

# TDP 用户手册 3.1.1

2021.4

TDP

# 前言

TDP 通过分析网络镜像流量，基于规则检测、机器学习模型、大数据技术，可以实时感知用户系统的安全威胁，检测到外部攻击、内网渗透以及失陷破坏的威胁。同时支持对网络内部的资产进行梳理，帮助用户建立全局安全意识。

本文档介绍了微步在线威胁感知平台 (Threat Detection Platform, 以下简称“TDP”) 的使用方法。帮助安全运营工程师了解产品功能, 熟悉产品用法, 以满足实际使用需求。

本文档适用对象为普通用户、安全运营人员、实施工程师。本文档假设读者具备如下相关网络和安全知识:

网络拓扑结构

网络协议 (DNS、HTTP、TCP、UDP、DHCP)

威胁情报

网络沙箱原理

如需获得更多信息, 请联系我方支持团队([contactus@threatbook.cn](mailto:contactus@threatbook.cn))。

# 一、监控

TDP 监控功能包含“首页”、“大屏”和“系统运行状态”三个功能模块页面。

首页功能为用户提供基础的系统安全评级，展示整体的安全概况；

大屏页面，支持用户展示需求，友好的展示当前系统的攻防态势，以及威胁检出情况；

系统运行状态页面，支持用户进行系统运行状态诊断，并对当前系统的流量、处理量、网口状态做了友好展示，帮助用户确认系统运行状态，排查问题。

## 1.1 首页

用户登录后，默认来到首页页面，首页时间段默认展示近 7 天，用户可以自行调整为“24 小时”或者“近 30 天”，用户可通过切换业务组查看不同组下设备的告警总览。

页面路径：

从导航菜单进入监控页面（登录系统默认来到此页面）

选择“监控-首页”子菜单项

系统首页为用户提供 TDP 检测到的安全概况，分别从以下角度呈现：



### 1.1.1 运行状态

TDP 在此展示系统的运行状态，包含以下信息：

【当前处理量】展示了系统的实时处理速度。

【已接流量】展示了系统接入的流量路数，鼠标浮动上去可以看到具体的接入信息。

【已接日志】展示 TDP 接入 syslog 的数量，鼠标浮动上去可以看到具体的接入的日志信息。

【已接入 Agent】展示 TDP 接入 Agent 的数量，点击页面跳转进入终端取证页面，用户可以查看所有接入的 Agent。

【已开启检测功能】展示系统当前开启的检测功能数量，鼠标浮动上去可以看到具体开启的功能信息。

### 1.1.2 整体安全态势

TDP 会对当前系统所选时间内的安全情况做一个评级，用户可以视情况修改评级，修改后 24h 内生效。



关键指标如下：

【已失陷主机】展示了系统内部已经失陷的主机数量。

【告警主机】展示了受到威胁的主机数量。（告警主机中也展示了已处理主机数量）

【已处理主机】展示已处理的告警主机数量

【外部攻击成功】展示了所选事件范围内，系统遭受外部攻击的攻击种类数量

【针对性攻击】展示了系统遭受的针对性攻击的数量。

【Webshell】展示了遭受 Webshell 攻击的数量

【建立远程连接】展示了所选时间范围内，系统被黑客控制失陷的事件，以及被黑客操纵向外发起攻击进行破坏的事件。

【其他告警及风险】点击可查看所有告警数据及风险数据

【操作】以上核心指标，用户均可以点击，进入详情页面，详细了解相关的内容。

### 1.1.3 攻击链

TDP 为用户提供威胁告警的攻击链可视化展示。在威胁分类图中，用户首先应该关注是否存在漏洞利用攻击成功的威胁种类，若存在攻击成功，则应该尽快处理攻击成功事件。攻击链从两种威胁来源做了可视化，一种是渗透攻击，另一种是感染病毒木马等。



渗透反映了互联网对系统内部的攻击情况，统计展示了外对内的攻击类型数量，包括以下类型：

【侦查】来自外网的所有侦查扫描事件种类。

【漏洞利用事件】来自外网的所有漏洞利用攻击事件种类。

【漏洞利用成功的事件】会使用红色标签标志在漏洞利用类型数量之后。

【内网渗透】统计了系统内部的所有横向攻击类型种类。

感染的路径，可能包括以下类型

【恶意样本】系统下载或者传播恶意文件，以及系统尝试下载恶意文件行为

【命令与控制】包含以下恶意行为：

系统连接远控地址，该连接通常由木马和病毒等恶意程序发起；

系统进行 DGA 地址连接，意味着内网存在木马或者病毒等恶意程序；

内网主机发出符合木马特征的恶意流量；

内网主机对外流量中发现了远程管理工具相关的通信协议，可能正在使用远程控制工具；

内网主机连接新发布域名，新发布域名(Newly Observed Domain,NOD)是刚刚在全球 DNS 服务上注册和发布的域名。黑客经常使用 NOD 域名来发送垃圾邮件，进行恶意软件传播，组建僵尸网络或者作为远控服务器地址；

