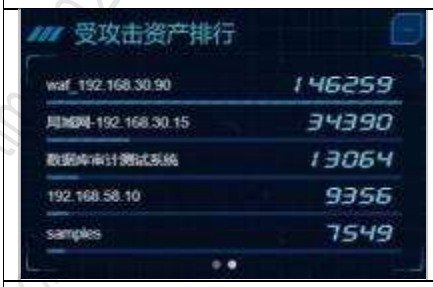
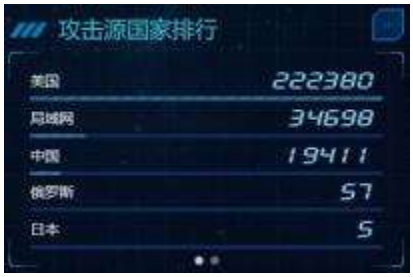
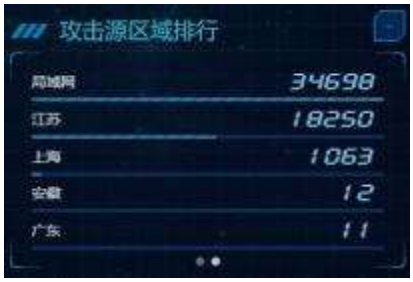
外部攻击态势大屏主要展示根据选择的时间范围内的来自互联网攻击的详情。

4.2.2 区块概要

选择 “**态势感知**” 菜单， 点击**外部攻击态势**页面查看外部攻击态势大屏。如下图所示。

数据源为安全告警， 数据流方向：外访问内， 整张大屏 5 分钟刷新一次。各模块详细说明见下表。

区块	说明	详细
时间控件/暂停	◆ 提供<**暂停**>按钮，支持轮播和暂停 暂停时，可鼠标点击切换任意模块 ◆ 时间范围： 默认显示最近 7 天。时间可选择： 最近24 小时、 最近 7 天、 最近 30 天、本日、本周、本月。	
告警数统计	◆ 大屏左下角显示统计时间内符合条件的（direction： 外访问内）安全告警总告警数、攻击源 IP 数（ srcAddress 的种类数）、攻击目的 IP 数（ destAddress 的种类数）。 ◆ 点击<**总告警数据**>，新打开**安全告警**页面。	
告警地图展示	◆ 可手动切换中国地图与世界地图， 世界地图单位到国、中国地图单位到区域。 ◆ 显示统计时间内所有源 IP 的地理分布，地图上进行攻击的路线模拟展示， 目标点为局域网的显示系统配置区域。	 
攻击来源/攻击类型排行	◆ 攻击来源排行与攻击类型排行统计每 5 秒切换。 ◆ 攻击来源排行： 统计时间段内攻击来源 IPTop5，点击可显示 Top100。点击某个来源 IP， 新打开**安全告警**页面，条件带入所选时间+来源 IP（srcAddress ）信息+direction:10。 ◆ 攻击类型排行： 统计时间段内攻击类型 Top5（针对 name 的统计），点击可以显示 Top100。点击某个告警类型， 新打开**安全告警**页面，条件带入所选时间+告警类型（name ）信息+direction:10。	 

区块	说明	详细
受攻击安全域排行/受攻击资产排行	◆ 每 5 秒切换。 ◆ 受攻击安全域排行： 统计时间段内被攻击安全域 Top5(针对 destSecurityZone 的统计)，点击可以显示 Top100。点击某个安全域名称，新打开**安全告警**页面，条件带入所选时间+安全域（destSecurityZone）信息+direction:10。 ◆ 受攻击资产排行： 统计时间段内被攻击资产 Top5(针对 destAddress 的统计，显示资产名称，无资产名称显示 IP)，点击可以显示 Top100。点击某个资产名称，新打开**安全告警**页面，条件带入所选时间+目的资产 IP(destAddress)+direction:10。	 
攻击源国家排行/攻击源区域排行	◆ 每 5 秒切换。 ◆ 攻击源国家排行： 统计时间段内攻击源国家 Top5(针对 srcGeoCountry 的统计)，点击可以显示 Top100。点击某个攻击源国家，新打开**安全告警**页面，条件带入所选时间+攻击源国家信息(srcGeoCountry)+direction:10。 ◆ 攻击源区域排行： 统计时间段内攻击源区域 Top5（针对 srcGeoRegion 的统计），点击可以显示 Top100。点击某个攻击源区域，新打开**安全告警**页面，条件带入所选时间+攻击源区域信息（srcGeoRegion）+direction:10。	 

区块	说明	详细
攻击链分布统计	◆ 根据攻击链的统计，逆时针轮播展示，被展示阶段的区域高亮显示。中间的统计数与下面的折线图、实时告警事件根据攻击链的不同显示不同，当对应的攻击链统计数据为 0 时， 该阶段的区域灰底，轮播直接跳过不显示。 ◆ 中间统计数及统计图轮播展示并根据攻击链轮播的变化而变化， 统计内容包含：境外告警数、境内告警数、影响资产数、影响网站数、攻击来源数、告警类型数。鼠标上移对应的告警数据， 出现对应攻击链统计范围内的统计图。 ● 境外告警数：显示境外攻击来源 IP Top10 排行境内告警数：显示国内攻击来源IP Top10 排行影响资产数：显示受影响资产（destAddress）Top10 排行。 ● 影响网站数：显示受影响网站（destHostName）Top10 排行。 ● 攻击来源数：显示来源IP Top10 排行。 ● 告警类型数： 显示告警类型（name）Top10 排行。	

4.3 横向威胁感知

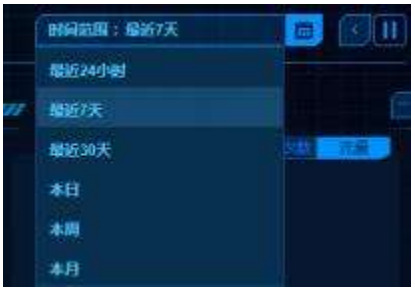
4.3.1 功能简介

关注企业网内部横向威胁态势， 分析内部安全域之间的威胁关系， 内部资产之间的攻击关系， 发现企业内部疑似被黑客控制的主机或内部员工的违规操作行为。

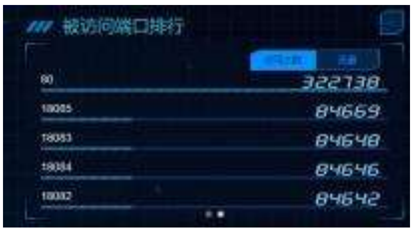
4.3.2 区块概要

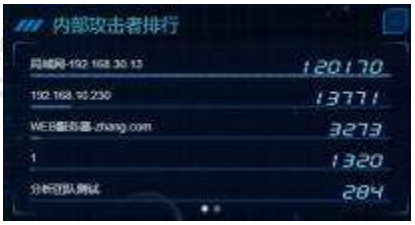
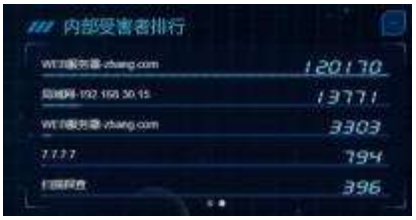
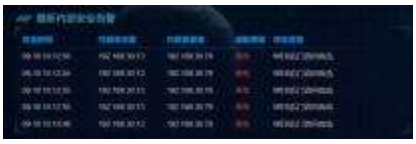
选择 “**态势感知**” 菜单， 点击**横向威胁感知**页面查看横向威胁感知大屏。如下图所示。

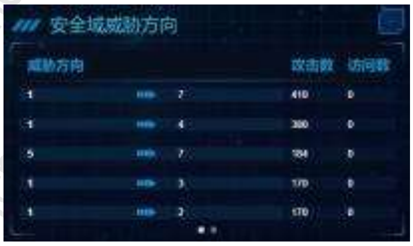
数据源为安全告警， 数据流方向:内访问内，整张大屏 5 分钟刷新一次。各模块详细说明见下表。

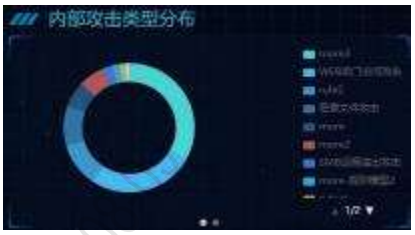
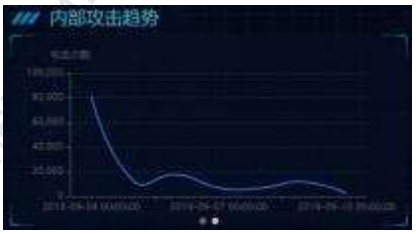
区块	说明	详细
时间控件/暂停	◆ 提供<**暂停**>按钮，支持轮播和暂停。暂停时，可鼠标点击切换任意模块。 ◆ 时间范围：默认显示最近 7 天。时间可选择：最近 24 小时、最近 7 天、最近 30 天、本日、本周、本月。	
安全域关系网络	◆ 无数据的时候显示暂无数据。 ◆ 安全域网络图： ● 展示选择时间范围内不同内部安全域之间的攻击关系（不展示同一安全域的攻击效果），按攻击次数排行最多显示 Top6。 ● 攻击方向连线上显示攻击次数和正常访问次数。 ● 连线上鼠标点击时显示： 攻击指向、异常访问次数、正常访问次数、累计流量。 ● 点击**异常访问**， 新打开**安全告警**页面，条件带入时间+来源安全域	 

区块	说明	详细
	(srcSecurityZone) 信息+ 目的安全域 (destSecurityZone) 信息 +direction:00+appProtocol != dns。 ● 点击正常访问， 新打开**原始日志**页面，条件带入时间+来源安全域 (srcSecurityZone) 信息+ 目的安全域 (destSecurityZone) 信息 +direction:00+appProtocol != dns。 ● 鼠标点击安全域图标时显示：安全域名称、安全域描述。	
资产网络图	◆ 无数据的时候显示暂无数据。 ◆ 资产网络图： ● 支持自由布局和圆形布局切换，默认是自由布局资产按风险评级展示不同的颜色： 已失陷为红色，高风险为橙色、低风险为黄色， 健康为绿色， 不在资产管理的为蓝色； 属于资产管理的 IP，显示资产名称，其他显示资产 IP。 ● 展示选择时间范围内不同资产之间的攻击关系（不展示同一资产的攻击效果），按攻击次数排行最多显示Top60。 ● 连线上鼠标浮动时显示： 攻击指向、异常访问次数、正常访问次数、累计流量。 ● 点击异常访问， 新打开**安全告警**页面，条件带入所选时间+来源 IP(srcAddress) 信息 + 目的 IP(destAddress) 信息 +direction:00+appProtocol != dns。 ● 点击正常访问， 新打开**原始日志**页面，条件带入所选时间+来源 IP(srcAddress) 信息 + 目的 IP(destAddress) 信息 +direction:00+appProtocol != dns。 ● 点击实体圆点， 浮动时显示：	  

区块	说明	详细
	● 圆点有对应资产时显示： 资产名称、风险评级、安全告警 Top3（告警名称：事件数量）、最近异常发生时间、资产 IP、安全域（属于内部安全域显示所属安全域名称，不属于内部安全域但是属于内网 IP 时显示（内网），不属于内部安全域也不属于内网 IP 时显示未分配）、资产类型、组织架构、责任人。 ● 圆点无对应资产时显示： 资产 IP、安全域（属于内部安全域显示所属安全域名称，不属于内部安全域但是属于内网 IP 时显示（内网），不属于内部安全域也不属于内网 IP 时显示未分配）。	
告警统计	◆ 选择时间范围内内部告警数。 ◆ 选择时间范围内内部攻击者数（srcAddress）。 ◆ 选择时间范围内内部受害者数（destAddress）。 ◆ 平台安全域个数（与时间过滤无关）。	
被访问业务排行/被访问端口排行	◆ 每个页面每 5 秒轮播，默认先轮播访问次数， 再轮播流量； 鼠标点击之后， 暂停轮播，可查看完整数据。 ◆ 被访问业务排行： ● 统计时间段内被访问业务（destAddress）的被访问次数和流量 Top5，点击显示 Top100， 有资产名称显示资产名称，无则显示资产 IP。 ● 点击条目， 新打开**原始日志**页面， 带入条件： ● 时间 + 数据流方向 (direction)+ 目的 IP(destAddress)+appProtocol != dns。 ◆ 被访问端口排行：	 

区块	说明	详细
	● 统计时间段内被访问端口（ destPort ）的访问次数和流量 Top5，点击可以显示 Top100。 ● 点击条目， 新打开**原始日志**页面， 带入条件： ● 时间+数据流方向(direction)+目的端口(destPort)+appProtocol != dns。	
内部攻击者排行/内部受害者排行	◆ 每个页面每 5 秒轮播。 ◆ 内部攻击者排行： ● 统计时间段内内部攻击者（ srcAddress ）Top5，点击显示 Top100， 有资产名称显示资产名称，无则显示资产 IP。 ● 点击条目， 新打开**安全告警**页面， 带入条件： ● 时间 + 数据流方向 (direction)+ 来源 IP(srcAddress)+appProtocol != dns。 ◆ 3）内部受害者排行： ● 统计时间段内内部受害者（ destAddress ）的 Top5， 点击可以显示 Top100。 ● 点击条目， 新打开**安全告警**页面， 带入条件： ● 时间 + 数据流方向 (direction)+ 目的 IP(destAddress)+appProtocol != dns。	 
最新安全告警事件	◆ 滚动展示， 选择时间范围内最近 50 条告警数据： 攻击时间、内部攻击者： srcAddress。内部受害者： destAddress，威胁等级， 攻击类型： name。 ◆ 鼠标放上去，暂停滚动， 显示所指向信息 ◆ 点击条目，新打开**安全告警**页面，带入条件：eventId+时间范围。	

区块	说明	详细
安全域/资产威胁方向	◆ 安全域威胁方向： ● 显示源安全域-->目的安全域的攻击次数和访问次数；同一安全域相互攻击的数据不过滤 ● 默认显示 Top5，点击显示 Top100。 ● 鼠标放上去， 暂停轮播， 显示所指向信息。 ● 点击**条目**，新打开**安全告警**页面， 带入条件： ● 时间范围+数据流方向(direction):00+来源安全域(srcSecurityZone)+目的安全域(destSecurityZone)+appProtocol !=dns。 ◆ 资产威胁方向 ● 显示源 IP -->目的 IP 的攻击次数和访问次数 ● 有资产名称显示资产名称，无则显示资产 IP ● 默认显示 Top5，点击显示 Top100。 ● 鼠标放上去， 暂停轮播， 显示所指向信息 。 ● 点击**条目**，新打开**安全告警**页面， 带入条件： ● 时间范围+数据流方向(direction):00+来源 IP(srcAddress)+目的 IP(destAddress)+appProtocol !=dns。	 

区块	说明	详细
内部攻击类型分布/内部攻击趋势	◆ 内部攻击类型分布： ● 选择时间段内， 内部安全告警分布 Top10。 ● 点击某图例，环形图过滤掉该攻击类型数据。 ● 鼠标放上去右边图例，环状图联动显示告警类型以及百分比。 ◆ 内部攻击趋势： 显示选择时间段内的告警趋势。	 

4.4 资产失陷态势

4.4.1 功能简介

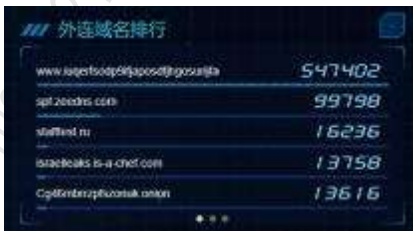
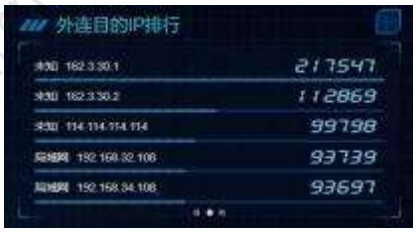
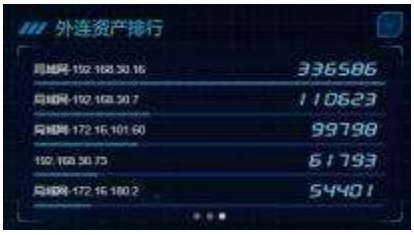
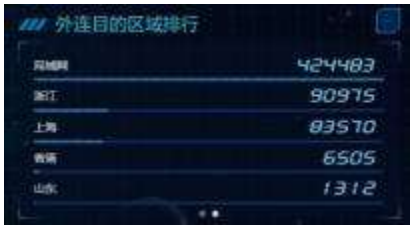
资产失陷风险态势： 数据流方向为内访问外的安全告警事件。即数据源为： 安全告警， 数据流方向： 内访问外。

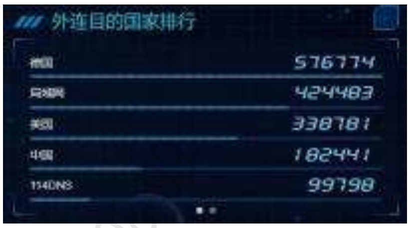
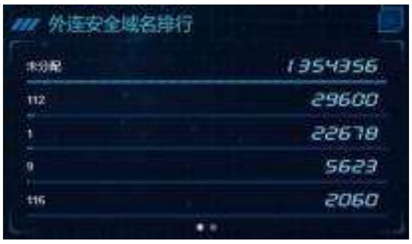
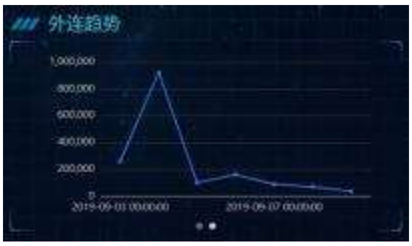
4.4.2 区块概要

选择 “**态势感知**”菜单， 点击**资产失陷态势**页面查看资产失陷态势大屏。如下图所示。

数据源为安全告警， 数据流方向:内访问外，整张大屏 5 分钟刷新一次。各模块详细说明见下表。

区块	说明	详细
时间控件	时间范围： 默认显示最近 7 天。时间可选择：最近24 小时、 最近 7 天、最近 30 天、本日、本周、本月。	
告警地图展示	◆ 地图可以手动切换中国地图与世界地图，世界地图单位到国、中国地图单位到区域。 ◆ 统计时间内，所有攻击源 IP 的地理分布显示在地图上， 并进行攻击的路线模拟展示。	 
告警数统计	◆ 外连主机数： 统计时间内， 外连主机数的种类统计（ srcAddress ）。 ◆ 外连告警数： 统计时间内外连告警数的统计。	

区块	说明	详细
外连域名排行/外连目的 IP 排行/外连资产排行	◆ 每个页面每 5 秒切换轮播，鼠标点上去，暂停轮播， 可查看完整数据 ◆ 外连域名排行： ● 统计时间段内攻击外连域名（requestDomin）Top5， 点击显示 Top100。 ● 点击**条目**，新打开**安全告警**页面， 带入条件： 时间 + “direction:01 OR appProtocol:dns” +dns 请求域名(requestDomain)。 ◆ 外连目的 IP 排行： ● 统计时间段内攻击外连目的 IP（ destAddress）Top5，点击显示 Top100。 ● 点击条目， 新打开**安全告警**页面， 带入条件： 时间 +” direction:01 OR appProtocol:dns” + 目的 IP(destAddress)。 ◆ 外连资产排行： ● 统计时间段内攻击外连来源 IP（ srcAddres ）的 Top5，来源 IP 如果是资产， 则显示资产名称， 点击显示 Top100。 ● 点击**条目**，新打开**安全告警**页面， 带入条件： 时间 + “direction:01 OR appProtocol:dns” + 来源 IP(srcAddress)。	  
外连目的国家排行/外连目的区域排行	◆ 每个页面每 5 秒切换轮播,鼠标点上去， 暂停轮播，可查看完整数据。 ◆ 外连目的国家排行： ● 统计时间段内外连目的国家（destGeoCountry）Top5，点击显示 Top100。	

区块	说明	详细
	● 点击**条目**，新打开**安全告警**页面，带入条件：时间+"direction:01 OR appProtocol:dns"+目的国家（destGeoCountry）。 ◆ 外连目的区域排行： ● 统计时间段内外连目的区域（destGeoRegion）的 Top5，点击可以显示 Top100。 ● 点击**条目**，新打开**安全告警**页面，带入条件：时间+"direction:01 OR appProtocol:dns"+目的区域(destGeoRegion)。	
最新外连事件	◆ 滚动展示选择时间范围内最近 50 条告警数据：攻击时间、外连源 IP、远控地址（appProtocol 如果是 dns 就显示外连域名，不是则显示外连目的 IP）、威胁等级、攻击类型。 ◆ 鼠标放上去，暂停滚动，显示所指向信息。 ◆ 点击**条目**，新打开**安全告警**页面，带入条件：eventId+"direction:01 OR appProtocol:dns"+时间。	
外连安全域排行/外连趋势	◆ 每个页面每 5 秒切换轮播。 ◆ 外连安全域威胁方向： ● 显示统计时间范围内，外连资产安全域(srcSecurityZone)Top5，点击显示 Top100。 ● 鼠标放上去，暂停轮播，显示所指向信息。 ● 点击**条目**，新打开**安全告警**页面，带条件：时间+"direction:01 OR appProtocol:dns"+来源安全域(srcSecurityZone)。 ● 外连趋势：显示时间范围内外连告警数趋势。	 

区块	说明	详细
可疑外连 Top10/外连告警类型 Top10	◆ 每个页面 5s 切换轮播。 ◆ 可疑外连 Top10： 选择时间范围内，可疑外连来源 IP 排行 Top10， 目标 Top3，以关系图方式显示来源 IP 对目的地址的连接关系。 ◆ 外连告警类型分布Top10： ● 选择时间段内， 外连安全告警分布 Top10。 ● 点击某图例， 环形图过滤掉该攻击类型数据鼠标放上去右边图例， 环状图联动显示告警类型以及百分比。	 

4.5 Web 业务系统态势

4.5.1 功能简介

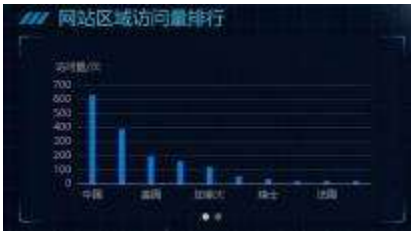
数据大屏直观展示 Web 业务系统态势，实时统计分析当天 Web 业务系统态势相关数据， 包括进出流量、访问量、攻击量、网站区域访问量、访问区域、访问 IP 排行、访问/攻击路线、详细攻击信息、网站攻击趋势、被攻击网站排行、攻击 IP 排行、攻击类型排行等数据。

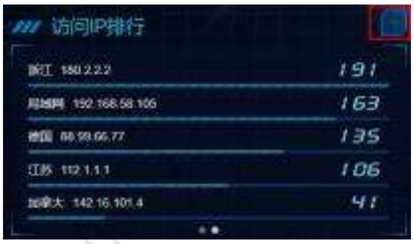
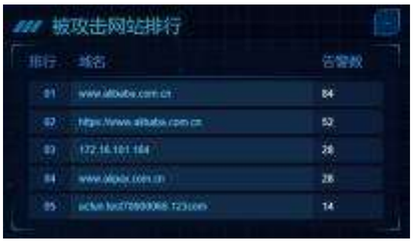
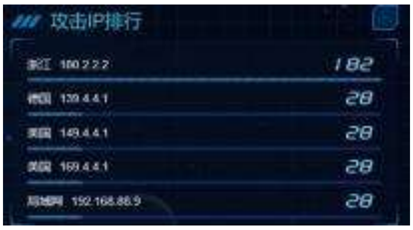
4.5.2 区块概要

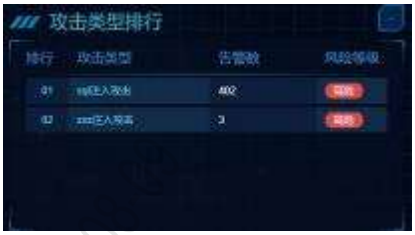
◆ 选择 “**态势感知**” 菜单， 点击 **Web 业务系统态势**页面查看 Web 业务系统态势大屏。如下图所示。

- 点击大屏中**被攻击网站排行**任意一个网站， 进入该网站实时监控， 仅查看该网站Web 业务态势。如下图所示。

以上区块概要信息说明参见下表，以下各区块均实时展示当天数据。

区块	说明	详细
进流量/出流量 访问量/攻击量	大屏左上方实时统计当天的进出流量、访问量、攻击量。	
网站区域访问量	以不同颜色展示区域访问量数据。	
网站区域访问量排行	实时统计各区域访问量，展示访问量最多的 10 个区域及对应访问量。	

区块	说明	详细
访问 IP 排行	实时统计访问 IP， 展示访问量最多的 5 个 IP 及对应访问量， 点击更多显示Top50。	
访问/攻击路线	◆ 实时展示监控地区的访问/攻击路线， 蓝色路线表示正常访问路线， 橘色路线表示攻击路线； 监控地区设置请查看 **“系统管理➢配置管理”** ，如图， 监控地区为浙江省。 ◆ 当没有告警事件发生时， 无橘色路线。	
当天详细攻击信息	◆ 展示当天最近 10 条详细攻击信息。 ◆ 当无告警事件发生时， 该区块显示暂无数据。	
网站攻击趋势	时序图分析网站攻击趋势， 包含访问分析、流量分析。	
攻击网站排行	◆ 展示被攻击次数（告警事件发生）最多的 5 个网站， 点击更多展示Top50。 ◆ 当无告警事件发生时， 该区块显示暂无数据。 ◆ 单击其中某一个攻击网站， 进入该站点实时监控。	
攻击 IP 排行	◆ 展示攻击次数最多的 5 个攻击 IP（告警事件），点击更多展示 Top50。 ◆ 当无告警事件发生时， 该区块显示暂无数据。	

区块	说明	详细
攻击类型排行	◆ 展示攻击次数最多的 5 个攻击类型（告警事件攻击类型），点击更多展示 Top50。 ◆ 当无告警事件发生时， 该区块显示暂无数据。	

4.6 数据中心态势

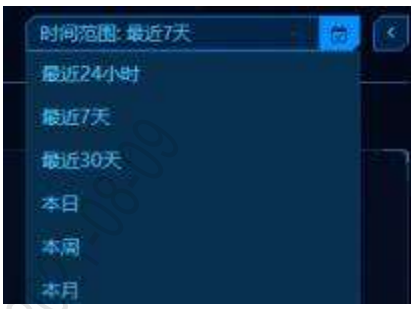
4.6.1 功能简介

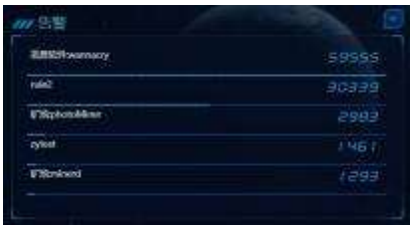
大屏页面使用 3D 逻辑安全域展示内部网络系统发生的安全态势， 用户能进行自定义的安全域划分， 并根据具体安全域的告警与漏洞信息进行统计。

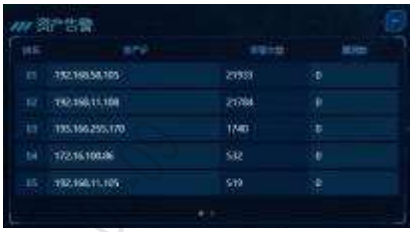
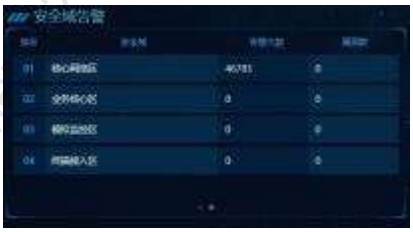
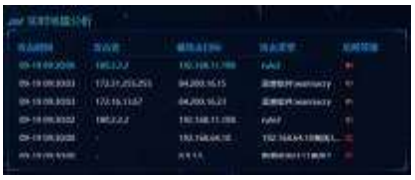
4.6.2 区块概要

选择 “**态势感知**” 菜单， 点击**数据中心态势**页面查看数据中心态势大屏。如下图所示。

以上区块概要信息说明参见下表，数据源为安全告警，大屏整体 2 分钟刷新一次。

区块	说明	详细
时间控件	◆ 时间范围：默认显示最近 7 天。时间可选择：最近24 小时、 最近 7 天、最近 30 天、本日、本周、本月。 ◆ 默认收起， 点击 可展开时间控件。	
拓扑图	◆ 默认有四个区域：核心网络区、业务核心区、模拟监控区、终端接入区。 ◆ 点击 ，弹出安全域组配置： ● 选中任一区域可修改区域名称，可**添加/移除**平台安全域至区域。 ● 同一安全域不可重复添加。 ● 配置安全域组后，拓扑图上该区域显示总资产数量、所选时间范围内告警数量、漏洞数。 ● 无配置安全域组时显示**资产： 0 告警： 0 漏洞： 0**。	 

区块	说明	详细
攻击者基本信息/攻击者画像信息	◆ 攻击者基本信息： ● 默认显示实时场景分析中第一条记录中攻击者 IP 对应的相关信息：黑客 IP、信誉度、来源地、情报信息、攻击类型、危险等级、最近攻击时间。 ● 点击黑客 IP 旁边的，可添加联动策略至 “**资产管理➢处置联动➢联动策略**”，且变成；点击快速删除联动策略。 ◆ 攻击者画像信息 ● 显示实时场景分析中第一条记录中攻击者 IP 对应的相关信息。 ● IP 反查：攻击 IP 在全时间段范围内攻击的 destAddress 个数。 ● IP 主要攻击类型：攻击 IP 在全时间段范围内的攻击类型，取事件数量最多的 10 个。 ● 处置建议：实时场景分析中第一条记录对应的处置建议。 ● 攻击资产显示该 IP 所有时间段的攻击网站（ destAddress ）Top10。	
告警	默认显示： 安全告警Top5 点击显示 Top100	

区块	说明	详细
资产告警/安全域告警	◆ 每个页面 10s 切换轮播。 ◆ 资产告警： 资产 IP、告警次数， 漏洞。 默认显示： Top5 点击 显示 Top50。 ◆ 安全域告警： ● 显示资产所属安全域、告警次数（资产为 srcAddress 或者 destAddress）、漏洞数（资产为受害主机）。 ● 资产所属安全域告警次数排行。	 
实时场景分析	◆ 统计时间段内按时间倒序显示 Top50：攻击时间、攻击者、被攻击目标（ destAddress）、攻击类型和危险等级。 ◆ 进入数据中心态势大屏时，默认展示实时场景分析中第一条记录中事件的弹框。 ◆ 选中某条事件， 攻击者基本信息、攻击者画像显示该指定事件攻击者信息（ srcAddress）以及事件弹框。	

4.7 AI 异常分析

4.7.1 功能简介

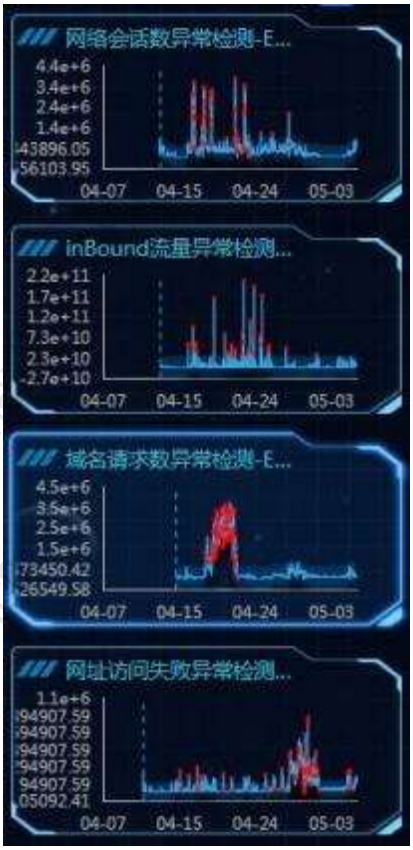
通过模型管理支持针对不同类型的数据采集与处理（全部日志 SOC 接收解析后统一放入原始日志中），配置对应的监控模型策略（规则模型、统计模型、关联模型、 AI 模型、其他）及告警策略（处理结果统一放入安全事件中，当模型中标记为安全告警时， 放入安全事件中同时放入安全告警中）。在元数据统一管理下， 用户可以根据不同的关注领域灵活操作， 包括对数据处理逻辑的新增、删除、修改、查询、启动、停止等。

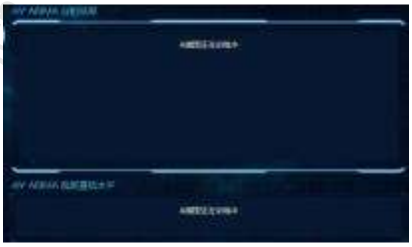
4.7.2 区块概要

选择 “**态势感知**”菜单， 点击 **AI 异常分析**页面查看 AI 异常分析大屏。如下图所示。

大屏 5 分钟刷新一次， 各模块详细说明见下：

区块	说明	详细
时间控件	时间范围： 默认收起组件，默认显示最近 30 天。 时间可选择：最近 24 小时、 最近 7 天、最近 30 天、本日、本周、本月。	
设置	◆ 点击右上角 ，弹出场景设置。 ◆ 一共可配置四个场景： ● 选择模型， 下拉单选模型列表中的 AI 模型，支持模糊查询。 ● 选择算法， 下拉单选对应 AI 模型中包含的算法，支持模糊查询。 ◆ 场景不能重复，4 个场景中不能出现某个场景的模型和算法与其他场景完全一致；场景不足时可以空缺。	
暂停按钮	支持页面暂停/开启轮播。	

区块	说明	详细
区域 1 场景缩略图展示	◆ 显示配置的 4 个场景模型，大屏从上至下依次轮播 4 个场景，用户超过 30 秒不点击时，自动进行场景轮播， 每 20s 换一个场景 ，高亮显示。 ◆ 点击缩略图切换对应场景展示内容到 “区域 2” 和 “区域 4” 。 ◆ 轮播时继续当前场景向后轮播。 ◆ 5 分钟刷新数据时，轮播从第一个场景重新开始。	
区域 2 场景模型、算法介绍	◆ 展示每个场景的 AI 模型名称，模型描述。 ◆ 该模型使用的算法名称，算法描述、相关专利和论文。 如果没有， 该部分不显示。	
区域 3 AI 分析示意图	从左到右流动效果代表 AI 实时计算过程。 形状说明： ◆ 服务器图标：表示监控指标来源。 ◆ 算法图标： 表示算法特征。 ◆ 折线图图标：表示分析结果。	

区块	说明	详细
区域 4 分析结果展示	◆ AI 分析算法结果： ● AI 分析算法结果，标题为“某算法分析结果”。 ● 曲线支持滚轮时间缩放，时间序列数据过多时需要放大时间查看详情，缩放不影响红色异常点显示。 ● 历史数据中部分为训练数据时，模型训练数据与异常检测数据用竖线隔开。 ◆ AI 算法辅助评分柱状图： ● AI 算法辅助评分柱状图，标题为“某算法标准差偏离”等，柱状图中异常点对应柱子为红色。 ● 鼠标浮动在辅助评分的标题上方时提示对应评价参数描述。 ● 折线图和柱状图时间轴范围、布局保持一致。 ● 当返回结果无数据或接口数据异常时提示“AI模型正在训练中”。 ● 当时间序列不适合算法计算时提示“AI 模型数据不适合使用当前算法进行训练”。	 
区域 5 多场景异常信息综合分布	◆ 泳道图展示 4 个 AI 异常分析场景的异常分布情况 ◆ 异常等级分为 3 级： ● 1 黄色 一般 ● 2 橘黄 中度 ● 3 红色 严重 ● 0 透明 无异常 ◆ 时间间隔 ● 最近24 小时：共 45个间隔，10 分钟一个间隔。 ● 最近 7 天：共 45 个间隔，70 分钟一个间隔，级别均值向上取整。	

区块	说明	详细
	• 最近 30 天： 共 45 个间隔， 300 分钟一个间隔， 级别均值向上取整。 • 鼠标浮动在标题上方时提示：场景、时间、异常等级。	

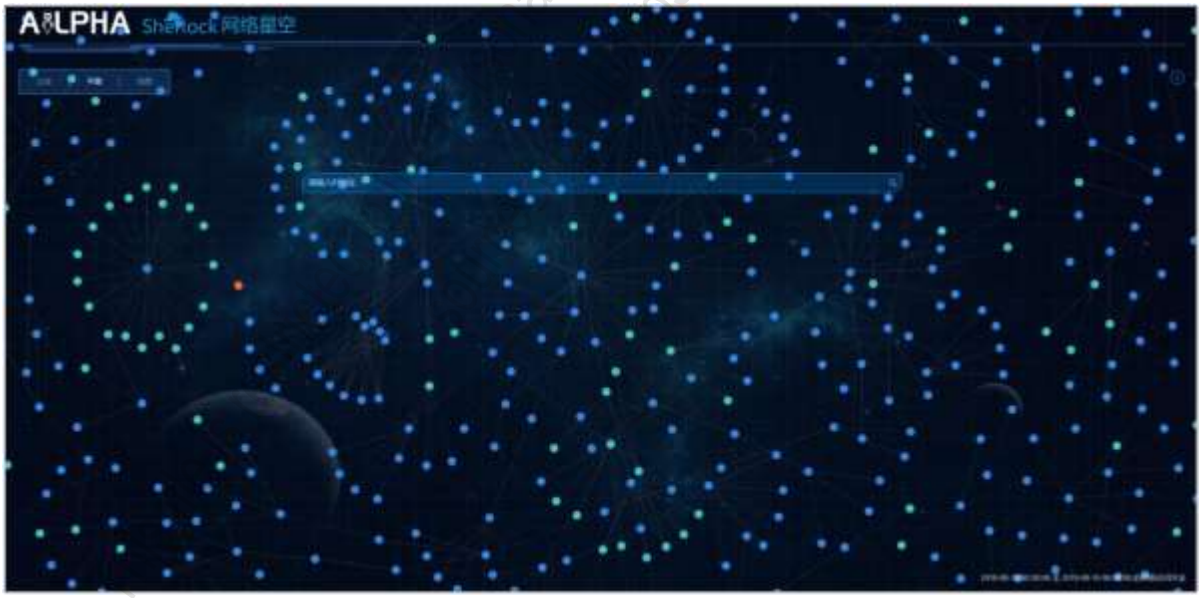
4.8 Sherlock 网络星空

4.8.1 功能简介

夏洛克（ Sherlock）帮助用户透视整个网络，追踪网络实体的连接关系， 发现访问行为的蛛丝马迹。大数据标签画像分析寻找相似的受害团体和黑客组织， AI 算法发现观测指标中隐藏的未知威胁， 情报、弱点信息辅助安全事件的追根溯源。

4.8.2 区块概要

选择 **“态势感知”** 菜单，点击 **Sherlock 网络星空**页面查看 Sherlock 大屏， 支持Tab 切换， 有立体， 平面，球面三个Tab 页， 默认展示立体效果。切换至平面，如下图所示。



数据源： 原始日志， 区块概要信息说明参见下表。

区块	说明	详细
总体	◆ 根据起始时间、结束时间到原始日志索引中取 destAddress+srcAddress 事件数量最多的 800 个 IP。 ◆ 圆点有对应资产时： 根据资产风险等级显示相应的颜色。 ● 已失陷：红色 ● 高风险：橙色 ● 低风险：黄色 ● 健康： 绿色 ● 资产为 Web 服务器时， 圆点标记为 W ● 资产为邮件服务器时，圆点标记为m ● 资产为 DNS 服务器时， 圆点标记为 D ◆ 圆点无对应资产： ● IP 属于内部安全域或内部 IP 时显示浅蓝色。 ● IP 不属于内部安全域，也不属于内网 IP 时显示深蓝色。 ● IP 是情报 IOC 且类型是黑客组织、监管单位时，显示情报标记； 其他类型显示深蓝色。	
输入框	搜索框中输入待追踪的网络实体 IP，点击<**搜索**>或者是回车键， 跳转至 **"威胁感知➤Sherlock"** ，租户只能查询安全域过滤后的 IP。	
图示按钮	点击图示按钮， 显示不同的图标与资产类型和情报类型的对应关系。	
实体详情	◆ 点击实体圆点， 浮动时显示： ● 圆点有对应资产时显示： 资产名称、风险评级、安全告警 Top3（告警名称：事件数量）、最近异常发生时间、资产 IP、安全域（属于内部安全域时显示安全域名称， 不属于内部安全域但是属于内网 IP 时显示（内网）， 不属于内部安全域也不属于内网 IP 时显示未分配）、资产类型、组织架构、责任人。当没有相关信息时，该项内容不显示。	  

区块	说明	详细
	● 圆点无对应资产且为浅蓝色时显示： IP、安全域（属于内部安全域时显示安全域名称， 不属于内部安全域但是属于内网 IP 时显示（内网））。 ● 圆点无对应资产且为深蓝色时显示： IP，安全域： 未分配， 地理位置： 国家-省-市， 例如“中国-浙江-杭州”。 ● 圆点为情报时显示： 情报类型， 情报标签， 置信度， 地理位置， 组织名称， 运营商。当没有相关信息时，该项内容不显示。 ◆ 点击 **Sherlock**，可跳转至“**威胁感知➢Sherlock**”页面，带条件： IP。	

切换至立体， 查看 Sherlock 大屏的立体效果。图标之间的连线会不定时随机高亮， 有对应资产时， 图标下方显示资产名称， 无对应资产， 情报则显示 IP。资产颜色同平面效果， 情报都为深蓝色。鼠标移动时， 立体图旋转效果停止， 鼠标停止移动， 5s 后继续开始旋转， 如下图所示。

切换至球面， 查看 Sherlock 大屏的球面效果。有对应资产时， 图标下方显示资产名称， 无对应资产， 情报则显示 IP。如果是情报中的黑客组织，监管单位或资产类型为 Web 服务器， 邮件服务器， DNS 服务器，则同平面效果中图标一致。除此之外， 全部展示主机图标。鼠标点击某个卡片时， 相关联的线高亮。同样，点击线时， 相关的卡片高亮。

如下图所示。

4.9 资产态势感知

4.9.1 功能简介

感知资产风险情况。

4.9.2 区块概要

选择 “**态势感知**” 菜单，点击**资产态势感知**页面查看资产态势感知大屏，如下图所示， 当用户为租户时，资产态势感知大屏只显示安全域过滤后的 IP 对应的资产。

区块概要信息说明参见下表。

区块	说明	详细
总体	◆ 资产管理下所有资产。 ◆ 首先以风险评级（已失陷、高风险、低风险、健康）排序，其次是资产 ID 倒序排列。 ◆ 默认显示三行， 滑动鼠标可以往下滚动。 ◆ 大屏整体 5 分钟刷新一次。	-
标签	◆ 默认显示全部资产， 点击根据标签过滤资产。 ◆ 默认展开， 点击可以收起。	
风险评级分布	◆ 大屏顶部条状图显示不同风险评级资产所占百分比： 风险资产/资产管理所有资产。 ◆ 鼠标悬停此处会显示具体分布信息。	
缩略图资产信息	◆ 缩略图左上角显示资产名称，右上角是快速跳转链接： Sherlock， 资产威胁溯源，点击图标可跳转至相应页面， 带条件： IP。 ◆ 详细信息： ● 7 天告警： IP 作为 srcAddress 或者是 destAddress 的最近 7 天状态为“未处理”的告警数据；有数据时为黄色高亮，没有数据置灰。 ● 本日日志： IP 作为 srcAddress 或者是 destAddress 的本日日志数量；日志量监控开关关闭时显示--； 有数据时为蓝色高亮， 没有数据时置灰。 ● 漏洞： IP 受害主机的漏洞数； 有数据时为蓝色高亮，没有数据时置灰。 ● 本日流量： IP 作为 srcAddress 或者是 destAddress 的本日流量；流量监控开关关闭时显示--；有数据时为蓝色高亮，没有数据灰掉。 ● 资产评分：资产管理页面打开资产评分， 缩略图显示资产评分， 替换掉本日流量； 有数据时为蓝色高亮， 没有数据	

区块	说明	详细
	灰掉； 资产评分详见资产管理模块（没有实时更新）。 ● 其他： 资产 IP、资产类型、资产重要性、安全域、责任人，同资产管理资产信息。	

4.10 攻击者追踪溯源

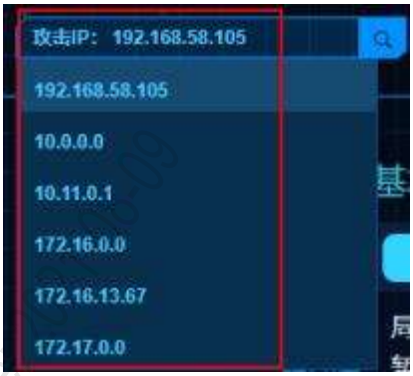
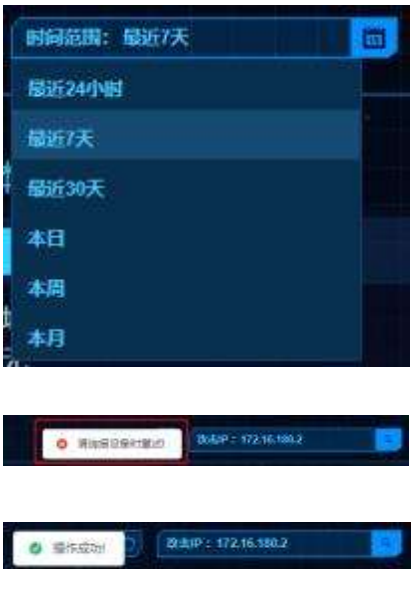
4.10.1 功能简介

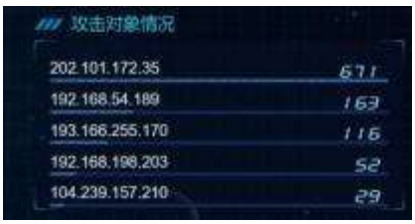
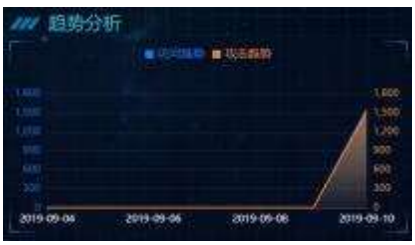
攻击者可视化溯源分析大屏， 为安全运维人员提供包括攻击行为分析、团伙分析、攻击取证信息、攻击趋势、攻击手段， 攻击影响范围等信息； 以攻击 IP 为中心， 对该 IP 产生的告警类型、所攻击的受害主机 IP，以及使用攻击手段类似相似 IP 等信息进行展示。支持任意攻击者信息查询，可生成详细的攻击者溯源报告，并能够一键导出报告。

4.10.2 区块概要

选择 “**态势感知**” 菜单， 点击**攻击者追踪溯源**页面查看攻击者追踪溯源大屏，如下图所示。

以上区块概要信息说明参见下表， 以下各区块均实时展示当天数据。当用户为租户时， 只显示安全域过滤后的 IP 及过滤后各区块的数据。

区块	说明	详细
攻击 IP	◆ 默认溯源最近一次安全告警事件中的攻击者 IP； 攻击 IP 列表显示安全告警数 Top10 的攻击者 IP，点击选择 IP 即可。 ◆ 支持手动输入 IP， 点击搜索，查询出相应数据。	
添加联动策略	◆ 快速添加联动策略： ● 若没有添加联动设备或者是设备未连接， 点击<**添加**>提示： **请连接设备重试**。 ● 有连接状态的联动设备，点击添加，提示操作成功，添加联动策略至 “**资产管理➤处置联动➤联动策略**” ，且变成。 ◆ 点击快速删除联动策略。	
时间控件	时间范围： 默认显示最近 7 天。时间可选择： 最近24 小时、 最近 7 天、最近 30 天、本日、本周、本月。	

区块	说明	详细
下载报告	◆ 点击，下载选择时间范围内的攻击者取证报告。 ◆ 点击收起、展开左侧 IP 查询框时间控件等组件。	
拓扑图	显示选择时间范围内： ◆ 该攻击者（ srcAddress ）的相似 IP Top20 ◆ 告警类型（ name ）Top20 ◆ 攻击主机（ destAddress ）Top20	
攻击者基本信息	◆ 攻击者 IP ◆ 该 IP 地理信息 ◆ 经纬度 ◆ 运营商 ◆ 情报信息 ◆ 没有值则显示暂无	
攻击对象情况	选择时间范围内攻击者攻击对象及攻击次数的 Top20。	
攻击取证	◆ 取得为前 2000 条数据中的聚合20 条。 ◆ 显示时间、攻击链、攻击 IP、攻击对象、攻击结果（显示指定攻击 IP 对应的安全告警数据， 包括开始时间、攻击链、攻击源地址、目的地址、攻击事件名称等）。	
趋势分析	选择时间范围内攻击者访问趋势与攻击趋势。	

区块	说明	详细
告警分布	◆ 选择时间范围内攻击 IP 攻击次数 Top20 的安全告警。 ◆ 鼠标指向告警名称， 显示 name：攻击次数。	

4.11 资产威胁溯源

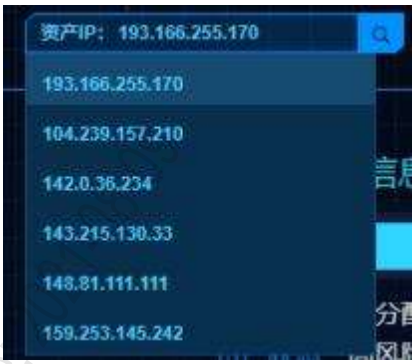
4.11.1 功能简介

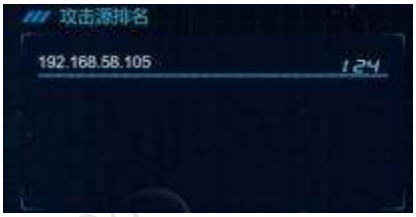
资产威胁溯源大屏从资产的角度考虑， 为安全运维人员提供包括被攻击行为分析、影响资产范围分析、攻击取证信息等； 可呈现被访问趋势、被攻击趋势、被攻击手段、资产状态， 资产评分等信息。帮助用户分析现有资产安全状况，了解资产被攻击详情， 帮助事后取证溯源。

4.11.2 区块概要

选择 “**态势感知**” 菜单，点击**资产威胁溯源**页面查看资产威胁溯源大屏，如下图所示。当用户为租户时，只显示安全域过滤后的 IP 及过滤后各区块的数据。

区块概要信息说明参见下表。

区块	说明	详细
资产 IP	◆ 默认溯源攻击次数最多的资产 IP；资产 IP 列表显示安全告警数 Top10 的资产 IP， 点击选择 IP 即可。 ◆ 不支持手动输入 IP。	
时间控件	时间范围： 默认显示最近 7 天。时间可选择： 最近24 小时、 最近 7 天、最近 30 天、本日、本周、本月。	
收起/展开组件	点击  收起、展开左侧 IP 查询框时间控件组件。	
拓扑图	显示选择时间范围内如下信息： ◆ 该资产（ destAddress ）的相似 IP Top10。 ◆ 告警类型（ name ）Top10。 ◆ 攻击来源（ srcAddress ）Top10。 ◆ 弱点 TOP10。	
攻击者基本信息	◆ 安全域： 没有值显示暂无。 ◆ 资产状态： 取风险评级， 没有值显示暂无。 ◆ 资产 IP： 没有值显示暂无。 ◆ 资产评分： 需要在 “**资产管理▶资产管理▶设置**”中打开资产评分，此处才显示，且每天凌晨更新一次；关闭则显示暂无。 ◆ 资产类型： 没有值显示暂无。 ◆ 资产名称： 没有值显示暂无。	