发现僵尸网络行为，通常为机器被控后利用计算机资源进行其他非法操作，如对外发起 DDoS、对外发送垃圾邮件等。

【挖矿】内网主机主动连接或查询了加密货币矿池地址，对应主机上可能正在执行挖矿程序。

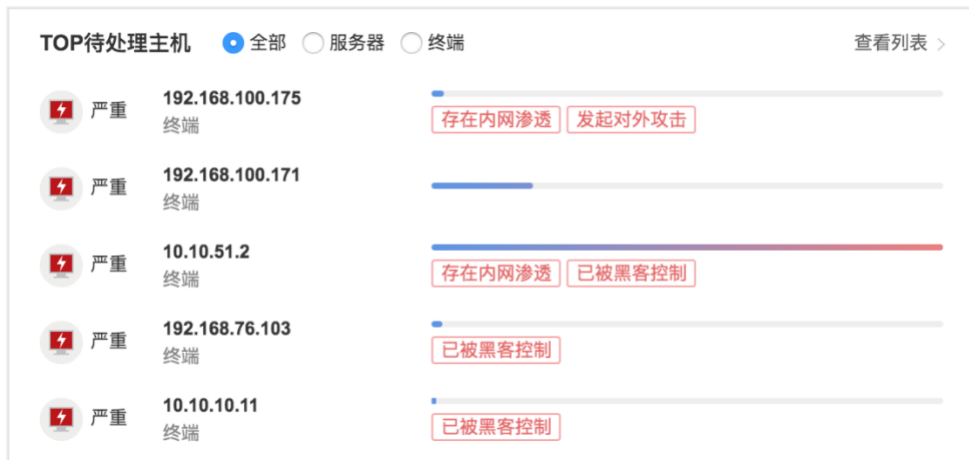
通过

【数据窃取】内网主机发现数据窃取行为。

【系统内部对外攻击】内网主机发现对外攻击行为，有可能已经成为黑客跳板机。

【操作】在威胁类型中，每一种威胁类型，都支持点击下钻，点击后会展示所选威胁类型的具体事件列表，用户可以继续追踪相应的事件详情。

## 1.1.4 待处理主机



【TOP 待处理主机】模块展示了所选时间范围内，主机检测到告警，并且安全运营人员未处理的主机，按照严重级别进行了排序，用户应该首先关注严重级别较高的主机。

【待处理主机模块】展示内容包括主机的 IP，主机的类型（服务器或者终端）、告警严重级别、以及主机的状态。用户点击对应的主机 IP，就可以跳转到此主机的主机详情中，从而详细查看主机的告警状况，同时可以在主机详情页面进行告警处理。

【操作】此模块支持对服务器或者终端进行筛选，默认展示全部待处理主机，点击右上角“查看列表”按钮后，页面跳转到所有待处理主机页面，用户可以在此页面查看全部告警主机，然后进行处理。

## 1.1.5 威胁事件和趋势



【TOP 威胁趋势】模块展示了所选时间范围内的告警趋势，并展示了 TOP4 严重程度的威胁事件。

【威胁事件】展示内容包括：告警时间、威胁类型（包括外部攻击、失陷破坏、内

网渗透)、攻击类型、攻击名称、严重程度以及涉及到的服务器和终端数量。

【操作】鼠标滑动到对应的服务器和终端数量上，可以看到具体的机器 IP。

## 1.1.6 资产与服务



【资产与服务】模块展示了用户系统检测到的资产和服务，系统通过一段时间的流量监听和判断以后，会逐步的梳理以下内容：服务器 IP 资产、终端 IP 资产，全部服务列表和最近 3 天新上线服务列表。

【操作】点击对应的标签，页面会跳转到对应的“资产&风险-资产和服务”页面，详细展示具体信息。

## 1.1.7 登录风险



【登录接口】TDP 自动识别系统内部的登录接口。

【弱密码】统计系统中用户使用的弱密码组数。

【正常登录/撞库比例】统计系统内所有登录接口正常登录与撞库的比例，从而体现了用户登录接口的安全状况。

点击【登录接口】、【正常登录或者撞库】，跳转到“风险-登录风险-登录接口”页面，支持查看系统内部所有登录接口，以及登录接口被撞库的情况；



点击【弱密码】标签，跳转到“风险-登录风险-弱密码”页面，用户可以查看系统内有哪些用户使用了弱密码。

### 1.1.8 接口风险

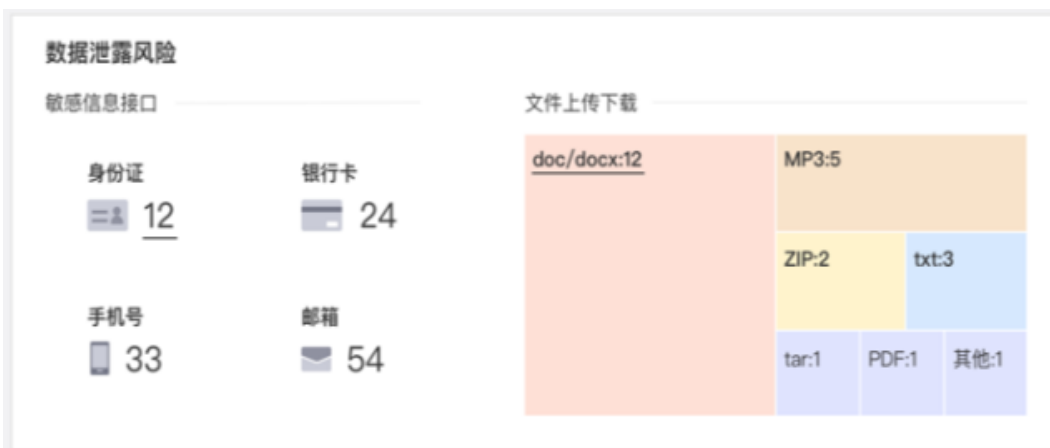
API风险			
接口名称	PV数量	UV数量	API总数
192.168.100.175...../lessonverview.mvc	1367665	1367665	137 /个
192.168.100.175...../lessonverview.mvc	763454	737463	
192.168.100.175...../lessonverview.mvc	5567	7865	
192.168.100.175...../lessonverview.mvc	4345	3456	
192.168.100.175...../lessonverview.mvc	344	737	

【API 风险】模块展示 TDP 监控到的系统内部的开放接口情况。

【API 总数】为监控到的接口总个数，点击可以查看具体的接口信息。

使用列表的形式展示了访问量 TOP5 的接口，包括以下内容：接口名称，接口的 PV 数量，接口的 UV 数量。

### 1.1.9 数据泄露风险



数据泄露风险展示了 TDP 对系统内部敏感信息泄漏接口，以及文件上传下载的监控结果。

【敏感信息接口】展示了系统检测到的明文传输身份证号码、银行卡、手机号和邮箱这几类敏感信息的接口，用户点击可以看到对应的接口详情。能够帮助用户梳理系统内部敏感信息存在泄漏风险的点。