区块	说明	详细
攻击源排名	选择时间范围内该资产的攻击源 IP 及攻击次数的 Top10。	
攻击取证	◆ 取得为前 2000 条数据中的聚合20 条。 ◆ 显示时间、攻击链、攻击 IP、攻击对象、攻击结果（显示指定攻击 IP 对应的安全告警数据： 显示指定攻击 IP 对应的安全告警数据，包括开始时间、攻击链、攻击源地址、目的地址、攻击事件名称等）。	
趋势分析	选择时间范围内攻击者访问趋势与攻击趋势。	
告警分布	◆ 选择时间范围内资产 IP 受攻击次数 Top10 的安全告警。 ◆ 鼠标指向告警名称， 显示 name：攻击次数。	

4.12 平台运行状态监测

4.12.1 功能简介

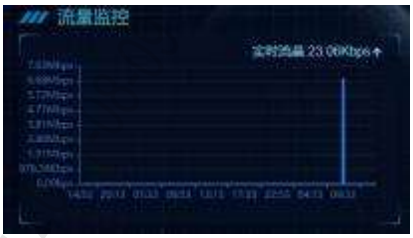
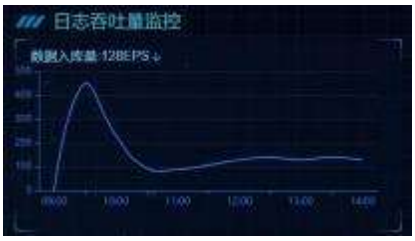
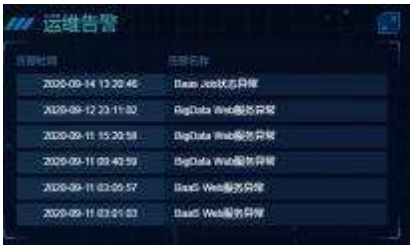
AiLPHA 大数据智能安全分析平台运行状态监测， 凸显 AiLPHA 具备来自全网安全设备的多元异构数据接入能力， 打破数据孤岛， 内置丰富的规则和知识库， 利用多种计算分析引擎和安全分析工具， 可长期保障用户全网资产安全， 实时告警威胁情况。同时平台具备良好的数据存储和计算性能，支持动态扩容缩容，根据需求灵活配置。包含安全运营、安全监测、流量监控、 AiLPHA 引擎、日志吞吐量监控、平台性能监控、磁盘容量监控/运维告警模块。

4.12.2 区块概要

选择“**态势感知**”菜单， 点击**平台运行状态监测**页面查看平台运行状态监测大屏， 如下图所示。

区块概要信息说明参见下表。

区块	说明	详细
安全运营	◆ 平台运行天数。 ◆ 本周告警：点击本周告警跳转到“**安全分析➤Investigation➤安全告警**”页面， 条件： 时间本周。 ◆ 待办工单：该用户待处理工单，点击跳转至“**安全运营➤工作台**”。 ◆ 通报： 开启状态的通报， 点击跳转至“**安全运营➤工作台**”。	
安全监测	◆ 已失陷资产：不支持跳转。 ◆ 风险资产： 包含已失陷、高风险、低风险资产数，点击跳转到“**威胁感知➤资产感知**”界面。 ◆ 安全域： 安全域的个数， 点击跳转到“**资产管理➤安全域**”界面。 ◆ Web 业务系统： Web 业务系统的个数， 点击跳转到“**资产管理➤Web 业务系统**”界面。	

区块	说明	详细
	◆ 资产：资产的个数，跳转到“**资产管理▶资产管理**”界面。	
流量监控	◆ 展示最近 48 小时入流量+出流量监控情况。 ◆ 鼠标悬停趋势图，展示时间及流量监控值。 ◆ 展示实时流量， 上升/下降箭头表示与前一分钟实时流量对比。	
AiLPHA 引擎	◆ 展示已添加到大屏的安全设备、管理引擎、可视化引擎、情报引擎、 AI 引擎、态势感知、横向威胁、外部态势、 sherlock、资产感知、业务拓扑。 ◆ 点击跳转到相应的页面。	
日志吞吐量监控	◆ 展示最近 48 小时日志监控情况， EPS 向上取整。 ◆ 数据入库量： ES 全集群的数据写入速率。 ◆ 鼠标悬停趋势图，展示时间及数据入库量。 ◆ 展示实时数据入库量，上升/下降箭头表示与前一分钟数据对比。	
运维告警/监控窗口	1）展示运维告警，点击每条告警，跳转至“**系统管理▶运维管理▶运维告警**”页面， 查看详细告警信息。条件：时间+事件名称；最多展示最近 1000 条运维告警。 2）点击  ，展开监控窗口。 ◆ 采集设备： 展示所有设备状态， 灰色表示未检测， 红色表示离线， 绿色表示在线；当刚添加采集设备时，状态为灰色； 直到下一次	 

区块	说明	详细
	运维告警产生， 状态会依据运维告警变为绿色/红色； 状态根据最近一次运维告警确定：最近一次运维告警周期内存在日志采集服务异常， 则该设备节点离线；若最近一次运维告警周期内不存在日志采集服务异常，则设备在线；周期默认为1h； 设备厂商为安恒，资产类型为审计组件大类下的采集器、通信服务器、关联引擎， 或者安全类下的日志审计系统的资产， 在指标:探针发送数据量统计中该资产 IP 对应的最后一条统计结果的时间跟当前时间对比，超过 X 小时表示异常， 在 X 小时之内表示正常。 ◆ 消息队列： 消息队列展示所有 kafka 节点的状态，红色表示离线、绿色表示在线； 状态根据最近一次运维告警确定：最近一次运维告警周期内存在 kafka 节点状态异常， 则该 kakfa 节点离线； 若最近一次运维告警周期内不存在 kafka 节点状态异常， 则 kafka 节点在线； .运维告警周期默认 1 小时。 ◆ 实时流计算引擎：展示所有关联引擎、自定义引擎、规则引擎、日志 ETL 引擎、告警 ETL 引擎的状态，红色表示离线、绿色表示在线。 ◆ 数据仓库： 展示所有 ES 节点的状态， 红色表示离线、绿色表示在线； 状态根据最近一次运维告警确定： 最近一次运维告警周期内存	

区块	说明	详细
	在 ES 集群健康状态异常， 则该 ES 节点离线；若最近一次运维告警周期内不存在 ES 集群健康状态异常， 则 logstash 节点在线；运维告警周期默认 1 小时。 ●	
磁盘容量监控	磁盘容量监控和平台运维告警可切换， 10 秒钟切换一次， 鼠标浮动时不切换。 ◆ 展示总容量/剩余/昨日新增/日志已存储/预估剩余可存储/宿主机系统盘，数据盘容量。 ● 总容量取宿主机数据盘总和， 剩余取数据盘剩余容量。 ● 昨日新增： 取昨天原始日志/会话流量/会话审计索引大小， 版本安装或者升级前两天昨日新增无数据展示。 ● 日志已存储：取原始日志索引个数。 ● 预估剩余可存储： 剩余容量/昨日新增， 版本安装或者升级前两天昨日新增无数据展示。 ◆ 点击每条告警， 跳转到安全告警。	
安全设备设置	◆ 点击 弹出**选择安全设备**界面， 可勾选安全设备展示在<**AiLPHA引擎**>模块中， 最多同时勾选 7个。 ◆ 点击<**确定**>生效， 点击<**返回**>退出选择安全设备界面。	

4.13 安全态势

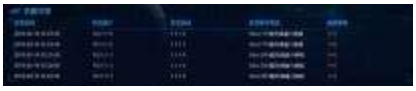
4.13.1 功能简介

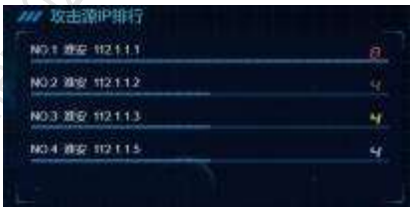
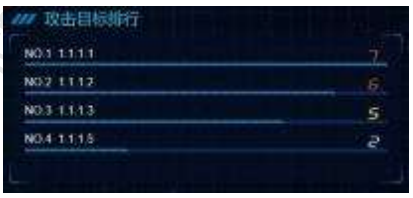
安全态势大屏为分部安全管理员和分部安服人员提供包括攻击类型、攻击源、攻击目标等实时的攻击信息，使用户能够实时准确的了解全球攻击轨迹。

4.13.2 区块概要

选择 “**态势感知**”页面， 点击**安全态势**查看安全态势大屏。如下图所示。

数据源为安全告警， 数据流方向： 内访问外， 整张大屏 5 分钟刷新一次。各模块详细说明见下表。

区块	说明	详细
时间控件	时间范围： 默认显示最近 7 天。时间可选择： 最近 24 小时、 最近 7 天、最近 30 天、本日、本周、本月。	
告警详情	◆ 滚动展示， 选择时间范围内最近 50 条告警数据： 攻击时间、 攻击源 IP：srcAddress、攻击目标： destAddress、威胁等级、 攻击事件类型：name。 ◆ 鼠标悬停该位置， 暂停滚动， 显示所指向信息。 ◆ 点击条目， 新打开安全告警页面，带入条件：eventId+时间范围。	

区块	说明	详细
攻击类型分布	◆ 选择时间段内， 攻击类型分布Top10。 ◆ 点击某图例，环形图过滤掉该攻击类型数据。 ◆ 鼠标悬停右边图例， 环状图联动显示攻击类型以及总数。 ◆ 鼠标移动至环形图上， 显示攻击类型， 总数以及百分比。	
攻击源 IP 排行	显示统计时间段内攻击源 IP Top10。	
攻击类型排行	显示统计时间段内攻击类型 Top10（针对 name 的统计）。	

4.14 重保方案

以缩略图形式显示发布状态（详见重大保障页面）的重保方案，点击图片进入重保方案大屏预览页面。

4.15 AiView

以缩略图形式显示发布状态（详见AiView 设计器页面）的 AiView，点击图片进入 AiView 大屏预览页面。

4.16 仪表盘

以缩略图形式显示发布状态（详见仪表盘管理页面）的仪表盘，点击图片进入仪表盘预览页面。

4.17 大屏轮播

使用系统管理员角色下的用户登录平台， 支持态势感知菜单下的大屏及安全设备相关大屏设置轮播。如下图所示。

轮播设置

在**态势感知**页面点击页面右上方的**轮播设置**按钮 ，展开**配置自动轮播大屏**页面， 可自定义设置轮播时间间隔、轮播大屏等。如下图所示。

- 轮播时间间隔默认为 10 秒，支持设置范围 5~1200 秒。
- 支持自定义选择轮播大屏，默认不选择。

  不选择大屏的情况下， 点击**轮播**按钮 支持态势感知菜单下所有大屏轮播， 轮播顺序为解决方案大屏、重大保障大屏、安全设备相关大屏；
- 当自定义选择轮播大屏并保存后，点击**轮播**按钮 ，按照自定义选择的大屏及顺序轮播。

5. 威胁感知

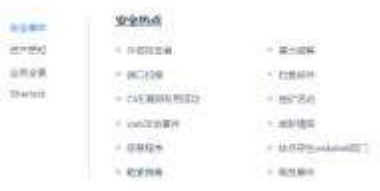
5.1 安全事件

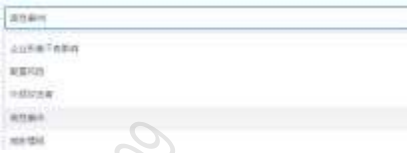
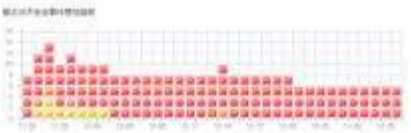
5.1.1 功能简介

安全事件页面展示最近 7 天安全事件汇总情况以及最近的安全事件管控趋势。 安全事件根据高危事件、中危事件、低危事件分别汇总显示；在事件列表区域逐条展示安全事件。

5.1.2 区块概要

选择 “**威胁感知➤安全事件**” 菜单， 进入**安全事件**页面， 如下图所示。 其区块概要如下表所示：

区块	说明	详细
安全热点	◆ 展示 “**安全分析➤Investigation➤安全告警**” 页面分析场景。 ◆ 点击跳转至 “**安全分析➤Investigation➤安全告警**” 页面，带入分析场景。	

区块	说明	详细
筛选框	◆ 支持输入名称、描述、标签、攻击者或者受害者等进行查询。 ◆ 输入时有下拉提示最近 30 天安全事件名称，支持模糊查询。	
时间选择框	支持最近 7 天、最近 30 天、本日、本周、本月。	
安全事件	◆ 展示时间范围内高危事件、中危事件、低危事件数量，单位： 起。 ◆ 点击**高危事件/中危事件/低危事件**，其它等级灰色显示，系统会自动根据事件危险等级过滤。	
安全事件管控趋势	展示最近 60 天安全事件数量变化趋势。其中： Y 轴：安全事件数量。 X 轴：日期， 颜色代表等级。	
安全事件列表	◆ 显示时间范围内安全事件卡片， 按照结束时间排序。 ◆ 安全事件卡片内容： 事件名称、标签、描述、首次发生时间、最近发生时间、举证、事件等级等。 ◆ 点击卡片， 跳转到 **“安全分析➤Investigation➤安全告警”** 页面，带入保存查询模板的条件。	

5.2 资产感知

5.2.1 功能简介

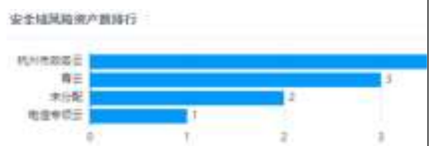
以资产为核心视角， 直观了解自身网络环境中存在风险资产。资产感知通过攻击链形式展示， 剖析从扫描

探查阶段到资产破坏阶段资产失陷过程。感知失陷、异常资产， 从海量的日志中提取有价值的资产溯源路线。平台简单易用， 支持一键全方面钻取，降低运维成本，提高运维效率。

5.2.2 区块概要

选择 “**威胁感知➢资产感知**” 菜单， 进入**资产感知**页面，如下图所示，当用户为租户时，只显示安全域过滤后的资产。

资产风险评级基于最近 7 天内未处置的安全告警中攻击链、攻击意图、威胁方向等进行多因子融合建模，评估资产的 “已失陷” 、 “高风险” 、 “低风险” 状态。其中， “已失陷” 说明攻击者已经攻陷该资产，下一步可能会进行窃取敏感信息或资产破坏， 需要引起高度重视。区块概要见下表。

区块	说明	详细
风险资产统计	◆ 不同颜色展示已失陷资产数、高风险资产数、低风险资产数。 ◆ 点击对应图标， 联动过滤风险资产列表。	
安全域风险资产数排行	◆ 展示风险资产所属安全域 Top5 排行。 ◆ 点击柱状图， 与风险资产列表联动， 过滤安全域。	
风险资产列表	◆ 支持风险评级、安全域下拉选择过滤。 ◆ 右上角可基于资产名称或 IP 关键字进行搜索；支持模糊查询。 ◆ 列表以最近异常发生时间倒序排列。	

区块	说明	详细
	● 主展示区展示资产名称、资产 IP 地址、安全域、风险概况、风险评级（已失陷、高风险、低风险状态）、最近异常发生时间、操作等共 7 列展示。其中部分支持 进行正序倒序排行。 ● 操作栏点击**查看详情**，钻取至“**威胁感知➤Sherlock**”页面，带条件：资产 IP。 ◆ 列表数据 10 分钟更新一次。	

5.3 业务全景

5.3.1 功能简介

将拓扑绘制的内容进行实时监控。 提供列表模式和缩略图两种展示界面。业务全景可以通过业务拓扑图的方式展示当前整个业务拓扑的威胁分析。

5.3.2 区块概要

选择 “**威胁感知➤业务全景**”菜单， 默认进入业务全景缩略图模式页面，如下图所示。

缩略图模式

- 出厂内置三个业务拓扑， 分别为：企业网(3D)、企业网、通用 Web 应用， 随机排序。
- 内置的业务拓扑不关联资产、安全设备、 Web 业务系统、安全域， 显示业务拓扑的截图。
- 鼠标移到缩略图上时，显示缩略图的业务描述，并且右上角显示<**编辑拓扑**>按钮。
- 点击页面左上角“**列表模式**”图标， 进入业务拓扑列表模式， 如下图所示。

列表模式

- 列表显示业务名称、业务描述、操作等 3 列， 操作列中有业务监控、编辑拓扑、编辑业务、删除业务等图标。
- 出厂内置三个业务拓扑， 分别为：企业网(3D)、企业网、通用 Web 应用， 按名称排序。

新建业务

点击<**新建业务**>， 打开新建业务页面。

标题： 新建业务，业务名称：必填项，业务描述非必填， 如下图所示：

填写完毕后，点击<**保存**>，缩略图区域显示“**请配置业务拓扑**”。

点击<**保存并编辑拓扑**>， 进入**业务全景编辑**页面， 如下图所示：

编辑业务拓扑

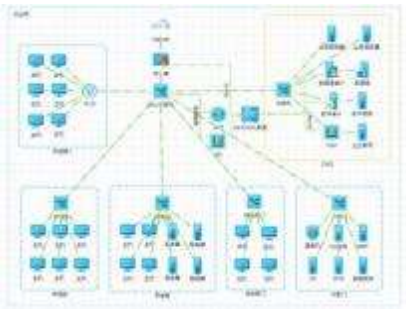
点击<**编辑拓扑**>按钮， 进入业务拓扑编辑页面， 左侧是左上显示资产选择器（资产列表）、 Web 业务系统、安全设备、安全域， 左下显示元素选择器， 中上显示工具栏， 及<**更多设置**>、<**保存**>和<**返回**>按钮， 中下

显示拓扑绘制区，右侧显示元素编辑器。如下图所示。

业务拓扑编辑页面各模块详细信息见下表。

区块	说明	详细
资产选择器	◆ 按资产名称显示资产，并且按资产 ID 倒序排序。 ◆ 资产都用一个图标显示，每个图标下方显示资产名称。 ◆ 当资产过多一屏无法显示时，会显示分页。 ◆ 支持资产 IP、资产名称模糊查询。 ◆ 可拖拽到拓扑绘制区， 拖拽后的资产还是会显示在资产选择器中，但是会置灰显示。	

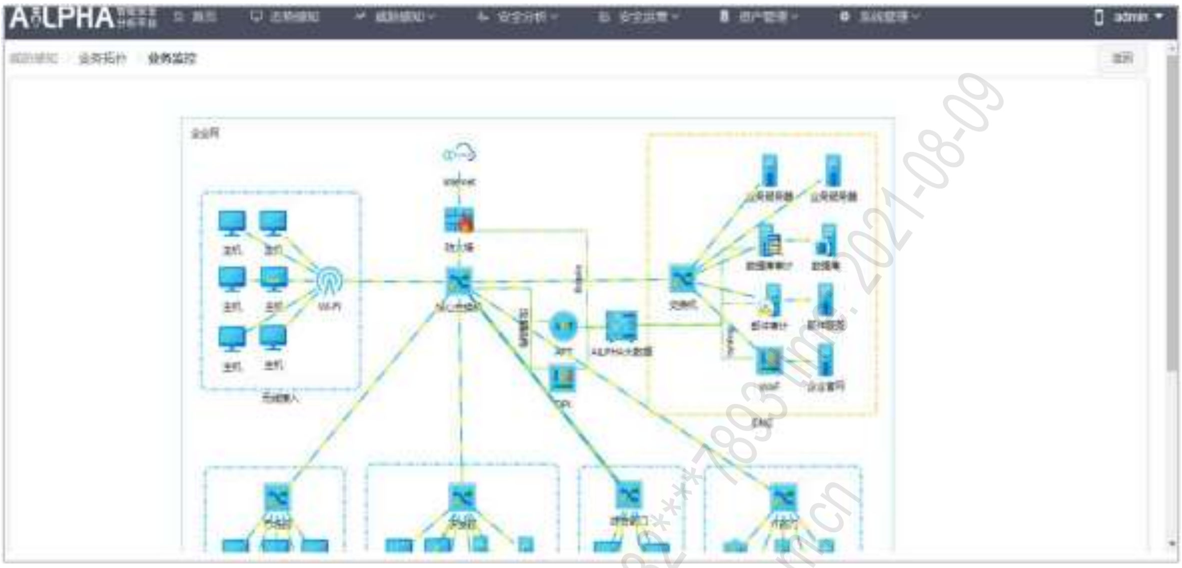
区块	说明	详细
安全域	◆ 按照安全域名称显示安全域， 并且按照创建时间正序， 最早创建的放最前面。 ◆ 图标显示， 并且每个图标下方显示安全域名称。 ◆ 当安全域过多一屏无法显示时， 会显示分页。 ◆ 支持根据名称模糊查询。 ◆ 可拖拽到拓扑绘制区， 拖拽后的安全域还是会显示在安全域选择器中，但是会置灰显示。	
安全设备	◆ 按照安全设备名称显示安全设备， 并且按照 ID 正序，最早创建的放最前面。 ◆ 图标显示， 并且每个图标下方显示安全设备名称。 ◆ 当安全设备过多一屏无法显示时，会显示分页。 ◆ 支持根据名称模糊查询（区分大小写）。 ◆ 可拖拽到拓扑绘制区， 拖拽后的安全设备还是会显示在安全设备选择器中，但是会置灰显示。	
Web 业务系统	◆ 按照系统名称显示 Web 业务系统，并且按照 ID 倒序，最晚创建的放最前。 ◆ 都用同一个图标显示， 并且每个图标下方显示系统名称。 ◆ 当 Web 业务系统过多一屏无法显示时，显示分页。 ◆ 支持根据名称模糊查询。 ◆ 可拖拽到拓扑绘制区， 拖拽后的 Web 业务系统还是会显示在 Web 业务系统选择器中， 但是会置灰显示。	

区块	说明	详细
元素选择器	按组显示， 具体分组有： ◆ 基本元素： 包含元素种类为文字、矩形、多边形、分组、信号塔、云、用户、用户组、管理员、端口、服务器集群、数据库服务器、无线、移动终端、应用服务器、邮件服务器、云数据库、中间件服务器、AiLPHA 大数据、 API 接口、 FTP、服务器、终端。 ◆ 网络设备元素： 包含元素种类为路由器、交换机、负载均衡、 VPN。 ◆ 安全设备元素： 包含元素种类为安全管理系统、APT、数据库审计系统、日志审计系统、抗 DDoS 系统、流量监测设备、入侵防护系统(IPS)、入侵检测系统（ IDS ）、上网行为审计系统、统一威胁管理（ UTM ）、网页防篡改、下一代防火墙、运维审计系统、主机安全管理系统（ EDR ）、Web 应用防火墙(WAF)。 ◆ 3D 设备元素： 包含元素种类为服务器、防火墙等。	
工具栏	◆ 默认显示<**撤销**>、<**恢复**>、<**删除**>、<**缩放**>、<**网格**>、 <**布局**>、 <**标尺**>等按钮。 ◆ 点击<**更多设置**>， 弹框显示更多设备页面。 **主题选择**： 浅色、深色。 **导入导出**：导出图片、导出拓扑数据、导入拓扑数据。	
拓扑绘制区	◆ 默认是 100%的比例显示， 可点击按钮或鼠标滚动放大、缩小。 ◆ 显示内容跟上一次编辑保存时的一致， 如果是第一次编辑则显示为空。 ◆ 拖拽元素至绘制区，利用工具栏、元素编辑器等绘制拓扑图。	

区块	说明	详细
元素编辑器_资产	◆ 拓扑绘制区中选中单击元素， 显示该元素对应的编辑页面。 ◆ 打开元素编辑页面后，可编辑组件属性，是否绑定资产、资产名称、资产 IP、资产描述、资产图片、宽度、高度； 选择绑定资产， 带出选择资产框， 下拉选择要绑定的资产，元素即可绑定资产。 ◆ 点击<**收回**>，关闭元素编辑器。	 
元素编辑器_安全域、安全设备、Web 业务系统	安全域、安全设备、 Web 业务系统的元素编辑器一样，都是可设置边框粗细、边框颜色、背景颜色， 是否缩略图。	

5.3.3 业务监控

缩略图点击图标，或列表模式中点击操作列的<**业务监控**>，打开业务监控页面，如下图所示：



点击拓扑中的元素图标， 不同元素所展示信息见下表。

区块	说明	详细
未绑定资产的元素显示	点击拓扑图的元素， 显示资产元素显示资产名称。	
绑定资产的元素显示	资产元素显示以下信息： ◆ 资产名称 ◆ 风险评级（已失陷、高风险、低风险、健康， 并以不同颜色标记； 并且当资产为已失陷、高风险、低风险时资产元素上需要标记） ◆ 安全告警Top3（告警名称：事件数量） ◆ 最近异常发生时间 ◆ 资产 IP ◆ 安全域（属于内部安全域时显示**安全域名称**， 不属于内部安全域但是属于内网 IP 时显示**内网**，不属于内部安全域也不属于内网 IP 时显示**未分配**） ◆ 资产类型 ◆ 组织架构	

区块	说明	详细
	◆ 责任人 ◆ 当没有相关信息时， 该项内容不显示。 提示信息下方显示<**Sherlock**>按钮， 点击跳转到 Sherlock 页面， 带入条件： IP 为该资产 IP， 时间范围为最近 7 天。	
Web 业务系统_有绑定资产	◆ Web 业务系统显示以下信息： 图标-系统名称 域名 网络速率 访问次数 访问成功率 7 天告警 ◆ 如果Web 业务系统信息所需都存在的情况下，下方显示<**安全告警**>、 <**访问日志**>、<**访问系统**>、<**投屏演示**>。 **安全告警**： 新页面跳转到<**安全告警**>， 条件 destAddress = 所有关联资产 IP， 时间最近 7 天。 **访问日志**： 新页面跳转到<**原始日志**>， 条件 destHostName= 所有域名和子域名， 时间本日。 **访问系统**： 新页面跳转业务系统的<**访问地址**>。 **投屏演示**： 新页面跳转。	
Web 业务系统_无绑定资产	◆ Web 业务系统显示以下信息： 图标 系统名称 域名 网络速率 访问次数 访问成功率 7 天告警(高： 0 中： 0 低： 0) ◆ 如果Web 业务系统信息所需都存在的情况下，下方显示<**访问日志**>、 <**访问系统**>、<**投屏演示**>。 **访问日志**： 新页面跳转到<**原始日志**>， 条件 destHostName= 所有域名和子域名， 时间本日。 **访问系统**： 新页面跳转业务系统的<**访问地址**>。 **投屏演示**： 新页面跳转。	

区块	说明	详细
安全设备_有绑定资产	◆ 安全设备显示以下信息： 图标 安全设备名称 安全设备关联资产名称 本日日志数 关联资产数量 设备状态 日志量 ◆ 如果安全设备信息所需都存在的情况下， 下方显示<**日志检索**>，<**管理界面**>，<**处置联动**>和<**投屏演示**>按钮。 **日志检索**： 新标签页跳转<**原始日志**>，条件： 设备地址 deviceAddress=多个设备 IP，时间本日。 **管理界面**：新标签页跳转<**设备管理**>界面 URL，当多个资产有管理地址时， 下拉显示资产名称， 用户可选。 **处置联动**： 新标签页跳转“**资产管理▶处置联动▶联动策略**”，带入<**安全设备**>的条件。 **投屏演示**： 新标签页跳转投屏演示。	
安全设备_无绑定资产	◆ 安全设备显示以下信息： 图标-安全设备名称 本日日志数（ 0） 关联资产数量（ 0 台） 设备状态（未检测） 日志量（一条 0EPS）的直线 ◆ <**日志检索**>，<**处置联动**>和<**投屏演示**>按钮。 **日志检索**： 置灰状态 **处置联动**： 新标签页跳转“**资产管理▶处置联动▶联动策略**”，带入<**安全设备**>的条件（暂无数据） **投屏演示**： 置灰状态	
安全域_有绑定资产	◆ 安全域显示以下信息： 图标 安全域名称 网段 包含资产（资产 IP 在安全域里的资产数量） 风险资产（资产 IP 在安全域里的风险资产的数量）	

区块	说明	详细
	7 天告警 (安全域包含的资产 7 天告警高、中、低的总和) ◆ <**安全告警**>和<**资产管理**>按钮： **安全告警**：新页面跳转到<**安全告警**>，条件安全域，时间最近 7 天。 **资产管理**： 新页面跳转到<**资产管理**>， 条件左侧安全域选择该安全域。	
安 全域 _无绑定资产	◆ 安全域显示以下信息： 图标 安全域名称 网段 包含资产 (0 台) 风险资产 (0 台) 7 天告警 (高： 0 中： 0 低： 0) ◆ <**安全告警**>按钮： **安全告警**：新页面跳转到<**安全告警**>，条件安全域，时间最近 7 天。	
资产、 Web 业务系统、安全设备、安全域已删除	拓扑图的图标上标记已删除。	

5.4 Sherlock

5.4.1 功能简介

Sherlock 入口展示纷繁复杂网络中网络实体之间的访问和攻击连接关系，支持选中连接关系中的某个实体查看详情， 或在 IP 地址搜索框中输入待追踪的网络实体 IP 查看详情。

◆ 选择“**威胁感知➤Sherlock**”菜单，查看 Sherlock 页面，如下图所示。

- 点击右上角 ，显示不同的图标与资产类型和情报类型的对应关系， 同“**态势感知➤Sherlock 网络星空**”平面效果中的图示按钮的效果。

  此页面同 “**态势感知➤Sherlock 网络星空**”的平面效果， 点击右上角 ， 可投屏至“**态势感知➤Sherlock 网络星空**” 。

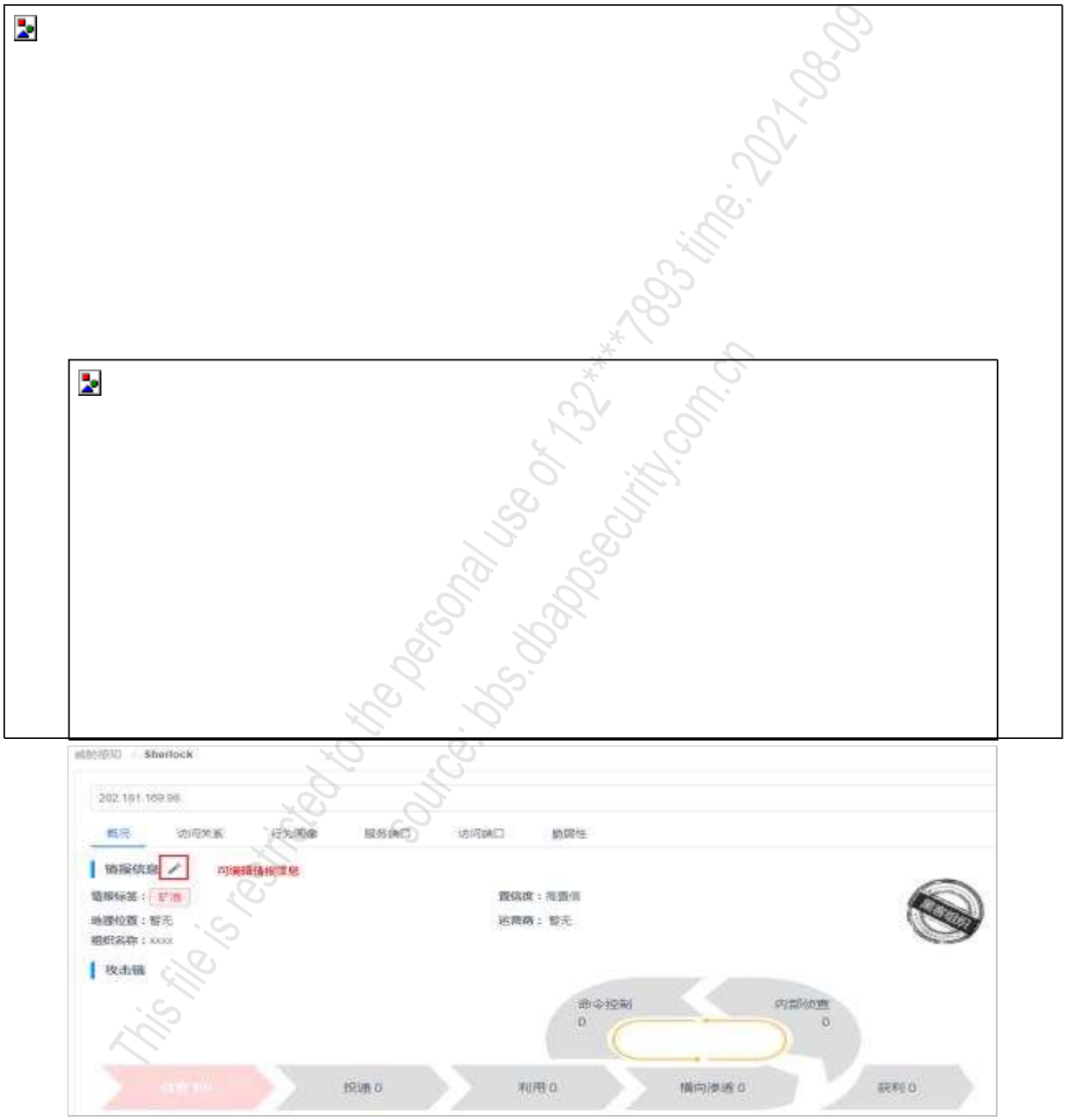
- 点击实体圆点Sherlock或者输入 IP 点击检索后跳至 Sherlock 详情页面，如下图所示，当用户为租户时，只能查询安全域过滤后的 IP。

- 搜索框、时间控件， 几个Tab 页通用， 切换至其他页面， 查询条件保留。
- 点击右上角 ，可选择投屏至攻击者溯源、资产威胁溯源大屏， 带条件： 搜索 IP。

5.4.2 页面详细介绍

点击 Sherlock 页面的某一个原点，可以查看该 IP 的相关信息。

点击<**Sherlock**>进入资产详细页面介绍：



- 资产信息/情报信息/实体信息

  搜索框支持所有 IPv4 格式的 IP 查询， 所以查询出的信息也有不同的情况：

  - 搜索框 IP 有对应资产，查询结果为资产信息。

    显示资产名称（搜索框 IP 对应的资产名称）、资产类型、安全域、 Web 业务系统、安全设备， 没有值的字段显示“暂无”。

    点击 ，跳转到编辑资产页面， 显示搜索框 IP 的资产信息， 编辑后点击<**保存**>，跳转回 Sherlock 概况页面， 刷新后显示编辑后的信息。

  - 搜索框 IP 属于情报 IOC， 查询结果为情报信息。

    显示情报标签、置信度、地理位置、运营商、组织名称， 没有值的字段显示“暂无”。
    以印章形式显示情报分类，优先级为**行业情报>分析团队情报>安全大脑>第三方**。

    点击 ，跳转至修改情报页面， 显示搜索框 IP 的情报信息， 编辑后点击<**保存**>，跳转回 Sherlock 概况页面， 刷新后显示编辑后的信息。

  - 搜索框 IP 无对应资产，查询结果为实体信息。

    属于内部 IP，显示实体名称（搜索框 IP）、地理位置、安全域（属于某一安全域显示安全域名称，反之是(内网)）。
    不属于内部 IP，但属于内部安全域， 显示实体名称（搜索框 IP）、地理位置、安全域（所属内部安全域名称）。

    不属于内部 IP，也不属于内部安全域， 显示实体名称（搜索框 IP）、地理位置、安全域（未分配）。

    点击 ， 有添加资产和添加行业情报两个选项，选择添加资产，跳转到新增资产页面，带入条件：资产名称为搜索框 IP，保存后跳转回 Sherlock 概况页面， 刷新后， 页面显示资产信息。

    选择添加行业情报， 跳转到添加情报页面，带入条件： IOC 类型： IP + IOC：搜索框 IP，保存后页面跳转回 Sherlock 概况页面， 刷新后， 页面显示情报信息。

- 攻击链

  以不同颜色展示 7 个攻击链： 侦查、投递、利用、横向渗透、内部侦查、命令控制、获利， 被搜索 ip 告警所在攻击链环节高亮， 并依照箭头高亮颜色逐渐加深， 每个攻击链上显示选定时间范围内搜索框中 IP 的未处理状态的安全告警数量， 超过 99 显示 99+。点击图标，与风险详情列表联动，过滤攻击链。

- 告警时序

  搜索框中 IP 的所有状态的安全告警数量， 鼠标移到柱子上时， 显示该柱子对应的时间以及告警数量。

- 风险详情

区块概要见下表。

区块	说明	详细
风险总结	显示以下内容（无对应资产时不显示）： ◆ 资产名称 ◆ 资产状态 ◆ 最近一次攻击发生时间 ◆ 遭受攻击 Top3 告警/事件名称及总数 ◆ 发起攻击 Top3 告警/事件名称及总数	
过滤条件	◆ 支持安全告警、安全事件切换。 ◆ 支持处置状态（切换至安全事件，无处置状态项）、威胁方向、攻击链、威胁等级下拉选择过滤。	
安全告警列表	◆ 安全告警主展示区： 告警、威胁方向、攻击链、攻击方法、威胁等级、告警次数、最近异常发生时间、操作（处置、告警详情）。 ◆ 点击处置， 支持添加白名单、处理状态、禁用模型、添加至联动策略、 EDR 联动， 更改告警状态， 风险评级稍后也相应更新； 点击查看告警详情， 跳转至安全告警， 带条件： 处置状态(alarmStatus)+事件名称(name)+模型 ID(modelName)+来源 IP(srcAddress)或者是目的 IP(destAddress)。	
异常记录列表	异常记录主展示区： 威胁方向、异常记录、攻击链、威胁等级、记录次数、最近异常发生时间、操作（点击查看事件详情， 跳转至异常记录， 带条件： 事件名称(name)+模型 ID(modelName)+ 来源 IP(srcAddress) 或者是目的 IP（destAddress））。	

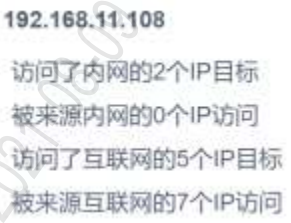
区块	说明	详细
告警事件详情_非情报模型	◆ 点击 ，展开告警、事件详情列表，包含详细信息、原理描述、处置建议。 ◆ 每条记录显示“srcAddress 对 destAddress 发生了 X 次[name]”，并根据聚合后的事件数量降序显示，只显示 Top100。	
告警事件详情_情报模型	告警、事件为情报模型时显示碰撞的情报信息，包括情报分类、情报标签、地理位置、置信度、运营商、组织名称、第三方链接，点击更多跳转至情报查询页面，查询更多情报信息。	
详情链接	◆ 详细信息中的 srcAddress 或 destAddress，点击 ，显示下拉钻取列表。 ◆ 情报查询：新打开情报查询页面。 带入条件：IP，并且默认显示查询结果。 ◆ 安全告警查询：新打开安全告警页面。 带入条件：IP、时间范围，并且默认显示查询结果。 ◆ 异常记录查询：.新打开异常记录页面。 带入条件：IP、时间范围，并且默认显示查询结果。 ◆ 原始日志查询：.新打开原始日志页面。 带入条件：IP、时间范围，并且默认显示查询结果。 ◆ Sherlock：新打开 Sherlock 详情页面。 带入条件：IP，并且默认显示查询结果。 ◆ 攻击者追踪溯源：新打开攻击者追踪溯源大屏。 带入条件：IP。 ◆ 资产威胁溯源：新打开资产威胁溯源大屏。 带入条件：IP。	

5.4.3 访问关系

切换至**访问关系**Tab 页，进入 Sherlock **访问关系**页面，默认展示如下图所示。

区块概要见下表所示：

区块	说明	详细
模式切换	◆ 图形模式、列表模式，默认选中图形模式。 ◆ 访问方向： 所有方向、访问内网、来源内网、访问互联网、来源互联网， 默认选中所有方向。 ◆ 访问类型： 所有类型、异常访问、正常访问， 默认选中异常访问。	
高级	◆ 默认收起。 ◆ 异常访问类型： 文本输入框，默认为空。 ◆ 攻击链： 下拉选项有扫描探查、渗透攻击、获取权限、命令控制、资产破坏、其他，可以多选， 默认为空。 ◆ 应用协议： 下拉选项为日志字典中 appProtocol 的值，可以多选， 默认为空；支持模糊查询。 ◆ 访问目的端口： 文本输入框，默认为空。 ◆ 连接关系 TOP：可选项有 10、30、50，默认选中 10。	
扩展关系网络	◆ 提供<**自动拓展关系网络**>按钮， 开启时支持在现有关系网络下自动拓展，关闭时维持现有关系网络。 ◆ 提供<**扩展下一级关系网络**>按钮， 随机选择现有关系网络中的一个资产每点击一次按钮扩展一次下一级关系网络。	

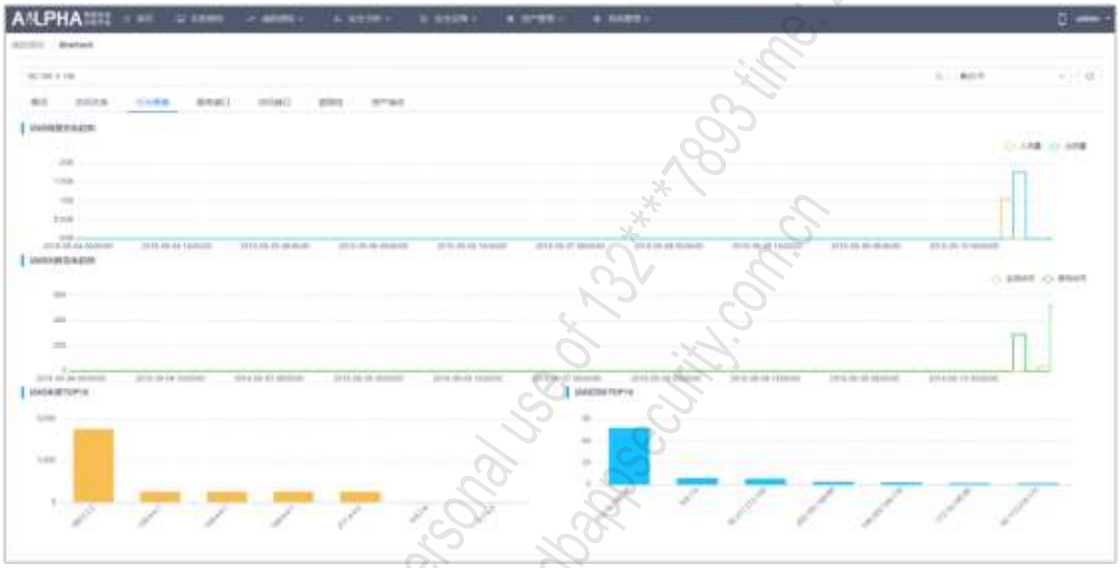
区块	说明	详细
访问关系统计信息	◆ 访问了互联网 IP 的 X 个 IP 目标： 原始日志索引中指定时间范围内 direction=11 或 01，并且 srcAddress 为搜索框中 IP 的事件中 destAddress 的个数。 ◆ 访问了内网 IP 的 X 个 IP 目标：原始日志索引中指定时间范围内 direction=10 或 00，并且 srcAddress 为搜索框中 IP 的事件中 destAddress 的个数。 ◆ 被来源互联网的 X 个 IP 访问： 原始日志索引中指定时间范围内 direction=11 或 10，并且 destAddress 为搜索框中 IP 的事件中 srcAddress 的个数。 ◆ 被来源内网的 X 个 IP 访问： 原始日志索引中指定时间范围内 direction=01 或 00，并且 destAddress 为搜索框中 IP 的事件中 srcAddress 的个数。	
历史访问	按点击时间正序显示当前页面最近点击的 5 个资产名称。	
连线和图标	◆ 连线颜色： 正常访问为蓝色，异常访问为红色。 ◆ 图标：显示不同的图标与资产类型和情报类型的对应关系， 具体见右图。	
图形模式	◆ 默认 Top10。 ◆ 根据资产类型和情报类型显示相对应的图标，图标下方显示资产名称，并且不同的风险等级显示不同的颜色： 已失陷：红色 高风险：橙色 低风险：黄色 健康： 绿色 其他： 蓝色	

区块	说明	详细
资产详情	◆ 鼠标点击图标时浮出显示资产详细信息， 内容包含： ● 有对应资产 资产名称、风险评级、安全告警 Top3 （告警名称：事件数量）、最近异常发生时间、资产 IP、安全域（属于内部安全域时显示安全域名称， 不属于内部安全域但是属于内网 IP 时显示（内网），不属于内部安全域也不属于内网 IP 时显示未分配）、资产类型、组织架构、责任人。 当没有相关信息时， 该项内容不显示。 <**Sherlock**>、<**关系拓展**>按钮（搜索框 IP 对应的图标不显示<**关系拓展**>按钮）。 ● 无对应资产_内网 显示 IP、安全域（所属安全域或者是（内网））。 ● 无对应资产_互联网 显示 IP、安全域：未分配、地理位置。 ◆ 点击关系拓展， 展示该图标对应的 IP 的访问关系； 点击<**Sherlock**>， 跳转至“**威胁感知➤Sherlock**”页面，带条件： IP。	
连线详情	◆ 浮出框显示以下内容 ● 两个图标之间的访问方向，两者相互访问时显示两条线。 ● 访问类型（正常访问： XXX 异常访问 XXX），支持钻取。 ● 累计流量： 原始日志中 bytesIn+bytesOut 之和。 ● 最近访问时间：原始日志中满足条件的最近一条日志的时间。 ● 异常访问类型 Top3： 没有异常访问时不显示该项。 ● 正常访问类型 Top3（appProtocolTop3）：没有正常访问时不显示该项。 ◆ 连线粗细根据访问次数变化 连线粗细根据当前数据自动计算，最多的固定显示最粗。	

区块	说明	详细
列表模式	◆ 以列表展示访问关系。 默认显示 Top10， 高级查询设置过滤可增加展示条数。 ◆ 列表中正常访问、异常访问支持钻取。	

5.4.4 行为画像

切换至**行为画像**页签，进入行为画像页面，如下图所示。



- 访问流量变化趋势（折线图显示请求流量、出流量）
- 访问次数变化趋势（折线图显示主动访问、被动访问）
- 访问来源Top10（柱状图）
- 访问目标Top10（柱状图）

5.4.5 服务端口

切换至**服务端口**页签，进入服务端口页面，如下图所示。

区块概要见下表。

区块	说明	详细
端口个数统计	◆ 统计时间段内搜索 IP 作为目的 IP 的目的端口中。 ◆ 开放端口、不常用端口、风险端口个数。	
流量统计	◆ 统计时间段内搜索 IP 作为目的 IP 的目的端口中。 ◆ 端口响应总流量、请求总流量、风险端口响应流量、风险端口流请求流量、风险端口流量占比。	
开放端口详情列表	◆ 支持多个端口查询， 以英文逗号隔开。 ◆ 列表显示 Top50 端口，按端口被访问次数倒叙排列。 ◆ 主展示区展示： 开放端口： 属于风险端口时红色字体显示，非风险端口时黑色字体显示。 端口类型、响应流量、请求流量、被访问次数、操作（显示流量日志）。	
端口详情_流量变化趋势	显示选择时间范围内流量变化趋势 ◆ 鼠标移到线上时浮出显示时间、响应流量、请求流量。 ◆ 点击<**流量日志**>，跳转至原始日志页面，带条件： 目的 IP(destAddress)、目的端口(destPort)。	
端口详情_访问来源 Top5	◆ 指定时间范围内按事件数量取Top5。 ◆ 每个 IP 对应的记录显示以下内容： ● IP：支持跳转溯源。 ● 事件数量柱状图： 被访问 XXX 次、请求流量 XXX（单位自动切换，bytesIn 总和）、响应流量 XXX（单位自动切换， bytesOut 总和）、应用协议（ appProtocol 事件数量最多的 Top3），应用协议支持跳转溯源。	

5.4.6 访问端口

切换至**访问端口**页签，进入访问端口页面，如下图所示。

访问端口页面同服务端口，只是搜索中 IP 是作为源 IP 的数据， 区块概要如下表。

区块	说明	详细
端口个数统计	统计时间段内搜索 IP 作为源 IP 的目的端口中开放端口、不常用端口、风险端口个数。	
流量统计	统计时间段内搜索 IP 作为源 IP 的目的端口中上传总流量、下载总流量、风险端口上传流量、风险端口流下载流量、风险端口流量占比。	
访问端口详情列表	◆ 支持多个端口查询， 以英文逗号隔开。 ◆ 列表显示 Top50 端口， 按端口访问次数倒叙排列。 ◆ 主展示区展示： 访问端口： 属于风险端口时红色字体显示， 非风险端口时黑色字体显示。 端口类型、上传流量、下载流量、访问次数、操作（显示流量日志）。 流量日志支持跳转溯源，带条件：来源 IP(srcAddress)、目的端口(destPort)。	
端口详情_流量变化趋势	◆ 显示选择时间范围内流量变化趋势。 ◆ 鼠标移到线上时浮出显示时间、上传流量、下载流量。 ◆ 点击<**流量日志**>，跳转至原始日志页面， 带条件：来源 IP(srcAddress)、目的端口(destPort)。	

区块	说明	详细
端口详情_访问目标 Top5	◆ 指定时间范围内按事件数量取Top5 目标 IP。 ◆ 每个 IP 对应的记录显示以下内容： ● IP ：支持跳转溯源。 ● 事件数量柱状图。 被访问 XXX 次、请求流量 XXX（单位自动切换，bytesIn 总和）、响应流量 XXX（单位自动切换，bytesOut 总和）、应用协议（取 appProtocol 事件数量最多的 Top3），应用协议支持跳转溯源。	
端口详情_访问域名 Top5	◆ 指定时间范围内按事件数量取 Top5 域名。 ◆ 每个 IP 对应的记录显示以下内容： ● 域名： 支持跳转溯源。 ● 事件数量柱状图。 被访问 XXX 次、请求流量 XXX（单位自动切换，bytesIn 总和）、响应流量 XXX（单位自动切换，bytesOut 总和）、应用协议（取 appProtocol 事件数量最多的 Top3），应用协议支持跳转溯源。	

5.4.7 脆弱性

切换至**脆弱性**页签， 进入脆弱性页面。脆弱性包含**弱点**和**弱口令**两个Tab 页， 支持 Tab 切换。 默认显示搜索框中 IP 的弱点信息（同弱点管理页面中根据该 IP 查询的结果），如下图。