【文件上传下载】展示了系统内部被下载文件类型的分布，可以帮助用户发现异常的文件上传下载行为，点击后可以跳转到“文件风险”页面，进行文件上传下载行为的详细分析。

## 1.2 大屏



页面路径：

- 1.从导航菜单进入监控页面
- 2.选择“监控-大屏”子菜单项，页面自动全屏，同时展示大屏相关的内容。

TDP 大屏满足安全态势实时展示的需求，大屏展示以下内容：

【核心指标】包括告警主机数量、威胁事件数量、告警次数、已安装 Agent 数量，用户可以根据这些指标直观的感受当前的安全态势。

【自转地球】展示了用户自身的地理位置，通过攻击飞线展示了收到攻击的来源。

【内网关系图】展示了用户系统内部的告警分布情况。

【告警主机】列表展示了当前严重程度最高的 TOP5 告警主机，展示内容包括主机 IP 以及主机告警威胁类型。

【恶意访问地址】列表展示了当前系统内连接的恶意地址，展示了恶意地址的 URL、所属地理位置、严重级别、告警次数的比例。

【TOP5 攻击来源】实时展示了攻击系统的来源 IP，展示内容包括攻击 IP、地理

位置、严重级别。

【实时攻击飞线】实时展示了互联网对系统内部的攻击，展示内容包括攻击名称、受害主机数量、严重级别。

【攻击链】展示了攻击在攻击链各个阶段的分布情况。

【实时流量】滚动展示系统当前的处理的流量，展示内容包括：源 IP、目的 IP 或者恶意地址、以及协议。

【24 小时输入趋势】展示了系统 24 小时内，接入的流量变化，用户可以分析系统流量是否正常。

【24 小时告警趋势】展示了 TDP 对系统镜像流量分析，产生的告警趋势。

## 1.3 系统运行状态

### 运行状态

 健康度: **100%** 最近一次检测完成时间: 01月13日 16:19:34

 系统启动 底层启动时间: 2020-01-09 15:19:52

 IOC更新

#### 硬件状态

-  CPU正常
-  内存正常
-  磁盘正常

#### 输入模块状态

 已开启1项

-  'unix\_socket\_input'正常

#### 存储状态

-  ES存储状态: yellow

#### 服务状态

-  核心服务: 正常, 服务启动时间 2020-01-09 15:19:52 [重启服务](#)
-  后台服务: 正常, 服务启动时间 2019-12-25 16:44:12 [重启服务](#)
-  流量分析服务: 正常, 服务启动时间 2019-12-25 11:23:27 [重启服务](#)
-  存储服务: 正常, 服务启动时间 2019-10-15 16:30:25 [重启服务](#)
-  文件引擎: 启动中 [重启服务](#) [查看日志](#)
-  web服务器: 正常, 服务启动时间 2019-12-25 11:41:11 [重启服务](#)
-  数据库: 正常, 服务启动时间 2019-10-15 16:30:19 [重启服务](#)
-  高速缓存: 正常, 服务启动时间 2019-10-15 16:30:19 [重启服务](#)

#### 云端连接

-  https://static.threatbook.cn连接正常
-  https://static-img.threatbook.cn连接正常

页面路径:

- 1.从导航菜单进入监控页面
- 2.选择“监控-系统运行状态”子菜单项

系统运行状态页面, 为用户展示 TDP 当前的运行状态以及关键的系统指标, 帮助用户检测 TDP 运行情况, 如有异常快速定位原因。

【运行状态】模块在用户进入此页面后, 自动进行系统诊断, 诊断后会告知用户诊

断结果，用户也可以手动点击“重新诊断”按钮重测。

运行状态页面会测试以下内容：

系统状态：检测系统状态，展示健康度

系统启动时间

IOC 是否更新

云端连接状态：是否连接正常

硬件状态：CPU、内存、磁盘

输入模块状态

存储状态：ES 存储状态

服务状态：如果遇到某些服务异常，可以尝试手动重启

【CPU 使用率】展示了 CPU 实时使用率以及近 72 小时内的 CPU 使用情况，用户遇到异常可以查看 CPU 实时使用情况做异常排除，三天内故障可以通过 72 小时使用率进行 CPU 异常状况排查。

【内存使用率】展示了内存实时使用率以及近 72 小时内的内存使用情况，用户遇到异常可以查看内存实时使用情况做异常排除，三天内故障可以通过 72 小时使用率进行内存异常状况排查。

【磁盘使用率】展示了磁盘实时使用率，用户遇到异常可以查看磁盘实时使用情况做异常排除。

【实时网卡流量】展示了所有网口的 FLOW 和 PACKET 的实时流量状况，可以通过下拉菜单切换网卡查看。

【历史网卡流量】展示了所有网口的 FLOW 和 PACKET 的历史流量状况，可以通过下拉菜单切换网卡查看，时间范围可以通过时间控件进行调整。

【实时处理量】展示了 TDP 的实时处理量，用户查看此模块可以初步判断系统处理流程是否正常。

【历史处理量】展示了 TDP 近 3 天内，TDP 对各个协议的解析趋势。

【输入模块】展示了系统的主要输入模块状态，数据为每 24 小时累计值，每 10 分钟更新一次。

【检测模块】展示了系统的主要检测模块状态，数据为每 24 小时累计值，每 10 分钟更新一次。

【输出模块】展示了系统的主要输出模块状态，数据为每 24 小时累计值，每 10 分钟更新一次。

## 二、威胁

威胁模块在威胁的视角，为用户展示当前系统的威胁事件以及告警主机，同时提供处置建议和处理流程。告警主机以主机的维度展示当前系统告警，并且提高主机处置功能；威胁事件分为外部攻击、内部攻击、失陷破坏以及智能聚合。接下来做详细说明：