切换至**弱口令**， 显示搜索框中 IP 的弱口令信息，如下图。

若资产处于防护中状态， 除**弱点**和**弱口令**两个Tab 页外， 增加**漏洞补丁**、**病毒木马**、**网站后门**三个Tab 页。

切换至**漏洞补丁**， 显示搜索框中 IP 的漏洞补丁， 数据来源于 EDR， 点击右上角<**EDR 扫描**>， 可跳转至 EDR 设备页面。

切换至**病毒木马**， 显示搜索框中 IP 的病毒木马，数据来源于 EDR，如下图所示：

切换至**网站后门**， 显示搜索框中 IP 的网站后门，数据来源于 EDR，如下图所示：

5.4.8 资产指纹

切换至**资产指纹**（有对应资产时，才会显示该 Tab 页），进入**资产指纹**页面， 默认显示搜索框中 IP 的资产详情， 数据来源于 “**资产管理▶资产管理▶资产详情**” ，如下图所示：

若资产处于**防护中**状态， 支持Tab 切换， 除资产详情外， 增加**监听端口**、**软件信息**、**账号信息**、**运行进程**四个 Tab 页。

切换至**监听端口**页签，显示搜索框中 IP 的监听端口，数据来源于 EDR，如下图所示：

切换至**软件信息**页签，显示搜索框中 IP 的软件信息，数据来源于 EDR，如下图所示：

切换至**账号信息**页签，显示搜索框中 IP 的账号信息，数据来源于 EDR，如下图所示：

切换至**运行进程**页签，显示搜索框中 IP 的运行进程，数据来源于 EDR，如下图所示：

6. 安全分析

6.1 Investigation

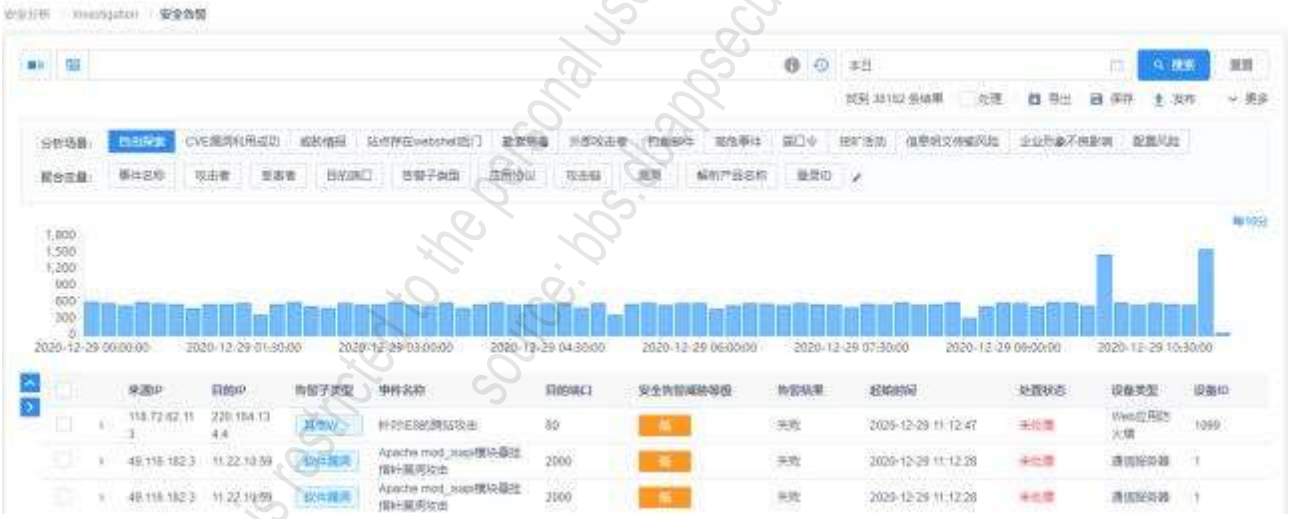
6.1.1 功能简介

Investigation 可以使用不同查询条件对安全告警、 异常记录和原始日志进行查询。当用户为租户时， 只显示根据来源安全域过滤后的数据。

- 安全告警、原始日志和异常记录支持弱密码敏感信息隐藏功能。
- 系统默认开启该功能。如果想查看弱密码等敏感信息，需要输入 admin 用户登录密码进行密码校验。

6.1.2 安全告警

选择 “**安全分析➤Investigation➤安全告警**” 页面， 查看安全告警页面，如下图所示。



1、 查询

可通过时间、表达式、字段（处置状态、攻击链、威胁等级等）、分析场景、聚合变量等多种变量对安全告警筛选及查询， 如下图所示。

点击  可以查看搜索语法：

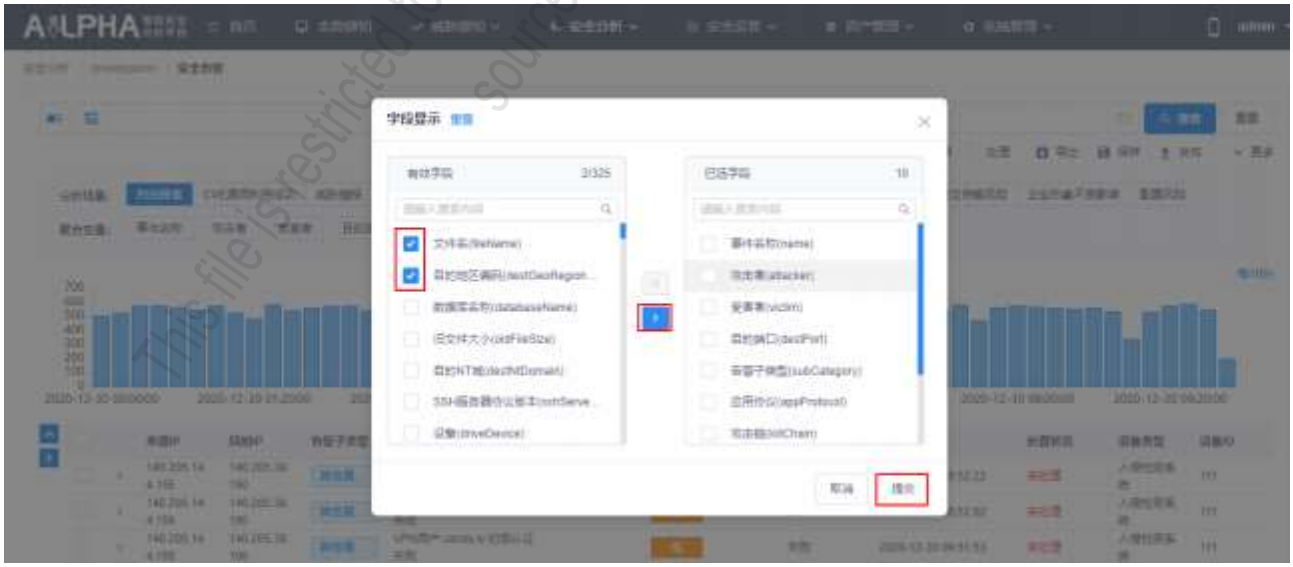
搜索语法说明：

语法	描述	示例	语法	描述	示例
AND	与	srcAddress == "192.168.1.101" AND destAddress == "192.168.1.102"	<=	小于等于	destPort <= 1024
OR	或	srcAddress == "192.168.1.101" OR destAddress == "192.168.1.102"	exist	存在	destAddress exist
NOT	非	NOT (srcAddress == "192.168.1.101")	notexist	不存在	destAddress notexist
==	等于	srcAddress == "192.168.1.101"	in	属于	destAddress in ["192.168.1.101","192.168.1.102"]
!=	不等于	srcAddress != "192.168.1.101"	notin	不属于	destAddress notin ["192.168.1.101","192.168.1.102"]
>	大于	destPort > 1024	contains	包含	message contains "SQL注入"
<	小于	destPort < 1024	ea.any	全文检索	ea.any("注入攻击")
>=	大于等于	destPort >= 1024			

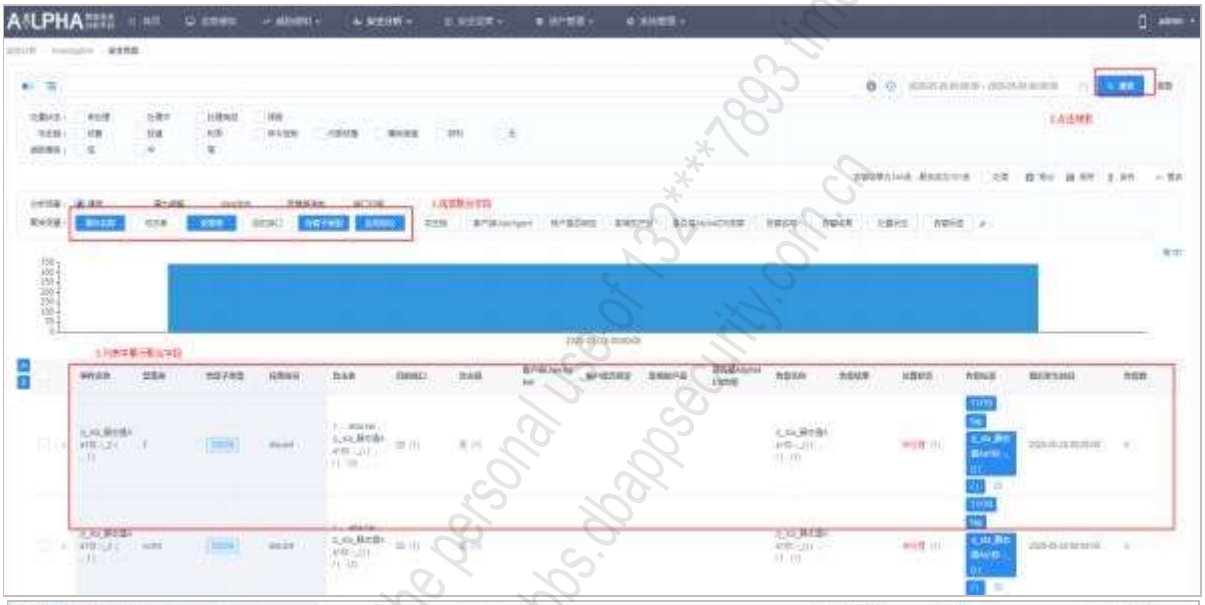
2、 聚合

安全告警支持变量聚合查询。基于不同的分析场景对应不同的聚合变量和聚合列表名。自由探索下默认聚合维度有： 事件名称、攻击者、受害者、目的端口、告警子类型、应用协议、攻击链， 支持自定义， 最多可添加 15 个变量， 聚合时最多可选择 4 个变量来聚合。

点击聚合变量后边的  按钮，可自定义聚合字段，最多可添加 15 个聚合变量。



然后选择要聚合的字段， 点击<**搜索**>即可（可聚合条数不能超过 200000 条）。 选中时变蓝色， 再次点击取消置灰， 选择的聚合变量越多粒度越细， 最多选 4 个字段。不选聚合变量时表示直接查询。聚合后效果如下图所示。

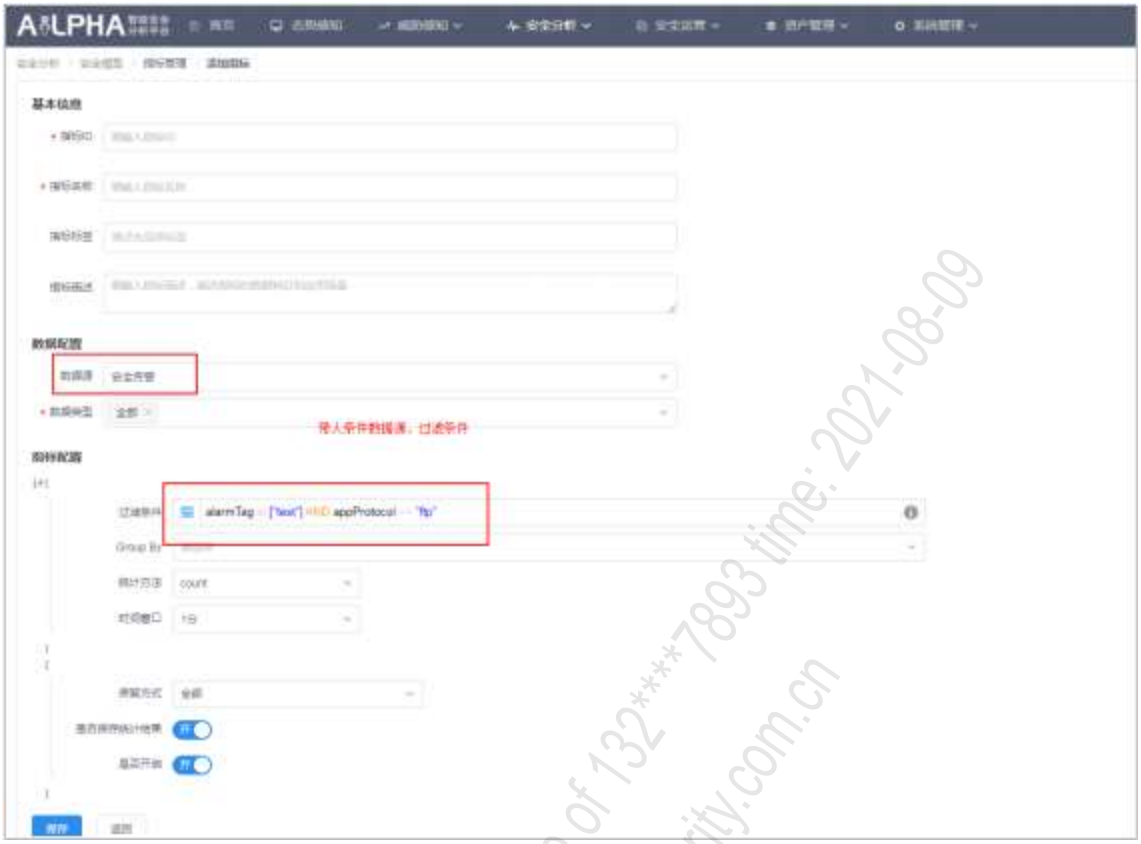


3、 保存发布

输入相关查询条件， 点击<**保存**>， 填写名称、描述、建议、分组及保存搜索时间， 保存。保存后的条件可

点击左上角 按钮查看。

输入相关查询条件， 点击<**发布**>， 选择要跳转的功能模块， 如创建统计指标， 带入查询框内表达式并写入指标配置过滤条件以及数据源（安全告警）。



4、 字段显示

点击 按钮重置告警显示字段，可选择安全告警列表展示的字段内容。如下图所示。

其中， 点击已选择字段后面的 号可以删减显示字段， 点击未选择字段后的 号可以增加显示字段， 然后点击<**重置**>， 完成显示字段的重新设置。

5、 导出

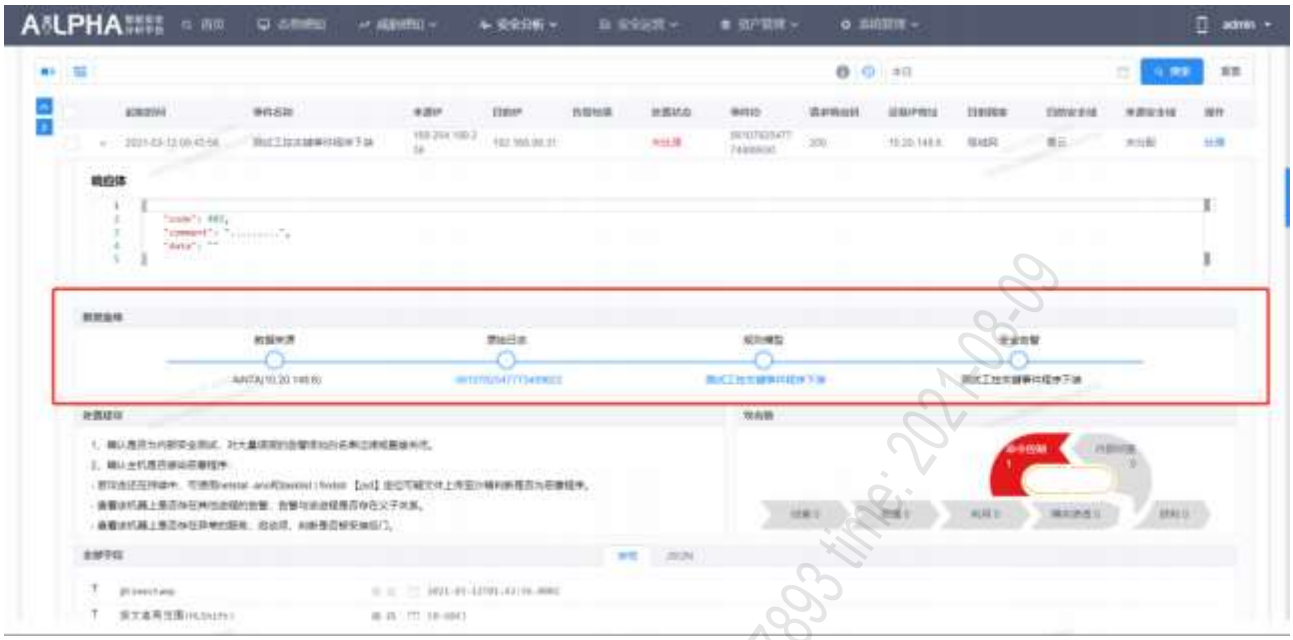
点击 导出 按钮， 可按照告警列表展示字段格式，导出最近 10000 条告警， 导出文件格式为 CSV。如下图所示。

	A	B	C	D	E	F	G	H	I
1	起始时间	事件名称	威胁等级	攻击链	攻击意图	来源IP	目的IP	模型类型	处置状态
2	2019/9/16 14:32	规则引擎故	高	其他	异常事件			离线模型	未处理
3	2019/9/16 14:32	消息队列故	高	其他	异常事件			离线模型	未处理
4	2019/9/16 14:32	统计引擎故	高	其他	异常事件			离线模型	未处理
5	2019/9/16 14:32	定制规则引	高	其他	异常事件			离线模型	未处理
6	2019/9/16 14:32	CEP引擎故	高	其他	异常事件			离线模型	未处理
7	2019/9/16 14:30	mfjtestut	高	其他	异常事件		123.123.1	离线模型	未处理
8	2019/9/16 14:30	其它离线3	高	其他	异常事件		111.111.1	离线模型	未处理
9	2019/9/16 14:30	140.205.1	高	其他	异常事件		140.205.1	离线模型	未处理
10	2019/9/16 14:30	Waf离线30	高	其他	异常事件		10.10.10.	离线模型	未处理
11	2019/9/16 14:30	192.168.3	高	其他	异常事件		192.168.3	离线模型	未处理
12	2019/9/16 14:30	fishcococ	高	其他	异常事件		34.89.99.	离线模型	未处理
13	2019/9/16 14:30	221.0.92.	高	其他	异常事件		221.0.92.	离线模型	未处理
14	2019/9/16 14:30	欢乐豆07离	高	其他	异常事件		90.2.2.11	离线模型	未处理
15	2019/9/16 14:30	192.7.1.2	高	其他	异常事件		140.205.1	离线模型	未处理
16	2019/9/16 14:30	apt-editi	高	其他	异常事件		12.10.13.	离线模型	未处理

6、 告警详情查看

告警列表单击某一条事件， 展开该条告警详细信息， 如来源 IP、目的 IP、端口、地理位置、攻击方法、模型类型等信息。如下图所示。

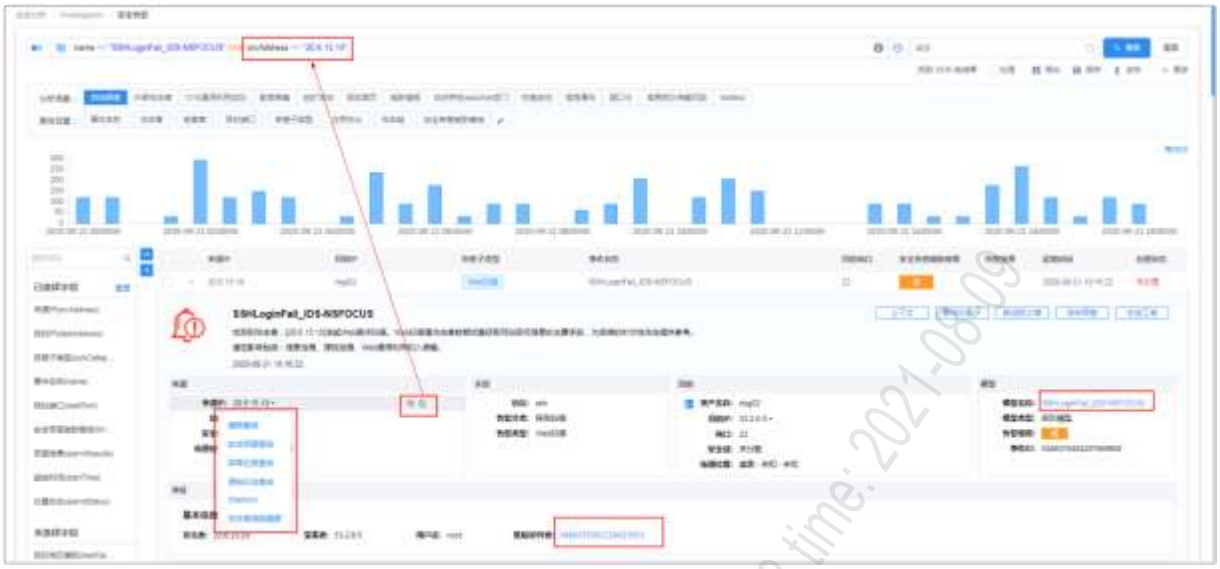
在**数据血缘**区域， 可以查看该安全告警信息的数据来源、原始日志/异常记录和模型类型等， 方便用户掌握数据的来龙去脉。如下图所示。



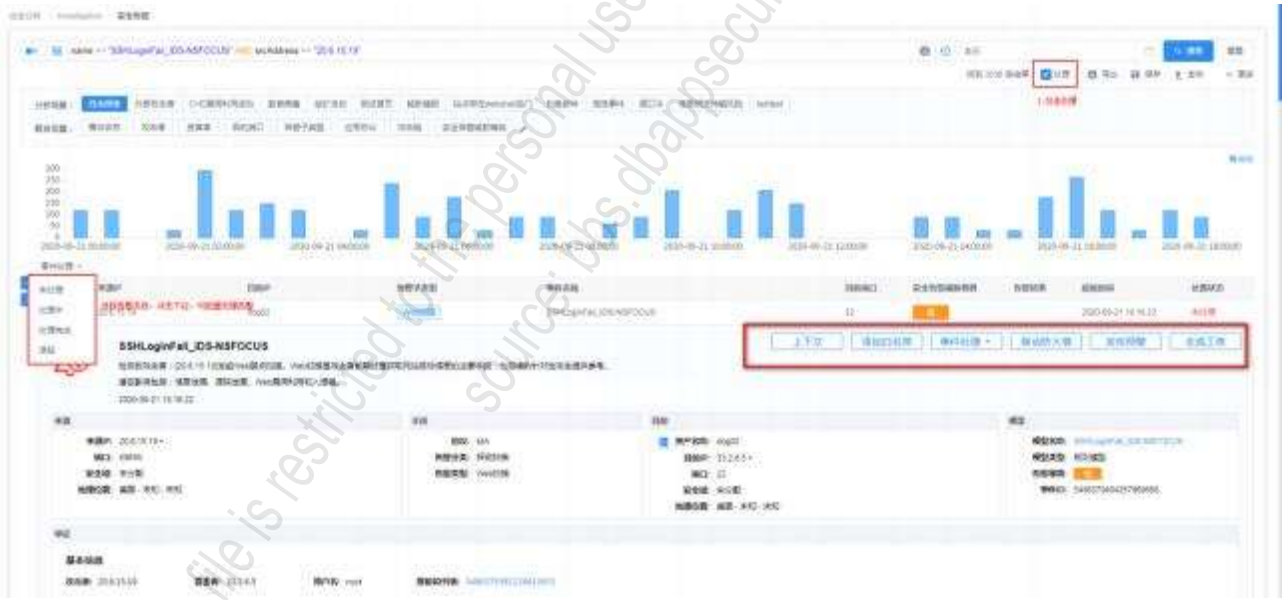
已阻断标记： 在告警详情中如果告警相关 IP 已经添加到阻断策略中时， 告警详情页面会显示“已阻断”标记。如下所示。

7、 告警详情联动

查看告警详情后， 点击某字段前的 按钮， 可将该字段内容快速联动到查询框； 点击 可链接到相关页面， 如情报查询、追踪溯源、模型详情等页面。如下图所示。

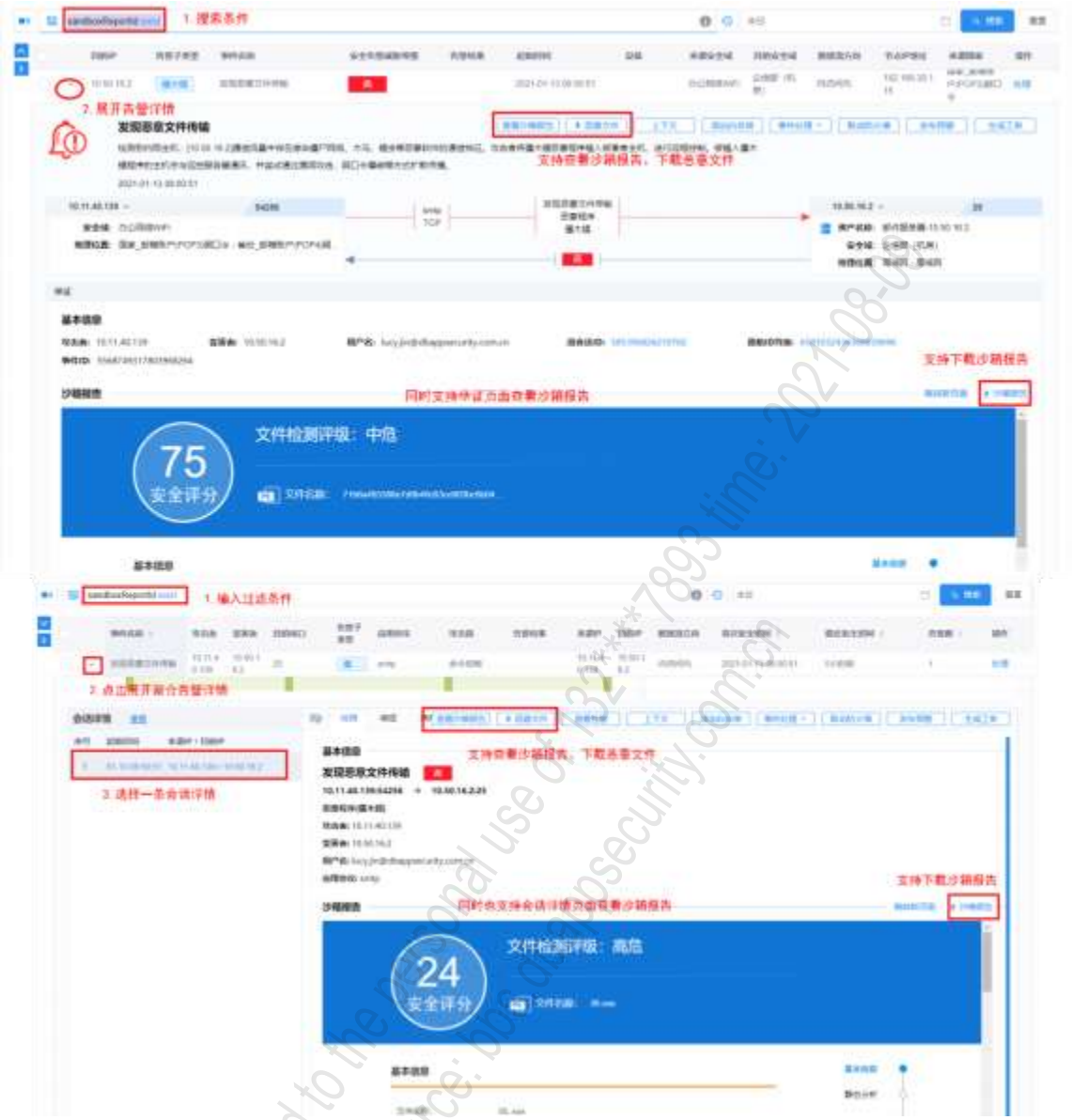


事件处理。选择一条告警， 查看告警详情， 点击<**事件处理**>， 可将该事件标记为**未处理/处理中/处理完成/误报状态**； 点击告警列表上方的<**事件处理**>可批量标记事件； 点击<**上下文**>可以查看前后 10 分钟的原始日志， 点击<**添加白名单**>可以把该告警 IP 添加到系统白名单； 点击<**联动防火墙**>可以通过防火墙联动处理该条告警信息；点击<**发布预警**>可以发布告警预警信息；点击<**生成工单**>可以对该告警进行派单处理。如下图所示。



8、 告警详情沙箱报告

当告警满足 sandboxReportId exist 条件时， 普通查询/聚合查询列表中， 选择一条告警， 点击展开详情， 支持查看沙箱报告、下载恶意文件和下载沙箱报告操作，如下图所示。



6.1.3 原始日志

选择 “**安全分析➤Investigation➤原始日志**”页面， 查看原始日志页面，如下图所示。

1、 查询

可通过时间、表达式、标签、日志类型、字段对原始日志进行筛选及查询， 如下图所示。

点击 按钮弹出表达式框， 可添加表达式条件以及组，选择后自动写入表达式搜索框内， 如下图所示。

时间筛选器下方可设置聚合页面自动刷新， 默认关闭， 开启后支持刷新频率： 15 秒、 30 秒、 1 分钟、 5 分

钟、 10 分钟、 15 分钟。如下图所示。

输入相关查询条件， 点击<**发布**>，选择要跳转的功能模块， 如创建统计指标， 带入查询框内表达式并写入指标配置过滤条件以及数据源（原始日志）。如下图所示。

2、 保存发布

输入相关查询条件， 点击<**保存**>，填写名称、 分组及保存内容（默认为搜索， 可多勾选保存为可视化）并保存， 已存搜索条件创建完成。保存后的条件可点击左上角 按钮查看。 如下图所示。

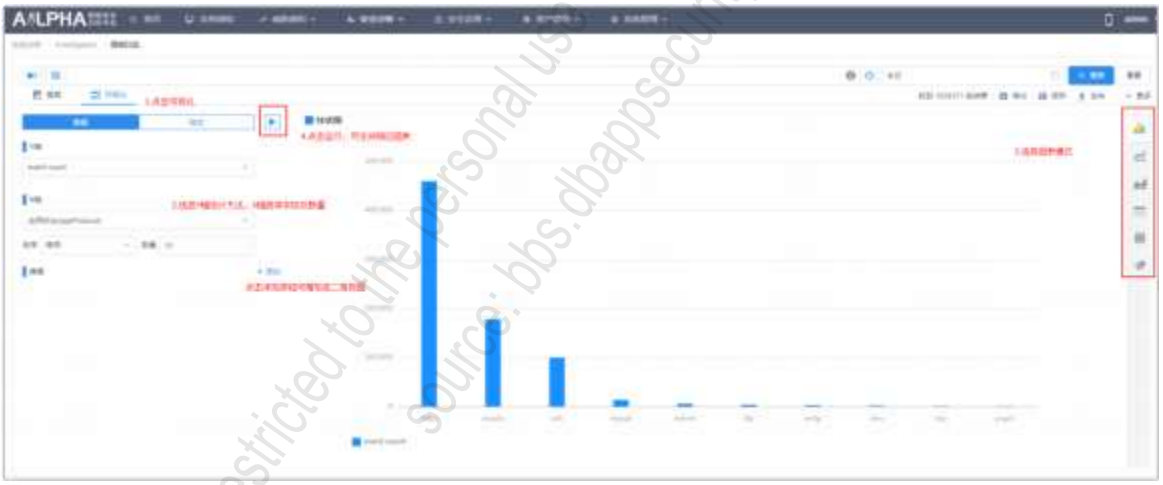
保存查询条件

查询已存搜索

输入相关查询条件， 点击<**发布**>， 选择要跳转的功能模块， 如创建统计指标， 带入查询框内表达式并写入指标配置过滤条件以及数据源（原始日志）。 如下图所示。

3、 可视化数据

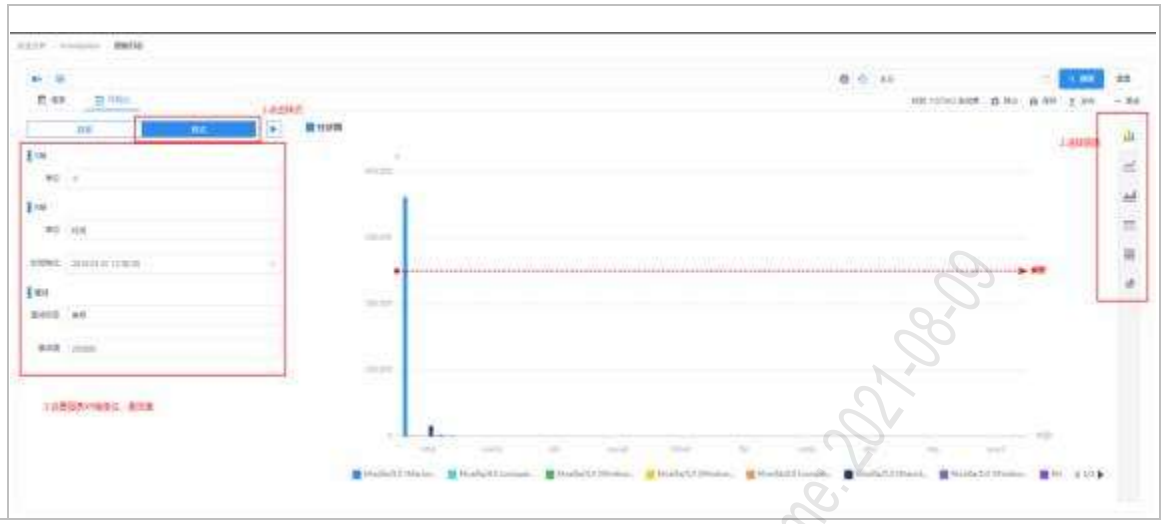
点击<**可视化**>，以图表模式展示原始日志分布情况。可手动对图表进行配置， 支持的图表类型有柱状图、折线图、面积图、表格、饼图、 单值图等。如下图所示。



- Y 轴支持统计方法： event count,count,avg,sum,max,min,distinct count(默认 event count)。
- X 轴配置： 默认按照采集器接收时间(collectorReceiptTime)， 根据 Y 轴统计方法可筛选不要的字段：event count、 distinct count：所有字段； avg、 sum、 max、 min： 数值类型字段。
- 维度配置： 默认没有维度字段， 可点击<**添加**>按钮添加聚合维度字段， 最多添加一个； 鼠标移动到字段筛选框， 显示删除图标。

可视化样式

在**可视化**页签点击<**样式**>， 可对图表样式进行设置， 手动输入 X、Y 轴单位， 基线值设置， 所有内容非必填。设置好的图表样式可在数据可视化处展示。 如下图所示。



4、 时序图查看

点击<**时序图**>， 查看原始日志时序分布情况， 支持手动选择时间粒度。如下图所示。

5、 字段显示

点击 按钮， 可设置原始日志列表展示的字段内容。如下图所示。

其中， 点击已选择字段后面的 号可以删减显示字段， 点击未选择字段后的 号可以增加显示字段， 然后点击<**重置**>， 完成显示字段的重新设置。

6、 日志导出

点击 导出 按钮， 可按照列表展示字段格式， 导出最近 10000 条日志， 导出文件格式为 CSV。如下图所示。

	A	B	C	D	E	F	G	H
1	采集器接收时间	事件名称	来源IP	目的IP	来源用户名	事件设备大	设备名称	URI
2	2019/9/16 14:02	SMB远程溢	192.168.1	192.168.198.203		网络IDS	192.168.30.57	
3	2019/9/16 14:01	SMB远程溢	192.168.1	192.168.198.203		网络IDS	192.168.30.57	
4	2019/9/16 14:00	SMB远程溢	192.168.1	192.168.198.203		网络IDS	192.168.30.57	
5	2019/9/16 13:59	恶意文件R	192.168.1	192.168.30.15		网络IDS	192.168.30.57	
6	2019/9/16 13:59	恶意文件R	192.168.1	192.168.30.15		网络IDS	192.168.30.57	
7	2019/9/16 13:59	WEB行为分	192.168.1	192.168.33.211		WEB审计设	192.168.30.57	
8	2019/9/16 13:59	HTTP请求L	112.1.1.1	172.16.100.2		审计设备	ftp-test	
9	2019/9/16 13:59	HTTP请求L	112.1.1.1	172.16.100.2		审计设备	ftp-test	/ls5/forum.exe,jsessionid=6F9D40E2110D3F64D0AB95525290CE75
10	2019/9/16 13:59	SMB远程溢	192.168.1	192.168.198.203		网络IDS	192.168.30.57	
11	2019/9/16 13:59	服务器遇到	11.11.11.2	2.2.2.5		应用程序	SOC资产同	/to_pages.do?method=select * from substring
12	2019/9/16 13:59						SOC资产同步-APT	
13	2019/9/16 13:59	请求的文件名，参数名和参数包含HTTP响应分割攻击					SOC资产同步-APT	
14	2019/9/16 13:59	HTTP请求L	11.11.11.1	192.168.11.9		审计设备	SOC资产同	/ls5/forum?meta='user'
15	2019/9/16 13:59	IIS短文件名泄露漏洞	16026020				SOC资产同步-APT	
16	2019/9/16 13:59	系统命令注入攻击	12040050				SOC资产同步-APT	
17	2019/9/16 13:59	HTTP请求L	11.11.11.1	192.168.11.6		审计设备	SOC资产同	/images?boot.ini
18	2019/9/16 13:59						SOC资产同步-APT	
19	2019/9/16 13:59	netstat命令字符串	12040065				SOC资产同步-APT	
20	2019/9/16 13:59	请获请求的文件名、参数名和参数包含SSI注入	12070				SOC资产同步-APT	

7、 日志详情查看

日志列表单击某一条日志， 展开该条日志详细信息， 如来源 IP、目的 IP、端口、地理位置、报文、原始日志等等信息。如下图所示。

8、 日志详情联动

查看日志详情后，点击某字段前的 按钮， 可将该字段内容快速联动到查询框。如下图所示。

9、 日志详情二维码

在日志详情的**原始日志**区域， 可以查看原始日志内容， 点击二维码图标可生成二维码。扫描二维码可获取该条原始日志， 点击<**X**>按钮可关闭二维码。当原始日志超过 2950 字节长度，二维码扫描内容自动截断。如下图所示。

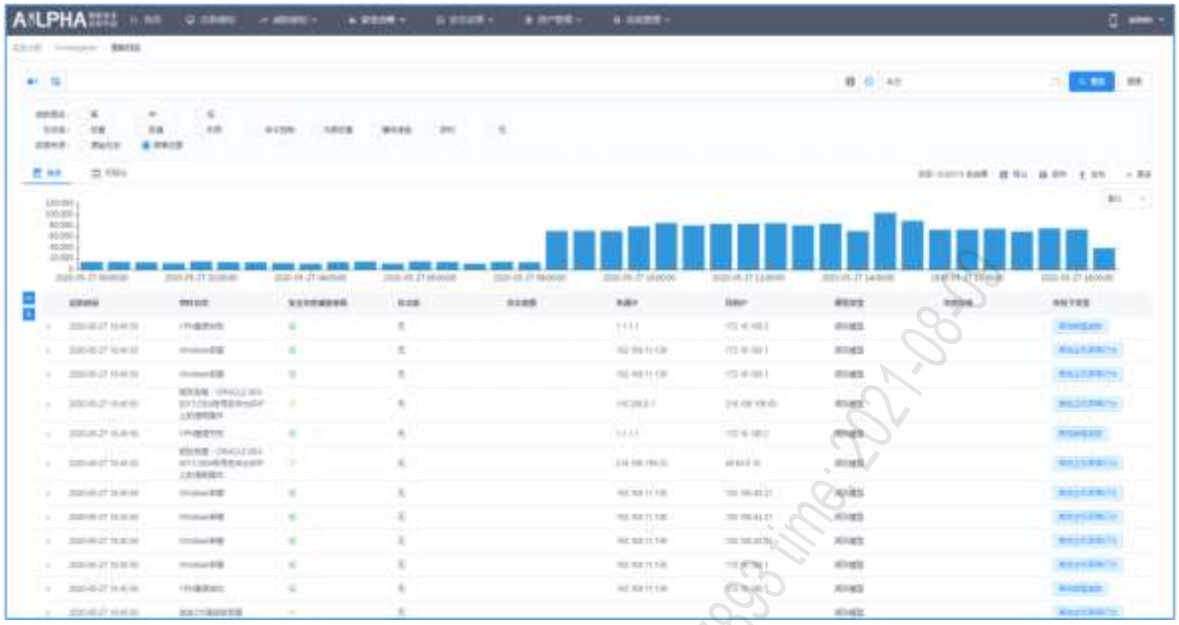
10、 更多查询

点击<**更多**>，可过滤日志类型（流量/日志）、 切换数据来源（原始日志/异常记录）。如下图所示。

切换至**异常记录**， 页面重新加载。

6.1.4 异常记录

选择 “**安全分析➤Investigation➤原始日志**” 页面，点击<**更多**>，在弹出的页面**数据来源**选择 “**异常记录**” ，可以查看异常记录页面， 如下图所示。



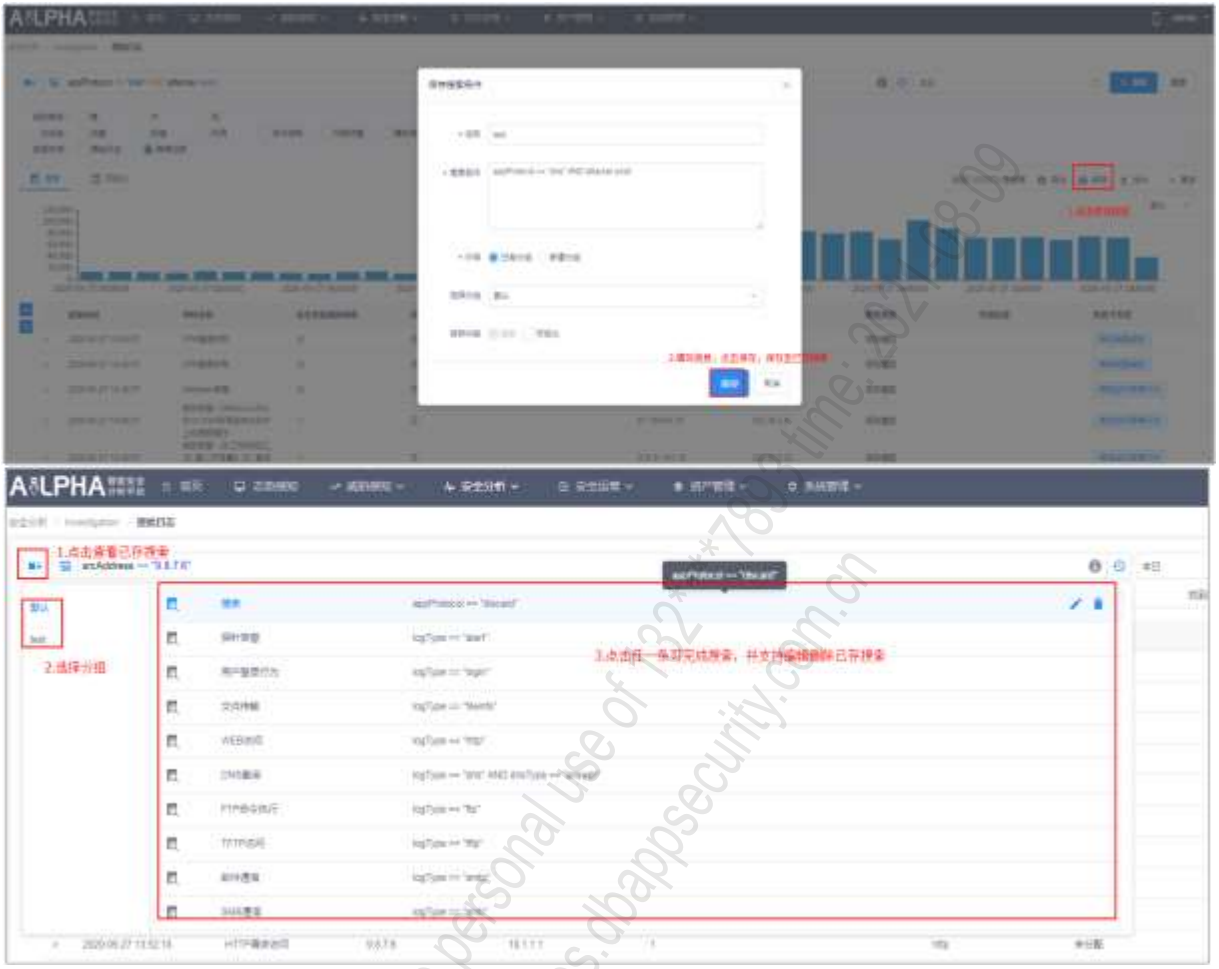
1、 查询异常记录

可通过时间、表达式、字段对异常记录进行筛选及查询， 如下图所示。

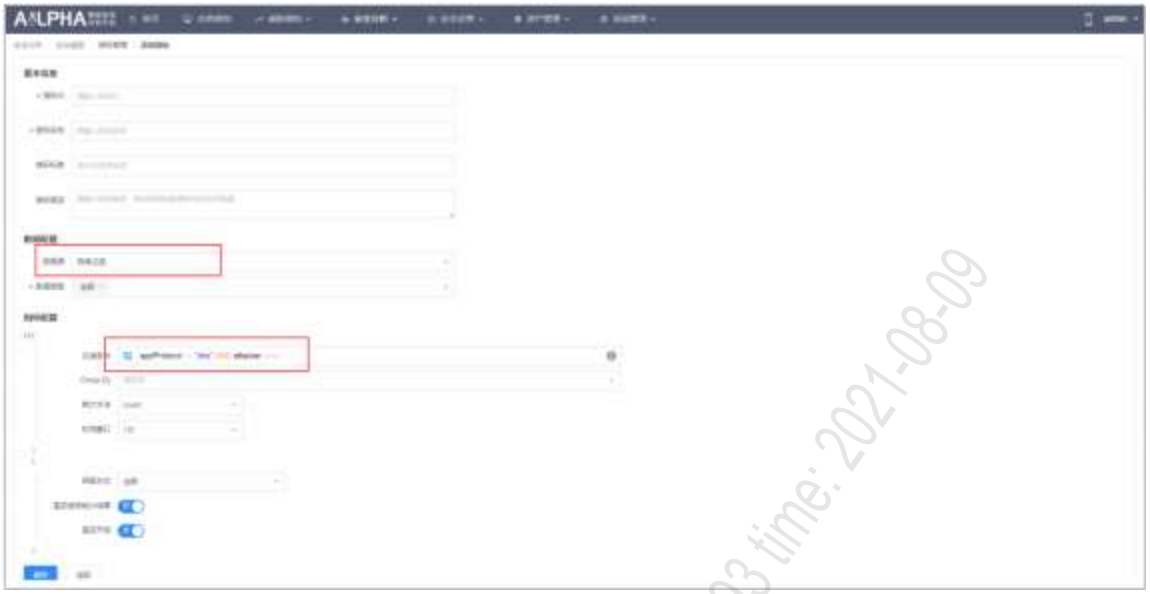
2、 保存发布

输入相关查询条件， 点击<**保存**>， 填写名称、分组及保存内容（默认为搜索， 可多勾选保存为可视化）并

保存， 已存搜索条件创建完成。保存后的条件可点击左上角  按钮查看当前已经保存的搜索条件。

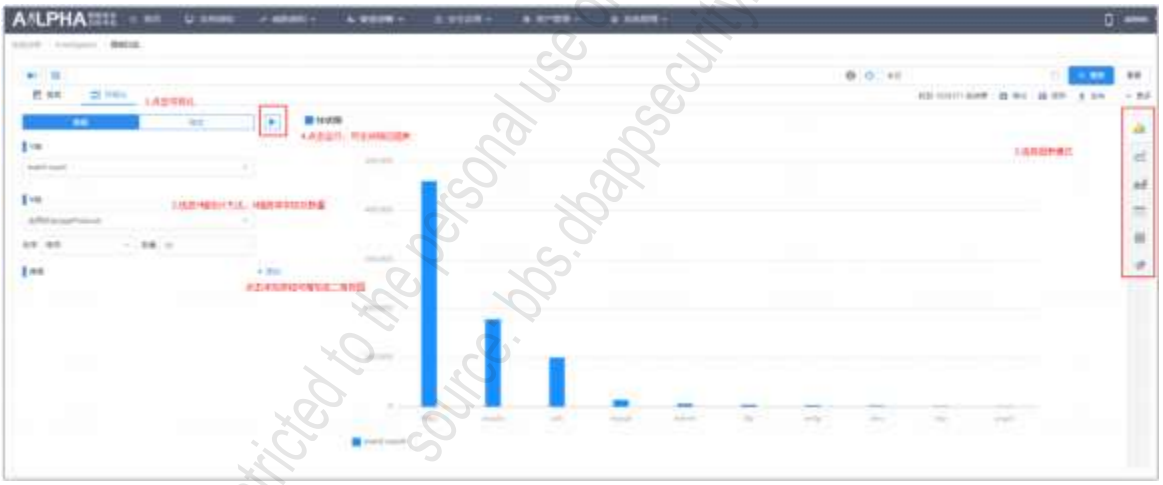


输入相关查询条件， 点击<**发布**>按钮， 选择要跳转的功能模块， 如创建统计指标， 带入查询框内表达式并写入指标配置过滤条件以及数据源（原始日志）。 如下图所示。



3、 数据可视化

点击**可视化**页签，以图表模式展示原始日志分布情况，可手动对图表进行配置，支持的图表类型有柱状图、折线图、面积图、表格、饼图、单值图。 如下图所示：



- Y 轴配置： 从下拉框选择，主要有 event count、 count、 avg、 sum、 max、 min 等(默认 event count)。
- X 轴配置： 从下拉框选择， 默认按照采集器接收时间(collectorReceiptTime)，根据 Y 轴统计方法可筛选不要的字段： event count、 distinct count：所有字段； avg、 sum、 max、 min：数值类型字段。
- 维度配置： 默认没有维度字段， 可点击<**添加**>按钮添加聚合维度字段， 最多添加一个； 鼠标停留到字段筛选框， 会显示删除图标，点击删除图标可以删除该字段。