### 2.1 外部攻击

#### 2.1.1 外部攻击列表

页面路径：

- 1.从导航菜单进入威胁页面（登录系统默认来到此页面）
- 2.选择“威胁-外部攻击”子菜单项，来到外部攻击页面



【严重性分布】TDP 对所选时间范围内的所有外部攻击事件，统计事件严重程度分布情况。

【攻击成功】TDP 对所选时间范围内的所有外部攻击事件，统计攻击成功、攻击结果未知和攻击失败的比例。



【TOP 攻击者】TDP 将所选时间范围内，所有的外部攻击事件涉及到的攻击者，根据告警次数做了排列，展示攻击最为频繁的攻击者。

【筛选功能】TDP 支持对外部攻击列表做多种筛选，包括以下条件：时间范围、严重级别、是否攻击成功。

【搜索功能】支持根据主机 IP、主机名称、域名、告警名称和目标地址进行搜索。

【外部攻击列表】列表中展示包括以下内容：事件中最近一次攻击的告警时间、严重级别、攻击阶段、攻击名称、告警主机、攻击 IP、事件中告警检出次数、攻击成功次数。

## 2.1.2 外部攻击详情页

使用方法：

1.从导航菜单进入威胁页面

2.选择“威胁-外部攻击”子菜单项，点击对应的威胁事件列表中，对应威胁的“查看详情”按钮；来到此威胁事件详情页面。

攻击者(70)	时间	严重级别	检出	内网主机	目标地址
103.233.156.168 印度尼西亚-印度尼西亚 38 攻击 成功 11	2019/09/19 15:58:15	中	MySQL注入	192.168.100.175	192.168.100.175:9070/sqli-labs/fess-5/
103.233.156.58 印度尼西亚-印度尼西亚 37 攻击 成功 9	2019/09/19 15:58:15	中	MySQL注入	192.168.100.175	192.168.100.175:9070/sqli-labs/fess-5/
103.58.151.45 泰国 泰国 33 攻击 成功 9	2019/09/19 15:58:15	中	MySQL注入	192.168.100.175	192.168.100.175:9070/sqli-labs/fess-5/
103.58.151.90 泰国 泰国 39 攻击 成功 13	2019/09/19 15:58:15	中	MySQL注入	192.168.100.175	192.168.100.175:9070/sqli-labs/fess-5/
107.183.23.82 美国 加利福尼亚州 洛 34 攻击 成功 7	2019/09/19 15:58:15	中	MySQL注入	192.168.100.175	192.168.100.175:9070/sqli-labs/fess-5/
110.53.247.101 攻击 成功	2019/09/19 15:58:16	攻击成功	MySQL注入	192.168.100.175	192.168.100.175:9070/sqli-labs/fess-5/

在详情页开头，系统以卡片展示对应威胁事件的主要信息，包括：严重程度、威胁名称、攻击者数量、受害者数量、告警最早发现时间、告警最近发现时间、已处理主机个数、未处理主机个数。

在详情页面中，系统通过以下角度描述威胁事件：

## 威胁发现

点击“威胁发现”TAB，来到威胁发现模块：

在威胁发现模块，系统对所选的外部攻击事件，展示具体的告警信息，帮助用户溯源追踪。包括以下功能：

【筛选与导出】可以根据内网主机、结果进行筛选，并且筛选后的结果进行导出。

【检出明细】点击“检出明细+”按钮可以展示此威胁事件的告警趋势图。

【攻击者列表】系统将次事件中涉及到的攻击者列出，用户点击具体的攻击者 IP，可以查看此攻击 IP 之下的具体告警。

【告警详情】用户点击攻击者列表中的具体 IP，可以看到此攻击 IP 的告警信息，每一条告警信息卡片中包括以下内容：告警事件、检出信息（攻击阶段、攻击类型、威胁名称、威胁描述）、内网主机、目标地址。告警信息卡片可以通过点击展开，展开后依次展示攻击示意图、攻击信息、原始请求日志以及 PCAP 包。这四种信息对于不同的协议，包含的内容不同，如有缺某一项为正常现象。

点击其中的“全屏显示”按钮，用户可以全屏查看协议内容。

## 主机

【主机】模块展示此攻击事件涉及到的具体主机，主要信息有：内网主机 IP、资产名称、关联域名、主机的当前威胁检出次数、最近一次检出事件，用户可以在此模块对已经处理的主机，做“已处理”标记。