样式设置

点击<**样式**>， 可对图表样式进行设置， 手动输入 X、 Y 轴单位， 基线值设置， 所有内容非必填。设置好的

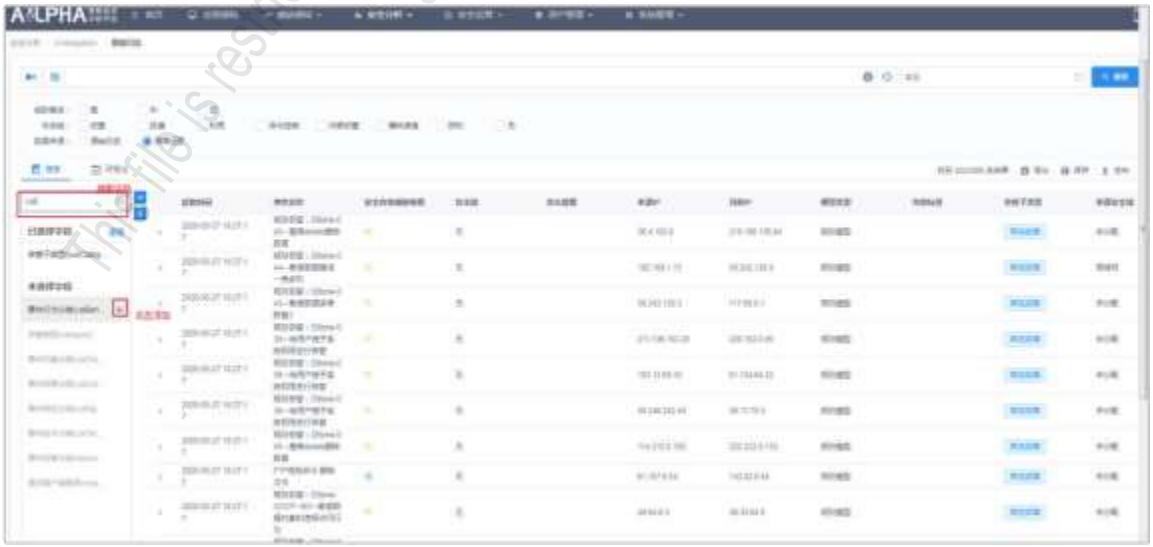
图表样式可在数据可视化处展示。如下所示。

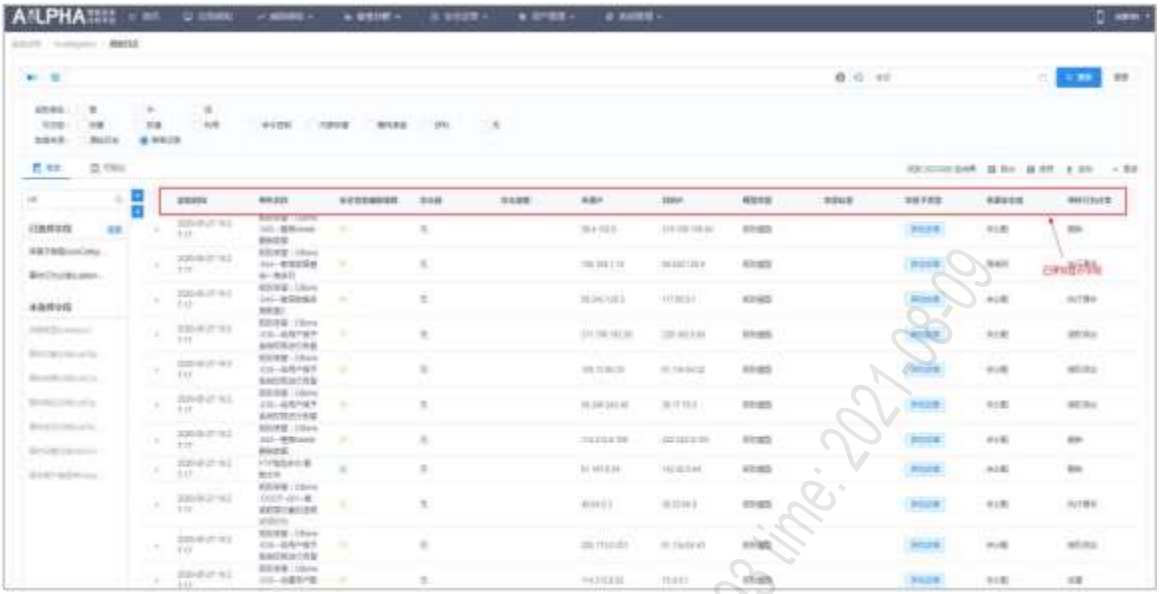
4、 时序图查看

点击**时序图**，查看原始日志时序分布情况，支持手动选择时间粒度。如下图所示：

5、 字段显示

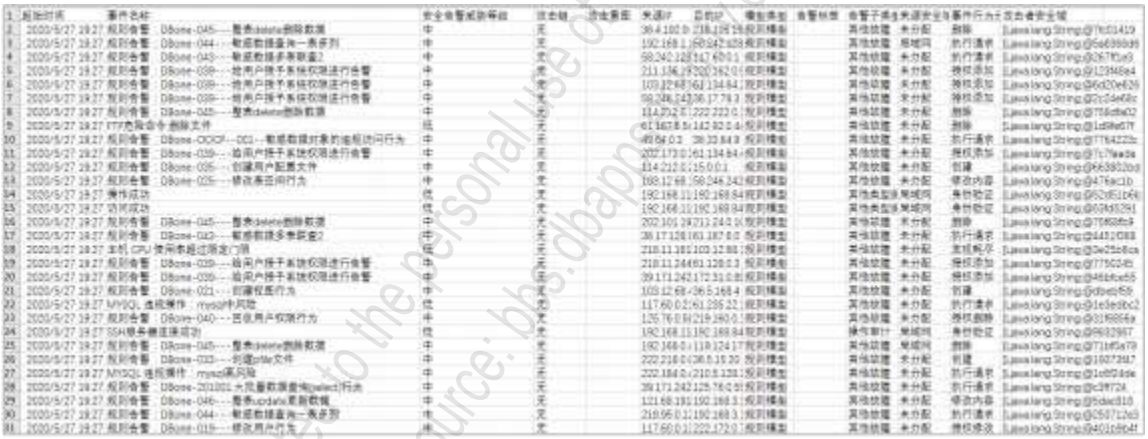
点击按钮， 可选择异常记录列表展示的字段内容。如下图所示：





6、 导出

点击 导出 按钮， 可按照列表展示字段格式，导出最近 10000 条日志，导出文件格式为 CSV。如图所示：



7、 异常记录详情查看

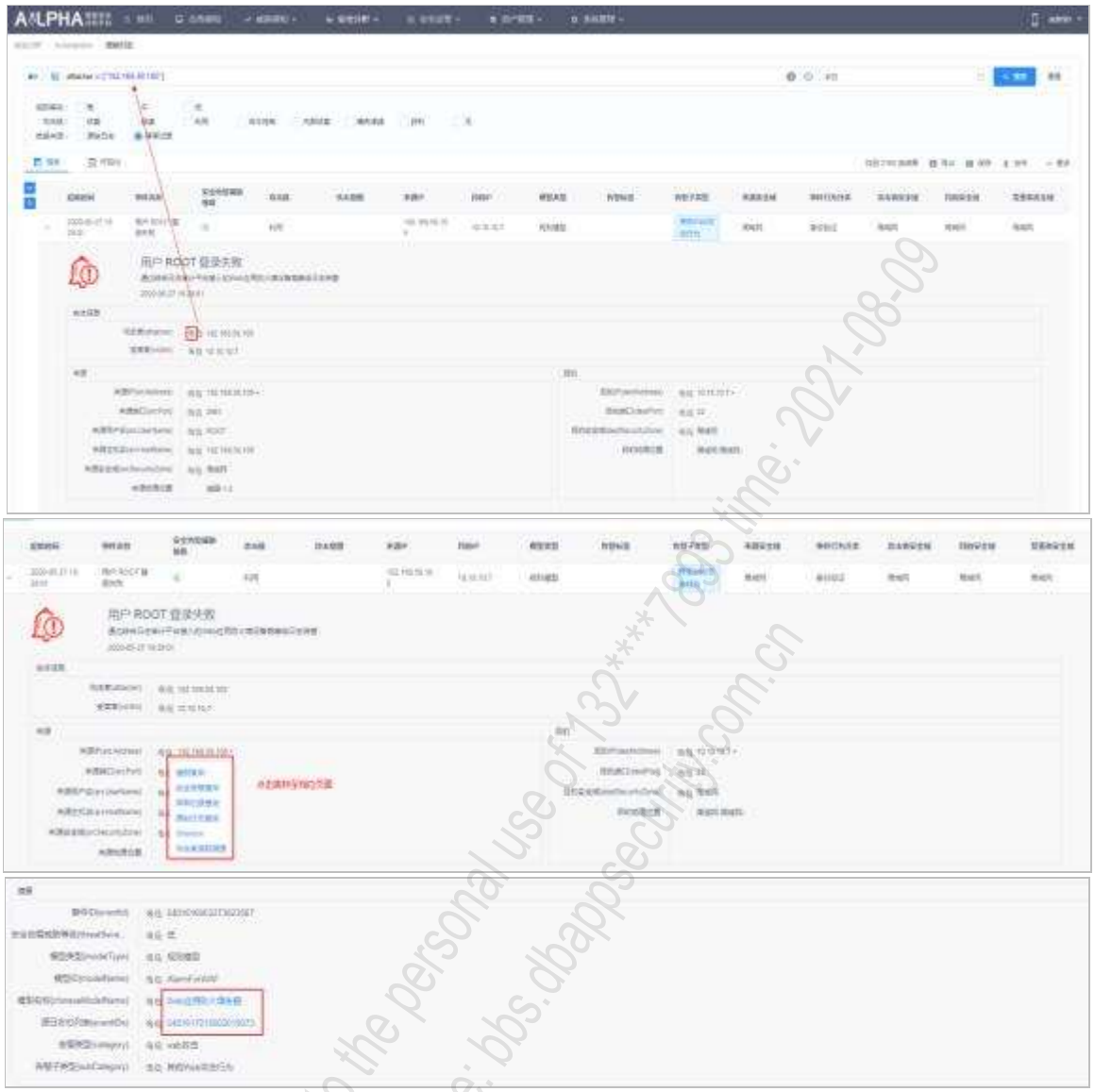
异常记录列表单击某一条日志， 展开该条记录详细信息， 如攻击者、受害者、来源 IP、目的 IP、端口、地理位置、攻击链、模型等信息。 选择一条异常记录，查看记录详情，点击<**上下文**>可以查看前后 10 分钟的原始日志，点击<**添加白名单**>可以把该异常记录 IP 添加到系统白名单； 点击<**联动防火墙**>可以通过防

火墙联动处理该条异常信息。 如下图所示。

已阻断标记：在异常记录详情中如果异常记录相关 IP 已经添加到阻断策略中时，详情页面会显示“已阻断”标记。如下所示。

8、 异常记录详情联动

查看日志详情后， 点击某字段前的 按钮， 可将该字段内容快速联动到查询框， 点击 可链接到相关页面， 如情报查询、追踪溯源、模型详情等页面。如下图所示：



9、 异常记录详情沙箱报告

当异常记录满足 sandboxReportId exist 条件时，查询列表中，选择一条异常记录，点击展开详情， 支持查看沙箱报告、下载恶意文件和下载沙箱报告操作， 如下图所示。

10、 更多查询

点击<**更多**>，可根据威胁等级、攻击链快速查询， 切换数据来源（原始日志/异常记录）。如下图所示：

6.2 威胁情报

6.2.1 功能简介

威胁情报通过标签化录入方式， 支持登记恶意 IOC、黑客组织、监管机构。情报信息将作为威胁、whois 知识库， 识别互联网中的网络实体， 情报知识将赋能到 Sherlock 概况和告警详情部分。情报库的不断更新与丰富， 为用户提供更准确的告警信息，以便用户及时做出应对措施。

6.2.2 情报查询

选择 “**安全分析➤威胁情报➤情报查询**” 页面， 输入 IP、域名、文件 HASH(MD5/SHA1/SHA256)、邮箱进行情报查询， 展示查相关情报类型、情报源、情报标签、地理位置、置信度、运营商及组织名称信息。如

下图所示。

第三方链接。情报查询结果支持跳转第三方链接： 安恒数据大脑、微步在线、 Whios、VirusTotal，补充相关情报信息。如下图所示。

6.2.3 情报源

选择 “**安全分析➤威胁情报➤情报源**” 页面， 查看情报源， 包括安恒安全数据大脑、安恒 AiLPHA 分析团队、行业情报三种情报源。安恒安全数据大脑、安恒 AiLPHA 分析团队情报源为内置情报源， 定期会更新情报源；行业情报为用户自定义维护情报源， 用户可在行业情报中添加相关情报信息。如下图所示。

1、 情报源管理

选择一个情报源， 点击 管理 按钮， 进入情报源管理界面； 输入需要修改的情报信息， 点击修改或者删除。安恒安全数据大脑、安恒 AiLPHA 分析团队管理界面可以对情报信息修改、删除； 行业情报管理界面可以对情报信息进行添加、修改、删除。如下图所示。

2、 情报源设置

选择待设定的某一个情报源，点击对应的情报源页面的 设置 按钮， 进入到情报源设置界面。

- 安恒安全数据大脑支持在线更新、离线更新， 离线更新需要上传相关离线更新包， 更新成功后会有相应更新时间及更新状态提示，如下图所示。

- 安恒 AiLPHA 分析团队仅支持离线更新， 离线更新需要上传相关离线更新包， 更新成功后会有相应更新时间及更新状态提示， 如下图所示。

- 行业情报支持离线更新， 同时支持情报导出， 如下图所示。

6.3 UEBA

6.3.1 功能简介

UEBA 提供画像及基于各种分析方法的异常检测， 通常是基本分析方法来评估用户和其他实体(主机， 应用程序， 网络， 数据库等)，来发现与用户或实体标准画像或行为相异常的活动所相关的潜在事件。这些活动

包括内部或第三方人员对系统的异常访问(用户异常)，或者外部攻击者绕过防御性安全控制的入侵(异常用户)。通过对用户日常行为的聚类以及 AiLPHA 大数据智能安全分析平台安全域信息，将不同类别的使用者（ User ）区分出来。当这些用户实体有非职责内操作时， 平台会将该用户标记较高异常评分（Anomaly Score）。

6.3.2 UEBA 用户画像

1、 UEBA 用户画像

选择“**安全分析➤UEBA➤UEBA 用户画像**”菜单， 打开 UEBA 用户画像界面。如下图所示。

UEBA 用户画像页面布局见下表。

序号	名称	说明
1	查询	支持用户信息、账号、邮箱模糊查询。
2	风险用户	显示风险评分不为 0 的用户，根据风险评分倒序排列。
3	重点关注用户	显示重点关注用户。
4	用户管理	点击跳转至 UEBA 用户管理界面。

2、 UBEA 用户画像详情

行为时间轴：记录该用户 vpn 账户登录期间行为， 包括访问、遭受攻击情况等，如下图所示。

参数说明如下所示：

序号	名称	说明
1	编辑	点击跳转至该用户编辑页面。
2	时间控件	支持最近 24 小时、最近 7 天、最近 30 天、本日、本周、本月时间查询。
3	风险评分	根据用户登录期间攻击及遭受攻击情况来进行评分，分数越高风险越大。
4	行为时间轴	展示用户 VPN 登录期间行为，点击时间可跳转至安全分析页面。
5	用户风险评分	展示用户最近 7 天风险评分。
6	用户活跃时间段	展示最近 7 天用户在线时间段。

访问关系

访问关系说明见下表：

项目	说明	详细
图形模式	◆ 用户 ◆ 客户端 ◆ 分配身份 ◆ 互联网 ◆ 内网 ◆ 图标下方显示资产名称，并且不同的风险等级显示不同的颜色： 已失陷：红色 高风险：橙色 低风险：黄色 健康： 绿色 其他： 蓝色	

项目	说明	详细
图标详情	鼠标点击图标时浮出显示资产详细信息， 内容包含： ◆ 有对应资产 资产名称、风险评级、安全告警 Top3（告警名称：事件数量）、最近异常发生时间、资产 IP、安全域（属于内部安全域时显示安全域名称， 不属于内部安全域但属于内网 IP 时显示(内网)，不属于内部安全域和内网 IP 时显示互联网）、资产类型、组织架构、责任人。 ◆ 无对应资产_内网 显示 IP、安全域（所属安全域或者是（内网））。 ◆ 无对应资产_互联网 显示 IP、安全域：未分配、地理位置。	
连线详情	◆ 两个图标之间的访问方向，两者相互访问时显示两条线。 ◆ 访问类型（正常访问： XXX 异常访问 XXX）。支持钻取。 ◆ 累计流量： 原始日志中 bytesIn+bytesOut。 ◆ 最近访问时间：原始日志中满足条件的最近一日志的时间。 ◆ 异常访问类型 Top3，没有异常访问时不显示该项。 ◆ 正常访问类型 Top3（appProtocolTop3），没有正常访问时不显示该项。	

登录地区： 展示该用户登录地区分布热力图， 如下图所示。

6.3.3 UEBA 用户管理

1、 UEBA 用户新增

点击<**添加用户**>，打开 UEBA 用户添加页面，输入相关信息点击<**保存**>，如下图所示。

2、 UEBA 用户编辑

点击<**编辑**>，打开 UEBA 用户编辑页面， 修改相关信息， 点击<**保存**>， 如下图所示。

3、 UEBA 用户删除

点击操作列<**删除**>， 即可删除该用户。

4、 UEBA 用户批量导入

点击<**批量导入**>， 弹出导入文件弹框，下载模板填写导入即可，如下图所示。

5、 UEBA 用户画像

点击操作列的<**UEBA**>， 跳转至该用户 UEBA 用户画像界面。

6、 查询

UEBA 用户管理支持状态查询及全局搜索。

6.4 可视化中心

6.4.1 功能简介

平台数据经过分析聚合， 各类图表将数据可视化， 为用户更直观的展示数据分布、数据排行情况。

- 支持用户自定义添加报表。

- 支持用户导出报表。
- 支持用户引用图表自定义仪表盘。
- 支持用户创建“数据可视化大屏”，满足用户报表、仪表盘、Aiview 大屏定制需求。

6.4.2 图表管理

选择“**安全分析➤可视化中心➤图表管理**”菜单，查看图表管理界面，默认存在内置的报表。

如下图所示。

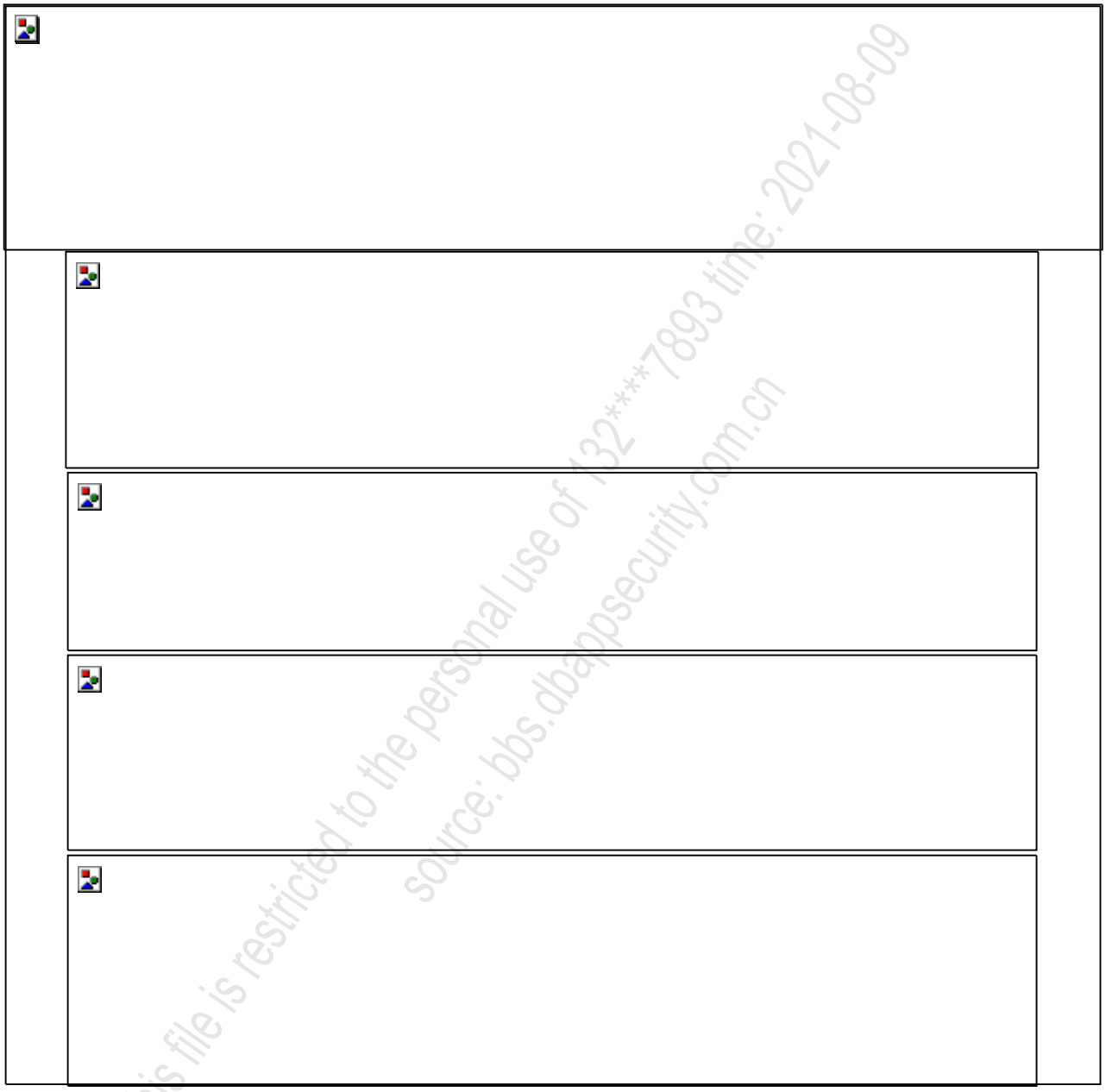
1、 报表查询

输入标签或者名称，可查询到相关报表；点击<**重置**>，清空所有查询条件。如下图所示。

2、 报表类型

支持生成一维时序折线图、一维时序面积、一维时序柱状图、一维分布饼状图、一维分布环状图、一维分布柱状图、一维分布横向柱状图、一维分布列表、一维分布文字云、二维时序折线图、二维时序面积、二

维时序柱状图、二维分布饼状图、二维分布环状图、二维分布柱状图、二维分布横向柱状图、二维分布列表和大字报 18 种报表。生成一维时序图、大字报需要引用没有 groupby 的统计指标； 一维分布图、二维时序图需要引用有 1 个 groupby 的统计指标； 二维分布图需要引用 2 个 groupby 的统计指标。部分报表预览效果， 如下图所示。



3、 报表新增

点击 新增 按钮， 进入报表新增界面， 输入相关信息， 选择报表类型、统计指标， 点击<**保存**>， 报表新增成功。

如下图所示。

4、 报表其他操作

报表列表支持编辑、预览、编辑和删除操作， 选择某一个报表，点击操作栏相关按钮， 可进行相关操作。如下图所示。

5、 报表导出

报表支持单个/多个导出， 导出格式为 PDF、 WORD，点击<**报表导出**>， 即可获得相应格式报表。

如下图所示。

6.4.3 仪表盘管理

选择“**安全分析>可视化中心>仪表盘管理**”页面，用户可按实际情况定制仪表盘、管理仪表盘，将重点关注的数据可视化展示在仪表盘中。

1、 新增仪表盘

点击 新建 ，进入仪表盘新建页面。

- 填写仪表盘名称、仪表盘描述。
- 选择仪表盘布局，布局可选择一行四个/三个/两个/一个报表， 也可以选择不同宽度。
- 选择报表， 报表即“**安全分析>可视化中心>图表管理**”中的报表， 点击<**添加到选中布局**>。
- 最后点击<**保存**>，仪表盘新增成功。如下图所示。

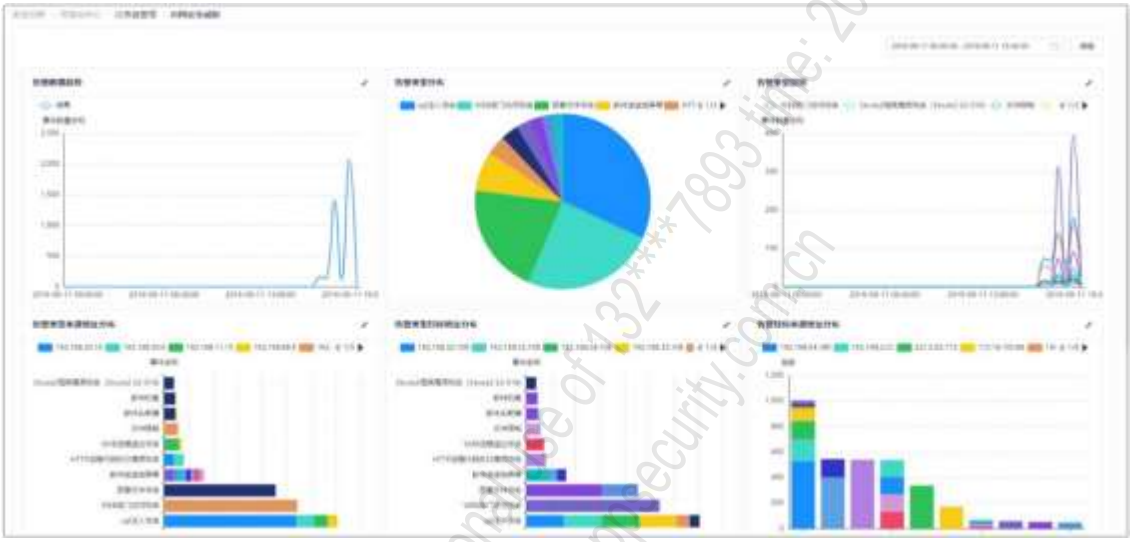
2、 仪表盘其他操作

仪表盘支持禁用/启用操作；支持预览、编辑、删除操作； 支持排序操作。

如下图所示。

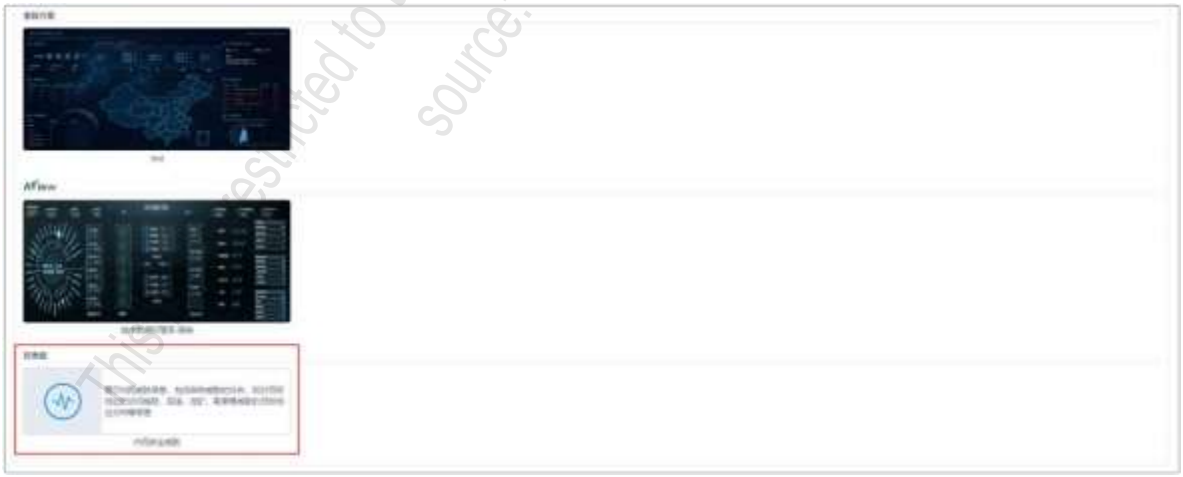
3、 仪表盘预览

在 “**安全分析➤可视化中心➤仪表盘管理**” 页面， 选中某个仪表盘， 点击<**预览**>，预览页面支持放大报表、编辑报表， 如下图所示。



4、 态势感知仪表盘预览入口

态势感知页面支持仪表盘预览， 如下图所示。



6.4.4 AiView 设计器

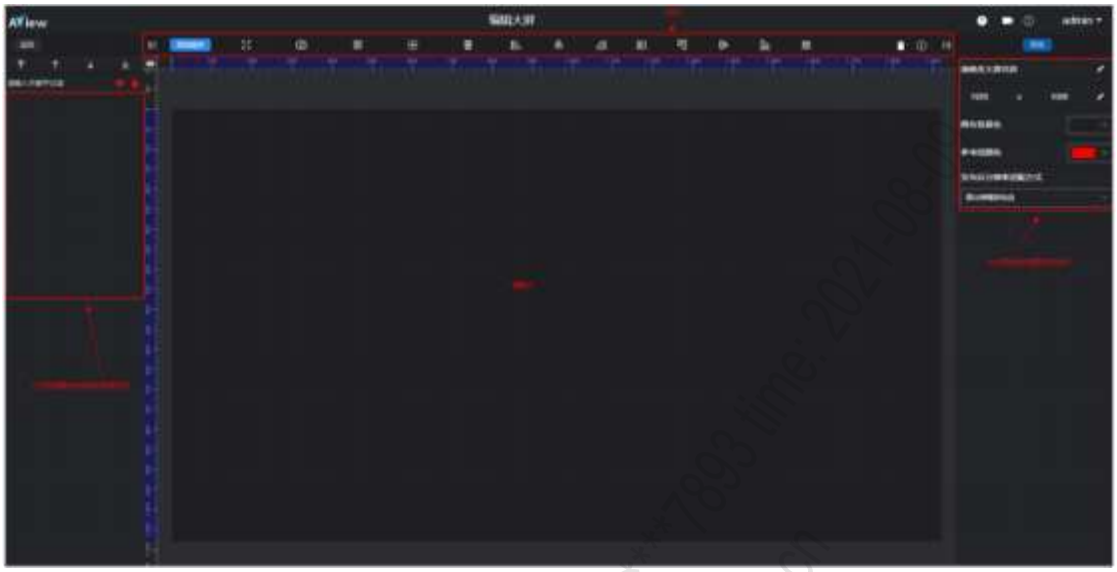
选择 “**安全分析➤可视化中心➤Aiview 设计器**” 菜单，新打开一个 Aiview 大屏管理页面，显示已发布/未发布大屏数量以及大屏的名称和分辨率，并支持用户登录，用户管理， 授权管理，大屏管理，大屏编辑，

大屏发布， 创建演示预案等操作。如下图所示。

1、 创建 AiView 大屏

- 点击 从模板创建 新增 Aiview 大屏， 在现有的模板中进行选择并在其基础上进行编辑， 可点击<**预览**>随时查看大屏最终结果，如下图所示。

- 点击 创建空白大屏 新增 Aiview 大屏， 在空白的编辑页面上进行编辑，可点击<**预览**>随时查看大屏最终结果，如下图所示。



2、 AiView 大屏其他操作

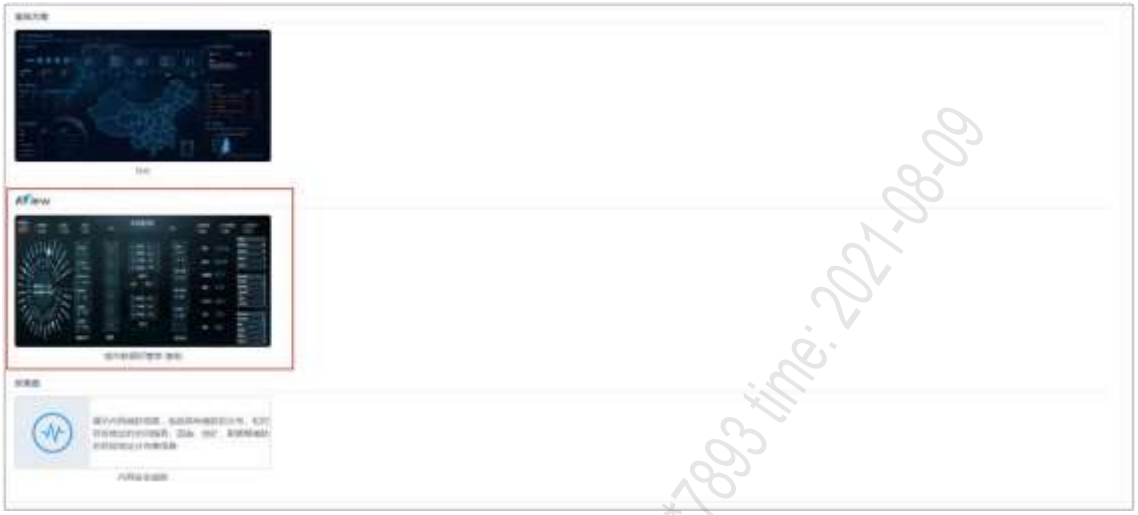
用户登录大屏管理页面后， 可发布/取消发布某大屏， 查看已发大屏的链接地址， 也可进行编辑、预览、复制、删除操作， 如下图所示。

3、 AiView 大屏预览

在大屏管理界面选中一个 Aiview 大屏，点击<**预览**>，即可预览该大屏， 如下图所示。

4、 态势感知 AiView 大屏预览入口

态势感知页面也支持 Aiview 大屏预览， 如下图所示。



6.5 报告管理

6.5.1 功能简介

报告管理支持用户引用报表（选择 “**安全分析➤可视化中心➤图表管理**” 菜单中的报表）定制报告，同时为用户提供深度威胁分析报告及报告订阅服务。

6.5.2 报告中心

选择 “**安全分析➤报告中心➤报告管理**” 页面，页面列表展示所有报告，包含内置的深度威胁报告。用户可按照实际情况定制报告。

1、 自定义报告

- 新增

点击<**新增**>，进入报告新增界面。填写基本信息、标签、选择报表、勾选报告输出项，点击<**保存**>，报告新增成功。如下图所示。

- 显示描述信息： 勾选该项，则导出报告中，会展示报表的描述信息。
- 显示有数据报表： 勾选该项， 则导出报告中， 仅会展示有数据的报表， 暂无数据的报表不展示。

- 其他操作

报告列表支持编辑、删除操作， 点击操作栏相关按钮，可进行相关操作。如下图所示。

- 导出

报告导出支持 PDF、 WORD、 HTML 等格式导出， 点击<**导出报告**>即可。如下图所示。

2、 深度威胁分析报告

报告列表内置深度威胁分析报告， 报告从总体威胁态势感知、资产分析、外部攻击者行为分析和分析取证四个方面进行分析， 并且结合分析为用户提供分析说明和处置建议。深度威胁报告不支持编辑与删除， 仅支持 WORD 格式导出报告。深度威胁报告如下图所示。

6.5.3 报告订阅

选择 “**安全分析➤报告中心➤报告订阅**” 页面，页面列表展示所有报告订阅服务，用户可对报告设置报告订阅， 报告会按照设置周期定时发送至用户邮箱。

1、 订阅条目查询

支持报告名称/邮箱关键字、发送周期、启用状态查询订阅条目，如下图所示。

2、 订阅新增

点击<**新增**>， 进入报告订阅新增界面。

- 选择发送周期， 发送周期可选每天/每月/每年。
- 选择生成时间， 某天某个整点， 报告统计时间为上一天/上一周/上一个月。
- 选择是否开启自动发送， 即启用/禁用报告订阅。
- 选择需要订阅发送的报告。
- 选择发送格式。
- 填写收件人邮箱。

提交完成后点击<**保存**>即可。如下图所示。

需在“**系统管理▶推送管理▶邮件服务器配置**”菜单配置邮件服务器后，报告订阅才会生效。

3、 订阅其他操作

订阅条目列表支持启用/禁用订阅条目；支持查看报告订阅发送历史记录；支持订阅条目编辑、删除。如下图所示。

6.6 SOAR

6.6.1 功能简介

SOAR 通过剧本编排将平台上现有的模型、指标和设备联动组件整合到一起， 使现有模型高度复用， 并为用户提供了丰富的告警事件响应能力。任务看板中的任务依据剧本自动化、半自动化手动执行， 既节省了时间， 人力和成本， 也可避免人在处理大量数据的过程中带来的误差或失误。

6.6.2 任务看板

选择 “**安全分析➤SOAR➤任务看板**” 页面， 查看任务看板页面。任务看板页面主要包括**任务概览**和**任务详情**两部分内容， 如下图所示。

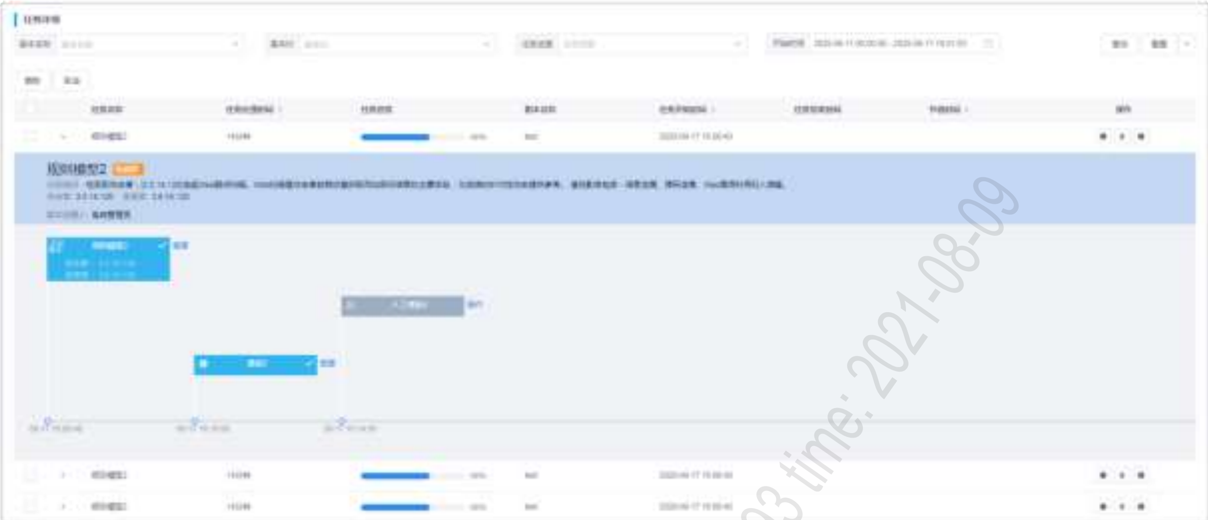
6.6.2.1 任务概览

任务概览显示在当前时间窗口下， 任务的概览情况， 包括任务总数、任务平均处理时间、节约时间、任务状态占比（进行中、已完成、已取消的任务比例）、任务趋势（总任务数的时间趋势）和时间控件（默认最近 7 天）。如下图所示：

6.6.2.2 任务详情

任务详情区域默认支持剧本名称、剧本 ID、任务进度、开始时间等查询；点击 ，可支持任务名称查询；点击<**重置**>，可清空所有查询条件。

任务列表默认根据任务开始时间倒序排序，默认展开第一条， 每 10 秒左右刷新一次，如下图所示。



任务详情功能详情

- 任务甘特图：已完成的节点为蓝色， 未进行的节点为灰色，有输出的节点可查看输出结果。
- 模型： 最终模型的甘特图时间为触发告警的时间； 非最终模型的甘特图时间根据最终模型追溯模型触发异常记录的时间。
- 防火墙：

  防火墙甘特图的时间为 WAF 阻断核查的时间，若告警信息里有来源 IP 且联动设备连接成功， 点击<**查看**>跳转到“**资产管理➤处置联动➤联动策略**”页面，携带条件为资产 IP 和阻断 IP。反之， 则不跳转。
- 通报： 通报甘特图的时间为短信、邮件、工单第一个触发的事件， 点击<**查看**>，弹出框显示通报记录。
- 预警：预警甘特图的时间为预警生成的时间，点击<**查看**>，跳转到 “**安全运营➤通报预警➤预警**”页面，携带的查询条件为该条预警的预警编号。
- EDR 联动： EDR 联动甘特图的时间为 EDR 联动核查的时间。如果有目的 IP 且是 EDR 防护资产， 点击<**查看**>跳转到“**威胁感知➤Sherlock➤脆弱性**” ， 携带的查询条件为目的 IP。反之，则不跳转。
- 人工查验： 人工查验甘特图的时间为人工查验处理时间。进行时右边为<**操作**>图标， 点击后弹出人工查验框，展示告警内容， 点击<**查看详情**>，跳转到 “**安全分析➤检索中心➤安全告警**”页面，携带的条件为 “eventId” ，时间范围为告警 startTime 的本日时间(00:00:00-23:59:00)。

  点击<**处理**>可对告警进行处理，处理后右边变成<查看>图标， 且告警的处置状态变成 “处理完成” 。
- 操作栏：
  - 取消操作

    可单个取消任务， 也可批量取消。任务取消后， 状态更新为 “已取消” ， 任务结束时间为取消时间。在人工查验前取消， 人工查验的<**操作**>按钮不显示， 未执行的节点不显示<**查看**>按钮。在人工查验后取消， 已完成的节点不变， 未进行的节点不显示<**查看**>按钮。
  - 删除操作

可单个删除任务， 也可批量删除。选择当前页任务详情全部任务时， 操作左上角显示<**删除查询结果所有**>按钮。

- 查看操作

  点击<**剧本查看**>， 跳转到该任务对应剧本的剧本查看界面。若剧本已删除点击按钮提示“该剧本已删除”。

6.6.3 剧本编排

选择“**安全分析➤SOAR➤剧本编排**”页面，默认进入剧本编排缩略图模式页面，如下图所示。

缩略图模式

- 页面右侧上方有<**创建剧本**>按钮。
- 缩略图展示剧本名称和剧本描述；鼠标悬浮在剧本编排的缩略图上， 缩略图显示<**编辑**>、 <**查看**>、 <**安全告警**>、<**异常记录**>、<**删除**>和<**剧本状态**>等按钮， 若该剧本有任务进行中， 则左下角显示<**任务中+num （任务中的事件数量）**>按钮。
- 系统出厂内置六个剧本， 分别为： **SQL 注入攻击成功阻断、安全产品联动、内部横向移动防护、 WAF 绕过残余攻击防护、挖矿主机处置响应、勒索病毒处置响应**， 默认状态为未启用。
- 点击页面左上角<**列表模式**>按钮， 进入剧本编排列表模式， 如下图所示。

列表模式

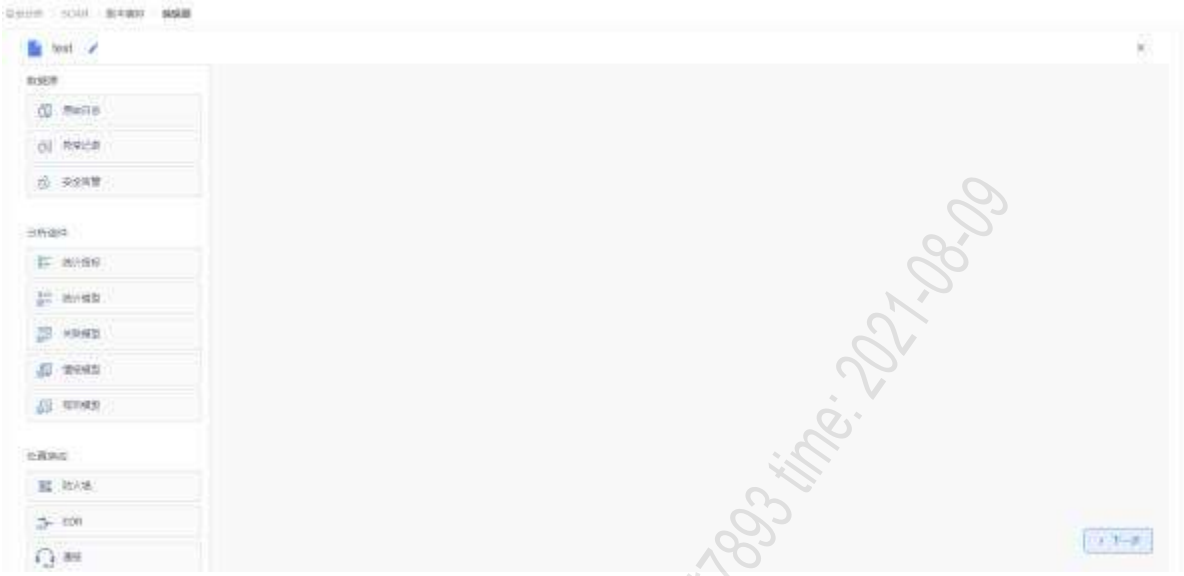
- 页面左侧上方<**启用**>、<**禁用**>、<**删除**>三个按钮，页面右侧上方有<**创建剧本**>按钮。
- 列表显示剧本 ID、剧本名称、标签、状态、事件状态、操作等。事件状态中只有有任务在进行中的剧本才显示<**任务中+num（任务中的事件数量）**>按钮， 操作列中有<**查看**>、<**剧本查看**>、<**编辑**>、<**安全事件**>、<**安全告警**>、<**删除**>等按钮。
- 出厂内置六个剧本， 分别为： **SQL 注入攻击成功阻断、安全产品联动、内部横向移动防护、 WAF 绕过残余攻击防护、挖矿主机处置响应、勒索病毒处置响应**， 默认状态为未启用。

6.6.3.1 新增剧本

点击<**创建剧本**>，若存在历史进度， 在弹出的对话框中可选择<**继续上次**>，进入历史创建剧本界面既**编辑器**页面；也可选择<**新创建**>，进入创建剧本界面既**剧本详情**页面。

编辑器页面界面左侧显示数据源、分析组件、处置响应。页面上方两侧显示<**编辑详情**>、<**返回**>按钮， 中

间显示剧本名称和威胁程度（与剧本详情一致），页面下方右侧展示<**下一步**>按钮， 如下图所示。



进入界面的同时弹出**剧本详情**弹窗， 包括基本信息和剧本分类， 点击<**确定**>可保存剧本详情， 点击<**取消**>则不保存， 点击<**编辑详情**>展开具体内容。

编辑器页面各模块详细信息见下表所示。

区块	说明	详细
数据源	◆ 数据源： 安全日志、异常记录、安全告警。 ◆ 将数据源拖拽至编辑页面时， 显示图标、描述信息和<**编辑**>、<**删除**>按钮。点击<**删除**>或键盘上<**Backspace**> 、<**Delete**>即可删除数据源。	

区块	说明	详细
	◆ 数据源中数据类型默认：全部，点击<**编辑**>可编辑数据类型。 ◆ 安全日志和安全事件能连线到统计指标，情报模型，规则模型。安全告警只能连线到统计指标。分析组件和处置响应不可连线到数据源。	
分析组件	◆ 分析组件：统计指标、统计模型、关联模型、情报模型、规则模型。 ◆ 将分析组件拖拽至编辑页面时，显示图标、<**编辑**>和<**删除**>按钮，需连线后才能对组件进行编辑，点击<**删除**>或键盘上<**Backspace**>、<**Delete**>即可删除组件。 ◆ 最后一个分析组件的告警默认输出，如果没有连接处置响应组件，界面提示“缺少处置响应模块无法保存”，无法进行下一步操作。 ◆ 同一个节点不能同时连接分析模型（指标）和响应组件。 ◆ 统计指标：处置响应元素和统计模型自身不可连线，其他都可连线。 ● 统计模型：仅统计指标可连线。 ● 规则模型：除安全告警、统计指标、处置响应元素不可连线，其他都可连线。 ● 情报模型：除安全告警、统计指、AI 模型、处置响应元素和情报模型自身不可连线，其他都可连线。 ● 关联模型：仅统计模型、规则模型、情报模型和关联模型自身可连线。	 

区块	说明	详细
处置响应	◆ 处置响应： 防火墙、 EDR、通报、预警、人工查验。 ◆ 将分析组件拖拽至编辑页面时， 右上方显示<**编辑**>、<**删除**>按钮， 需连线后才能对组件进行编辑， 点击<**删除**>按钮或键盘上<**Backspace**>、<**Delete**>即可删除。 ◆ 防火墙、 EDR、通报、预警： 仅统计模型、规则模型、情报模型、关联模型和人工查验可连线。 ◆ 人工查验： 统计模型、规则模型、情报模型、关联模型、防火墙、 EDR、通报、预警可连线。 ◆ 处置响应组件只能有一个输入， 响应组件在一个剧本中也只能添加一次，且只能添加在同一个最终分析组件之后。 具体内容见处置响应详情。	
按钮	◆ 点击<**返回**>，返回到剧本编排页面。 ◆ 点击<**编辑详情**>， 弹出剧本详情弹窗，可进行编辑。 ◆ 点击<**下一步**>，跳转到新页面， 显示剧本详情的内容（置灰不可编辑）和组成元素， 点击<**上一步**>，返回编辑页面， 点击<**完成**>，平台新增剧本中的指标和模型， 并跳转到剧本编排页面，页面显示新增剧本。	
组件删除	◆ 任何组件的输入组件或连线删除后，该组件配置内容清空并标红出错， 连线后重新添加配置保存校验。 ◆ 关联模型之前的任一模型删除， 关联模型的配置标红报错。 ◆ 统计模型有两个指标输入时， 删除任一指标，统计模型自动更新不报错。	

区块	说明	详细
	◆ 指标修改后默认新生成一个指标， 指标的后一个组件统计模型阈值不变，如果修改了时间窗口自动修改后面统计模型的时间窗口。其他任何组件的配置修改不影响后面组件的配置。	

6.6.3.2 处置响应详情

1、防火墙

拖拽图标到页面中间，图标详情显示<**编辑**>和<**删除**>按钮，如下图所示。

点击<**编辑**>，弹出防火墙编辑页面， 页面内容主要分为**告警来源、处置联动-联动设备、处置联动-处置策略**三个部分， 如下图所示。

◆ 告警来源： 显示告警来源的字段“模型 ID”，不可编辑。

- 处置联动-联动设备： 联动设备为状态是已连接的安全设备的资产 IP。阻断 IP 默认为“来源 IP”，不可编辑不可选。
- 处置联动-处置策略： 默认 3 次阻断且阻断时间分别为 10 分钟， 30 分钟， 6 小时。除了第一个阻断，其他每个阻断后都有一个删除图标， 可删除阻断策略； 最后一个阻断后有新增图标， 可新增阻断， 最多 6 次阻断。

2、 EDR

拖拽图标到页面中间，图标详情显示<**删除**>按钮， 如下图所示。

3、通报

拖拽图标到页面中间，图标详情显示详情， <**编辑**>和<**删除**>按钮， 如下图所示。

- 点击<**编辑**>，弹出通报编辑页面，页面内容主要分为告警来源、结果通知两个部分，如下图所示。

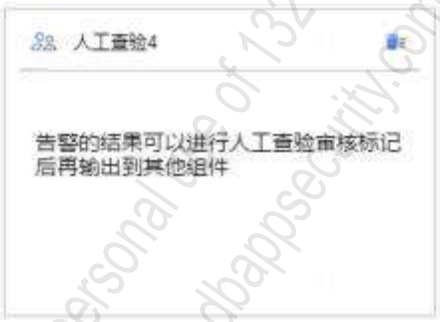
- 告警来源： 显示告警来源的字段“模型 ID”，不可编辑。
- 结果通知： 通过工单、邮件或短信的方式通知所选组织下的通知人。

4、 预警

拖拽图标到页面中间，图标详情显示详情和<**删除**>按钮， 如下图所示。

5、 人工查验

拖拽图标到页面中间，图标详情显示详情和<**删除**>按钮， 如下图所示.



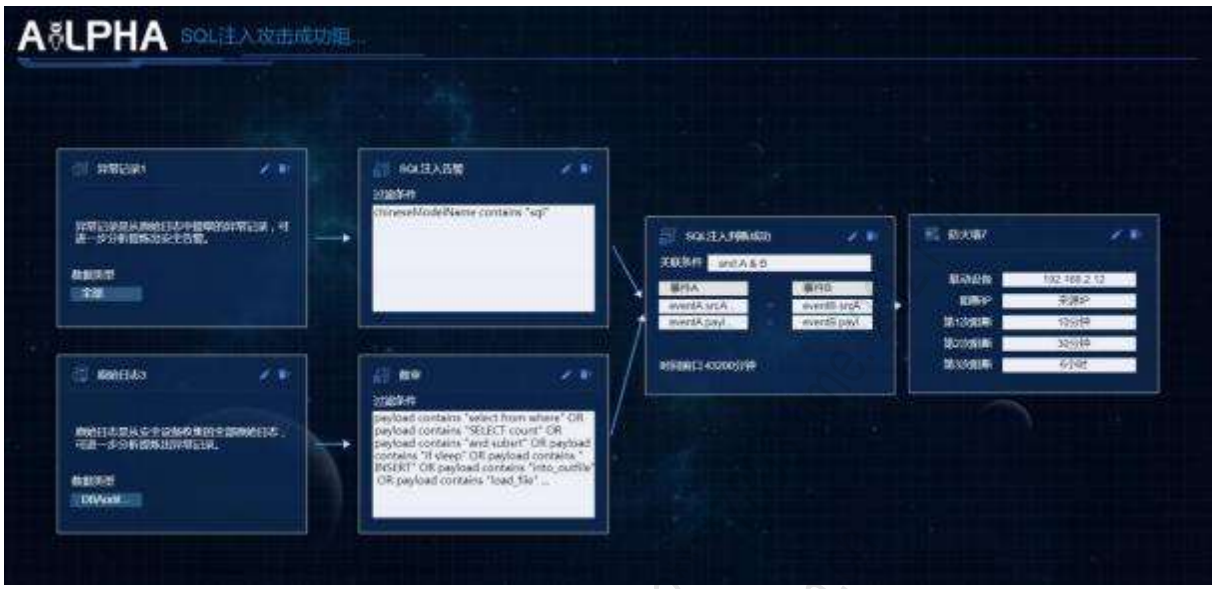
6.6.3.3 其他操作

1、查看

点击<**查看**>， 跳转到查看页面， 上方显示<**返回**>按钮和剧本名称以及威胁程度， 点击<**返回**>可返回到剧本编排界面。下方显示剧本内容， 如下图所示。

2、剧本查看

点击<**剧本查看**>，新打开一个页面显示剧本内容， 如下图所示。



3、编辑

点击<**编辑**>，跳转到剧本编辑页面， 可对剧本详情和剧本内容进行编辑，具体操作步骤同剧本新增。

4、异常记录/安全告警

点击<**异常记录**>或<**安全告警**>，新打开异常记录页面或安全告警页面， 带条件：时间（最近 7 天） +最终模型的 modelName。

5、删除

缩略图模式下仅可进行单个剧本删除，列表模式下可进行单个剧本删除，也可进行批量删除。删除剧本时，可选择该剧本的模型和指标是否一并删除。

6、启用/禁用

缩略图模式下仅可对单个剧本进行启用/禁用。列表模式下可对单个剧本进行启用/禁用，也可进行批量启用/禁用。 当剧本禁用时对应的模型都禁用，有被其他剧本引用的自建指标或引用的是内置指标则不禁用，只禁用在该剧本内自建的指标。剧本在禁用时不生成新任务。

7、任务中

点击<**任务中**>， 可跳转到任务看板页面， 显示该剧本下所有进行中的任务。

6.7 安全模型

6.7.1 模型管理

用户选择 “**安全分析**>**安全模型**>**模型管理**” 菜单，进入模型管理界面。模型管理支持对系统中所有的模

型进行编辑、删除、启用、禁用、查询等操作。

1、 模型查询

- 查询条件默认有关键字搜索栏、 模型标签、 告警状态、异常记录、 模型类型、 定制模型， 所有条件默认都为不限。
- 模型标签有：从下拉框选择。
- 告警状态有：不限、开启、关闭。
- 异常记录有：不限、开启、关闭。
- 模型类型有：不限、规则模型、关联模型、统计模型、 AI 模型、情报模型、离线模型。
- 定制模型有：不限、是、否。
- 所有条件都为单选， 被选择的条件字体变色区分。并且模型管理列表信息自动进行过滤。
- 关键字搜索栏可以通过关键字查询模型 ID 及模型名称， 只能输入字母或者文字， 不能输入特殊字符。

2、 模型列表

- 列表中显示列： 模型 ID、模型名称、标签、模型类型、定制、 异常记录、 告警、状态和操作。操作包含查看详情、复制、编辑、安全事件、安全告警、删除。
- 列表默认显示出厂后出厂模型及自定义模型的所有模型。
- 用户定制模型通过创建时间降序放入列表中。点击列表中的列名称可以进行升序降序显示， 每个列名都支持排序。
- 可以对模型进行启用、禁用操作，启用后模型才会生效。
- 可以对模型进行编辑、删除操作。
- 可以对模型进行复制。

扩展流程

- 出厂模型只能在列表中显示、启用禁用、是否告警操作， 不能进行编辑、删除操作。
- 可以进行对模型进行批量启用、批量禁用、批量删除操作。出厂模型不能进行删除。

规格及限制

列表中每页显示 50 条记录，超过 50 条时分页显示。

所有出厂的模型不能进行删除、编辑、复制。

3、 模型创建

在**模型管理**页面， 点击<**添加模型**>， 进入创建模型页面，如下图所示。

- 规则模型： 根据安全分析的应用场景， 从日志数据中筛选出安全事件， 触发告警或进行后续高级安全分析。
- 关联模型： 跨越多个设备来源及数据种类， 从多个安全事件中检测行为模式， 发现隐藏的高级威胁及安全风险， 触发严重安全告警。
- 统计模型： 从安全事件中， 发现重要的统计型特征， 通过阀值过滤， 找出异常指标， 可以发现如频繁暴力破解尝试等恶意行为。
- 情报模型：利用威胁情报增强网络安全威胁检测和应急处置能力，支持通过已知线索筛选原始日志，进行恶意 IP、恶意域名、恶意文件识别等威胁分析。
- AI 模型：根据历史数据， AI 引擎持续构建并更新基线信息，自适应的发现异常和偏离， 发现不曾想象过的攻击来源及方式。

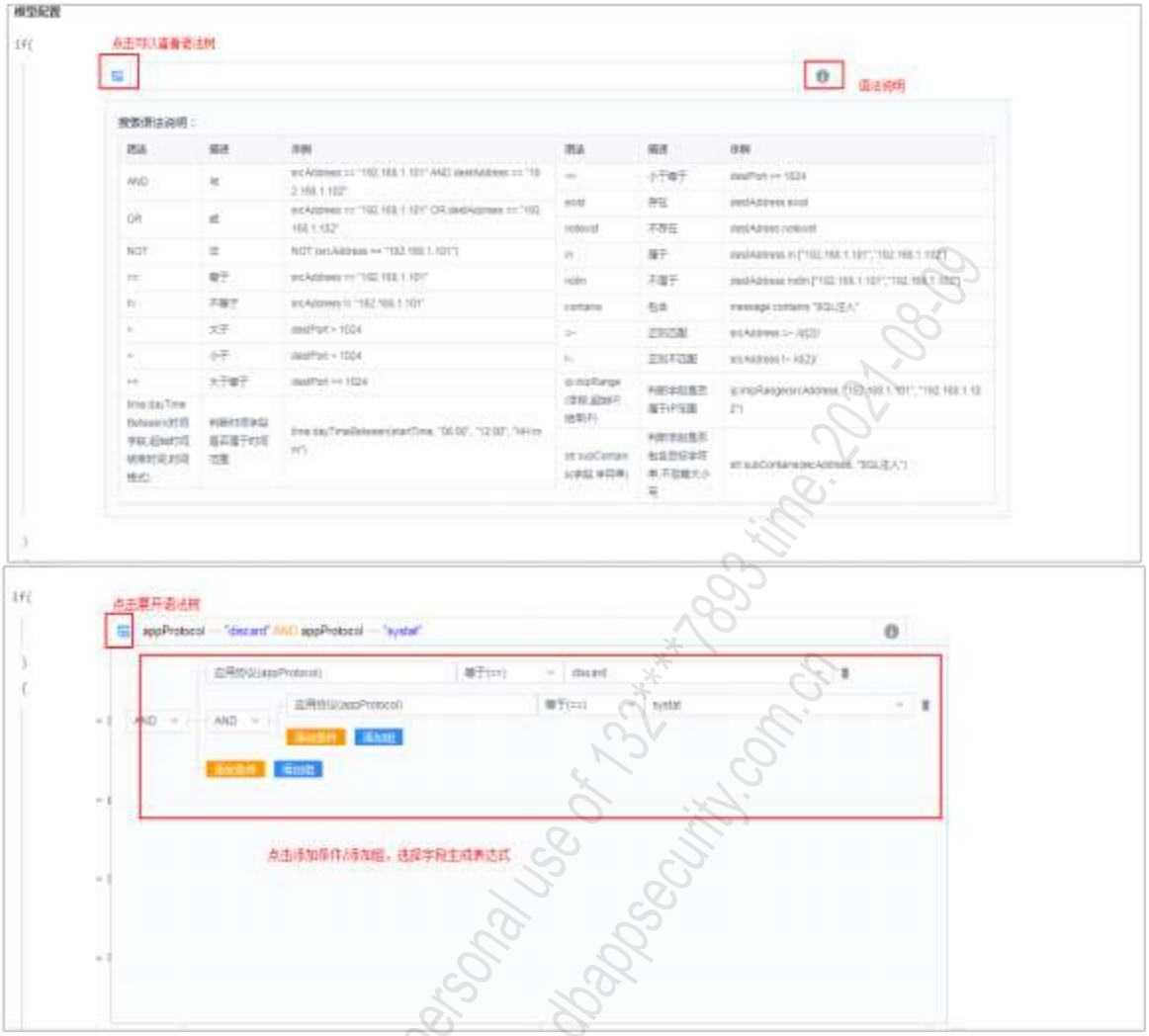
4、 创建规则模型

在**创建模型**页面， 点击**规则模型**， 显示新增规则模型页面，如下图所示。

新增规则模型页面包含以下字段：

- 基本信息： 模型 ID、模型名称、 模型标签、 模型描述等。
- 数据配置： 数据源、数据类型等。
- 模型配置： 配置规则模型的条件语句。 包括告警名称、威胁等级、告警类型、攻击链、可选字段、告警描述、处置建议、是否触发安全告警、是否输出异常记录等。

配置模型时， if ( ) 判断条件筛选过滤条件， {}输出模型字段配置， 如下图所示：



- 默认表达式为空，根据语法树/字段搜索生成表达式。
- 字段选择内容来自于数据字典， 选择的数据源不同，可选字段也不同。
- 字段信息包括字段名称及字段 ID 显示， 如： 目标地址（ destAddress ）。
- 支持字段模糊检索。可以通过中文名称或者英文字母过滤。
- 关系运算符根据字段数据字典的类型不同，内容不同。
- 匹配字段内容根据数据类型及关系运算符不同选择而不同。
- 点击 ，展开语法树， 点击<**添加条件**>或<**添加组**>选择字段添加， 在表达式框内生成一条表达式， 每一个条件后面都有**删除**按钮，可以对条件进行删除。
- 多条件输入自动组合传入后端。

  相同字段带入以（ ）组合都为 or 组合， 不同字段之间以 and 组合，如： a=1， b=2， c=3， a=2， b=4，带入后端的条件自动组合为(a=1 or a=2) and (b=2 or b=4) and c=3。
- {}大括号内是模型输出字段， 默认有告警名称、威胁等级、告警类型、攻击链告警描述、处置建议字段，也可自定义添加字段：如受害者、攻击者、标签等告警字典中字段。
- 字段值输出支持字段映射、静态值、模板、表达式。
  当选择静态值时，下方显示输入框， 可输入文字。

当选择字段映射时， 下方下拉显示可选字段。

当选择模板时， 下方显示输入框，可输入模板。

当选择表达式时，下方显示 if 判断语句。

- 可开启/关闭是否输出异常记录/触发告警。

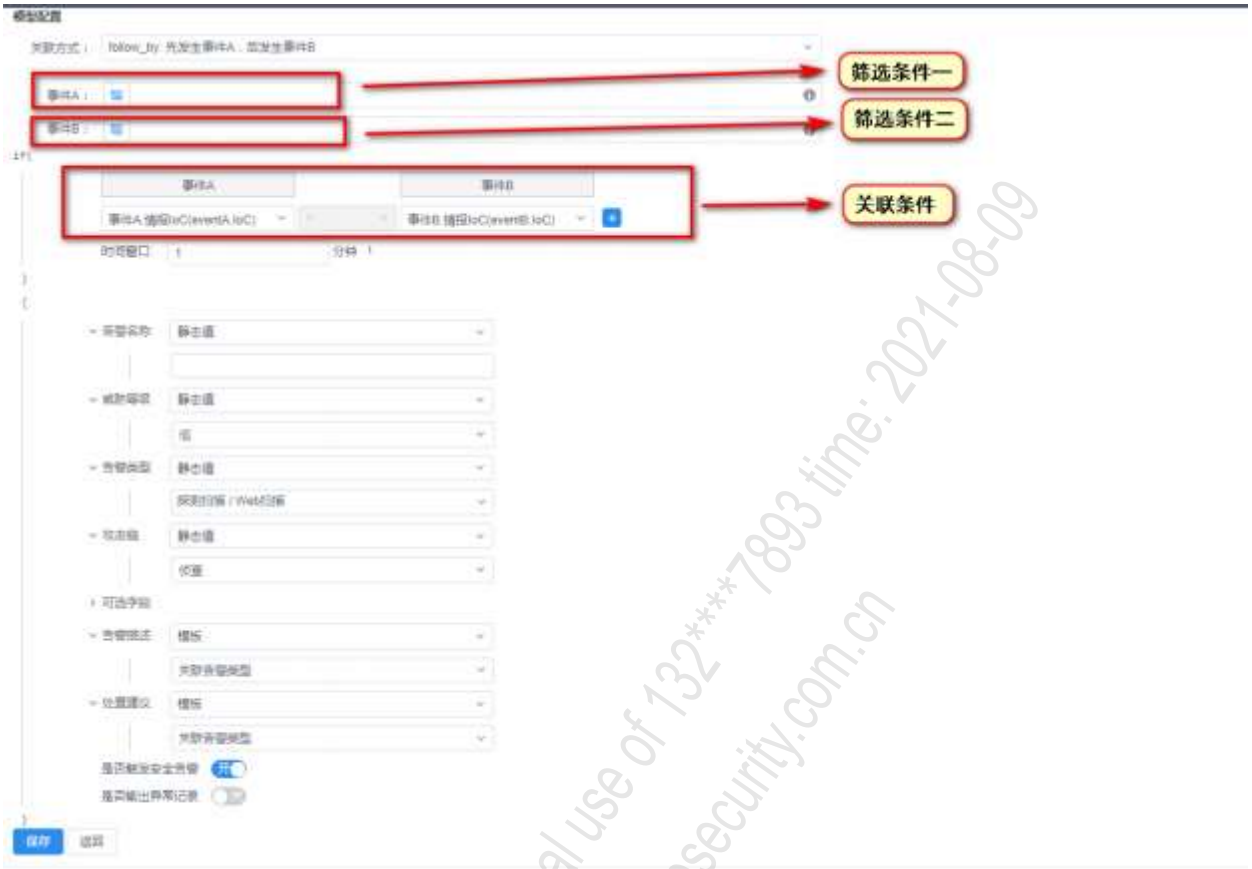
5、 创建关联模型

在**创建模型**页面，点击**关联模型**， 显示新增关联模型页面，如下图所示。

新增关联模型页面包含以下字段：

- 基本信息： 模型 ID、模型名称、模型标签、模型描述等。
- 数据配置： 数据源、数据类型等。
- 模型配置： 配置规则模型的条件语句。包括关联方式、 if 过滤条件（事件 A、事件 B， 告警名称、威胁等级、告警类型、攻击链、可选字段、告警描述、处置建议、是否触发安全告警、是否输出异常记录） 等。

配置关联模型时，筛选条件有字段筛选和表达式筛选，默认为字段筛选，如下图所示：



- 默认关联方式： follow_by: 先发生事件 A，后发生事件 B。
  下拉可选择其他方式：
  - and： 事件 A 和事件 B 同时发生。
  - not_follow_by： 先发生事件 A，但没有发生事件 B。
  - repeat_until： 事件 A 发生 n 次或以上，再发生事件 B。
- 事件 A、 B 通过表达式过滤。
- 支持字段模糊检索， 可以通过中文名称或者英文字母过滤。
- 匹配字段内容根据数据类型及关系运算符不同选择而不同。
- 点击 ，展开语法树， 点击添加条件或添加组选择字段添加， 在表达式框内生成一条表达式， 每一个条件后面都有删除按钮， 可以对条件进行删除。
- 多条件输入自动组合传入后端。

  相同字段带入以 ( ) 组合都为 or 组合， 不同字段之间以 and 组合，如： a=1， b=2， c=3， a=2， b=4，带入后端的条件自动组合为(a=1 or a=2) and (b=2 or b=4) and c=3。
- if 条件过滤事件 A 和事件 B 之间的关联关系。

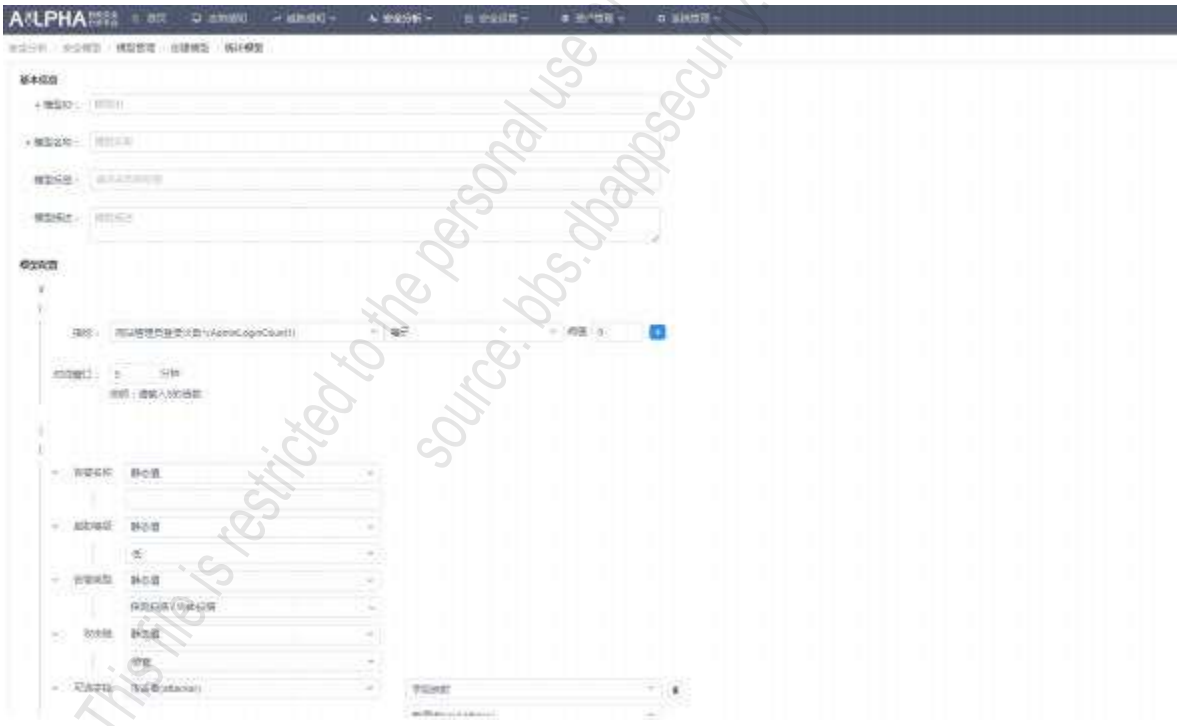
  关系符当前版本仅为 “=” 号，其他暂不用支持。
- 每一个条件后面都有删除按钮， 可以对关联条件进行删除。

- {}大括号内是模型输出字段， 默认有告警名称、威胁等级、告警类型、攻击链告警描述、处置建议字段，也可自定义添加字段：如受害者、攻击者、标签等告警字典中字段。
- 字段值输出支持字段映射、静态值、模板、表达式等多种形态。
  - 当选择静态值时，下方显示输入框， 可输入文字。
  - 当选择字段映射时， 下方下拉显示可选字段。
  - 当选择模板时， 下方显示输入框，可输入模板。
  - 当选择表达式时，下方显示 if 判断语句。
- 可开启/关闭是否输出异常记录/触发告警。

- 关联模型只支持二个事件的关联。
- 筛选条件约定同筛选条件一。
- 筛选条件二与筛选条件一不能相同。
- 同一个关联模型中， 关联条件不能相同。

6、 创建统计模型

在**创建模型**页面，点击**统计模型**， 显示新增统计模型页面，如下图所示：



新增统计模型页面包含以下字段：

- 基本信息： 模型 ID、模型名称、模型标签、模型描述等。

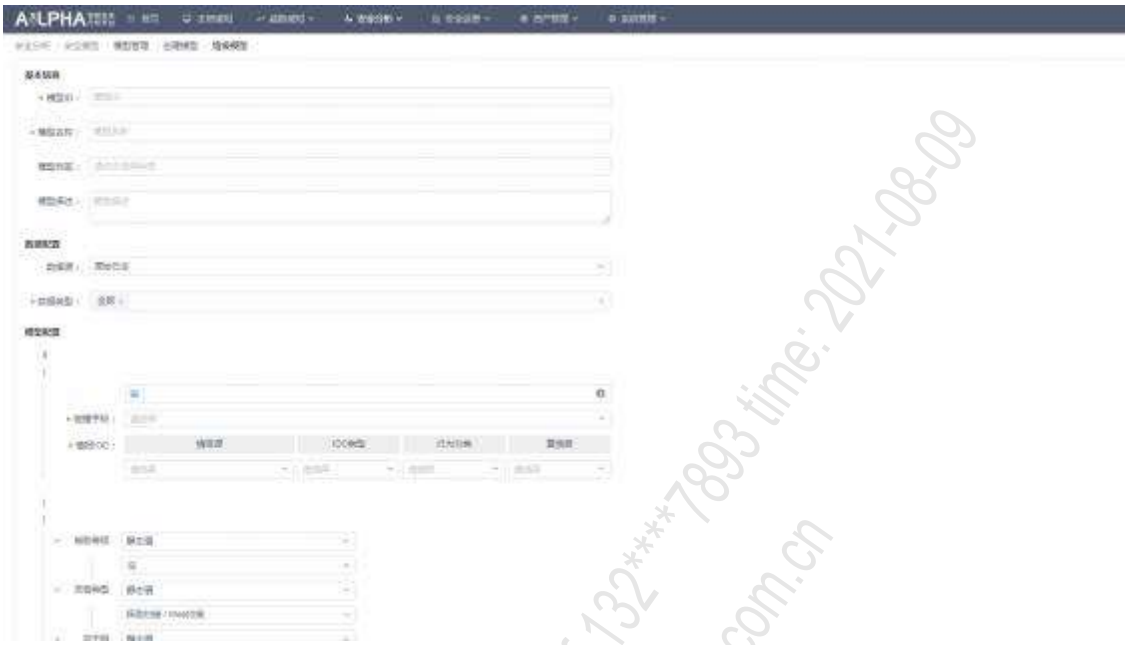
- 模型配置： 配置规则模型的条件语句。包括 if 过滤条件、统计指标、时间窗口，模型输出等。

- 默认显示一条统计指标选择框， 阀值输入框。
- 统计指标为下拉框选择， 内容来自统计指标管理中，可以进行模糊查询统计指标项。
- 点击  ，在已有条件下新增一行统计指标。
- 每个条件后面有个删除按钮，点击删除可以对指标进行删除操作。
- {}大括号内是模型输出字段， 默认有告警名称、威胁等级、告警类型、攻击链告警描述、处置建议字段，也可自定义添加字段：如受害者、攻击者、标签等告警字典中字段。
- 字段值输出支持字段映射、静态值、模板、表达式。
  - 当选择静态值时，下方显示输入框， 可输入文字。
  - 当选择字段映射时， 下方下拉显示可选字段。
  - 当选择模板时， 下方显示输入框，可输入模板。
  - 当选择表达式时，下方显示 if 判断语句。
- 可开启/关闭是否输出异常记录/触发告警， 默认开启触发告警。
- 当符合条件的事件阀值满足阀值设置数， 产生告警。

时间窗口默认显示多个统计指标时间窗口的公倍数。并且动态提示时间窗口应该输入统计指标的公倍数信息。如：请输入 5、 10、 15、 20 等 5 的倍数值。

7、 创建情报模型

在**创建模型**页面，点击**情报模型**， 显示新增情报模型页面，如下图所示。



新增情报模型页面包含字段：模型基本信息（模型 ID、模型名称、模型描述、处置建议），数据配置（数据源、数据类型），模型配置（if 过滤条件： 表达式筛选、碰撞字段、情报 IOC， 模型输出）。

情报模型筛选原始日志或安全事件数据与威胁情报库进行碰撞， 碰撞时需要选择指定字段与指定威胁情报库进行碰撞，碰撞上产生安全事件， 亦可产生安全告警。

8、创建 AI 模型

在**创建模型**页面，点击 **AI 模型**， 显示新增 AI 模型页面。如下图所示。

新增 AI 模型页面包含字段： 模型基本信息（模型 ID、模型名称、模型标签、模型描述），模型配置（统计指标、检测周期，处置建议）。

配置统计指标： 统计指标为下拉框中过滤出已保存统计结果并且未配置 group by 的统计指标。

检测周期： 检测周期为 10 的倍数。

被 AI 模型依赖的统计指标不能被删除。

9、 离线模型

选择 “**安全分析▶安全模型▶模型管理**” 菜单， 进入模型管理页面，可以看到**模型类型**还有**离线模型**。

离线模型仅支持查看，不能新增、修改、删除。

10、 模型重置

选择 “**安全分析▶安全模型▶模型管理**” 菜单， 进入模型管理页面。 点击 重置 按钮， 然后在弹出的 “**确定重置系统内置模型状态**” 对话框点击<**确定**>， 内置模型的告警和状态恢复出厂设置。

11、 模型导入导出

模型管理界面， 按下 “**ctrl+?**“组合键弹出隐藏 导出 按钮， 勾选定制模型， 点击<**导出**>， 导出定制模型规则包。

选择 “**系统管理▶系统管理▶升级管理** “页面， 点击<**点击上传升级包**>可以上传已导出定制模型规则包，可导入定制模型，若环境中已存在相同名称定制模型，无法导入该规则包。如下图所示。

6.7.2 指标管理

指标管理主要是将安全数据以某些条件过滤后进行统计， 生成的指标信息可以作为统计模型及 AI 模型的

模型指标项。 选择“**安全分析>安全模型>指标管理**”菜单进行编辑功能。

1、 指标检索

查询指标参数如下所示：

参数名称	参数含义	参数取值
关键字	设置查询指标的关键字。	手工输入，可以有统计指标 ID、统计指标名称。
指标标签	可根据内置或自定义指标标签检索。	下拉框选择。
数据源	设置查询指标的数据来源。	不限、原始日志、安全事件、安全告警等。
统计方法	设置查询指标的统计方法。	COUNT、 AVG、 SUM、 MAX、 MIN、 DISTINCT_COUNT。
保存结果	设置查询指标是否保存结果。	不限、是、否。
定制统计	设置查询指标是否为定制统计。	不限、是、否。
状态	设置查询指标的状态。	不限、开启、关闭。

2、 指标新增

点击 添加指标 按钮， 打开添加指标页面。如下图所示：

需要输入指标基本信息（指标 ID、指标名称、指标标签、指标描述）,数据配置（数据源、数据类型）, 指标配置（if 过滤条件、指标输出配置）。

新增指标参数如下所示：

参数名称	参数含义	参数取值
基本信息		
指标 ID	设置指标的 ID 标识。	手动输入。统计指标 ID 在整个数据字典中必须为唯一。
指标名称	设置指标名称。	手动输入。统计指标名称在整个数据字典中必须为唯一。
指标标签	设置指标的标签类型。	点击输入框选择，可以多选。在弹出的指标标签对话框，点击<**添加标签**>新增自定义标签信息。
指标描述	添加指标的个性化描述。	手动输入。
数据配置		
数据源	设置指标的数据来源。	原始日志、异常记录和安全告警。内容对应相应数据字典的数据表，默认显示原始日志；数据源只能单选。

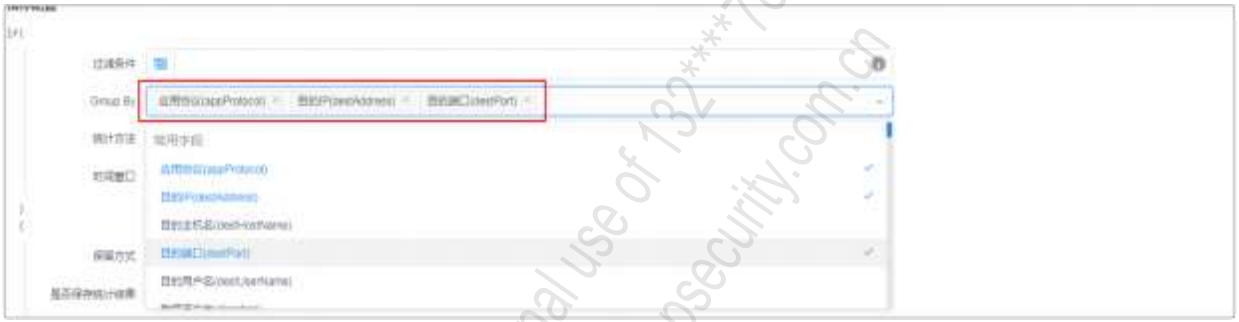
参数名称	参数含义	参数取值
数据类型	设置指标的数据类型。	默认全部， 取消全部后可选择其他数据类型， 支持多选。
指标配置		
过滤条件	设置指标的过滤条件。 筛选条件内容包含： 字段选择、关系运算符、匹配字段内容。字段和匹配字段内容都是来自数据字典。	非必选项。 点击 ， 展开语法树， 点击添加条件或添加组选择字段添加，在表达式框内生成一条表达式，每一个条件后面都有删除按钮，可以对条件进行删除。
Group By	设置指标的分类条件。 字段显示内容来自于数据字典。	可以下拉框进行选择，可以对字段进行快速查询，字段信息包含中文（英文）显示； 可以自定义顺序选择多个 group by 字段信息。 每个条件后面有个**删除**按钮， 点击删除可以对条件进行删除操作。
统计方法	默认显示一组统计指标，内容包含：统计方法函数选择、字段选择、统计指标 ID、统计指标名、详细描述等。	函数为下拉框选择， 内容包含： COUNT、AVG、SUM、MAX、 MIN、 DISTINCT COUNT， 只能进行单选。
时间窗口	设置指标保留的时间窗口。	时间窗口下拉可选， 默认 1min，还可选 5min、 10min。
保留方式	设置指标保留的方式。	保留方式可下拉选择，默认全部，可选 TOP X。
是否保存统计结果	设置添加指标的统计结果是否保存。	开关按钮选择。 如果选择不保存则缓存24 小时。
是否开启	设置指标添加后的状态是否开启。	开关按钮选择。

字段筛选截图如下所示

表达式筛选截图如下所示

表达式是直接写在 siddhiSQL 语法里,以下是常见语法。

Group By 筛选截图如下所示



3、 指标查看、复制、统计结果、删除

- 点击 按钮， 可查看指标详情。
- 点击 按钮， 打开复制页面，可复制指标。
- 点击 按钮， 可查看统计结果。
- 点击 按钮， 可删除指标。内置指标不可删除。

4、 指标启用、禁用

点击 按钮， 可以启用或禁用指标；指标支持批量启用或禁用。

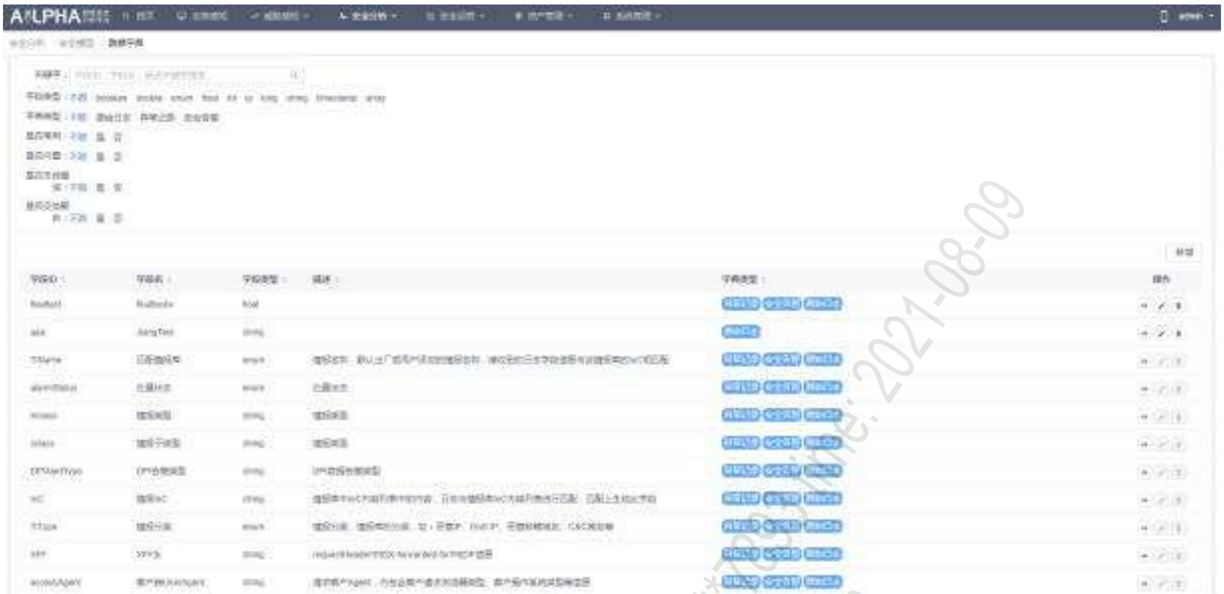
6.7.3 数据字典

选择 “**安全分析▶安全模型▶数据字典**” 菜单进入数据字典页面。

数据字典统一管理平台上的字段信息包括： 数据来源、数据的标准化字段格式说明、目标存储平台等基础信息以及攻击链、告警字典等数据。

通过数据字典可以查询接入的数据对应的字段信息， 包含表名， 表字段信息。支持数据字典中数据信息的维护， 包括数据信息的录入、修改、删除。

1、 数据字典检索



- 查询条件关键字搜索栏可以通过关键字查询任何关键字的信息，包括字段 ID、字段名、描述关键字。
- 字段类型： 不限、 boolean、 double、 enum、 float、 int、 ip、 long、 string、 timestamp、 array。
- 字典类型： 不限、原始记录、异常记录、安全告警。
- 是否常用： 不限、是、否。
- 是否内置： 不限、是、否。
- 是否常用： 不限、是、否。
- 否支持查询： 不限、是、否。
- 是否支持聚合： 不限、是、否。

2、 数据字典新增

点击 新增 按钮， 打开新增字典页面， 如下图所示：

- 字段 ID 字段名必填。
- 字段类型列表下拉选择， 默认为 string。
- 内置的字段类型有： boolean、 double、 enum、 float、 int、 long、 string、 timestamp、 ip。
- 字典类型分为原始日志、异常记录、安全告警，默认全选。

3、 数据字典查看、修改、删除

- 点击操作列 按钮，可查看字典详情。
- 点击操作列 按钮，可编辑字典。内置字典不可编辑。
- 点击操作列 按钮，可删除字典。内置字典不可删除。字典被模型或指标引用后不可删除。

6.7.4 数据清洗

功能简介

选择 “**安全分析➤安全模型➤数据清洗**” 菜单进入**数据清洗**页面，可配置系统的过滤项、检测项。数据源为原始日志， 数据（日志、流量）先通过检测项， 后通过过滤项。检测项不配置时， 所有数据通过过滤项。

数据清洗和白名单的作用分别是前置过滤和后置过滤， 确认要分析的数据和不分析的数据。首先要配置数据清洗，确认要分析哪些数据， 然后在数据清洗的基础上，配置白名单，确认不分析哪些数据。

数据清洗的作用是从海量的原始日志数据源中筛选出需要分析的数据， 只有通过数据清洗后原始日志数据才会进行进一步的分析。如果系统不配置数据清洗， 那么所有的原始日志数据都会直接进入下一步的白名单过滤。

6.7.4.1 检测项

检测项仅分析（统计、模型）检测项配置匹配的数据。 不同策略条目的关系： 逻辑或。数据满足其中一条检测项策略，支持存储、查询， 同时支持分析（统计、模型）。

1、查询

界面输入策略名称， 点击查询 按钮。支持策略名称模糊查询。如下图所示。

2、 创建

点击<**创建**>，打开新增检测项策略页面， 如下图所示。

参数说明如下表所示。

参数	参数说明	备注
名称	输入检测项策略名称。	必填项。
添加条件	点击<**添加条件**>添加筛选条件， 条件内容： 字段名称、运	条件之间的关系：相同字段逻辑

参数	参数说明	备注
	算符、字段取值、复制按钮、删除按钮。 运算符支持包括和通配符： ◆ 包括： 支持输入一个或多个值， 多个值以英文逗号分隔； ◆ 通配符：支持输入通配符，如：“192.168.111*” 。	或，不同字段逻辑与。

3、编辑

点击操作栏 按钮，弹出修改检测项策略弹框， 输入相关信息， 点击<**确定**>保存。如下图所示。

4、 删除

- 点击检测项策略可选框， 点击<**删除**>，支持删除指定检测项策略；
- 点击全选框，勾选当前页面所有检测项策略， 点击<**删除**>，支持删除指定检测项策略；
- 点击操作栏 按钮，删除该条检测项策略。

6.7.4.2 过滤项

过滤项不分析（统计、模型）过滤项配置匹配的数据。不同策略条目的关系： 逻辑或。数据满足其中一条过滤项策略，支持存储、查询， 不做分析（统计、模型）。出厂内置两条过滤项。

1、 查询

界面输入策略名称， 点击查询 按钮。支持策略名称模糊查询， 如下图**错误!未找到引用源。** 所示。

2、 创建

点击<**创建**>，打开新增过滤项策略页面， 如下图所示。

参数说明如下表所示。

参数	参数说明	备注
名称	输入检测项策略名称。	必填项。
添加条件	点击<**添加条件**>添加筛选条件， 条件内容： 字段名称、运算符、字段取值、复制按钮、删除按钮。 运算符支持包括和通配符： ◆ 包括： 支持输入一个或多个值， 多个值以英文逗号分隔；	条件之间的关系：相同字段逻辑或，不同字段逻辑与。

参数	参数说明	备注
	◆ 通配符：支持输入通配符，如：“192.168.111*”。	

3、 编辑

点击操作栏 按钮，弹出修改过滤项策略弹框， 输入相关信息， 点击<**确定**>保存。如下图所示。

4、 删除

- 点击过滤项策略可选框， 点击<**删除**>，支持删除指定过滤项策略；
- 点击全选框，勾选当前页面所有过滤项策略， 点击 按钮， 支持删除指定过滤项策略；
- 点击操作栏 按钮，删除该条过滤项策略。

6.7.5 白名单

选择“**安全分析>安全模型>白名单**”菜单， 可配置系统的白名单。

与数据清洗模块功能不同， 数据清洗模块属于前置过滤， 对数据进行全局过滤， 但无法进行细粒度添加策略，无法针对指定模型进行添加过滤策略；而白名单主要针对数据源为异常记录/安全告警的数据进行过滤，当发现异常记录/安全告警存在某一类误报较多时， 可以添加相关白名单 ，后续满足白名单过滤条件的异常记录/安全告警将不再入库，快速排除掉该类误报。

6.7.5.1 白名单相关操作

1、 查询

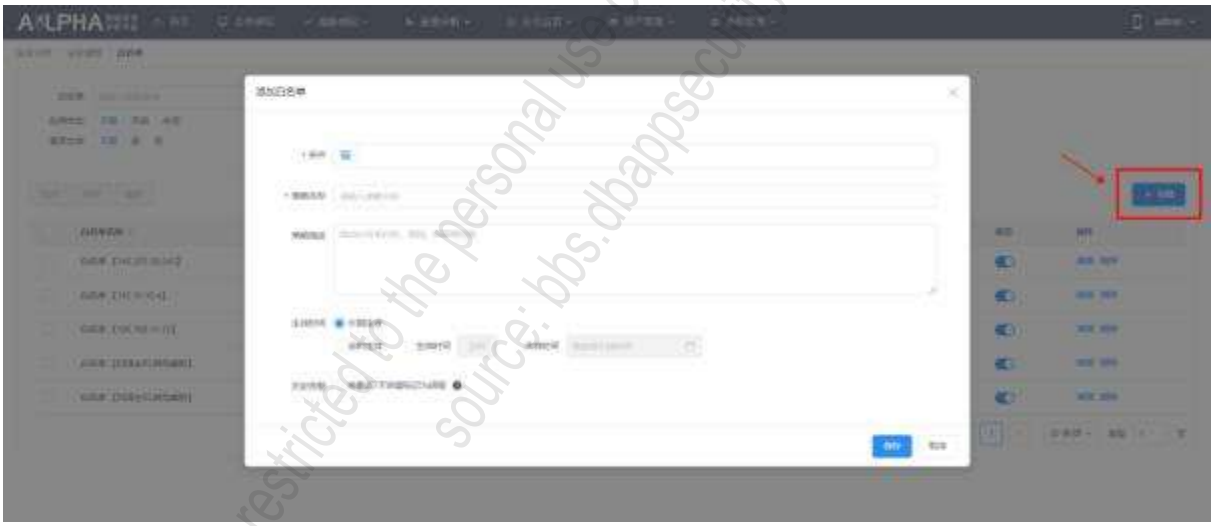
- 支持对白名单名称/条件进行模糊查询；
- 支持对白名单启用状态进行查询；
- 支持对白名单是否生效进行查询。

如下图所示。

2、 创建

点击<**创建**>，打开添加白名单页面。如下图所示。

添加白名单页面条件、策略名称必填，策略名称选填，生效时间支持长期生效和定时生效， 支持将最近 7 天历史告警标记成误报。



3、 编辑

在白名单列表中选择一条白名单，点击操作栏下的<**编辑**>，打开修改白名单页面，如下图所示。

支持修改白名单条件、策略名称、策略描述、生效时间、勾选将最近 7 天历史告警标记为误报。

4、 启用/禁用

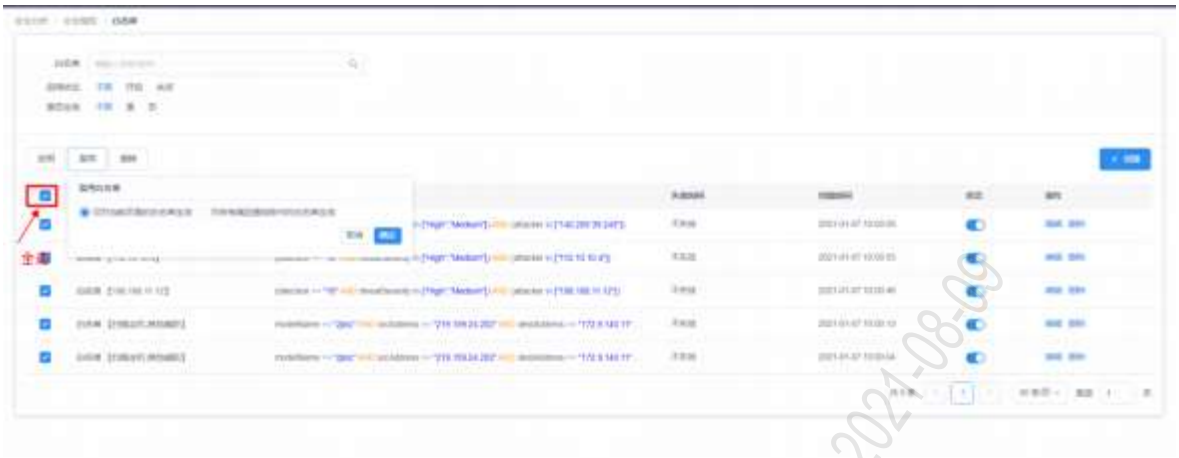
支持单条白名单启用/禁用， 也支持批量启用/禁用白名单。当启用白名单后， 白名单过滤立即生效； 禁用白名单后，白名单失效，不再对异常记录/安全告警进行过滤。

- 单条白名单启用/禁用

白名单列表中选择一条白名单， 点击**状态**栏下的启用/禁用按钮，白名单启用/禁用生效， 如下图所示。

- 批量启用/禁用白名单

白名单列表栏中多选白名单， 点击列表左上方<**启用**>或者<**禁用**>按钮，可**启用/禁用**选择的白名单； 当全选白名单列表， 点击列表左上方<**启用**>或者<**禁用**>按钮， 可选择对当前页面的白名单生效或者对所有满足查询条件的白名单生效，如下图所示。



5、 删除

支持单条白名单删除， 也支持批量删除白名单。当删除白名单后， 该条白名单失效， 不再对异常记录/安全告警进行过滤。

- 单条白名单启用/禁用

白名单列表中选择一条白名单， 点击操作栏下的<**删除**>，如下图所示。

- 批量删除白名单

白名单列表栏中多选白名单， 点击列表左上方<**删除**>，可删除选择的白名单； 当全选白名单列表， 点击列表左上方<**删除**>，可选择对当前页面的白名单生效或者对所有满足查询条件的白名单生效，如下图所示。

6、 白名单失效

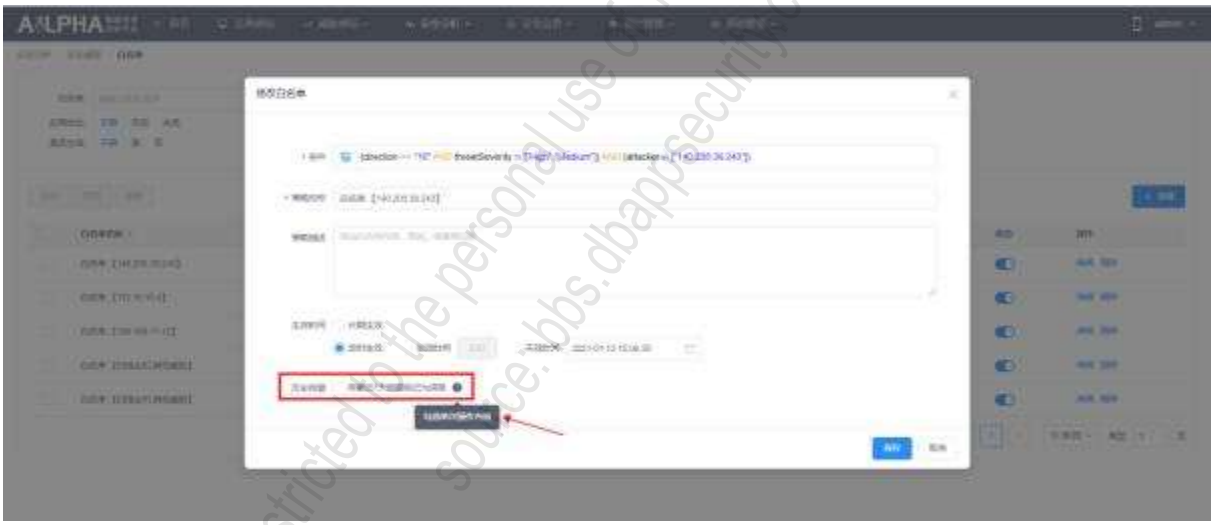
白名单列表中， 可以查看到有一栏为失效时间。失效时间与创建/编辑白名单时的生效时间/类型有关。

- 当创建/编辑白名单的生效时间/类型为“长期生效”时， 则白名单列表中失效时间为不失效， 如下图所示。

- 当创建/编辑白名单的生效时间/类型为“定时生效”时， 需要指定一个失效时间， 则白名单列表中失效时间即为指定的失效时间， 当时间到失效时间时， 该条白名单失效， 不再对异常记录/安全告警进行过滤，如下图所示。

7、 将最近 7 天历史告警标记为误报

在创建/编辑白名单时，在**历史告警**选项中可勾选“将最近 7 天告警标记为误报”。此选项勾选单次生效，即当勾选后，满足该条白名单过滤条件下的最近 7 天安全告警处置状态会置为“误报”，当再次编辑该白名单时，该选项置为未勾选，可再次勾选对相关安全告警进行标记误报， 如下图所示。



6.7.5.2 创建白名单其他方法

除了选择 “**安全分析➤安全模型➤白名单**” 菜单进入白名单页面创建白名单外，其他页面也有创建白名单入口， 如下所示：

- **入口一： 异常记录创建白名单**

  选择 “**安全分析➤Investigation➤原始日志**” 页面选择数据来源： 异常记录， 任意展开一条异常记录详情，支持添加白名单，如下图所示。

◆ **入口二：安全告警创建白名单**

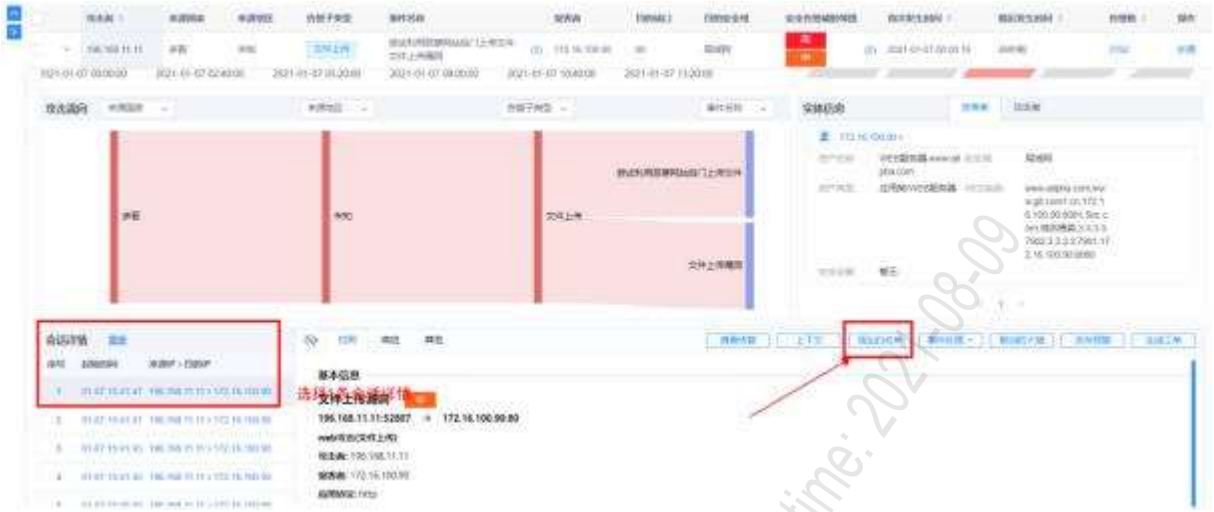
选择“**安全分析➤Investigation➤安全告警**”菜单， 在该页面普通查询/聚合查询下， 选择一条告警点击列表操作栏下<**处理**>，支持添加白名单， 如下图所示。