用户点击“导出”按钮，可以导出此事件相关的所有主机 IP。

## 外部攻击 IP

【外部攻击 IP】模块展示此攻击事件涉及到的外部攻击 IP，主要信息有：外部攻击 IP、地理位置、IP 相关的微步情报标签、外部攻击 IP 相关的当前威胁检出次数、最近一次告警检出时间。

用户点击“导出当前表格”按钮，可以导出此事件相关的所有外部攻击 IP。

## 终端取证结果

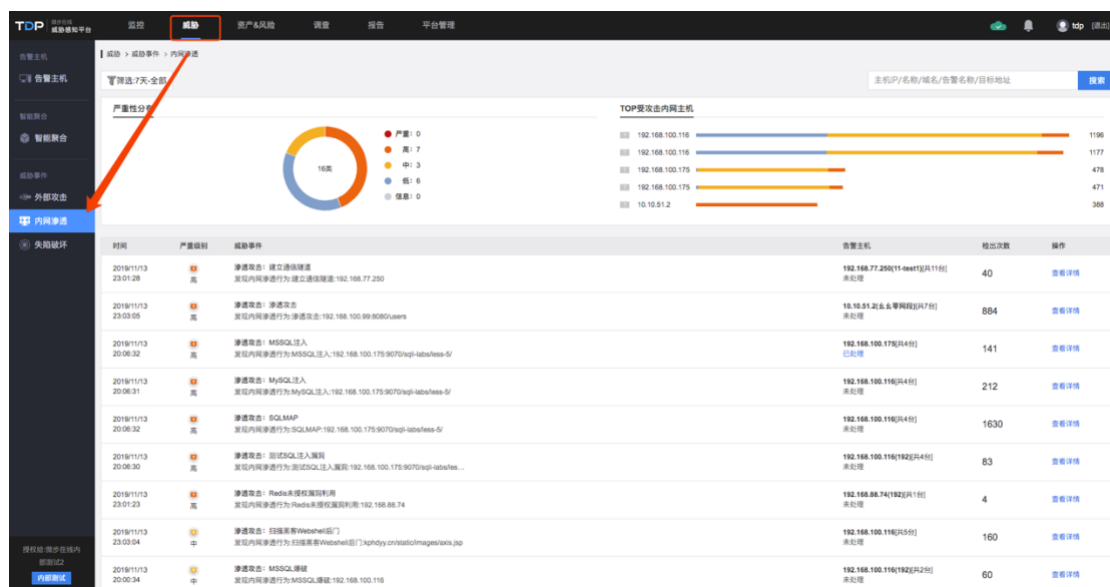
展示对应威胁事件已安装的 Agent 的终端取证结果。

## 2.2 内网渗透

### 2.2.1 内网渗透列表

页面路径：

- 1.从导航菜单进入监控页面（登录系统默认来到此页面）
- 2.选择“威胁-内网渗透”子菜单项，来到内部攻击事件页面。



【严重性分布图】TDP 对所选时间范围内的所有内网渗透事件，统计事件严重程度分布情况。

【TOP 受攻击内网主机图】TDP 将所选时间范围内，所有受到内部攻击的内网主机，根据告警次数做了排列，展示攻击最为频繁的内网主机。

【筛选功能】TDP 支持对内网渗透列表做多种筛选，包括以下条件：时间范围、严重级别、是否攻击成功。

【搜索功能】同时支持根据主机 IP、名称、域名、告警名称和目标地址进行搜索。

【内部攻击事件列表】展示了内部攻击事件的基本信息，包括：事件中最近告警的时间、严重级别、事件名称、告警主机、检出告警次数。点击“查看详情”按钮，用户来到内部攻击详情页面。

## 2.2.2 内网渗透详情页

使用方法：

1.从导航菜单进入威胁页面

2.选择“威胁-内网渗透”子菜单项，点击威胁列表中威胁的“查看详情”按钮，来到威胁事件详情页面。

The screenshot displays the 'Internal Network Penetration' details page. At the top, a summary card provides key information: '威胁名称: MS14068 Attack', '严重级别: 严重', '告警主机: 192.168.100.143等共3台主机', '最早发现时间: 2019-09-11 19:04:53', '已处理: 0台', '最近发现时间: 2019-09-11 19:52:58', and '未处理: 3台'. Below this, a table lists threat actions with columns for '威胁行为', '内网主机', and '检出次数'. A detailed view of an event on 2019-09-11 19:52:58 shows a '用户认证失败' (User authentication failed) event with a '成功' (Success) status, involving a '未知用户' (Unknown user) and target host 192.168.100.143. The event details include the protocol (TCP), source IP (54079), and target IP (192.168.100.141).