◆ **入口三：安全告警-查询下创建白名单**

选择“**安全分析➤Investigation➤安全告警**”页面， 普通查询/聚合查询下， 选择一条告警展开详情， 支持添加白名单， 如下图所示。

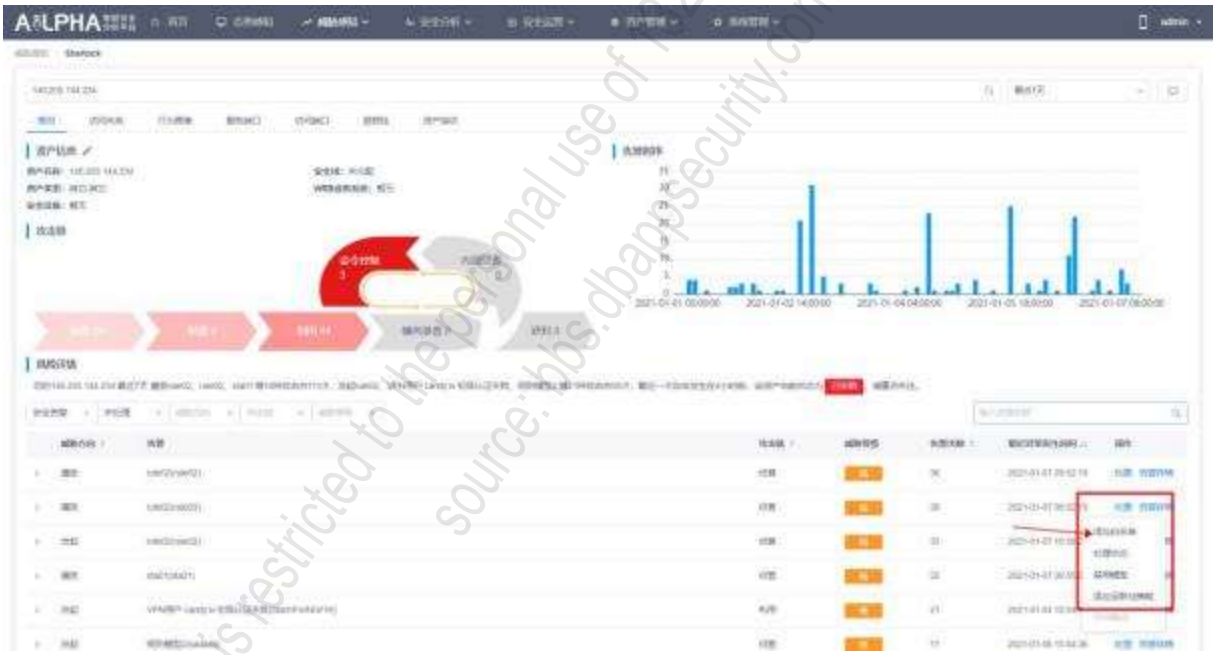
◆ **入口四：安全告警-聚合查询下创建白名单**

选择“**安全分析➤Investigation➤安全告警**”页面， 聚合查询告警详情中， 选择一条会话详情， 支持添加白名单， 如下图所示。



- **操作入口五： Sherlock 创建白名单**

选择“**威胁感知▶Sherlock**”页面， 对指定 IP 进行查询， 点击列表操作栏<**处置**>按钮， 支持添加白名单，如下图所示。

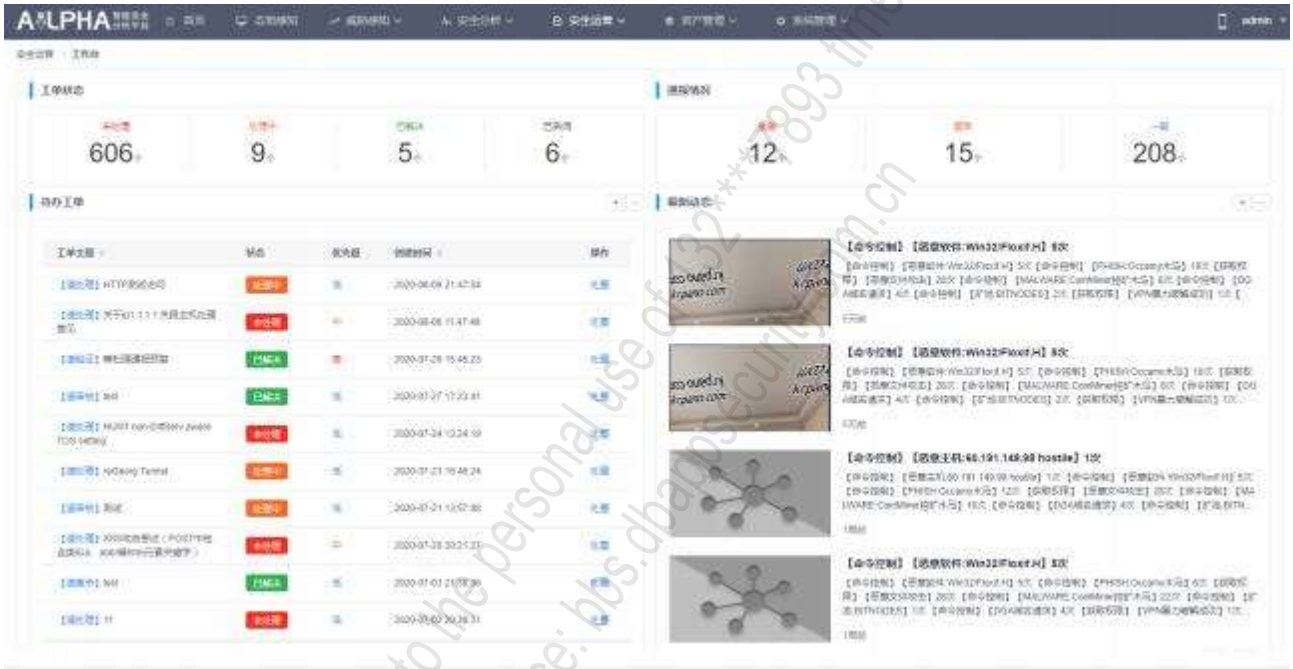


7. 安全运营

7.1 工作台

7.1.1 功能简介

选择 “**安全运营▶工作台**” 页面， 工作台概括了工单、通报情报， 从工单状态、待办工单、通报情况、最新动态为用户展示安全运营全局情况。如下图所示：



7.1.2 工单状态

工单状态展示未处理、处理中、已解决和已关闭的工单数量；点击某个状态可跳转到 “**安全运营▶工单管理**” 界面， 并带上状态条件。如下图所示：

7.1.3 待办工单

待办工单按照工单创建时间列表展示未关闭的工单，点击<**处置**>， 跳转到该工单详情页面。

点击 ··· 按钮， 可以跳转到“**安全运营▶工单管理**”界面， 如下图所示：

7.1.4 通报情况

展示未关闭的通报紧急、警告、一般级别的通报数量； 点击跳转到“**安全运营▶通报预警▶通报**”页面， 并带上优先级状态。如下图所示。

7.1.5 最新动态

展示最近通报的 4 条通报信息， 点击可跳转到该通报详情页面； 点击 ··· 按钮， 跳转到 “**安全运营➤通报预警➤通报**” 页面。如下图所示。

7.2 通报预警

7.2.1 功能简介

选择 “**安全运营➤通报预警**” 页面， 页面展列表预警和通报。用户对平台产生的安全告警进行新增预警，提示平台用户该告警可能存在一定风险隐患， 需要注意或确认； 当确认该告警的确存在风险隐患， 用户可即刻将该预警通报， 平台下所有用户可以看到该通报信息，及时采取安全防护措施。

7.2.2 预警

选择 “**安全运营➤通报预警➤预警**” 页面，页面列表按照创建时间倒序排列展示所有预警。

1、 查询预警

默认支持预警名称、创建人、标签、级别查询；点击<**高级查询**>，可支持编号、预警时间查询；点击<**重置**>，可清空所有查询条件。如下图所示。

2、 新增预警

点击<**新增**>，进入到新增预警页面，输入名称、标签、级别、对象、详情， 再添加举证信息，举证信息支持输入攻击者 IP、资产 IP、安全告警 ID、域名/URL，最后点击<**保存**>， 预警新增成功。如下图所示。

3、 安全告警入口预警新增

选择 “**安全分析➤Investigation➤安全告警**” ， 选择一条告警， 展开查看详情， 点击<**发布预警**>，进入新增预警界面； 安全告警名称会自动填入预警名称； 安全告警威胁等级会自动填入预警级别； 安全预警来源 IP 和目的 IP 会自动填入预警对象； 安全告警模型描述及模型建议会自动填入到预警详情； 安全告警来源 IP、资产 IP、事件 ID、目的主机名/URL 会自动填入到举证信息攻击者 IP、资产 IP、安全告警 ID、域名/URL，点击保存， 预警新增成功。详情可参考上图所示。

4、 预警查看

选择一条预警， 点击操作栏中的<**查看**>， 进入预警详情界面。

5、 预警详情

1) 页面元素： 展示预警标签、级别、创建人、预警时间、详情、举证信息等； 支持通报、编辑、删除、返回、查看上一条预警、下一条预警； 支持举证信息跳转； 支持添加备注信息； 支持查看历史记录。如下图所示。

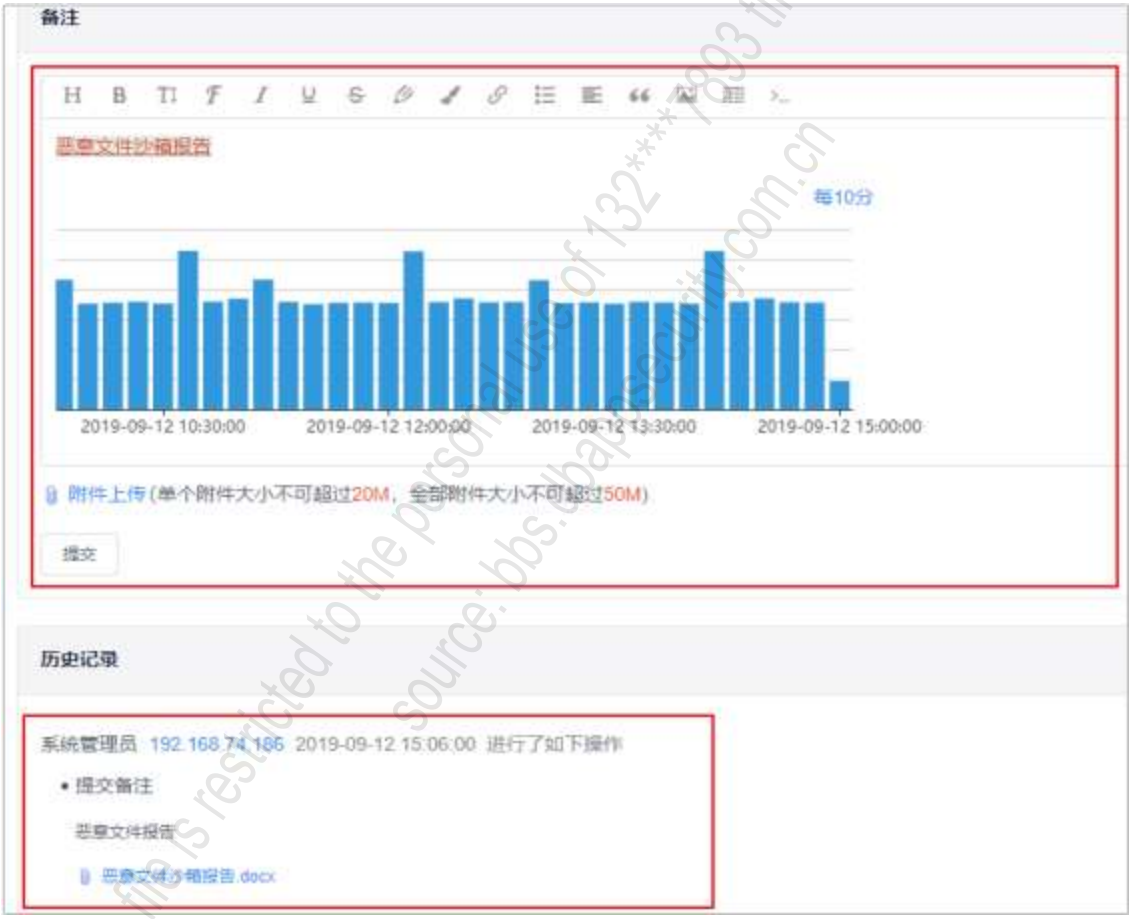
2) 举证信息跳转： 点击举证信息下拉按钮， 支持跳转到不同页面。详细请查看下表。

举证信息	跳转页面	详情
攻击者 IP	◆ 支持跳转：情报查询/安全告警查询/安全事件查询/原始日志查询/Sherlock/攻击者追踪溯源/资产威胁溯源。 ◆ 安全告警查询/安全事件查询/原始日志查询带条件： srcAddress:攻击者 IP+时间条件： 最近 30 天。	
资产 IP	◆ 支持跳转：情报查询/安全告警查询/安全事件查询/原始日志查询/Sherlock/攻击者追踪溯源/资产威胁溯源。 ◆ 安全告警查询/安全事件查询/原始日志查询带条件： srcAddress:资产 IP OR destAddress:资产 IP+时间条件： 最近 30 天。	
安全告警 ID	◆ 支持跳转到安全告警页面：查询条件：指定安全告警事件 ID。跳转方式：新增页面。 ◆ 携带时间条件： 最近一年。	

举证信息	跳转页面	详情
域名/URL	支持跳转： 情报查询/打开链接。	

3) 备注： 在备注框中填入相关信息，备注框支持贴图、插入链接、文字编辑等等操作。

支持附件上传， 单个附件大小不可超过 20M，全部附件大小不可超过 50M，点击<**提交**>。历史记录会保存备注信息。如下图所示。



4) 历史记录：预警编辑、备注提交都会保留相应的历史记录，历史记录可查看预警所有的变化及动

态，也支持下载备注提交的附件，如下图所示。

- 通报： 点击<**通报**>， 该条预警被通报，通报完成后当前页面自动切换到下一条预警详情页面。
- 编辑： 点击<**编辑**>， 进入到预警编辑页面， 编辑页面可编辑名称、标签、级别、对象、详情、举证信息等， 点击<**保存**>即编辑成功， 编辑操作会记录在预警详情页面历史记录中。
- 返回： 点击<**返回**>， 可返回到 **“安全运营➤通报预警➤预警”** 页面，并会保留之前的查询条件。
- 删除： 点击<**删除**>， 删除当前预警， 页面会自动切换到下一条预警详情页面。
- 上一条/下一条预警： 点击<**上一条/下一条预警**>，可切换上一条/下一条预警详情页面。

6、 预警编辑

选择 **“安全运营➤通报预警➤预警”** 页面，预警列表中选择某一条预警点击<**编辑**>，进入到预警编辑页面。

编辑页面可编辑名称、标签、级别、对象、详情、举证信息等， 点击<**保存**>即编辑成功， 编辑操作会记录在预警详情页面历史记录中。如下图所示。

7、 预警删除

选择 “**安全运营➤通报预警➤预警**” 页面，预警列表中选择某一条预警点击<**删除**>按钮，可删除该条预警；点击预警列表上方<**删除**>按钮支持批量删除预警。如下图所示。

8、 预警通报

选择 “**安全运营➤通报预警➤预警**” 页面，预警列表中选择某一条预警点击<**通报**>，该条预警被通报； 点击预警列表上方<**通报**>支持批量通报预警。

预警被通报后不再展示在预警列表中，可至 “**安全运营➤通报预警➤通报**”页面查看。如下图所示。

7.2.3 通报

选择 “**安全运营➤通报预警➤通报**”页面，页面列表按照通报时间倒序排列展示所有通报， 通报均由预警转化而来。

1、 通报查询

默认支持通报名称、状态、标签、级别查询； 点击<**高级查询**>，可支持编号、发布人、通报时间查询； 点击<**重置**>， 可清空所有查询条件。如下图所示。

2、 通报查看

选择一条通报， 点击操作栏中的<**查看**>， 进入通报详情界面。

3、 通报详情

1）页面元素。

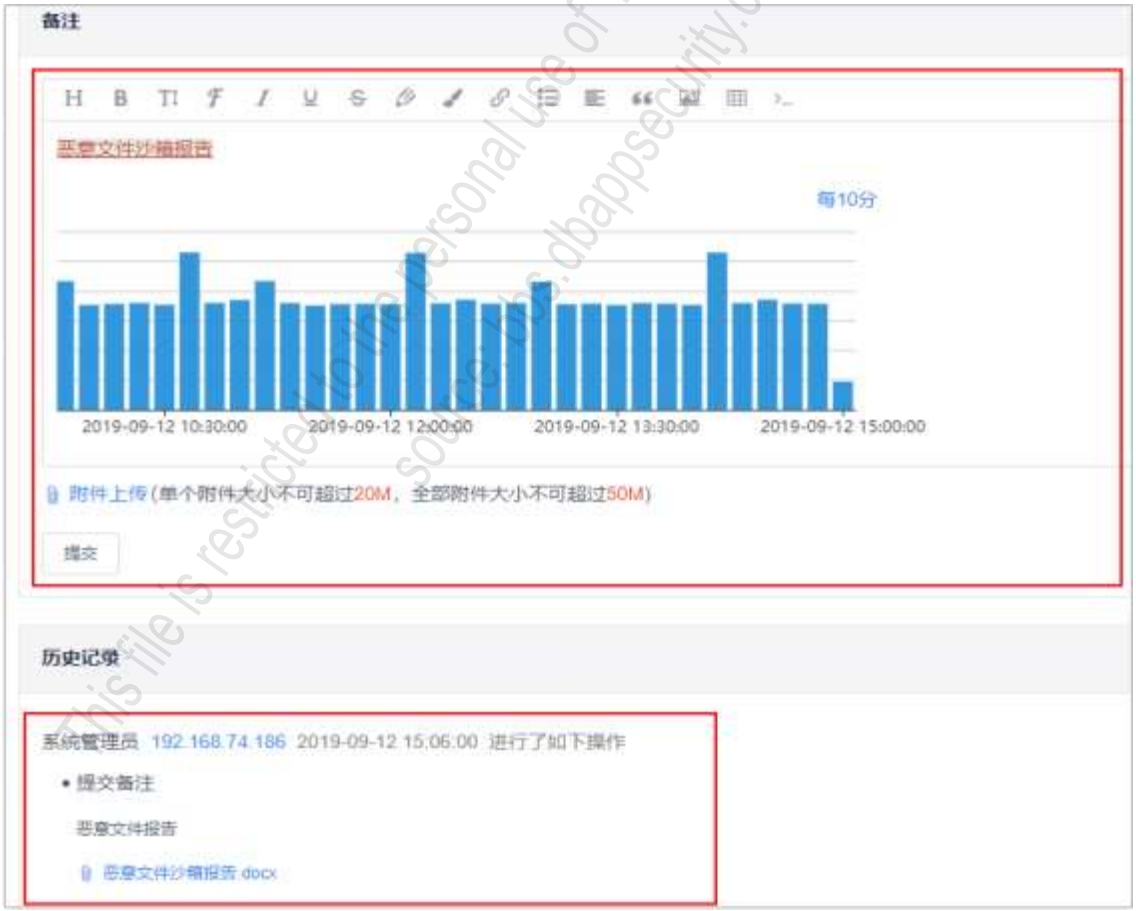
展示通报标签、级别、创建人、发布人、预警时间、发布时间、详情、举证信息等； 支持关闭、派发工单、编辑、删除、返回、查看上一条通报、下一条通报； 支持举证信息跳转； 支持添加备注信息；支持查看历史记录。如下图所示。

2）举证信息跳转： 点击举证信息下拉按钮，支持跳转到不同页面。详细请查看下表。

举证信息	跳转页面	详情
攻击者 IP	◆ 支持跳转:情报查询/安全告警查询/安全事件查询/原始日志查询/Sherlock/攻击者追踪溯源/资产威胁溯源。 ◆ 安全告警查询/安全事件查询/原始日志查询带条件： srcAddress:攻击者 IP+时间条件： 最近 30 天。	
资产 IP	◆ 支持跳转：情报查询/安全告警查询/安全事件查询/原始日志查询/Sherlock/攻击者追踪溯源/资产威胁溯源。 ◆ 安全告警查询/安全事件查询/原始日志查询带条件： srcAddress:资产 IP OR destAddress:资产 IP+时间条件： 最近 30 天。	

举证信息	跳转页面	详情
安全告警 ID	◆ 支持跳转到安全告警页面： 查询条件： 指定安全告警事件 ID。跳转方式： 新增页面。 ◆ 携带时间条件： 最近一年。	
域名/URL	支持跳转： 情报查询/打开链接。	

3) 备注： 在备注框中填入相关信息， 备注框支持贴图、插入链接、文字编辑等操作； 支持附件上传， 单个附件大小不可超过 20M，全部附件大小不可超过 50M，点击<**提交**>。历史记录会保存备注信息。如下图所示。



4) 历史记录： 通报编辑、备注提交都会保留相应的历史记录， 历史记录可查看通报所有的变化及动态， 也

支持下载备注提交的附件。如下图所示。

5） 关闭/开启： 点击<**关闭/开启**>，可以关闭/开启该通报。通报详情页面状态实时修改，如下图所示。

4、 派发工单

在**通报详情**页面点击<**派发工单**>，进入新增工单界面。

- 通报名称会自动输入到工单主题。
- 通报标签自动输入到工单标签中。
- 通报紧急/警告/一般级别会对应工单优先级高/中/低； 通报对象会自动输入到工单对象中。
- 通报详情会自动输入到工单详情。
- 通报举证信息也自动输入到工单举证信息。

最后需要手动选择工单受理人， 点击<**保存**>， 派发工单成功。如下图所示。

- 编辑： 点击<**编辑**>， 进入到通报编辑页面， 编辑页面可编辑名称、标签、级别、对象、详情、举证信息等， 点击<**保存**>即编辑成功， 编辑操作会记录在通报详情页面历史记录中。
- 返回： 点击<**返回**>， 可返回到“**安全运营▶通报预警▶通报**”页面，并会保留之前的查询条件。
- 删除： 点击<**删除**>，删除当前通报， 页面会自动切换到下一条通报详情页面。
- 上一条/下一条通报： 点击<**上一条/下一条通报**>，可切换上一条/下一条通报详情页面。

5、 通报编辑

选择 “**安全运营▶通报预警▶通报**”页面，预警列表中选择某一条通报点击<**编辑**>，进入到通报编辑页面。

编辑页面可编辑名称、标签、级别、对象、详情、举证信息等，点击<**保存**>即编辑成功。

编辑操作会记录在通报详情页面历史记录中。如下图所示。

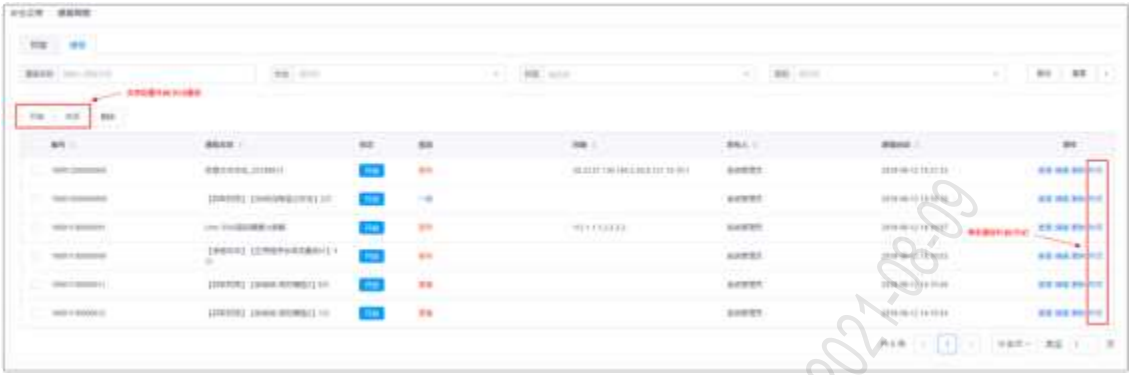
6、 通报删除

选择 “**安全运营➤通报预警➤通报**” 页面，通报列表中选择某一条通报点击<**删除**>按钮，可删除该条通报；点击通报列表上方<**删除**>。 支持批量删除通报。如下图所示。

7、 通报开启/关闭

选择 “**安全运营➤通报预警➤通报**” 页面， 通报列表中点击某一条通报点击<**开启/关闭**>按钮， 可开启/关闭该条通报。

点击通报列表上方<**开启/关闭**>， 支持批量开启/关闭通报。如下图所示。



7.3 工单管理

7.3.1 功能简介

选择 “**安全运营>工单管理**” 页面， 页面列表按照创建时间倒序排列展示所有工单。

用户可以通过工单管理界面新增工单、通报详情页面新增工单、安全告警页面新增工单， 并将工单指派给相应的处理人，经过各个环节的处理， 工单记录状态为**未处理/处理中/已解决/已关闭**，便于监督工单是否及时处理以及闭环。

7.3.2 查询工单

默认支持工单主题、状态、标签、优先级查询； 点击<**高级查询**>， 支持编号、创建人、受理人、创建方式和创建时间查询；点击<**重置**>，清空所有查询条件。如下图所示。

7.3.3 新增工单

手动新增工单有三种方式， 分别是工单管理界面新增工单、通报详情页面新增工单、安全告警页面新增工单，详细操作步骤如下：

1、 工单管理界面新增工单

选择 “**安全运营➤工单管理**” 页面， 点击<**新建**>， 进入新增工单界面。

输入主题、标签、优先级、受理人、对象、详情， 再添加举证信息， 举证信息支持输入攻击者 IP、资产 IP、安全告警 ID、域名/URL，最后点击<**保存**>， 工单新增成功。 若受理人有绑定邮箱，则工单生成时发送邮件给受理人，一个工单发送一封邮件。如下图所示。

2、 安全告警入口新增工单

安全告警入口预警新增。

选择 “**安全分析➤Investigation➤安全告警**” ， 选择一条告警， 展开查看详情， 点击<**生成工单**>，进入新增工单界面。

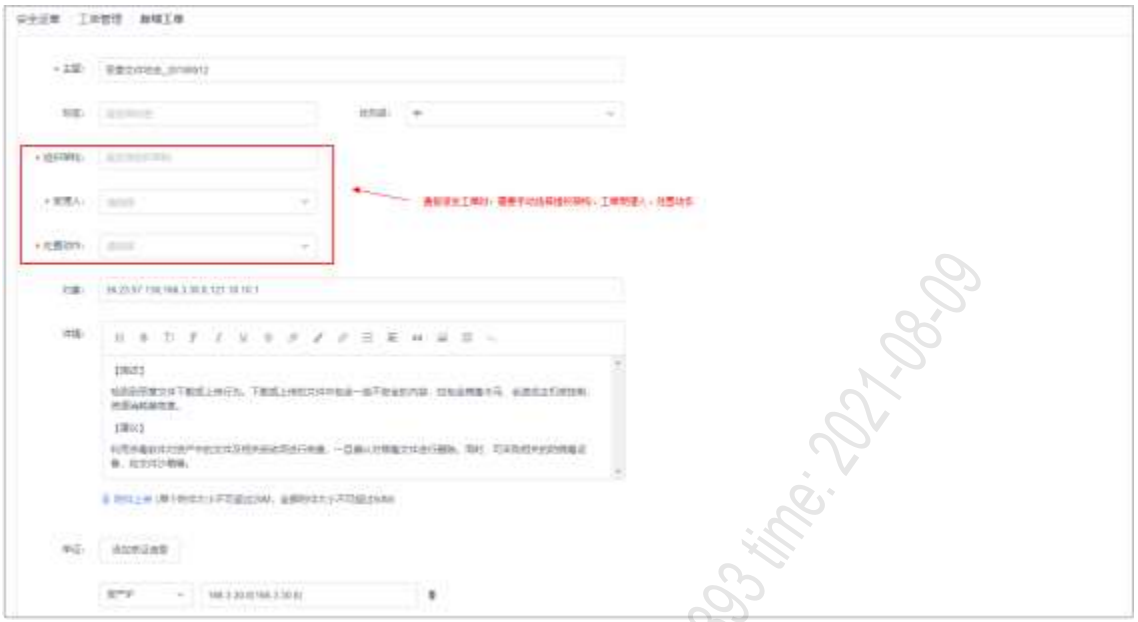
安全告警名称会自动填入工单主题； 安全告警威胁等级会自动填入工单优先级；安全告警来源 IP 和目的 IP 会自动填入工单对象；安全告警模型描述及模型建议会自动填入到工单详情；安全告警来源 IP、资产 IP、事件 ID、目的主机名/URL 会自动填入到举证信息攻击者 IP、资产 IP、安全告警 ID、域名/URL；最后需要手动选择组织架构、工单受理人、处置动作，点击<**保存**>， 工单新增成功。

若受理人有绑定邮箱，则工单生成时发送邮件给受理人，一个工单发送一封邮件。详情可参考下图所示。

3、 通报详情派发工单

选择 “**安全运营➢通报预警➢通报**” 页面， 选择一条通报， 点击<**查看**>，进入通报详情页面； 点击<**派发工单**>，进入新增工单界面。

通报名称会自动输入到工单主题；通报标签自动输入到工单标签中；通报紧急/警告/一般级别会对应工单优先级高/中/低;通报对象会自动输入到工单对象中；通报详情会自动输入到工单详情；通报举证信息也自动输入到工单举证信息； 最后需要手动选择组织结构、工单受理人、处置动作， 点击<**保存**>， 派发工单成功。如下图所示。



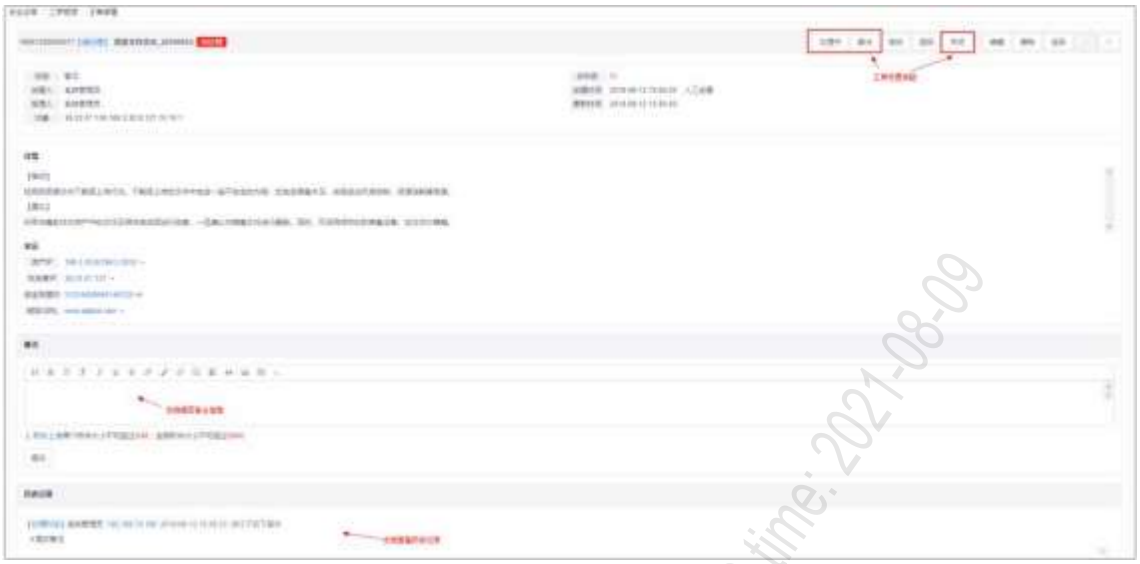
7.3.4 处置工单

1、 页面元素

选择 “**安全运营➤工单管理**” 页面， 选择一条工单，点击<**处置**>， 进入到工单详情界面，如下图所示。

工单详情界面展示工单标签、优先级、创建人、受理人、创建时间、更新时间、对象、详情、举证信息、备注、历史记录等； 支持工单处置、指派、退回、关闭、编辑、删除、返回、查看上一条工单、下一条工单。点击<**关闭**>，操作显示已完成。

关闭状态下的工单， 点击<**处置中**>， 操作显示请处理； 支持举证信息跳转； 支持添加备注信息； 支持查看历史记录。如下图所示。



2、 举证信息跳转

点击举证信息下拉按钮， 支持跳转到不同页面。 详细请查看下表。

举证信息	跳转页面	详请
攻击者 IP	◆ 支持跳转:情报查询/安全告警查询/安全事件查询/原始日志查询/Sherlock/攻击者追踪溯源/资产威胁溯源。 ◆ 安全告警查询/安全事件查询/原始日志查询带条件： srcAddress:攻击者 IP+时间条件： 最近 30 天。	
资产 IP	◆ 支持跳转：情报查询/安全告警查询/安全事件查询/原始日志查询/Sherlock/攻击者追踪溯源/资产威胁溯源。 ◆ 安全告警查询/安全事件查询/原始日志查询带条件： srcAddress:资产 IP OR destAddress:资产 IP+时间条件： 最近 30 天。	

安全告警 ID	◆ 支持跳转到安全告警页面： ◆ 查询条件： 指定安全告警事件 ID。跳转方式：新增页面。 ◆ 携带时间条件： 最近一年。	
域名/URL	支持跳转： 情报查询/打开链接。	

3、 备注

在备注框中填入相关信息，备注框支持贴图、插入链接、文字编辑等等操作。

支持附件上传， 单个附件大小不可超过 20M， 全部附件大小不可超过 50M， 点击<**提交**>。

历史记录会保存备注信息。如下图所示。

4、 历史记录

工单编辑、备注提交都会保留相应的历史记录， 历史记录可查看工单所有的变化及动态， 也支持下载备注提交的附件，默认正序。如下图所示。

5、 工单处置

点击<**处理中/已解决/关闭**>， 可以改变工单状态为处理中/已解决/关闭。工单详情页面状态实时修改。如下图所示。

6、 工单指派

点击<**指派**>，弹出指派工单框， 可选择工单状态、组织架构、受理人、处置动作、填写备注， 点击<**提交**>，工单指派成功， 该工单受理人将会更新为最新指派的受理人。

如下图所示。

- 编辑： 点击<**编辑**>，进入到工单编辑页面， 编辑页面可编辑主题、标签、优先级、受理人、对象、详情，再添加举证信息，举证信息支持输入攻击者 IP、资产 IP、安全告警 ID、域名/URL 等，点击<**保存**>即编辑成功， 编辑操作会记录在工单详情页面历史记录中。
- 返回： 点击<**返回**>，可返回到“**安全运营▶工单管理**”页面， 并会保留之前的查询条件。
- 删除： 点击<**删除**>，删除当前工单， 页面会自动切换到下一条工单详情页面。
- 上一条/下一条工单： 点击<**上一条/下一条工单**>，可切换上一条/下一条工单详情页面。

7.3.5 删除工单

选择 “**安全运营▶工单管理**”页面， 工单列表中选择某一条工单点击<**删除**>，可删除该条工单。

点击工单列表上方<**删除**>支持批量删除工单。

如下图所示。

7.3.6 批量处置工单

选择 “**安全运营▶工单管理**”页面， 勾选待处置的工单， 点击工单列表上方<**处置**>，选择处置状态为**未处理/处理中/已解决/已关闭**，支持批量处置工单。

如下图所示。

7.4 订阅规则

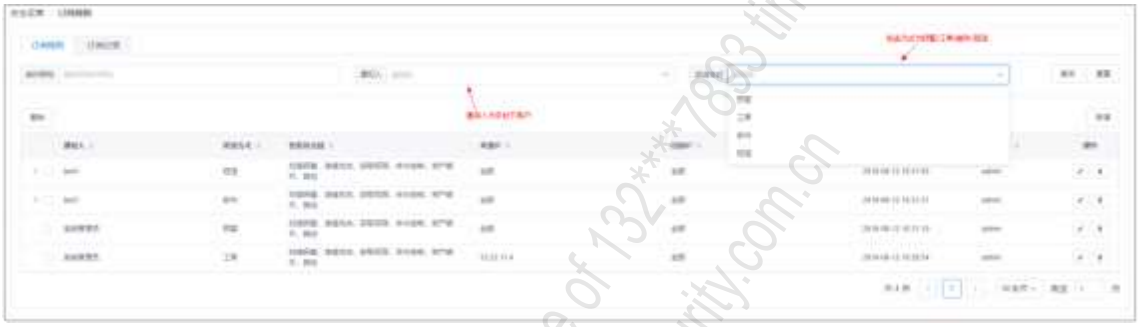
7.4.1 功能简介

选择 “**安全运营>订阅规则**” 页面， 列表展示所有订阅规则条目。

订阅规则数据源为： 安全告警， 支持添加工单/预警/邮件/短信相关规则，当安全告警满足订阅规则时， 平台对订阅规则通知人自动生成预警/工单、发送邮件/短信， 让用户可以实时关注到平台告警情况， 以便及时作出防护措施。

7.4.2 查询订阅规则

订阅规则支持通知人、发送方式查询；点击重置清空所有查询条件。如下图所示。



7.4.3 新增订阅规则

点击<**新增**>，弹出订阅规则新增窗口。

选择发送方式预警/工单/邮件/短信/钉钉； 选择通知人， 当发送方式为预警时， 无需选择通知人， 其他三种方式均需要填写通知人。

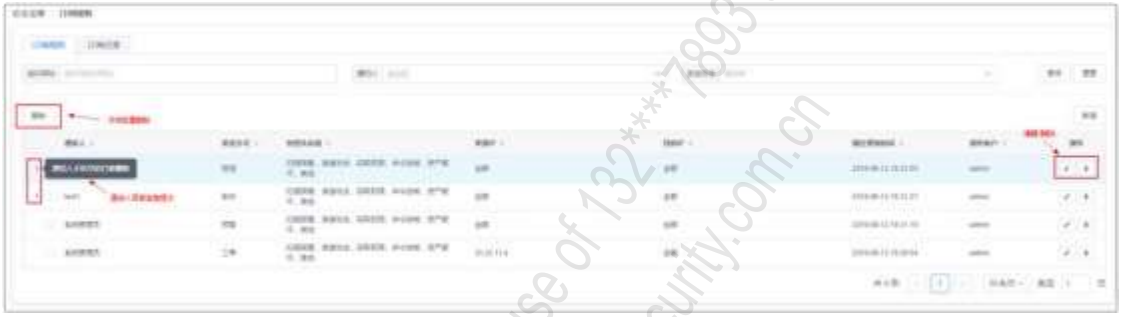
配置过滤条件， 点击<**确定**>， 新增订阅规则成功。

如下图所示。

- 订阅规则发送方式为邮件或者短信时， 订阅规则生效需至“**系统管理>推送管理>邮件服务器配置/短信服务器配置/钉钉服务器配置**”配置相关邮件服务器、短信服务器、钉钉服务器。
- 订阅规则发送方式为工单或者预警时，无需配置服务器。
- 订阅规则发送周期默认为 10 分钟， 如需调整订阅周期，请联系平台技术支持人员。

7.4.4 订阅规则其他操作

订阅规则支持编辑、删除操作； 点击操作栏<**编辑**>、<**删除**>等按钮即可。当订阅规则通知人用户没有配置手机号、邮箱或者用户被平台删除时， 该情况下， 通知人无法正常接收订阅信息， 订阅规则条目会有异常提示。如下图所示。



7.4.5 订阅记录

选择 “**安全运营>订阅规则>订阅记录**” 页面，页面记录所有订阅信息发送情况，可以通过通知人、发送方式、告警内容、时间范围查询订阅记录；也可以对订阅记录进行安全告警溯源。

如下图所示。

7.5 绩效考核

7.5.1 功能简介

选择 “**安全运营>绩效考核**” 页面。通过工单处理情况、总资产数、风险资产数、风险概率等信息， 对总

部及分部的工作行为及取得的工作业绩进行评估， 并运用评估结果对总部及分部的工作行为和业绩产生正面的引导。

7.5.2 查询绩效

可通过组织架构， 截止时间进行筛选和查询， 默认组织过滤框为空， 截止时间框为上周， 点击重置清空所有查询条件，如下图所示。

7.5.3 导出报告

- 点击 导出查询结果 按钮， 导出历史截止时间的数据，导出文件格式为Excel。如下图所示。

- 点击 自定义导出 按钮， 弹出弹框， 可选择组织架构及截止时间， 点击<**导出**>， 导出至截止时间过滤后的组织架构的数据。导出文件格式为Excel。如下图所示。

7.6 重大保障

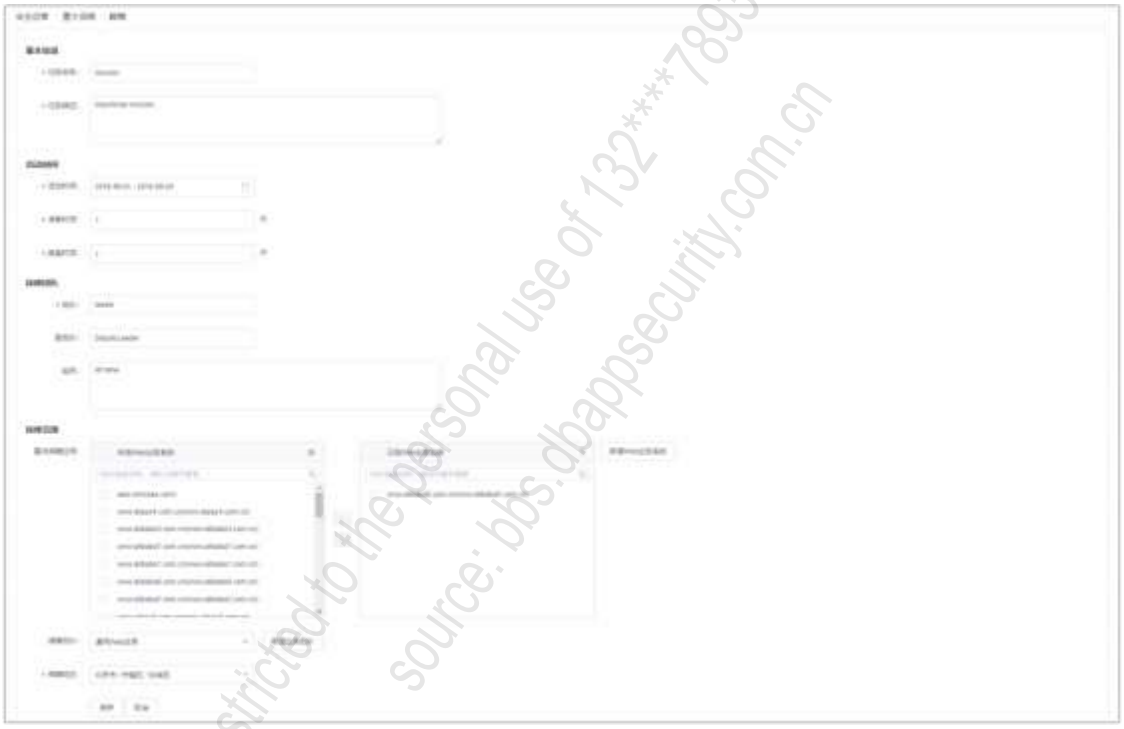
7.6.1 功能简介

选择“**安全运营**➤**重大保障**”页面， 保障团队以“事前重在预案， 事中在于保障， 事后在于复盘”的思想，在备战、临战、实战、战后复盘、结束各个阶段为活动的地区、应用和拓扑提供高质量的保障服务， 确保活动顺利进行。

7.6.2 新增重保任务

点击<**新增**>， 进入到新增页面， 输入基本信息、活动时间、保障团队、保障范围， 点击<**保存**>， 重保任务新增成功。

如下图所示。



7.6.3 管理重保任务

1、 统计信息

显示**已保障活动**（结束状态下的活动个数）、 **正在保障活动**（实战状态及复盘状态下的活动个数）、 **即将保障活动**（临战状态下的活动个数），如下图所示。

2、 查询过滤

支持任务名称， 保障阶段选择过滤， 点击<**重置**>， 清空查询条件， 如下图所示。

3、 列表内容

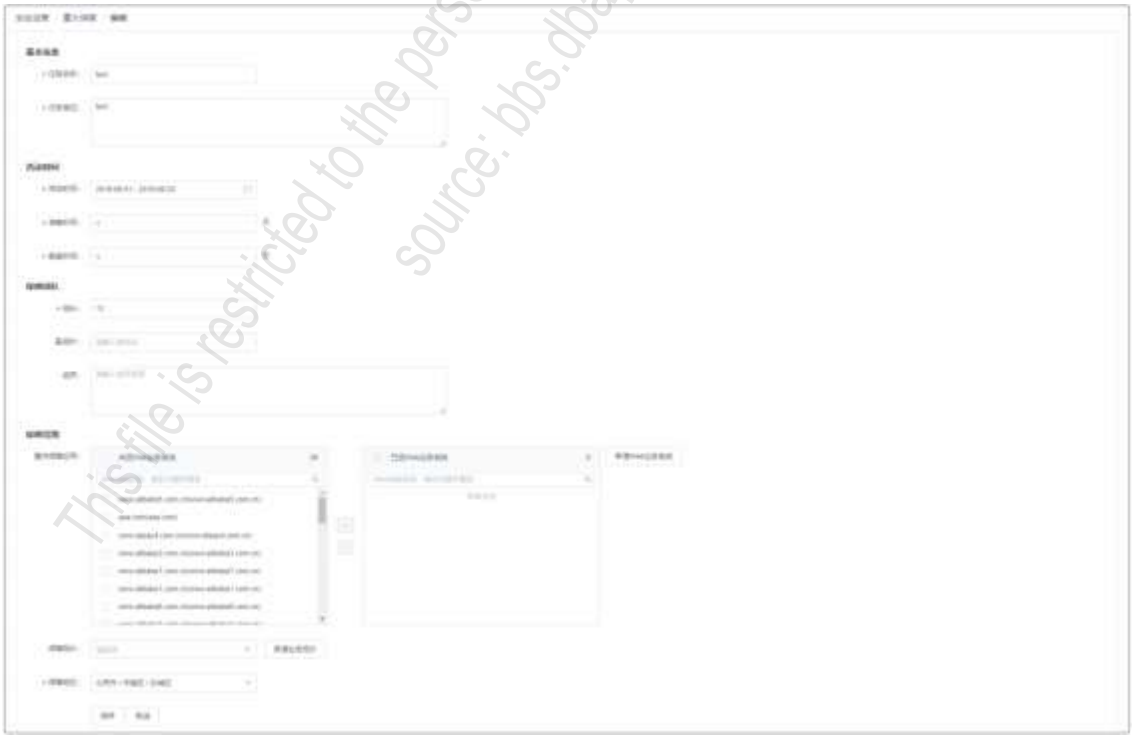
列表内容包括： 任务名称、活动时间、任务阶段、待办工单数、已处理工单数、保障组长、创建时间、发布大屏、操作栏。

各任务阶段的操作不尽相同， 备战： 上传预案； 临战： AI 异常， 保障拓扑， 安全告警， 下载预案， 创建预警，创建工单； 实战：同临战； 战后复盘：保障拓扑，下载预案， 上传保障报告； 结束：同战后复盘。

详情见下图。

7.6.4 编辑重保任务

任务列表中选择某一条重保任务点击<**编辑**>， 进入到编辑页面， 编辑页面可基本信息、活动时间、保障团队、保障范围， 点击<**保存**>即编辑成功，如下图所示。



7.6.5 查看重保任务

任务列表中选择某一条重保任务点击<**查看**>， 跳转到该任务的重保大屏如下图所示。

7.6.6 删除重保任务

任务列表中选择某一条重保任务点击<**删除**>， 可删除该条任务，如下图所示。

7.6.7 态势感知重保大屏预览入口

态势感知页面也支持重保大屏预览， 如下图所示。

8. 资产管理

8.1 资产管理

8.1.1 功能简介

选择 “**资产管理▶资产管理**” 界面， 展示接入的资产类型和数量， 对资产进行统一运维、监控、管理、联动。角色类型为分部安全管理员及分部安服人员的用户仅支持查看其所属组织架构下安全域的资产， 不支持操作。

8.1.2 页面布局

资产管理页面布局如下图所示， 在资产列表区有两种展示模式： 列表模式和缩略图模式。

列表模式

缩略图模式

资产管理页面布局序号说明参见下表。

序号	名称	说明
1	快速查询菜单	以不同的角度提供了资产管理快速查询功能， 方便用户根据实际需要进行查询。分为资产状态、安全域、资产类型、安全设备、资产重要性、网段分类等。
2	查询区	显示查询条件及<**查询**>、<**重置**>按钮。 查询条件： 资产名称、资产 IP、资产标签。 高级查询 高级查询 ：资产类型、资产来源、 EDR 防护状态。
3	资产列表	该区域主要用于资产信息展示以及相关功能的操作。 功能操作： 删除、新增资产、导入、导出、资产同步、设置、投屏。 资产信息展示： 列表模式、缩略图模式。

8.1.3 资产新增、编辑、修改

1、 资产新增

点击 新增资产 按钮，打开新增资产页面。新增资产页面包括基本信息、更多信息、操作系统信息、设备管理、流量监控。

- **基本信息**

资产 IP 与资产名称为必填项， 资产类型下拉选择， 资产重要性有普通、重要， 资产标签和资产类型按需填写。如下图所示。

◆ **更多信息**

更多信息包括资产编号、资产状态、使用人、 C-机密性、 I-完整性、 A-可用性、是否是等保资产、地理位置、描述等。如下图所示。

◆ **操作系统信息**

操作系统信息包括操作系统、 OS 版本、 MAC 地址，如下图所示。

◆ **设备管理**

设备管理包括设备厂商、设备型号、设备版本、设备存放地址、管理地址、日志量监控、在线状态检测、处置联动（见处置联动模块）。如下图所示。

◆ 流量管控

流量管控包括流量监控、开放端口监控、主动外连行为监控。如下图所示。

2、 资产编辑

点击 按钮， 打开编辑资产页面， 显示资产来源、更新时间、安全域、安全设备、 Web 业务系统。编辑相关信息， 最后保存。如下图所示。

3、 资产删除

点击 按钮， 即可删除该资产。关联安全设备和Web 业务系统的资产不能被删除。

资产可以批量删除； 列表模式勾选全选框，可删除查询结果所有。

8.1.4 资产导入和导出

1、 资产导入

点击 导入 按钮， 弹出导入资产弹框。如下图所示。资产导入分为资产增量导入和资产替换导入：

- **资产增量导入**： 当出现资产重名后 IP 相同时， 不能保存。
- **资产替换导入**： 当出现资产重名后 IP 相同时， 保留最新导入的资产。

2、 资产导出

点击 导出 按钮， 提供资产批量导出功能。

8.1.5 SOC 同步

点击 SOC同步 按钮， 可对探针上的所有资产信息即网络内部的资产信息进行同步。 SOC 同步需要在设置中开启 SOC 资产同步按钮。

8.1.6 设置

点击 ⚙ 按钮， 弹出资产设置页面。如下图所示。

1、 常用设置

◆ **资产评分**

资产评分开启， 对资产进行评分计算。

◆ **字段显示**

字段显示最多只能勾选 5 个， 资产评分勾选框置灰， 不可以勾选。开启 EDR 资产同步且 EDR 设备连接成功时 EDR 防护状态可勾选。

◆ **SOC 资产同步**

SOC 资产同步启用， 系统定时进行资产同步， 也可以手动同步； SOC 资产同步禁用，资产不会同步。

◆ **EDR 资产同步**

EDR 资产同步启用，系统 5 分钟进行资产自动同步。未添加联动 EDR 资产时，提示“**系统未配置联动 EDR 资产， EDR 资产同步不生效**”。

EDR 资产可在资产管理界面添加， **资产类型**选择“**安全类/主机安全管理系统（ EDR）**”，**设备厂商**选择“**安恒（DBAPPSecurity）**”， 管理地址填写，勾选是否联动 EDR。

如下图所示。

2、 流量自动发现资产

◆ **自动发现**

启用自动发现， 满足发现类型与发现区域的资产会被发现。 关闭自动发现， 资产发现立即关闭。

◆ **发现类型**

发现类型包括服务器和终端。

◆ **发现区域**

发现区域分为安全域、内网、网段。

- 安全域：点击 安全域配置 按钮， 跳转至“**资产管理▶安全域**”界面， 可根据需求配置安全域。

如下图所示。

- 内网： 点击 内网配置 按钮，跳转至“**系统管理▶配置管理**”界面， 可根据需求配置内部 IP。

如下图所示。

- 网段： 点击 添加网段 按钮，可根据需求配置 IP 区间。如下图所示。

8.1.7 投屏

- 点击 按钮投屏至“**态势感知▶资产态势感知**”大屏。
- 点击 按钮， 跳转至“**威胁感知▶Sherlock**”页面。
- 点击 按钮， 跳转至“**态势感知▶资产威胁溯源**”大屏。

8.2 Web 业务系统

8.2.1 功能简介

选择 “**资产管理➤Web 业务系统**” 界面， 对 Web 业务系统进行统一运维、监控、管理、联动。角色类型为分部安全管理员及分部安服人员的用户仅支持查看其所属组织架构的 Web 业务系统，不支持操作。

8.2.2 页面布局

Web 业务系统页面布局如下图所示。

其中系统列表区域有两种展示模式， 一种是列表模式，一种是缩略图模式。

Web 业务系统页面布局序号说明参见下表。

序号	名称	说明
1	查询区	显示查询条件及<**查询**>、 <**重置**>按钮。 查询条件： 系统名称、域名、标签、组织架构。

序号	名称	说明
2	操作	模式切换 （列表模式、缩略图模式）、 <**新增 Web 业务系统**>、<**导入**>、<**导出**>、 <**设置**>、<**投屏**>。
3	Web 业务系统列表	该区域主要用于 Web 业务系统信息展示以及相关功能的操作。 资产信息展示： 列表模式、缩略图模式。

8.2.3 Web 业务系统新增、编辑、修改

1、 Web 业务系统新增

点击 新增Web业务系统 按钮， 打开新增 Web 业务系统页面。

如下图所示。

基本信息

域名、系统名称为必填项， 系统类型默认 Web 业务系统； 系统重要性下拉普通、重要； 系统标签、责任人非必填。访问地址默认开启支持 http 与https，默认将域名赋值给访问地址， 也可以填写其它。

组织架构

组织架构为用户自定义组织，可在 “**资产管理▶组织架构**” 配置。

系统架构

系统架构包括开发商、系统版本、技术架构、服务组件版本、 Web 容器名称、 Web 容器版本。

更多信息

更多信息包括系统编号、系统状态、使用人、 C-机密性、 I-完整性、 A-可用性、是否是等保系统、地理位置、描述等。如下图所示。

关联信息

关联信息包括子域名、关联资产。关联资产分为前置机、负载均衡、数据库、 CDN、其他。资产下拉显示当前系统最新的 100 个资产。如下图所示。

流量监控

流量监控包括流量监控和访问成功率监控。流量监控强制开启，不可关闭。如下图所示。

2、 Web 业务系统编辑

列表模式点击操作列 按钮， 缩略图鼠标上移点击 按钮， 打开编辑 Web 业务系统页面， 显示系统来源、更新时间。如下图所示。

3、 Web 业务系统删除

列表模式点击操作列 按钮，缩略图模式鼠标上移点击右上角 按钮， 即可删除该 Web 业务系统。资产可以批量删除；列表模式勾选全选框， 可删除查询结果所有。

8.2.4 Web 业务系统导入和导出

1、 Web 业务系统导入

点击 导入 按钮， 弹出导入 Web 业务系统页面， 如下图所示。

Web 业务系统导入分为 Web 业务系统增量导入和 Web 业务系统替换导入：

- Web 业务系统增量导入： 当出现资产 IP 相同时，不能保存。
- Web 业务系统替换导入： 当出现资产 IP 相同时，保留最新导入的资产。

2、 Web 业务系统导出

点击 导出 按钮， 提供 Web 业务系统批量导出功能。

8.2.5 设置

点击 按钮， 打开 Web 业务系统设置页面。如下图所示。

- **自动发现**

自动发现出厂默认禁用， 启用后自动发现满足发现区域和发现类型的 Web 业务系统。关闭自动发现， 那么 Web 业务系统自动发现功能立即关闭。

- **发现区域**

发现区域分为安全域和内网。

安全域：点击 安全域配置 按钮，跳转至 “**资产管理>安全域**” 界面，可根据需求配置安全域。如下图所示。

内网： 点击 内网配置 按钮， 跳转至 “**系统管理>配置管理**” 界面， 可根据需求配置内部 IP。如下图所示。

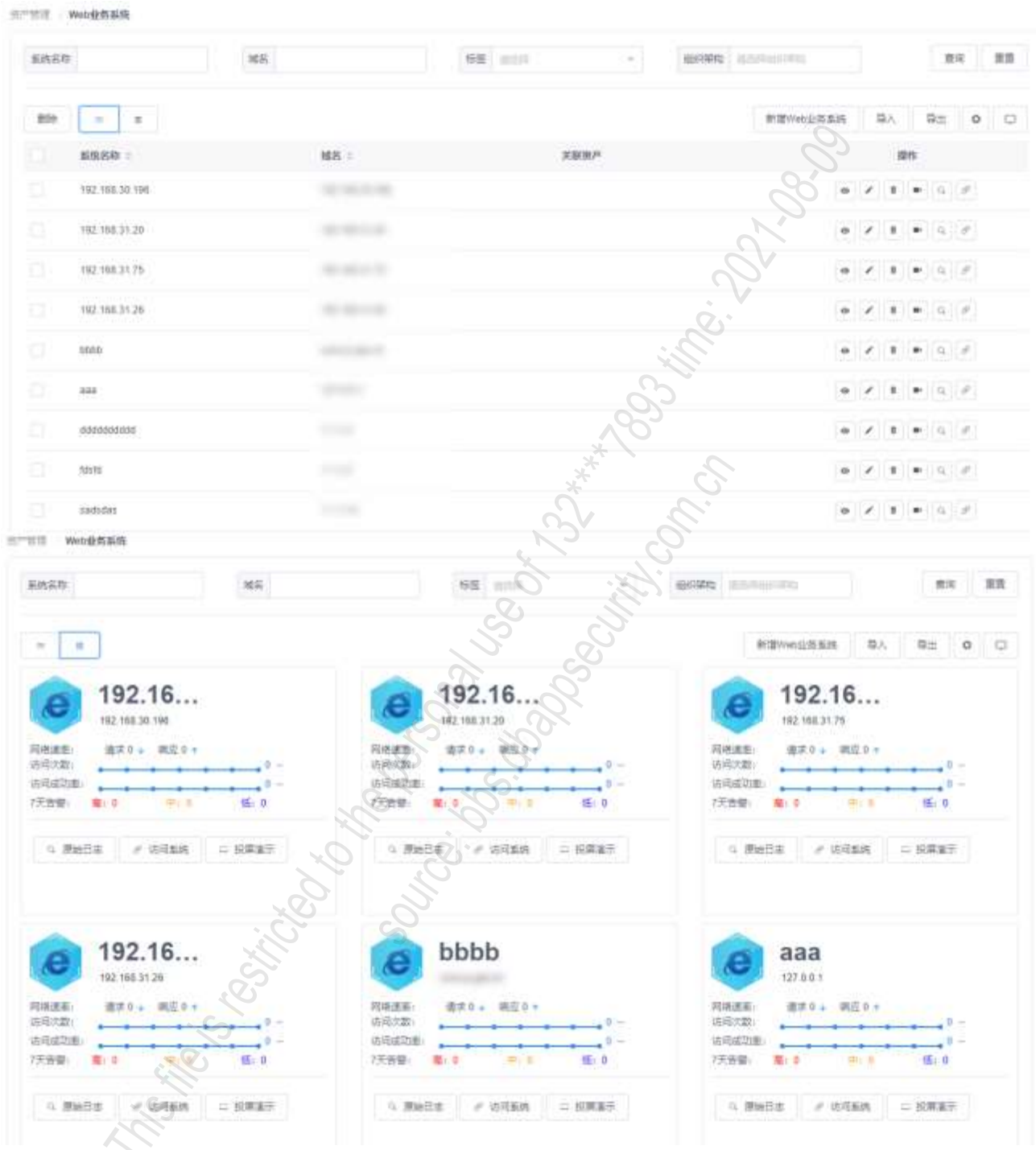
- 发现类型

发现类型包括访问域名和访问 IP 和端口。

8.2.6 投屏

- 点击 按钮投屏至 “**态势感知>Web 业务系统态势**” 大屏。

- 点击  按钮， 跳转至对应的 Web 业务系统的“**态势感知➤资产威胁溯源**”大屏。



投屏说明见下表。

序号	名称	说明
1	投屏	投屏至“**态势感知➤Web 业务系统态势**”大屏。
2	投屏演示	投屏至该系统“**态势感知➤Web 业务系统态势**”大屏。

3	安全告警	该系统关联资产，显示安全告警按钮，点击跳转到“**安全分析➤Investigation➤安全告警**”页面。 该系统不关联资产， 不显示<**安全告警**>按钮。
4	原始日志	点击跳转至“**安全分析➤Investigation➤原始日志**”页面。
5	访问系统	该系统开启访问地址，显示<**访问系统**>按钮，点击新打开配置地址。 该系统关闭访问地址，不显示<**访问系统**>按钮。
6	资产管理	该系统关联资产，显示<**资产管理**>按钮，点击跳转到**资产管理**界面。 该系统不关联资产， 不显示<**资产管理**>按钮。

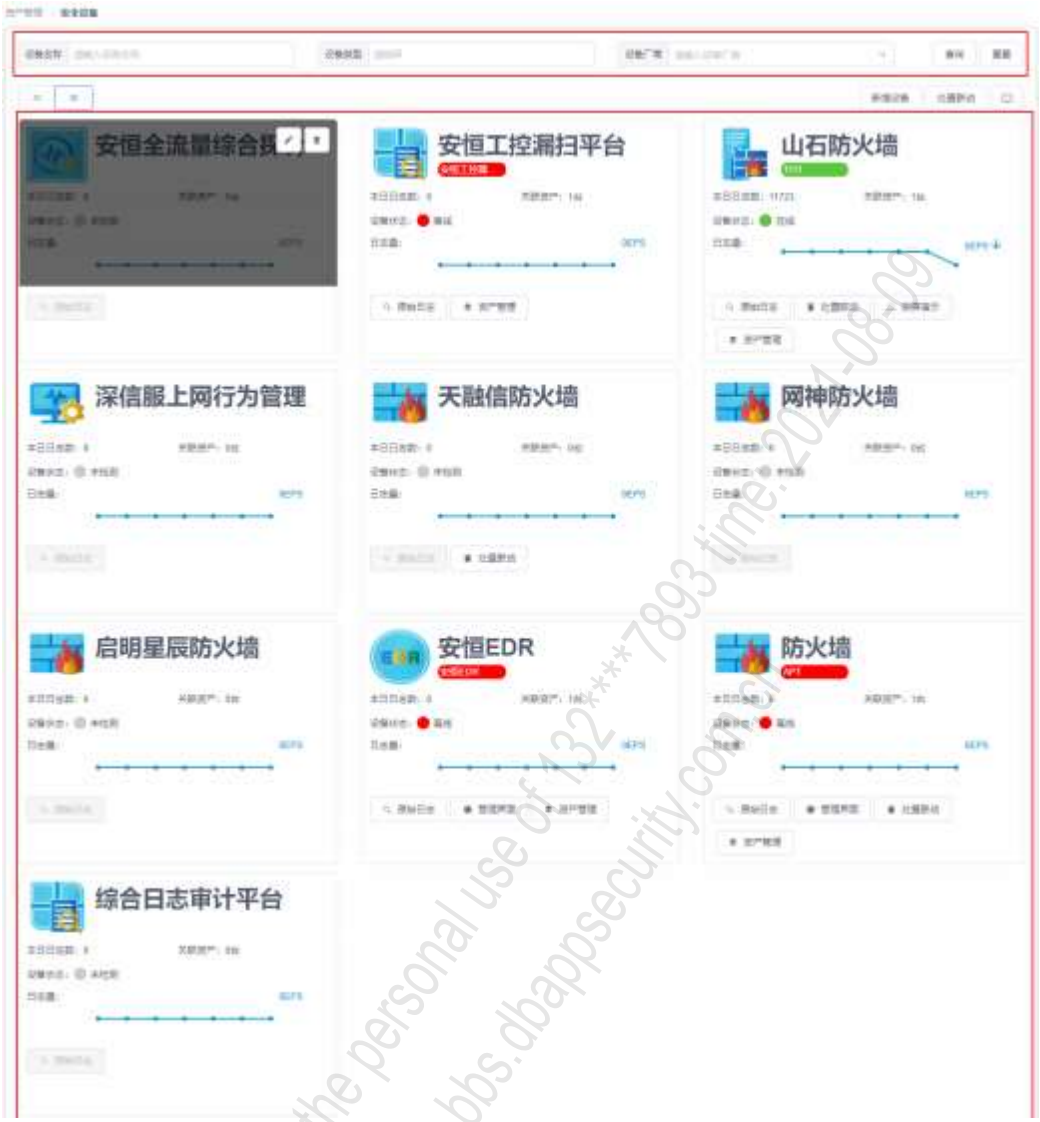
8.3 安全设备

8.3.1 功能简介

选择“**资产管理➤安全设备**”界面， 对安全设备进行统一运维、监控、管理。

8.3.2 页面布局

安全设备页面布局如下图所示。



安全设备页面布局序号说明参见下表。

序号	名称	说明
1	查询区	显示查询条件及<**查询**>、 <**重置**>按钮。查询条件： 设备名称、设备类型、设备厂商。
2	操作	模式切换 （列表模式、缩略图模式）、<**新增设备**>、<**处置联动**>、<**投屏**>。
3	安全设备列表	该区域主要用于安全设备信息展示以及相关功能的操作。 资产信息展示： 列表模式、缩略图模式。 列表模式： 显示设备名称、设备厂商、设备类型、关联资产、操作。 缩略图模式： 显示设备名称、本日日志数、关联资产、设备状态（根据资产管理界面在线状态检测获取设备状态，未关联资产显示未检测）、日志量。

8.3.3 安全设备新增、编辑、删除

1、 安全设备新增

点击 新增设备 按钮， 打开新增页面，如下图。

设备名称、设备类型、设备厂商为必填项。满足设备类型和设备厂商的资产才能被关联， 一个安全设备可以关联多个资产，同一个资产只能被一个安全设备关联。

2、 安全设备编辑

列表模式点击操作列 按钮，缩略图鼠标上移点击 按钮，打开修改页面。

如下图所示。

3、 安全设备删除

列表模式点击操作列 按钮， 缩略图模式鼠标上移点击右上角 按钮， 即可删除该安全设备。安全设备可以批量删除。

8.3.4 投屏

安全设备可以通过投屏功能在大屏展示安全设备的安全态势。

投屏说明见下表。

序号	名称	说明
1	日志检索	跳转至该系统“**安全分析▶Investigation▶日志检索**”页面。
2	管理界面	◆ 该安全设备关联资产的（“**设备管理▶管理地址**”）开启，显示按钮，点击新打开配置地址。 ◆ 该安全设备不关联资产或资产的（“**设备管理▶管理地址**”）关闭，不显示按钮。
3	处置联动	跳转至“**资产管理▶处置联动**”页面，带入该安全设备。
4	投屏演示	◆ 安全设备资产类型为安全类/Web 应用防火墙，点击跳转至 **WAF 监控安全态势**。 ◆ 安全设备资产类型为安全类/APT，点击跳转至 **APT 监控安全态势**。 ◆ 安全设备资产类型为安全类/数据库审计系统，点击跳转至**数据库安全分析智能平台**。
5	资产管理	◆ 该安全设备关联资产，显示资产管理按钮，点击跳转到**资产管理**界面。

序号	名称	说明
		◆ 该安全设备不关联资产， 不显示<**资产管理**>按钮。
6	处置联动	点击跳转至 “**资产管理➤处置联动**” 页面。
7	投屏	投屏至 “**态势感知➤平台运行状态检测**” 大屏。

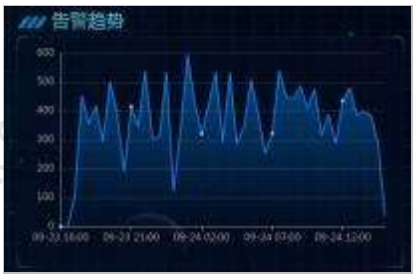
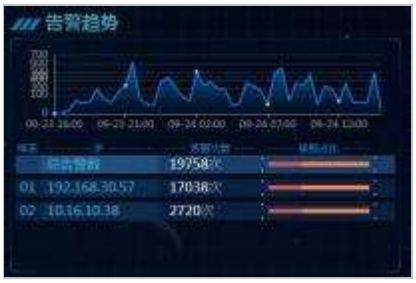
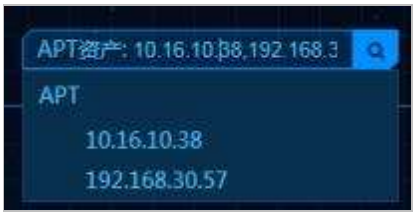
8.3.5 APT 大屏

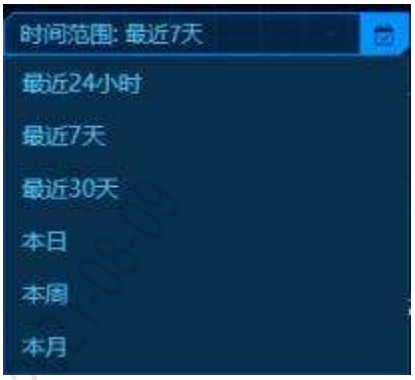
APT 监控安全态势大屏实时统计分析当天 APT 设备， 包括攻击源 IP 排行、攻击来源区域分布、攻击目标排名、被攻击目标数、累计攻击者、攻击路线、详细攻击信息、告警统计、告警趋势、告警类型分布等数据。 APT 大屏如下图所示：

以下各区块均实时展示当天数据。

区块	说明	详细
攻击源 IP 排行	默认展示时间范围内攻击次数最多的 5 个 IP 及对应攻击量， 点击更多显示 Top100；点击跳转至攻击者追踪溯源界面。	

区块	说明	详细
攻击来源区域分布	默认展示时间范围内攻击来源区域Top10。	
攻击目标排名	默认展示时间范围内攻击目标排名 Top5 及对应被攻击量，点击更多显示 Top100。	
被攻击者目标数/累计攻击者	显示该设备被攻击者目标数/累计攻击者。	
攻击路线	实时展示攻击路线， 根据经纬度显示最近 20 条。	
当天详细攻击信息	◆ 展示当天最近 50 条详细攻击信息。 ◆ 当没有告警事件发生时， 该区块不展示内容。	

区块	说明	详细
告警统计	◆ 共发现告警数。 ◆ 恶意文件数：点击可下载报告。 ◆ 高危： 威胁等级[7 to 10]。 ◆ 中危: 威胁等级[4 to 6]。 ◆ 低危: 威胁等级[0 to 3]。	 
告警趋势	◆ 关联 1 个资产， 显示统计时间范围内告警趋势。 ◆ 关联多个资产时， 轮播显示统计时间范围内告警趋势。	 
告警类型分布	南丁格尔玫瑰图显示时间范围内告警类型的Top10。	
APT 资产	APT 资产可选多个， 也可选单个。	

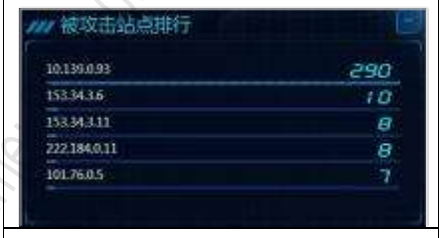
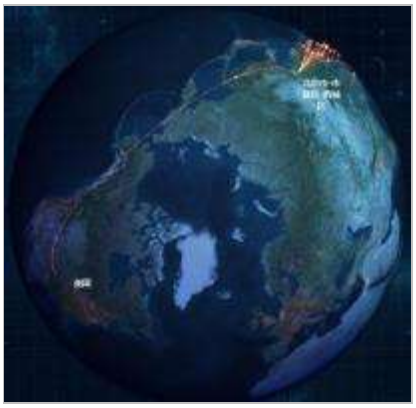
区块	说明	详细
时间范围	时间范围可选： 最近 24 小时、最近 7 天、最近 30 天、本日、本周、本月。	

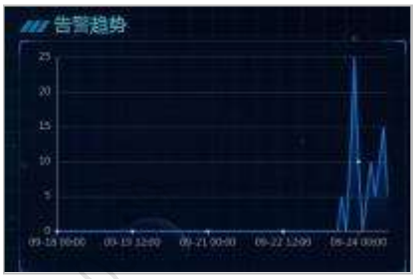
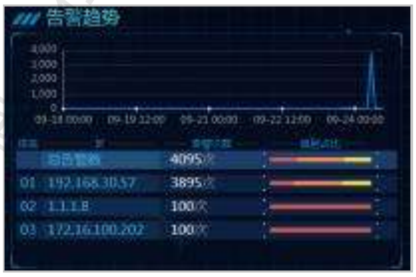
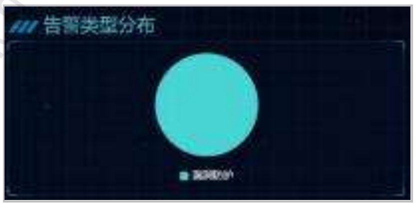
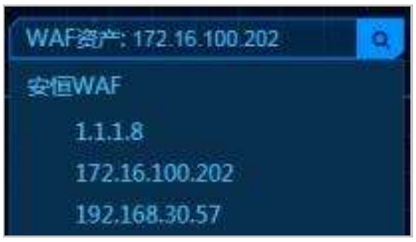
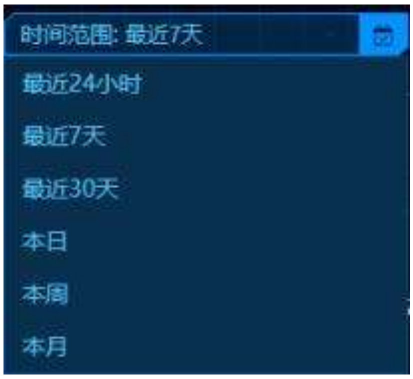
8.3.6 WAF 大屏

WAF 监控安全态势大屏实时统计分析当天 WAF 设备， 包括攻击源 IP 排行、攻击来源区域分布、被攻击站点排行、被攻击站点数、累计攻击者、攻击路线、详细攻击信息、告警统计、告警趋势、告警类型分布等数据。如下图所示。

以下各区块均实时展示当天数据。

区块	说明	详细
攻击源 IP 排行	默认展示时间范围内攻击次数最多的 5 个 IP 及对应攻击量， 点击更多显示 Top100；点击跳转至攻击者追踪溯源界面。	

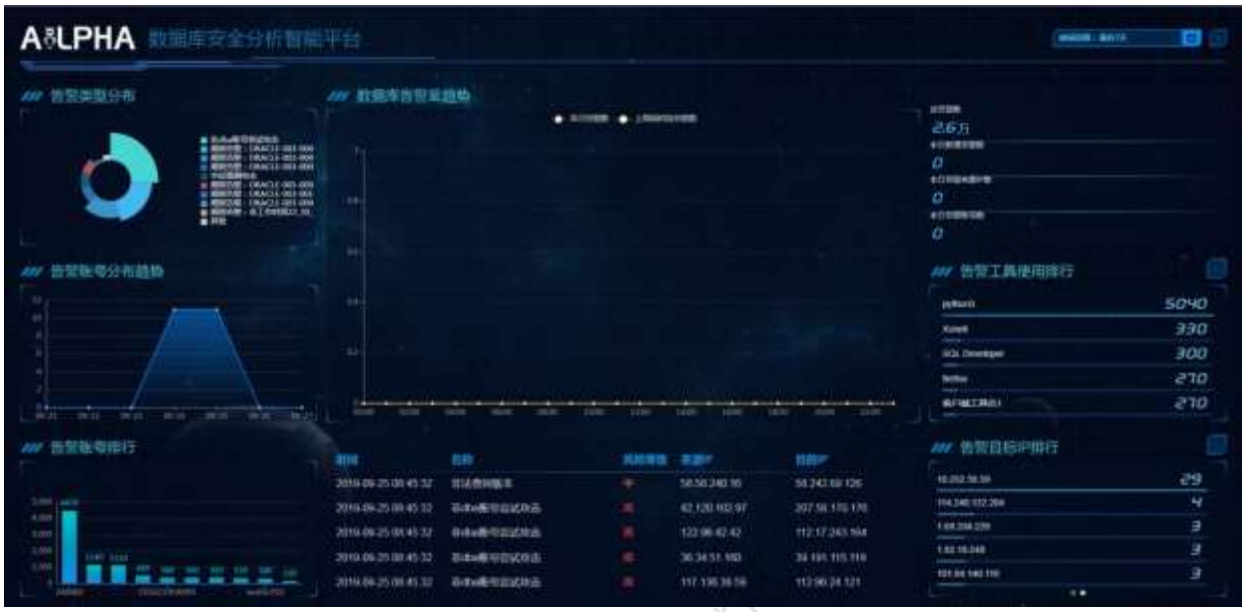
区块	说明	详细
攻击来源区域分布	默认展示时间范围内攻击来源区域Top10。	
被攻击站点排行	默认展示时间范围内被攻击站点 Top5 及对应被攻击量， 点击更多显示 Top100；点击跳转至该站点的 WAF 监控安全态势大屏。	
被攻击站点数/累计攻击者	显示该设备被攻击站点数/累计攻击者。	
攻击路线	实时展示攻击路线， 根据经纬度显示最近 20 条。	
当天详细攻击信息	◆ 展示当天最近 50 条详细攻击信息。 ◆ 当没有告警事件发生时， 该区块不展示内容。	
告警统计	◆ 总告警数 ◆ 阻断告警数： ◆ 高危： 威胁等级[7to 10] ◆ 中危: 威胁等级[4 to 6] ◆ 低危: 威胁等级[0 to 3]	

区块	说明	详细
告警趋势	◆ 关联 1 个资产， 显示统计时间范围内告警趋势。 ◆ 关联多个资产时， 轮播显示统计时间范围内告警趋势。	 
告警类型分布	南丁格尔玫瑰图显示时间范围内告警类型的 Top10。	
WAF 资产	WAF 资产可选多个，也可选单个。	
时间范围	时间范围可选： 最近 24 小时、最近 7 天、最近 30 天、本日、本周、本月。	

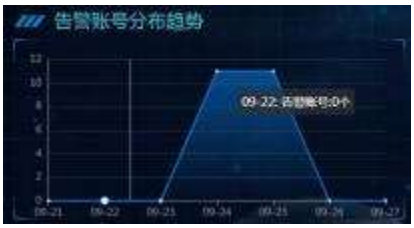
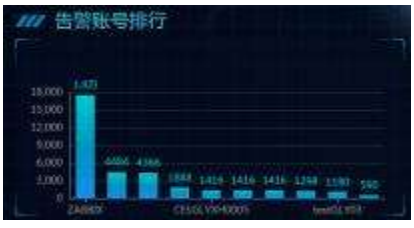
8.3.7 数据库审计大屏

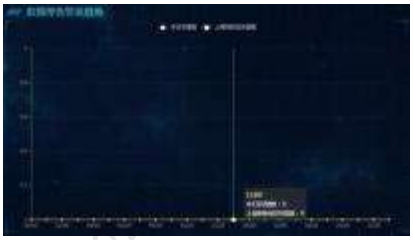
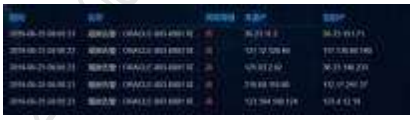
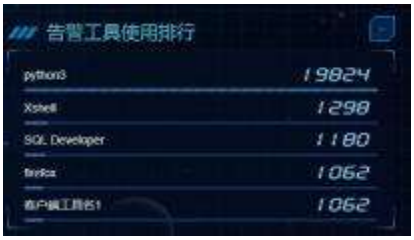
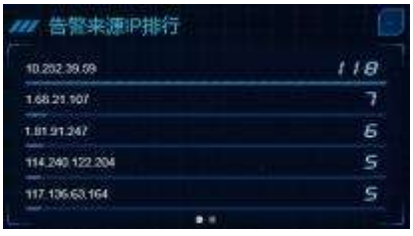
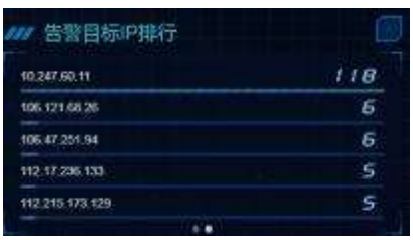
数据库安全分析智能平台大屏实时统计分析当天数据库审计系统设备， 包括告警类型分布、告警账号分布趋势、告警账号排行、数据库告警量趋势、实时列表、总告警数、本日新增告警数、本日告警来源 IP 数、本日告警账号数、告警工具使用排行、告警来源 IP 排行/告警目标 IP 排行等数据。

数据库审计大屏如下图所示：



以下各区块均实时展示当天数据。

区块	说明	详细
告警类型分布	默认展示时间范围内告警类型分布 Top9+其他。	
告警账号分布趋势	默认展示时间范围内告警账号分布趋势（distinct userName）。	
告警账号排行	默认展示时间范围内告警账号的分布 Top10。	

区块	说明	详细
数据库告警量趋势	展示本日告警数据量及上周同时段告警数。	
实时列表	◆ 滚屏显示 deviceAddress：xxx 的最新 50 条数据， 包括时间、名称、风险等级、来源 IP、目的 IP。 ◆ 点击溯源至原始日志， 带入条件： 时间+eventId。	
总告警数	展示时间范围内安全设备总告警数。	
本日新增告警数	展示本日安全设备告警数。	
本日告警来源 IP 数	展示本日告警来源 IP 数。	
本日告警账号数	展示本日告警账号数。	
告警工具使用排行	1.展示时间范围内告警工具使用 Top5，点击更多显示 Top10。 2.点击溯源至原始日志页面。	
告警来源IP排行/告警目标 IP 排行	◆ 展示时间范围内告警来源 IPTop5，点击更多显示 Top10；点击溯源至原始日志页面。 ◆ 展示时间范围内告警目标 IPTop5，点击更多显示 Top10；点击溯源至原始日志页面。	 

区块	说明	详细
时间范围	时间范围可选： 最近 24 小时、最近 7 天、最近 30 天、本日、本周、本月。	

8.4 弱点管理

8.4.1 功能简介

选择 “**资产管理➤弱点管理**” 界面， 支持安恒信息Web 应用弱点扫描器、绿盟扫描器和天镜脆弱性扫描与管理系统扫描报告导入、查看。

8.4.2 弱点管理

1、 查询

弱点管理支持弱点名称、威胁等级、受影响主机名、 CVE 编号和扫描器类型等查询。如下图所示。

2、 重置

弱点管理支持查询条件重置，如下图所示。

3、 详情

列表展示弱点名称、威胁等级、扫描器名称、受影响主机、 CVE 编号及操作列。如下图所示。

点击操作列的 按钮， 可查看弱点详情。弱点详情包括弱点名称、威胁等级、扫描器名称、受影响主机名、弱点描述和解决建议。如下图所示。

8.4.3 扫描报告的导入

本平台支持的扫描工具有安恒信息Web 应用弱点扫描器、绿盟扫描器和天镜脆弱性扫描与管理系统。

点击<**扫描报告导入**>，弹出扫描报告导入页面，如下图所示。

导入的信息都可以在扫描列表中显示，每个域名每个漏洞为一条。同一个系统保留最后一份漏洞信息。

1、 安恒信息 Web 应用弱点扫描器

安恒信息 Web 应用弱点扫描器支持的扫描报告格式为 xml。扫描报告导入页面选择安恒信息 Web 应用弱点扫描器， 选择需要导入的扫描报告导入。如下图所示。

2、 绿盟远程安全评估

1) 支持绿盟Web 应用漏洞扫描器在线导入， 要求必须购买接口模块。

扫描报告导入页面选择绿盟扫描器下绿盟Web 应用漏洞扫描器， 点击<**新增**>，打开新增扫描器弹框。

输入扫描器名称、扫描器地址、用户名、密码， 其中扫描器名称及扫描器地址唯一， 点击<**保存**>。如下图所示。

选择自己新增的扫描器， 对扫描器接口进行连接测试。或者点击连接测试按钮， 对扫描器接口进行连接测

试。选择需要导入报告任务 ID，提交。如下图所示。

2) 支持绿盟远程安全评估 5.0 离线导入。扫描报告导入页面选择绿盟扫描器下绿盟远程安全评估 5.0，选择需要导入的扫描报告导入。如下图所示。

3) 支持绿盟远程安全评估 6.0 在线导入， 要求必须购买接口模块。扫描报告导入页面选择绿盟扫描器下绿盟远程安全评估 6.0，点击<**新增**>，打开新增扫描器弹框。输入扫描器名称、扫描器地址、用户名、密码， 其中扫描器名称及扫描器地址唯一，点击<**保存**>。如下图所示。

选择自己新增的扫描器， 对扫描器接口进行连接测试； 或者点击<**连接测试**>按钮， 对扫描器接口进行连接测试。

选择需要导入报告任务 ID，显示任务名称，提交。如下图所示。

3、 天镜脆弱性扫描与管理系统

支持天镜脆弱性扫描与管理系统在线导入，要求必须购买接口模块。

扫描报告导入页面选择天镜脆弱性扫描与管理系统，点击<**新增**>， 打开新增扫描器弹框。

输入扫描器名称、扫描器地址、用户名、密码， 其中扫描器名称及扫描器地址唯一， 点击<**保存**>。如下图所示。

选择自己新增的扫描器，对扫描器接口进行连接测试。或者点击<**连接测试**>，对扫描器接口进行连接测试。

选择需要导入报告任务 ID，显示任务名称，提交。如下图所示。

8.5 处置联动

8.5.1 功能简介

选择 “**资产管理➤处置联动**” 界面， 支持 WAF 联动。

处理联动包含三个部分： 1.联动设备添加； 2.联动策略设置； 3.完成阻断事件。

8.5.2 联动设备

1、 新增联动设备

在**资产管理**页面点击<**新增资产**>，在**基本信息**区域， **资产类型**选择**安全类/Web 应用防火墙（ WAF）**，**厂商为安恒(DBAPPSecurity)**或者是 **Imperva**； 资产类型选择**安全类/下一代防火墙**，厂商为**山石防火墙(5.5R5)**或**华为(Huawei)**或**华三(H3C)**或**网御星云(leadsec)**或**天融信(Topsec)**; **资产类型**选择**网络类/防火墙**，厂商为**深信服(SANGFOR)**， 并**开启联动设备**。如下图所示。

联动设备页面新增一条记录，列表显示设备详细信息：安全设备、资产名称、资产 IP、设备类型、端口、状态、操作（编辑、连接测试）。

如下图所示。

若安全设备关联该资产， 联动设备界面显示该安全设备。

2、 编辑联动设备

联动设备页面点击操作列的编辑按钮， 进入资产编辑页面。保存后返回联动设备页面， 并更新列表相关信息。

3、 删除联动设备

资产管理页面编辑 WAF 设备，关闭<**处置联动**>，保存。联动设备界面不再显示该设备。如下图所示。

4、 测试连接

联动设备页面点击操作列连接测试按钮， 重新检测该 IP 对应 WAF 设备的连接状态， 并更新 “**状态**” 列；当状态异常时， 提示连接失败， 正常时， 提示连接成功。

5、 查询与重置

联动设备支持安全设备与资产 IP 查询，支持查询条件重置。

如下图所示。

8.5.3 联动策略

选择“**资产管理➤处置联动➤联动策略**”界面，显示被触发的联动策略信息。列表展示策略更新时间、阻断 IP、阻断时间、安全设备、资产名称、资产 IP、策略来源、本月事件次数、状态、策略阶段、操作（删除）。如下图所示。

联动策略来源有两种：一是自建；二是剧本编排。

用户自建联动策略优先级高于剧本编排创建。用户自建联动策略阻断时间为永久， 状态为已生效， 策略阶段；剧本编排创建策略阻断时间（ 10min、 30min、 6h、 24h、 72h、永久）可调整、可删除、可添加。

目前仅支持自建策略。

1、 联动策略增加

A. 点击 新增策略 按钮， 弹出**新增**页面，填写阻断 IP、资产 IP（资产 IP 多选），保存。如下图所示。

B. 选择“**态势感知▶数据中心态势**”大屏， 点击**攻击者基本信息**模块黑客 IP 右侧  。联动策略页面显示该阻断信息。如下图所示。

C. 选择“**态势感知▶攻击者追踪溯源**”大屏，点击攻击 IP 左侧  。联动策略页面显示该阻断信息。如下图所示。

2、 联动策略删除

A. 点击操作列 按钮，删除该条策略信息。

B. 选择“**态势感知▶内网安全态势**”大屏， 点击攻击者基本信息模块黑客 IP 右侧。联动策略页面不再显示该阻断信息。

如下图所示。

C. 选择“**态势感知▶攻击者追踪溯源**”大屏， 点击攻击 IP 左侧。联动策略页面不再显示该阻断信息。

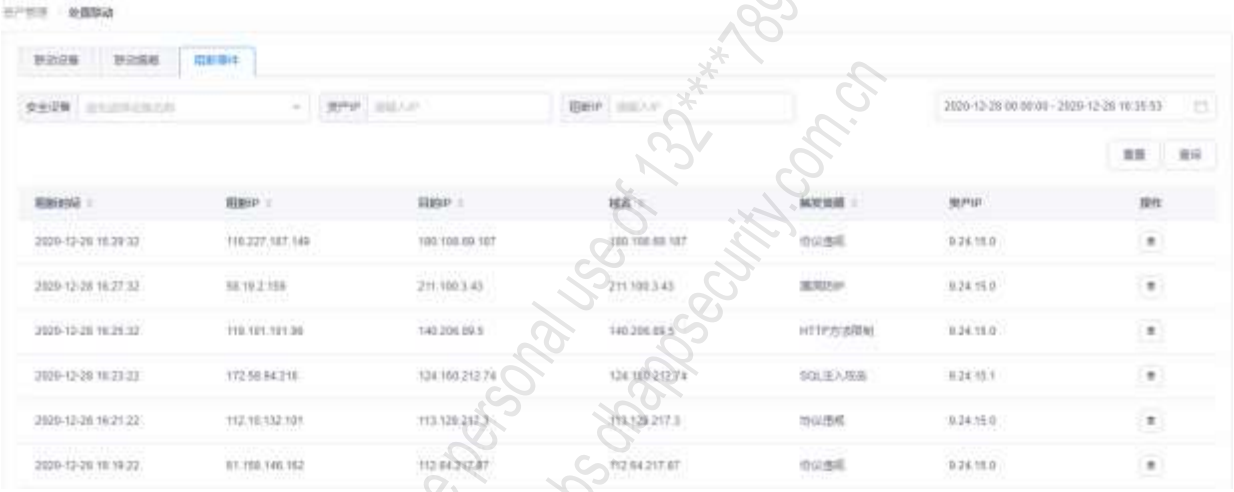
如下图所示。

3、 查询与重置

联动策略支持安全设备、资产 IP、阻断 IP 查询。支持查询条件重置。如下图所示。

8.5.4 阻断事件

选择“**资产管理▶处置联动▶阻断事件**”页面， 显示 WAF 发送过来的阻断事件信息， 包括阻断时间、阻断 IP、目的 IP、域名、触发策略、资产 IP、操作。支持安全设备、资产 IP、阻断 IP 和时间查询。支持查询条件重置。如下图所示。



8.6 安全域

8.6.1 功能简介

选择“**资产管理▶安全域**”页面，有缩略图和列表两种模式， 默认显示缩略图模式。

将收集到的客户在用 IP 段， 细化成各个安全域， 然后配置到安全域中， 以便在数据分析或数据展示中能够直观查看到对应 IP 所属部门或者使用用途。

安全域分为内部安全域和未分配，非内部安全域的 IP 自动归为未分配。出厂情况下，默认内置一个名为“**局域网**”的内部安全域。包括内置的安全域在内， 用户可进行安全域新增， 编辑， 删除， 导入导出等操作。

8.6.2 页面布局

安全域页面布局如下图所示。

安全域页面布局序号说明参见下表。

序号	名称	说明
1	查询区	显示查询条件及<**查询**>、 <**重置**>按钮。查询条件：安全域名称、标签、组织架构。
2	操作	模式切换 （列表模式、缩略图模式）、 <**导入**>、<**导出**>、<**新增安全域**>。
3	安全域列表	该区域主要用于安全域信息展示以及相关功能的操作。 安全域信息展示：列表模式、缩略图模式。
4	快速跳转	点击页面底部<**快速跳转： 内部 IP 配置**>， 页面跳转至配置管理页面。

8.6.3 安全域新增、编辑、修改

1、 安全域新增

点击 新增安全域 ，打开安全域配置页面，如下图所示，填写相关信息，点击<**保存**>。

基本信息

名称为必填项且唯一；描述为非必填项； 图标为必选项， 默认选择一个图标，点击图标可进行修改。

安全域标签

标签为非必填项，默认云和边界两个标签，用户可自定义添加标签。

组织架构

组织架构为非必选项， 支持多选， 选择时默认不带上下级， 点击后面的全部， 带上下级所有。当前用户若拥有组织架构权限， 显示<**编辑组织架构**>按钮，点击可新打开一个组织架构界面。

安全域网段

安全域网段必填， 必须配置一个及以上 IP 条目。安全域网段支持三种类型： IP 地址、 IP 区间、子网掩码。

内部安全域之间的网段不支持交集， 配置的安全域网段确保不在其它内部安全域中。

2、 安全域编辑

列表模式点击操作栏的 按钮， 缩略图鼠标上移点击 按钮， 打开安全域配置页面。显示安全域的相关信息， 包括基本信息， 安全域标签， 组织架构， 安全域网段， 可查看和修改安全域配置， 修改后点击<**保存**>，安全域信息更新，并返回到列表模式或缩略图模式的当前页。

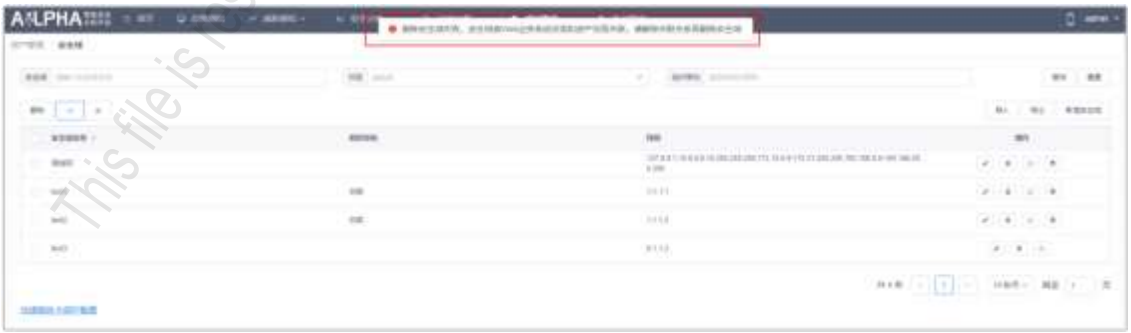
如下图所示：

3、 安全域删除

1) 列表模式下可点击操作栏的 按钮删除该安全域。也可选择单个安全域前的多选框或多个安全域前的多选框， 再点击<**删除**>进行单个安全域删除或安全域批量删除。

当选择全选框后， 可删除当前页的安全域， 也可选择删除查询结果所有（<**删除查询结果所有**>按钮需要全选安全域才会出现）。

若所选删除的安全域被 Web 业务系统发现或资产发现，则该安全域删除失败。如下图所示。



2) 缩略图模式上移点击右上角 按钮即可删除该安全域。

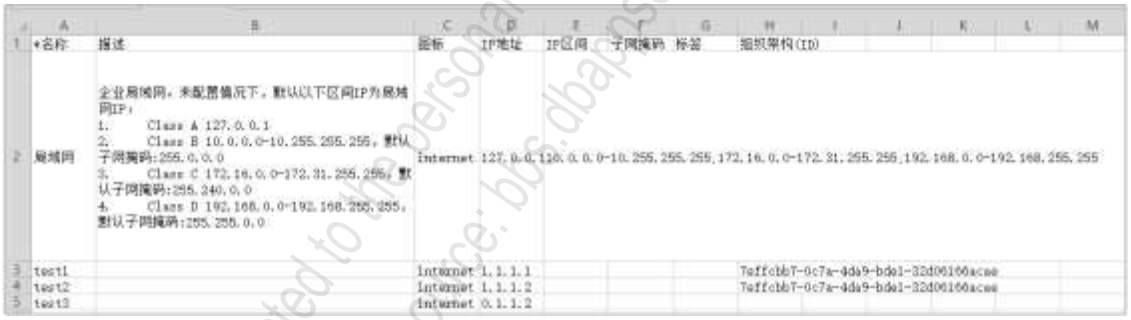
8.6.4 安全域导入和导出

1、 安全域导入

点击 导入 按钮， 弹出导入安全域页面， 如下图所示。可点击<**模板下载**>下载模板文件进行填写， 若文件中有一条安全域的字段填写错误，则整个文件导入失败。

2、 安全域导出

点击 导出 按钮， 导出平台中所有的安全域，导出的内容如下图所示。



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	*名称	描述	图标	IP地址	IP区间	子网掩码	标签	组织架构(ID)					
2	局域网	企业局域网，未配置情况下，默认以下区间IP为局域网IP： 1、 Class A 127.0.0.1 2、 Class B 10.0.0.0-10.255.255.255，默认子网掩码:255.0.0.0 3、 Class C 172.16.0.0-172.31.255.255，默认子网掩码:255.240.0.0 4、 Class D 192.168.0.0-192.168.255.255，默认子网掩码:255.255.0.0	Internet	127.0.0.1;10.0.0.0-10.255.255.255;172.16.0.0-172.31.255.255;192.168.0.0-192.168.255.255									
3	test1		Internet	1.1.1.1				7effcbb7-0c7a-4da9-bde1-32d06160acae					
4	test2		Internet	1.1.1.2				7effcbb7-0c7a-4da9-bde1-32d06160acae					
5	test3		Internet	0.1.1.2									

8.6.5 其他操作

1、 安全告警

列表模式下点击操作栏的 按钮， 缩略图模式下点击 安全告警 按钮， 新打开一个安全告警界面， 带入条件：时间（最近 7 天） +目的安全域(destSecurityZone)为该安全域名称。

2、 资产管理

当安全域下有资产时，列表模式下显示 按钮，缩略图模式下显示 资产管理 按钮， 没有资产则不显示。点击按钮， 先打开一个资产管理页面，带入条件： 左侧安全域选择该安全域。

8.7 组织架构

8.7.1 功能简介

选择 “**资产管理➤组织架构**” 页面，默认显示一级和二级节点。出厂情况下，会内置一个名为 “**总部**” 的根节点，不可删除。各节点下会显示对应的用户信息和关联业务。

8.7.2 组织结构查询

组织架构支持关键字搜索， 输入关键字自动匹配包含关键字的组织架构（模糊搜索），搜索结果需要显示上级组织，可点击展开查看对应的下级数据。查询数据为空，显示暂无数据。如下图所示。

8.7.3 组织架构新增

选中根节点， 点击<**添加子节点**>，填写组织架构的基本信息， 包括组织名称、组织编号、组织简称、单位地址、地区，然后点击<**保存**>，组织架构新增成功， 如下图所示。

8.7.4 组织架构编辑

选中节点， 右侧显示该节点的基本信息以及该节点对应的用户信息和关联业务， 若无用户信息或关联业务，则显示暂无数据。可对基本信息进行编辑， 点击关联业务中的安全域或 Web 业务系统， 新打开一个安全域/Web 业务系统页面， 带入条件： 安全域名称/Web 业务系统名称。