在详情页开头，系统以卡片展示对应内网渗透事件的主要信息，包括：严重程度、威胁名称、告警主机、告警最早发现时间、告警最近发现时间、已处理主机个数、未处理主机个数。

在详情页面中，系统通过以下角度描述威胁事件：

### 威胁发现

在威胁发现模块，系统对所选的内网渗透事件，展示相关的告警信息，包括以下信息：

【筛选】可以根据时间、告警主机进行筛选。

【检出明细】点击“检出明细”按钮可以展示此威胁事件的告警趋势图。

【告警列表】展示了内网渗透具体告警的严重级别、威胁行为描述、内网告警主机以及检出次数和成功次数。

【告警详情】用户点击攻击者列表进行展开，可以具体的告警信息，每一条告警展开后依次展示攻击示意图、攻击概况、原始请求日志以及 PCAP 包。这四种信息，对于不同的协议，包含的内容不同，如有缺某一项为正常现象。

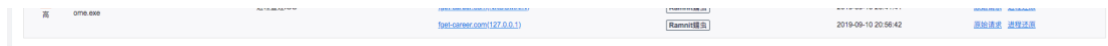
## 主机

【主机】模块展示此攻击事件涉及到的具体主机，主要信息有：内网主机 IP、资产名称、关联域名、主机的当前威胁检出次数、最近一次检出时间，用户可以在此模块对已经处理的主机，做“已处理”标记。