8.7.5 组织结构删除

- 删除节点时需要先解除所有绑定关系，没有解除绑定时不能删除。如下图所示。

- 组织架构有子节点时，不支持删除父节点，需要先删除子节点才支持删除父节点。

9. 系统管理

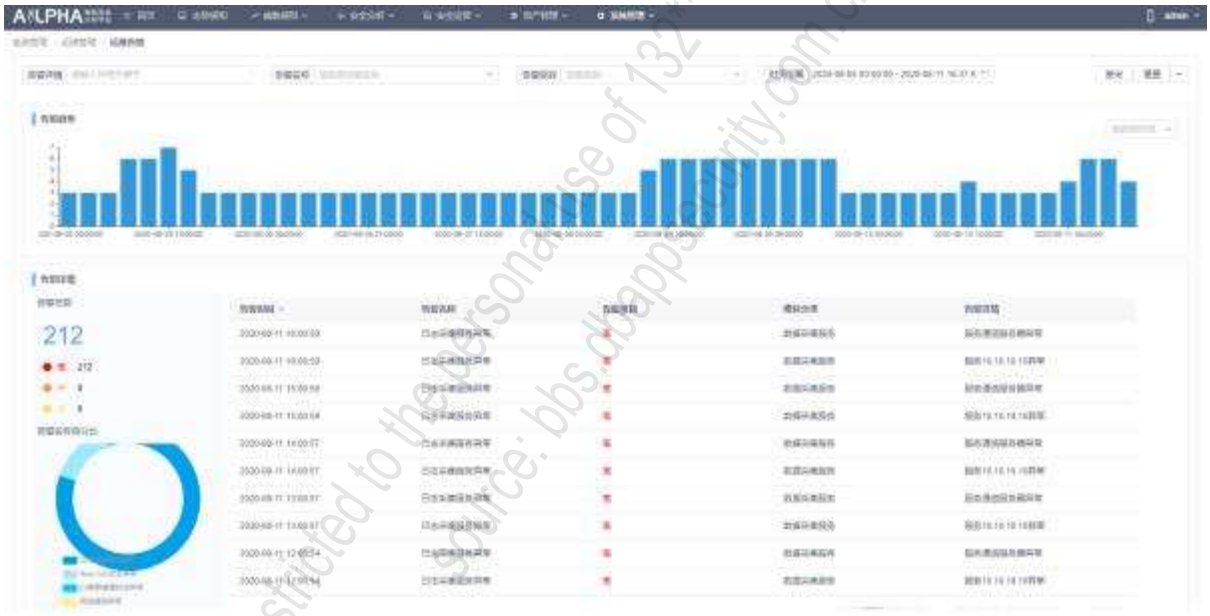
可对平台进行运维管理、配置管理、任务管理、系统管理等操作。

9.1 运维管理

运维管理包括运维告警、健康检查、存储管理、故障日志等功能， 便于用户实时且直观的了解平台的使用情况及其健康状况。

9.1.1 运维告警

选择 “**系统管理▶运维管理▶运维告警**” 进入**运维告警**页面。该页面汇总了平台中运维告警的信息并加以展示， 使用户更方便了解系统运维的健康状况。



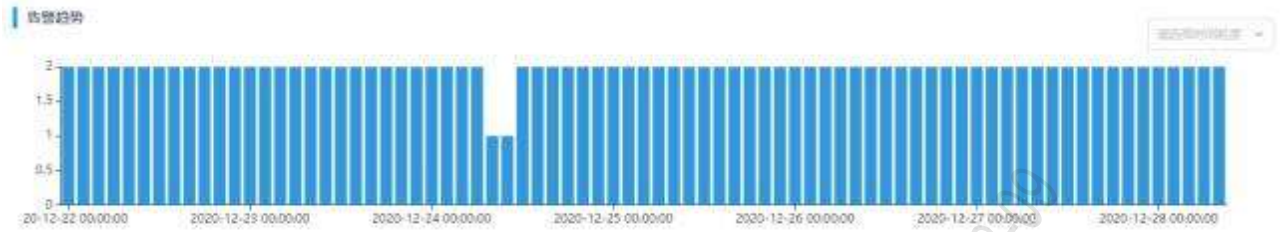
查询

可通过告警详情、告警名称、告警级别、时间范围、模块分类（点击**高级查询**图标出现）字段对运维告警进行筛选及查询，如下图所示。其中告警详情支持模糊查询， 告警名称支持多选，告警级别仅支持单选。

告警趋势

告警趋势以柱状图的形式展现， 如下图所示。时间范围默认与查询条件中的时间范围保持一致， 也可重新

选择时间粒度， 如 1 小时， 1 天，一个月，一年， 告警趋势图随着时间粒度的切换而变换。



告警详情

- 告警详情由告警总数、告警名称占比、告警列表三部分组成， 如下图所示。
- 告警总数显示总数和高、中、低每个级别的数量， 高、中、低分别用红、橙、黄 3 个颜色显示。
- 告警名称占比以环状图的形式展示。
- 告警列表包含告警时间、告警名称、告警级别、模块分类、告警详情， 列表默认按照触发时间倒序显示，点击表头**触发时间**支持排序。

9.1.2 健康检查

健康检查对平台使用情况、组件节点状态、集群状态、接口开放状态等进行巡检， 巡检结果以不同的图标进行展示， 并加以结果描述及处置建议， 使用户可精确定位系统故障并对其进行修复。

巡检结果

- 若没有历史巡检结果，巡检结果显示：未巡检，且无“**查看历史巡检结果**”字样。
- 若有历史巡检结果， 巡检结果显示： 最近一次巡检时间yyyy-mm-sshh:mm:ss （指巡检的开始时间），且有“**查看历史巡检结果**”字样， 点击后出现巡检结果弹窗， 可根据巡检结果， 巡检方式以及时间范围对其进行查询筛选，巡检记录可查看， 如下图所示。

点击右上方<**一键巡检**>可对运维检测项进行巡检。

点击右上方<**导出 PDF**>可导出健康检查报告。

运维检测项

运维检测项包括数据健康检查、探针健康检查、大数据集群健康检查、 Elasticsearch 健康检查、实时流计算引擎健康检查、管理服务健康检查、节点宿主机 IP 健康检查等， 检测结果以列表的形式展示在每个运维检测项的下方，如下图所示。

其中监测结果若正常，以✅展示； 若异常， 则以❌展示，并给出相应的处置建议。

宿主机节点健康检查的结果处置建议为“**查看主机监控**”，如下图所示：

节点 192.168.30.194 健康检查

监测结果	检查内容	描述	处置建议
✓	基本信息	CPU：32 核，内存：251.82GB，硬盘：39.76TB	[查看主机监控]
✓	CPU利用率	22.48%	[查看主机监控]
✓	磁盘利用率	8.39%	[查看主机监控]
✓	系统负载	5.53	[查看主机监控]
✓	网卡吞吐量	入流量：90.54KB/s，出流量151.51KB/s	[查看主机监控]
✓	磁盘IO使用率	3.36%	[查看主机监控]
✓	系统进程数	10	[查看主机监控]
✓	内存使用率	66.82%	[查看主机监控]

点击处置列的 “**查看主机监控**” 可跳转至Ambari 界面，如下图所示：

9.1.3 存储管理

选择 “**系统管理▶运维管理▶存储管理**” 页面， 可查看磁盘使用情况和磁盘使用趋势。

磁盘使用情况

展示当前磁盘使用情况。具体将磁盘使用量分为三个等级， 分别是普通（ 0-60%）、警告（60-90%）和危险（ 90-100%）。如下图所示。

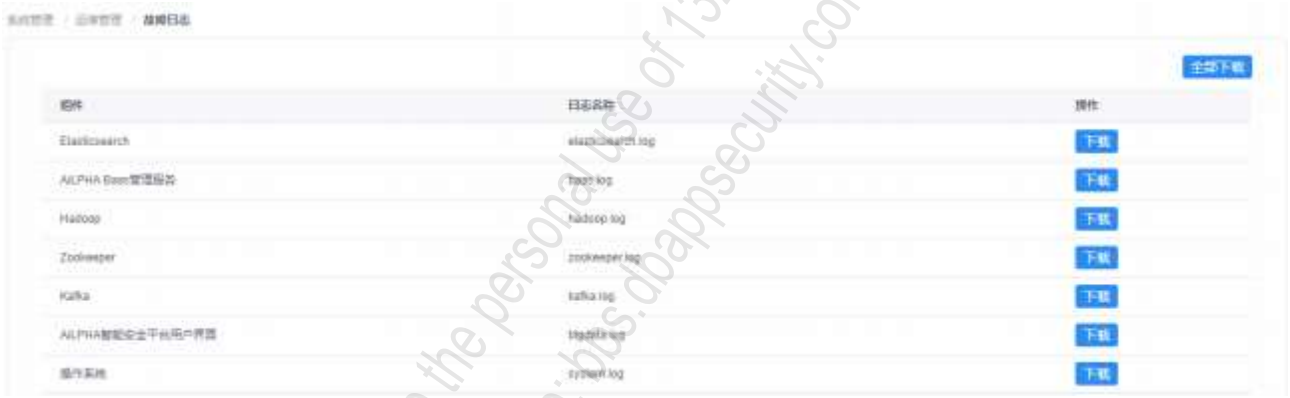
磁盘使用趋势

展示选择时间范围内磁盘使用趋势。如下图所示。

9.1.4 故障日志

选择 “**系统管理▶运维管理▶故障日志**，进入故障日志页面。， 可下载容器、宿主机等组件的日志信息， 相关人员可通过日志中的报错记录快速且准确地定位问题所在， 如下图所示。

- 点击<**下载**>，下载文件为 zip 包， 解压后包含对应组件的日志文件。
- 点击<**全部下载**>，下载文件为 zip 包， 解压后包含页面所有组件日志。



User Onboard 日志

在故障日志页面按下 “**Ctrl+?**” 组合键， 可以弹出User Onboard 日志信息界面。点击操作列<**下载**>可以下载User Onboard 日志， 采集用户使用信息用于提升产品易用性、有效性。

用户使用信息属于敏感信息，下载前必须获取用户的授权。

9.2 配置管理

配置管理包括系统配置、数据配置、推送管理、系统开关等功能， 将系统配置界面化， 使用户操作更加便捷。

9.2.1 系统配置

选择 “**系统管理▶配置管理▶系统配置**” 菜单进入**系统配置**页面，系统配置包括**系统配置、更多配置、 网络代理**和**界面美化**等， 系统配置与更多配置将配置参数界面化， 使用户易于操作， 界面美化支持用户自定义，可满足用户的定制需求。

9.2.1.1 系统配置

选择 “**系统管理▶配置管理▶系统配置**” 进入**系统配置**页面，点击**系统配置**页签。 系统配置分为**通用配置**和**内部 IP 配置**两个部分。

通用配置

1) 监控地区与大屏名称，配置监控地区与大屏名称。

配置监控地区与大屏名称， 如下图所示， 即对“**态势感知▶Web 业务系统态势**”名称及监控地区、“**态势感知▶资产失陷态势**”、“**态势感知▶外部攻击态势**”等监控地区生效，如下图所示。

Web 业务系统态势

资产失陷态势

外部攻击态势

2) SOC 地址、 SOC 端口、 SOC APIKey，配置 SOC 地址、 SOC 端口号与 SOC APIKey。
配置完成后进入 “**资产管理➤资产管理**” 页面， 点击<**SOC同步**>进行测试。

- 若 SOC 同步成功，则配置参数正确且生效。
- 若 SOC 同步失败，则配置参数错误， 需重新配置。

3) AiView 地址，配置AiView 地址。
配置完成后， 选择 “**安全分析➤可视化中心➤AiView 设计器**” ， 查看刚刚配置的 AiView 大屏是否可以正常显示。找到对应的大屏，点击查看大屏。

- 若可成功跳转， 则配置参数正确且生效。
- 若跳转失败，则配置参数错误， 需重新配置。

内部 IP 配置

收集客户现场在用 IP 段， 将其配置为内部 IP， 以便数据接入后可立即自发现资产和判断是否为内部 IP。

内部 IP 配置同步至 SOC、 APT、 AiNTA， 且在所有安全事件的分析结果中均有体现。

内部 IP 配置默认以下私网IP 地址区间 IP 为内部 IP：

- Class A 127.0.0.1
- Class B 10.0.0.0-10.255.255.255， 默认子网掩码:255.0.0.0
- Class C 172.16.0.0-172.31.255.255，默认子网掩码:255.240.0.0
- Class D 192.168.0.0-192.168.255.255， 默认子网掩码:255.255.0.0
- Class E 169.254.0.0/16

外部 IP：非内部 IP（IP 不为空）。

点击<**添加 IP 配置**>， 可以新增内部 IP 地址。 内部 IP 配置支持IP 地址、 IP 区间、子网掩码， 添加完成后

点击<**保存 IP 配置**>， 如下图所示。

9.2.1.2 更多配置

更多配置主要涉及**常用参数**和**更多参数**两个部分， 参数保存时， 若需重启， 需重启后方可生效， 若不重启，则不生效。

常用参数

配置项	说明
信任 IP	可配置多个，以英文逗号分隔， 配置生效后， 可免登录访问所有接口。
允许页面嵌套	开启时，平台上的页面可相互嵌套， 若关闭， 则不可相互嵌套。
是否导入内置情报	开启时， 导入威胁情报包， 威胁情报导入成功后， 按钮自动转换成关闭状态， 若关闭，则不导入威胁情报包。
首页缓存	开启时，首页进行缓存， 若关闭，则首页取消缓存。
告警推送主题/推送测试告警主题/推送测试告警内容	告警推送主题与推送测试告警内容对邮件和钉钉生效， 推送测试告警主题仅对邮件生效。
运维巡检地址	若可成功跳转则配置参数正确且生效； 若跳转失败， 则配置参数错误，需重新配置。
弱点管理平台地址	弱点管理平台的 IP 地址。若可成功跳转则配置参数正确且生效；若跳转失败，则配置参数错误， 需重新配置。
弱点管理平台用户/密码	弱点管理平台登录用户名/密码
Investigation 分析场景显示模板数	Investigation 分析场景显示模板数量。取值范围： 1~20。
Investigation 1/2/3/4 维聚合数量限制	设置 Investigation 的 1/2/3/4 维聚合数量。
原始日志查询时间最大范围	设置原始日志查询时间最大范围。取值范围： 30~365。

更多参数

点击<**添加参数**>， 可以选择已存在的配置参数，也可以创建新的配置参数。

点击对应参数行的删除图标 ，可以删除参数。

- 选择已存在的配置参数。可选择后台文件中已存在的配置参数添加至界面对其进行修改。
- 创建新的配置参数。可添加自定义参数， 参数名称不可重复， 参数不可为空。

更多参数中参数的添加与删除操作无需进行保存， 且上述操作仅对参数是否显示在前台页面有效，后台文件中参数并未被删除。

9.2.1.3 网络代理

用户启用网络代理后， “**威胁情报➤情报源➤安恒安全数据大脑**”设置中的在线更新功能通过代理服务器请求安恒安全数据大脑情报库更新。网络代理默认关闭。可设置开启/关闭使用网络代理、设置代理服务器地址端口、开启/关闭代理服务器认证。 点击<**保存代理配置**>即可保存已更改配置。 如下图所示。

9.2.1.4 界面美化

界面美化支持对大屏名称、 Logo 以及主题色的修改，其中大屏名称及 logo 的修改需输入许可码， 如下图所示。

参数配置保存成功后，如下图所示， 产品所涉及到上述参数的页面也将相应修改。

9.2.2 数据配置

选择 “**系统管理▶配置管理▶数据配置**” 进入**数据配置**页面， 进行**数据集管理**。

数据集管理

索引是集群用来存放数据的地方，数据集管理的作用就是对这些索引进行管理。

索引需写入磁盘中， 数量随时间增长， 磁盘空间占用过多会导致其性能下降， 因此数据集配置设定磁盘利用上限， 点击<**数据集配置**>， 如下图所示， 设置**安全日志时间**、**流量日志**时间以及**磁盘利用率上限**参数，若达到上限阈值，即对数据进行清理操作。

操作界面如下图所示：

索引以列表的形式展现， 如下图所示， 包括数据集名称， 启用状态， 数据集状态， 操作栏。索引可进行开

启、关闭、删除操作，也可使用右上角的时间控件对索引进行查询/筛选操作。

9.2.3 推送管理

选择 “**系统管理➤配置管理➤推送管理**” 进入**推送管理**页面，包括邮**件服务器配置**、**短信服务器配置**和**钉钉服务器配置**三个部分， 点击对用的页签分别进行相关配置。

邮件服务器配置

- 邮件服务器配置。进入邮件服务器配置页面， 点击**启用**， 填写邮件服务器（此处填写用户使用的邮件系统的发件服务器名称）、端口、发件箱地址和密码，点击<**保存**>。如下图所示：
- 点击<**发送测试邮件**>， 输入一个收件邮箱，点击<**发送**>。

短信服务器配置

- 进入短信服务器配置页面，点击**启用**， 填写短信 URL，点击<**保存**>，如下图所示：
- 点击<**发送测试短信**>， 输入一个手机号码，点击<**发送**>。

钉钉服务器配置

- 进入钉钉服务器配置页面，点击**启用**，填写Webhook，点击<**保存**>。如下图所示：
- 点击<**发送测试消息**>， 选择提醒所有人或提醒指定人员， 并输入其联系电话，点击<**发送**>。

9.2.4 系统开关

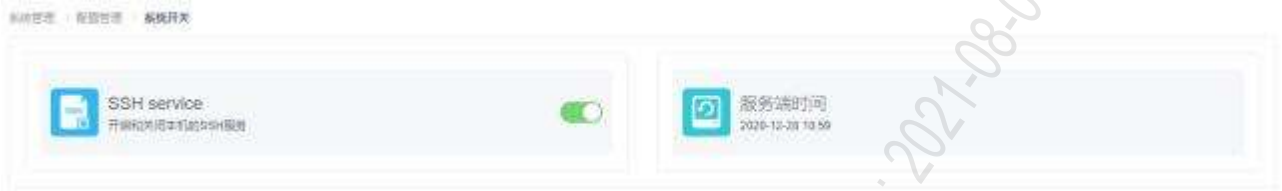
选择 “**系统管理➤配置管理➤系统开关**” 进入**系统开关**页面， 包括 **SSH Service 配置**和**服务器时间**设置两

部分。

SSH service 默认处于开启状态， 后台 SSH 可登录。 若关闭，则不可登录。

服务器时间与客户端时间一致或相差小于等于 10 分钟则正常显示。

若大于 10 分钟，则工具栏中字体显示橙色，系统开关界面上显示红色， 鼠标浮动时出现异常提示。



9.2.5 集群扩容

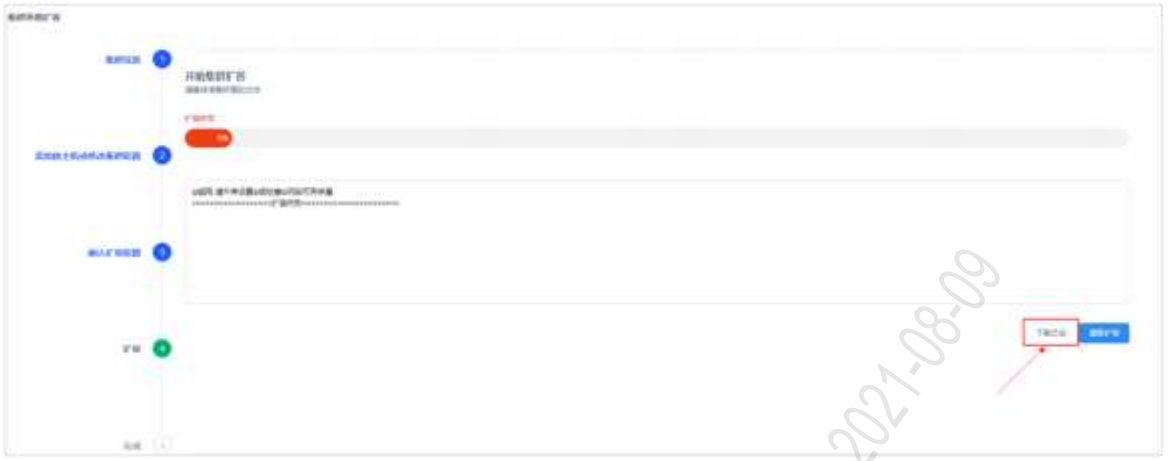
页面支持集群扩容， 支持添加宿主机，支持修改宿主机组件节点数配置。

操作入口

以系统管理员用户登录大数据智能安全分析平台， 选择“**系统管理➢配置管理➢系统开关**”，进入**系统开关**页面，在键盘按下“**Ctrl+?**”组合键， 页面弹出**集群扩容**相关功能按钮，如下图所示。

集群扩容注意事项

- 新增加的服务器设备跟原宿主机的操作系统版本必须一致。
- 集群扩容前，服务器**/home/init/conf/**目录下 **hostinfo.json** 文件不支持修改容器 IP。
- 集群扩容过程中， 如果出现扩容失败等异常， 可点击<**下载日志**>， 将日志发送至相关技术人员进行后续处理。



集群扩容步骤

步骤1. 准备好集群扩容的服务器。

注意需要保证扩容服务器的操作系统版本跟宿主机服务器操作系统版本一致。

步骤2. 以系统管理员用户登录大数据智能安全分析平台，选择“**系统管理**>**配置管理**>**系统开关**”，进入**系统开关**页面，在键盘按下“Ctrl+?”组合键，页面弹出**集群扩容**相关功能按钮。

步骤3. 点击<**集群扩容**>按钮，进入集群环境扩容页面，如下图所示。显示已有宿主机 IP 地址和已有宿主机的内存大小和 CPU（逻辑）核数。

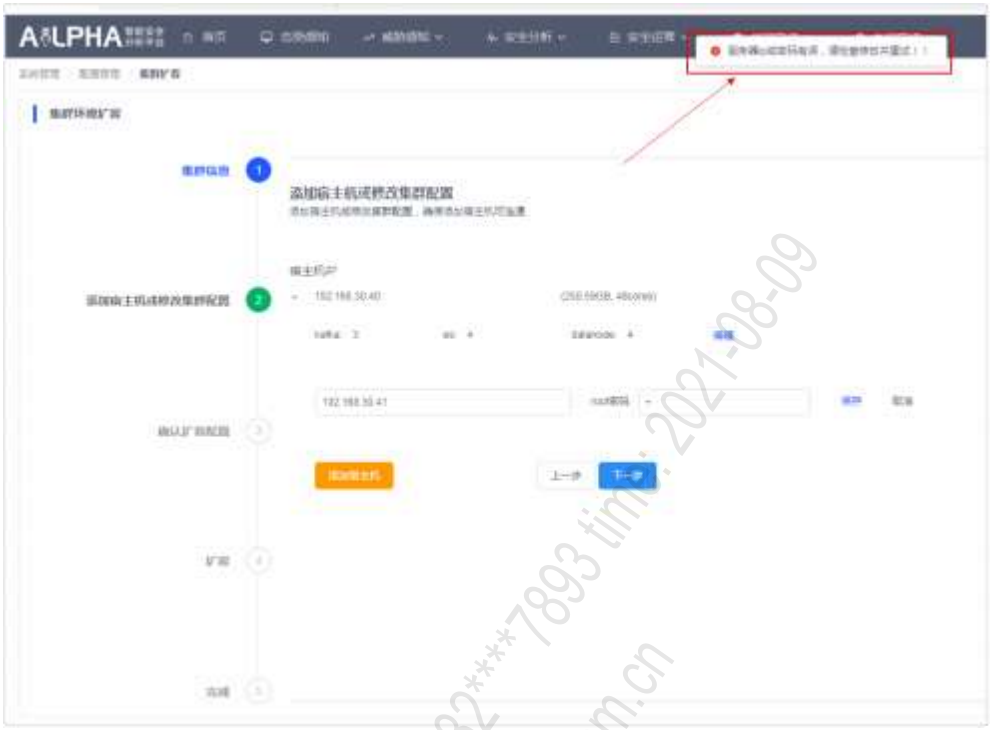
步骤4. 添加宿主机或修改集群配置。

1) 点击<**下一步**>，展开已有宿主机集群配置。
2) 点击<**编辑**>可修改集群配置。

- 已有宿主机 IP 下的集群配置仅支持在最大配置范围内增加，不支持减少（新添加但尚未执行扩容的宿主机，支持在最大配置范围内增加和减少；
- 执行扩容后的宿主机，视为已有宿主机）。

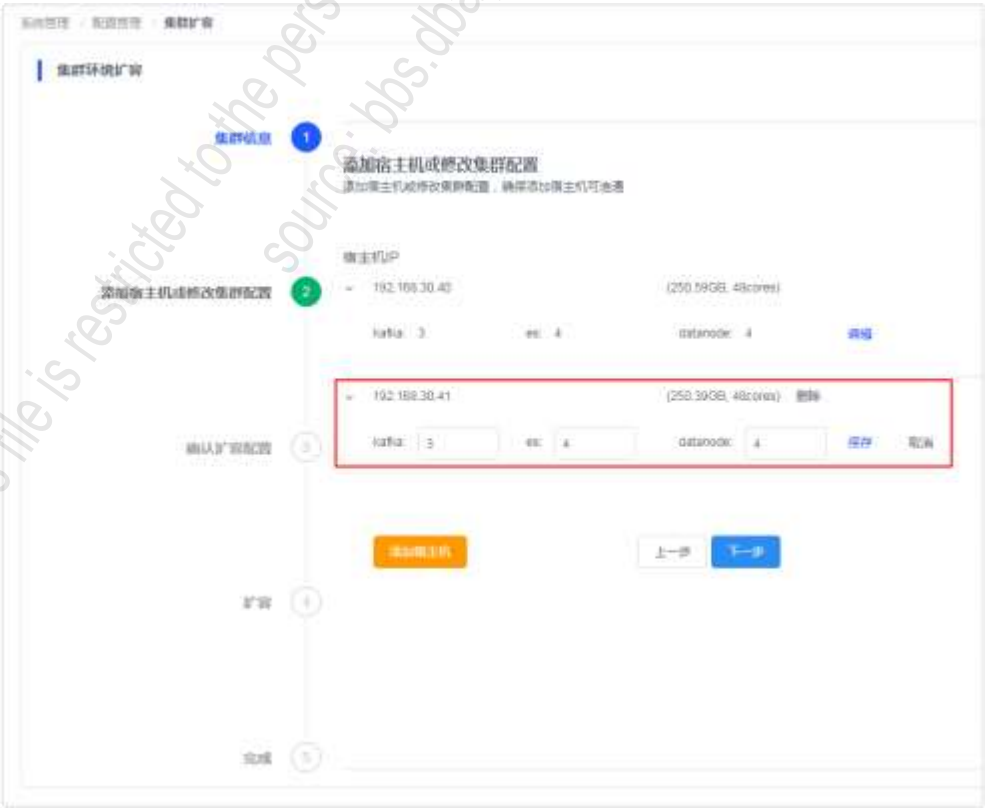
其中Kafka 节点最大配置范围是 3； ES 节点最大配置范围是 4； Datanode 节点最大配置是 4。 如下图所示。

3) 点击<**添加宿主机**>，展开宿主机 IP 及密码输入框， 输入正确的 IP 及 root 密码，点击<**保存**>，如果 IP 及密码错误，保存后会弹出相关提示；可以添加单台或者多台宿主机，如下图所示。



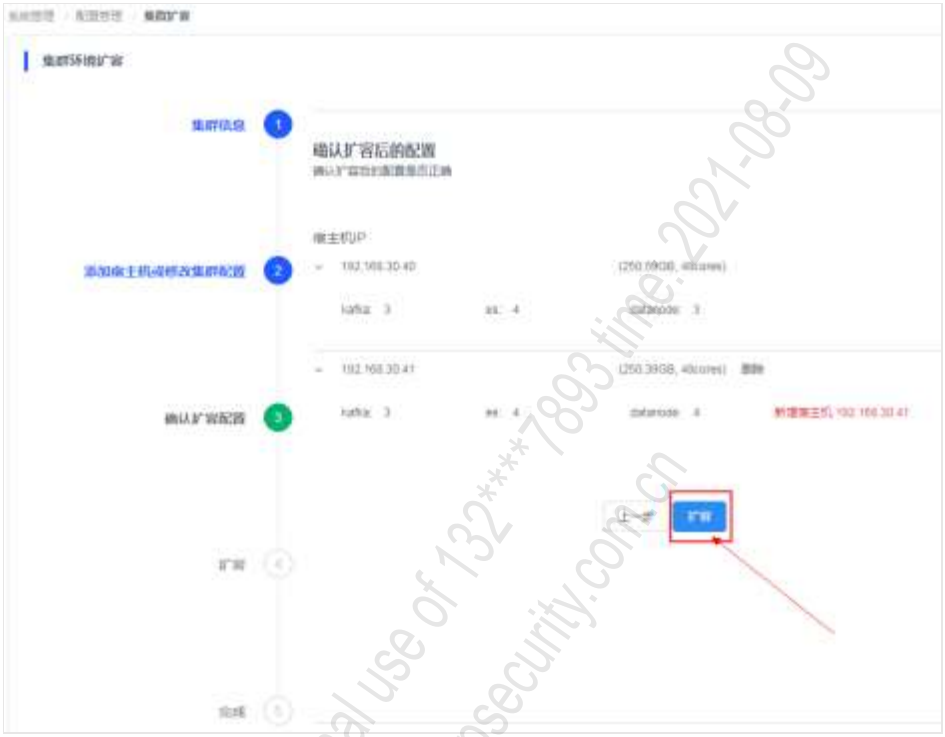
步骤5. 确认扩容配置。

添加宿主机后， 如果 IP 及密码正常， 展开集群配置， 可修改宿主机配置， 点击<**保存**>，可进入下一步操作， 如下图所示。



步骤6. 扩容配置。

点击<**扩容**>，进入集群扩容流程， 弹出扩容进度条及扩容日志信息， 等待扩容结束。如下图所示，扩容期间， 相关集群组件和服务会被停用（扩容成功后会自动启动）。



步骤7. 完成扩容。

当前进度条达到 100%， 扩容完成，可进入其他页面进行正常操作。 如下图所示。

步骤8. 检查流计算任务。

扩容完成后，流计算任务下各引擎会自动重启，以管理员用户登录大数据平台管理界面，选择“**系统管理▶任务管理▶流计算任务**”进入流计算任务页面， 检查各引擎是否重启成功， 如下图所示，引擎状态为**Running** 表示重启成功。

9.3 任务管理

任务管理包括流计算任务和定时任务两大功能，使用户能够实时了解引擎以及定时任务的执行动态。

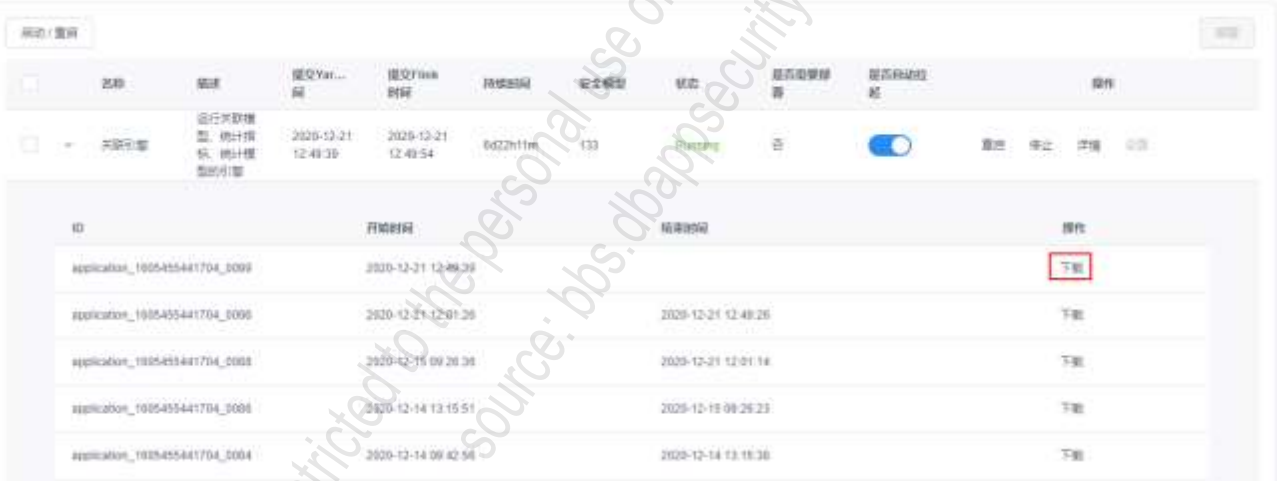
9.3.1 流计算任务

选择“**系统管理▶任务管理▶流计算任务**”进入流计算任务页面。

流计算任务以列表的形式展现， 如下图所示。列表显示名称、描述、提交Yarn 时间、提交Flink 时间、 持续时间、 安全模型、状态、是否需要部署、是否自动拉起、操作（重启、停止、详情）等信息。列表中有三条记录， 分别为**规则引擎**、**etl 引擎**、**统计引擎**。

9.3.1.1 历史状态

点击流计算任务名称前的 按钮， 可查看相关引擎的历史状态， 如下图所示， 点击操作列中的<**下载**>，即可下载引擎的日志信息。



9.3.1.2 相关操作

1) 启动/重启

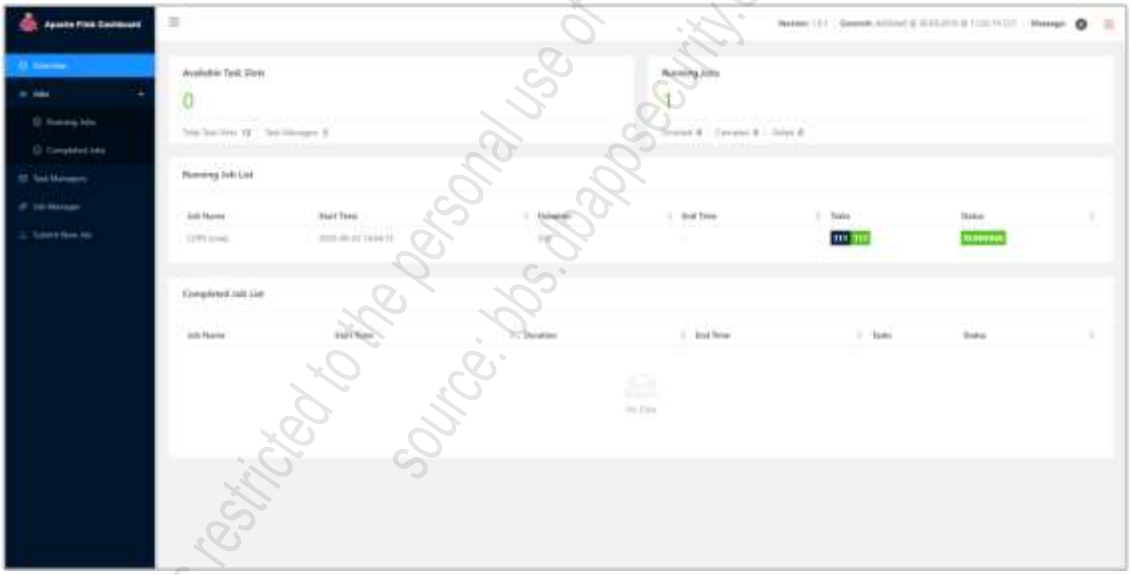
点击操作列中的<**启动/重启**>，也可勾选一条或多条，点击列表左上角的<**启动/重启**>，进行此操作时， 列表中引擎的状态变为 **Restarting**， 是否需要部署为否，且操作列中启动处于**加载中**状态， 不可操作，详情处于置灰状态， 不可点击，如下图所示：

2）停止

点击操作列中的<**停止**>， 进行此操作时， 列表中引擎的状态变为 **Stop**，是否需要部署保持不变， 且操作列中停止和详情处于置灰状态，不可点击， 如下图所示：

3）详情

点击操作列中的详情，新打开一个页面显示 job 详情，如下图所示。



4）实时消费

电脑键盘按键“ctrl+?”， 弹出<**实时消费**>按钮。当模型出现触发延迟或者数据出现入库延迟时， 点击相关引擎<**实时消费**>， 再点击右上方<**部署**>， 各引擎将实时消费数据， 如下图所示。

5）是否自动拉起

- “是否自动拉起”如果是开启状态， job10 分钟自动拉起；
- “是否自动拉起”如果是关闭状态， job 不会自动拉起。

6）部署

- 任一记录是否需要部署若为**是**，则<**部署**>按钮高亮。
- 配置变更时， <**部署**>按钮高亮， 鼠标浮动显示“**请点击部署,配置变更在分析引擎中生效**”。
- 部署过程中，按钮不可重复点击，鼠标浮动提示： “**部署中**”。
- 部署完成后，部署按钮置灰，鼠标浮动显示“**已保持最新状态**”。

9.3.1.3 Flink 监控

1）Flink 监控

电脑键盘按键“ctrl+?”， 弹出<**Flink 监控**>按钮。如下图所示。

点击<**Flink 监控**>进入 Flink监控页面， 展示各流计算任务流向框图、流计算任务运行配置、流计算任务资源分配等信息。如下图所示。

2）Flink 监控-流计算任务

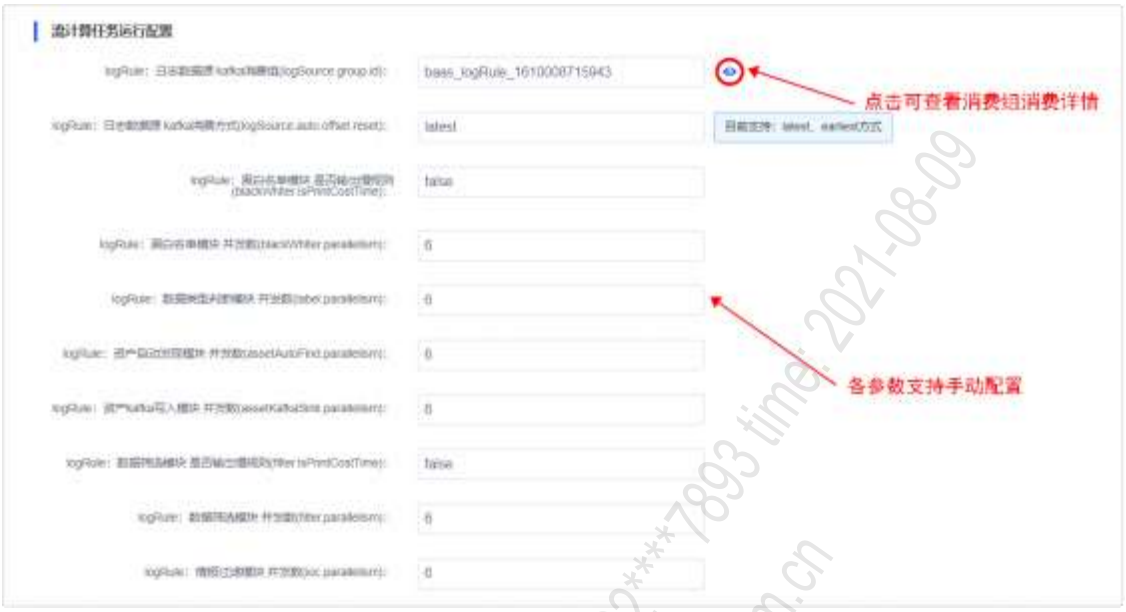
点击<**Flink 监控**>进入 **Flink 监控**页面， **流计算任务**可以下拉选择**规则引擎、 etl 引擎、统计引擎等。**

流计算任务选择不同引擎时， 展示不同流计算任务流向框图、流计算任务运行配置， 点击框图， 展示流计算任务指标监控。如下图所示。

3）Flink 监控-流计算任务运行配置

点击<**Flink 监控**>进入 **Flink 监控**页面， 流计算任务选择不同引擎时， 展示不同流计算任务运行配置， 支持手动修改各运行配置，部分配置支持查看消费详情。

流计算任务运行配置修改后， 需要点击页面最下方<**保存**>，再点击页面右上方<**部署**>，部署完成后， 配置生效。如下图所示。



4）Flink 监控-流计算任务资源分配

点击<**Flink 监控**>进入 **Flink 监控**页面， 流计算任务资源分配展示各引擎最大并发数、内存分配、引擎槽位等信息。

支持对内存分配、引擎槽位手动修改， 支持重置流计算任务资源分配。流计算任务资源分配修改后， 需要点击页面最下方<**保存**>，再点击页面右上方<**部署**>，部署完成后， 配置生效。如下图所示。

9.3.2 定时任务

选择 “**系统管理**▶**任务管理**▶**定时任务**”进入定时任务页面。

定时任务以列表的形式展现， 如下图所示， 列名包括任务名称、任务状态、触发类型、 cron 表达式、间隔时间等。

编辑

选择一条可编辑的定时任务， 点击<**编辑**>，进入编辑定时任务页面， 如下图所示， 任务名称置灰不可编辑，可对初始延迟时间、触发类型、时间间隔、任务描述进行编辑。

启用/停止

- 选择一条停止的定时任务，点击<**启用**>， 该定时任务会根据设置的 cron 表达式/时间间隔和最初延迟时间去调用对应的任务接口，调用任务接口后，最后运行时间更新。
- 选择一条启用的定时任务，点击<**停止**>， 该定时任务不会调用对应的任务接口。

9.4 系统管理

系统管理包括升级管理和许可证两大功能，可对系统进行版本及使用期限更新等操作。

9.4.1 升级管理

选择 “**系统管理**>**系统管理**>**升级管理**” ， 可查看版本信息、在线升级和查看升级历史。

版本信息

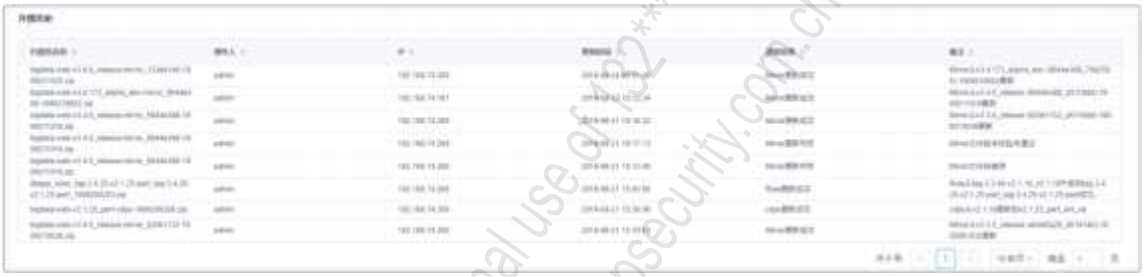
显示当前软件版本信息。如下图所示。

版本升级

点击 点击上传升级包 ，上传升级包， 升级包为.zip 格式，无需解压，如图所示。

升级历史

显示升级历史， 内容包括升级包名称、操作人、 IP、更新时间、更新结果和备注等信息。如下图所示。



9.4.2 许可证

功能简介

选择 “**系统管理**➤**系统管理**➤**许可证**” ， 进入**许可证**页面。

可查看系统许可证相关信息、 导出许可证申请文件、导入许可证等。

目前支持 AiLPHA 大数据智能安全分析平台及 Aiview 数据可视化中心。

许可证导出

展开**许可延期**， 点击 导出 ，可导出许可证申请文件。如下图所示。

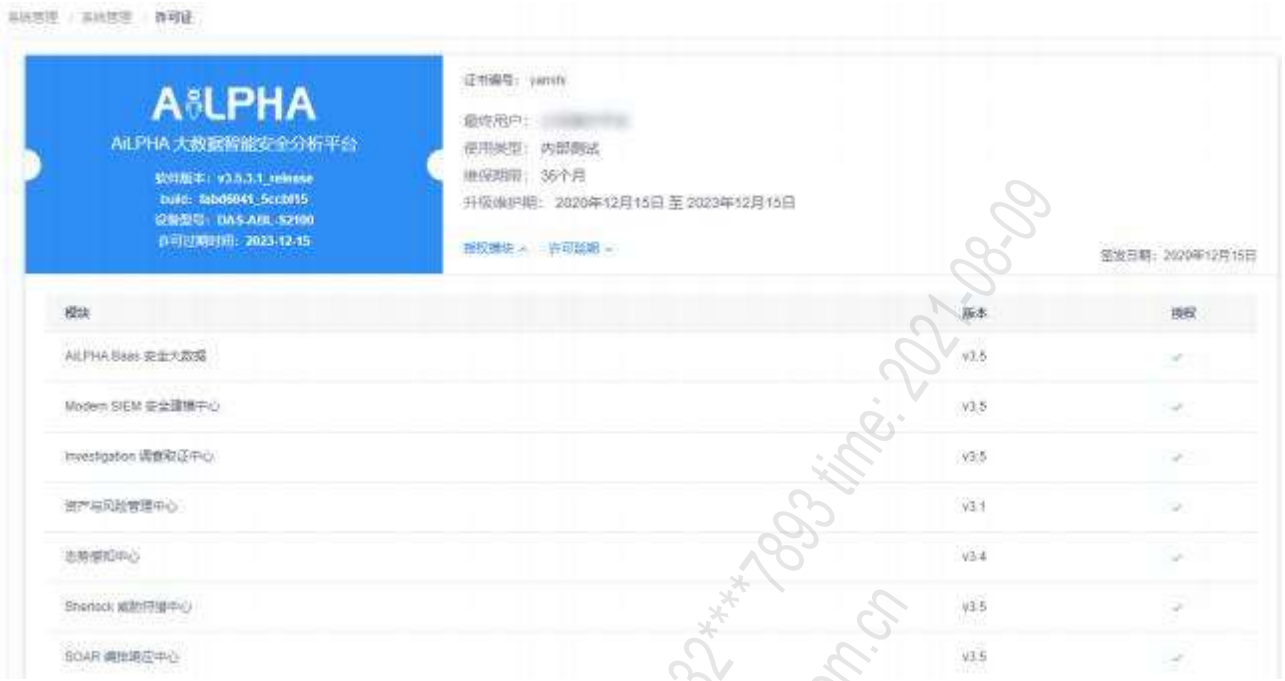
许可证导入

点击 导入 ，选择许可证文件， 导入许可证。如下图所示。

许可证书

导入许可后，页面可查看许可证信息。如下图所示。

点击**授权模块**，可展开并查看授权模块列表。如下图所示。



10. 用户权限管理

10.1 日志审计管理员

账户名/密码为： opadmin/略， 登录成功后的界面， 页面只提供一个操作日志查询功能菜单， 查询条件包括：操作用户名、操作者 IP、操作模块、操作类型、时间范围。同时界面提供操作日志的详细列表以及退出窗口。日志内容包括 AiLPHA 安全分析应用日志和 AiLPHA BaaS 安全大数据平台日志两部分。

操作界面如下图所示。

通过操作用户名、操作者 IP、操作模块、操作类型、时间范围进行条件检索， 方便审计日志。

10.2 权限管理员

账户名/密码为： useradmin/略，登录成功后的界面， 选择用户管理可以新增和删除用户；通过角色管理，可以新增和删除角色。

权限管理员具有角色管理和用户管理的权限。

10.2.1 角色管理

选择 “**权限管理▶角色管理**” 菜单进入角色管理界面，如下图所示。

系统内置 7 个角色， 分别为： 系统管理员、总部安全管理员、总部安服人员、分部安全管理员、分部安服人员、操作审计员和用户管理员。 不同的角色拥有不同的菜单权限。

系统内置的角色不可用修改或者删除。

1、 角色新增

点击 新增 按钮， 打开新增页面，如下图所示。

- 新增角色名称。
- 角色类型选择， 不同的角色类型拥有不同的数据权限。
- 菜单权限选择， 根据角色类型的不同，可选择的菜单权限也有所不同。

2、 角色编辑

点击操作列 按钮，支持角色编辑。内置角色不可编辑。

3、 角色删除

点击操作列 按钮，支持角色删除。内置角色不可删除。

10.2.2 用户管理

选择 “**权限管理>用户管理**” 菜单进入用户管理界面，如下图所示。

1、 用户新增

点击 新增 按钮， 打开新增页面，如下图所示。

- 基本信息包括： 用户名、真实姓名、手机号码和邮箱地址。其中用户名、真实姓名必填。
- 组织架构： 下拉可选择用户自定义的组织。
- 角色信息： 不同的组织架构可选择的角色也不同。
  - 组织架构为总部时， 只能选择角色类型为系统管理员、总部安全管理员、总部安服人员的角色。
  - 组织架构为分部时， 只能选择角色类型为分部安全管理员、分部安服人员的角色。
  - 用户角色选择使用户拥有角色赋予的菜单功能。
- 登录绑定： 默认关闭，可开启。类型： IP 地址、 IP 区间、子网掩码。
- 完成账户创建， 自动发送邮件， 默认密码为 do*JKfn7PK。未配置了邮件服务器或未配置了用户邮箱地址，不发送邮件。

2、 用户编辑

点击操作列 按钮，支持用户编辑。内置用户不可编辑。

3、 用户删除

点击操作列 按钮，支持用户删除。内置用户不可删除。

4、 重置密码

点击操作列 按钮，支持用户密码重置。

5、 解锁

点击操作列 按钮，支持用户解锁

10.3 认证安全

以权限管理员 **useradmin** 用户登录系统， 可以进行认证安全设置。

10.3.1 登录安全设置

登录安全设置如下图所示。

10.3.2 密码策略设置

密码策略设置支持密码最小长度、密码最大长度、密码有效期、密码修改提醒时间、密码复杂度及密码预期处理方式（首次登录是否强制修改密码）。如下图所示。

10.3.3 水印设置

水印设置模式有 IP、用户名、系统名称。如下图所示。

11. 术语和缩略语

术语	解释
AI	人工智能（ Artificial Intelligence ），英文缩写为 AI。它是研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的一门新的技术科学。
Ambari	Apache Ambari是一种基于 Web 的工具， 支持 Apache Hadoop 集群的供应、管理和监控。Ambari 已支持大多数 Hadoop 组件，包括HDFS、MapReduce、Hive、Pig、Hbase、Zookeeper、Sqoop 和 Hcatalog 等。
APT	APT（Advanced Persistent Threat）攻击，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。
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。
EPS	每秒可以采集或者处理的事件数量（ Event per Second ），用来表示设备数据采集和处理性能的一个指标。
ES	Elasticsearch 是一个基于Lucene 的搜索服务器。它提供了一个分布式多用户能力的全文搜索引擎， 基于RESTful web 接口。 Elasticsearch 是用 Java 语言开发的， 并作为Apache 许可条款下的开放源码发布，是一种流行的企业级搜索引擎。
Kibana	Kibana 是为 Elasticsearch 设计的开源分析和可视化平台。你可以使用 Kibana 来搜索，查看存储在 Elasticsearch 索引中的数据并与之交互。你可以很容易实现高级的数据分析和可视化， 以图表的形式展现出来。
SSL	SSL(Secure Sockets Layer，安全套接字协议)及其继任者传输层安全（ Transport Layer Security， TLS ）是为网络通信提供安全及数据完整性的一种安全协议。TLS 与 SSL在传输层与应用层之间对网络连接进行加密。
UEBA	UEBA（User Entity Behavior Analysis，用户及实体行为分析），是由 UBA（用户行为分析）概念演进而来。 UBA 最初的提出， 是为了应对日益增长的内部（人员）威胁。但是，更多的 IT 资产和设备， 即实体（Entity）的概念被渐渐引入。通过 UEBA，异常行为分析不仅可以发现内部失陷主机， 还能对外部网络攻击以及渗透成功后的内部横向移动有更强的洞察力。
VirusTotal	VirusTotal，是一个提供免费的可疑文件分析服务的网站。

术语	解释
WAF	Web 应用防护系统（ Web Application Firewall，简称： WAF），也称网站应用级入侵防御系统、 Web 应用防火墙。 WAF 是通过执行一系列针对 HTTP/HTTPS 的安全策略来专门为 Web 应用提供保护的一款产品。
容器技术	容器技术可以有效的将单个操作系统的资源划分到孤立的组中， 以便更好的在孤立的组之间平衡有冲突的资源使用需求，这种技术就是容器技术。
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。