用户点击“导出”按钮，可以导出此事件相关的所有主机 IP。

## 终端取证结果

展示对应威胁事件中，已安装的 Agent 的终端取证结果。



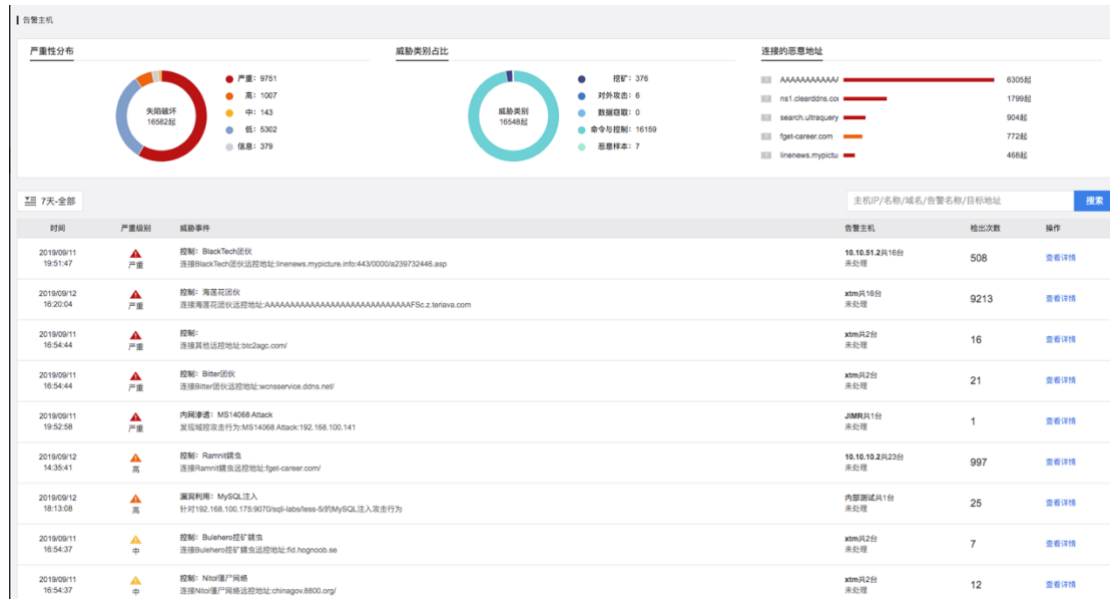
## 2.3 失陷破坏

威胁中的失陷破坏功能模块，展示了系统内部已经被病毒木马感染，导致访问恶意地址的威胁事件，以及主机已经被攻击者攻陷并且开始向外发起攻击的威胁事件。

### 2.3.1 失陷破坏事件列表

使用方法：

- 1.从导航菜单进入威胁页面（登录系统默认来到此页面）
- 2.选择“威胁-失陷破坏”子菜单项，来到失陷破坏威胁事件详情页面。



【严重性分布】TDP 对所选时间范围内的所有失陷破坏事件，统计事件严重程度分布情况。

【威胁类别占比】TDP 将所选时间范围内，所有失陷破坏事件的威胁类型占比，进行统计，用户可以直观看到失陷破坏事件中的主要威胁类型。

【连接的恶意地址】TDP 将所选时间范围内，对所有失陷破坏事件向外连接的恶意地址进行统计，用户可以直观看到失陷破坏事件中的主要恶意地址。

【筛选功能】TDP 支持对失陷破坏列表做多种筛选，包括以下条件：时间范围、严重级别、近看攻击成功。

【搜索功能】TDP 支持根据主机 IP、主机名称、域名、告警名称和恶意目标地址对失陷破坏事件进行搜索。

## 2.3.2 失陷破坏详情页

使用方法：

1.从导航菜单进入威胁页面

2.选择“威胁-失陷破坏”子菜单项，点击威胁列表中对应威胁事件的“查看详情”按钮，来到失陷破坏威胁事件详情页面。

在详情页开头，系统以卡片展示对应失陷破坏事件的主要信息，包括：严重程度、威胁名称、告警主机数量、告警最早发现时间、告警最近发现时间、已处理主机数、未处理主机数。

The screenshot shows the ThreatBook interface for a threat event. At the top, there's a header with '威胁发现' (Threat Discovery) and '连接远控地址: 海莲花团伙' (Connect remote control address: Sea Lotus group). Below this, there's a table of threat events. The table has columns for '时间' (Time), '类型' (Type), '协议' (Protocol), and '行为描述' (Behavior Description). The events listed are all 'DNS查询' (DNS Query) with '成功' (Success) status. To the right of the table, there's a detailed view of a specific event, showing 'DNS查询' details, host information (192.168.76.126), and PCAP data.

在详情页面中，系统通过以下角度描述失陷破坏威胁事件：

## 威胁发现

在威胁发现模块，系统对所选的失陷破坏事件，展示具体的告警信息，包括以下信息：

【筛选】可以根据告警主机、IOC 进行筛选。

【告警趋势】点击“检出明细”按钮可以展示此威胁事件的告警分图。

【告警列表】展示了失陷破坏的告警主机，以及具体告警的基本信息，包括：告警主机、严重程度、威胁描述、检出次数和联通次数。

【告警详情】用户点击攻击者列表进行展开，可以具体的告警信息，每一条告警展开后依次展示攻击示意图、攻击信息、原始请求日志以及 PCAP 包。这四种信息，不同的协议，包含的内容不同，如有缺某一项为正常现象。

## 主机

【主机】模块展示此失陷破坏威胁事件涉及到的具体主机，主要信息有：内网主机 IP、资产名称、关联域名、主机的当前威胁检出次数、最近一次检出时间，用户可以在此模块对已经处理的主机，做“已处理”标记。



IP	主机名称	IP	2019-11-13 10:54:47	导出
10.10.221.8		130		

用户点击“导出”按钮，可以导出此事件相关的所有主机 IP。

## IOC

此模块展示此攻击事件涉及到的 IOC。主要信息有：严重级别、IOC、微步标签、关联事件。

## 终端取证结果

展示对应威胁事件中，根据已安装的 Agent 的终端取证结果。



## 2.4 智能聚合

智能聚合功能会以攻击者角度，将不同的攻击者发起的攻击进行归纳和汇总，以时间线的形式呈现出来。这样用户可以清晰的看到，攻击者在什么时间，使用什么攻击方式，对哪些内网资产进行了攻击，产生了哪些危害。有利于用户对攻击者、受害主机以及失陷环节进行清晰的排查。

使用方法：

- 1.从导航菜单进入威胁页面（登录系统默认来到此页面）
- 2.选择“威胁-智能聚合”子菜单项，来到智能聚合页面。



### 2.4.1 攻击事件列表

智能聚合页面左侧，列出目前检测到的所有攻击事件，点击对应的攻击事件卡片，可以切换事件详情内容。

攻击事件列表支持以下功能：

【筛选功能】TDP 支持对智能聚合的列表做多种筛选，包括以下条件：时间、严重级别、攻击结果、攻击阶段、支持查看针对性攻击，同时支持对：攻击 IP、告警主机 IP、攻击手法、攻击工具以及事件 ID 的搜索。

攻击事件列表中展示以下内容：

统计事件的总数，并支持综合排序以及按照事件中最新攻击时间排序。

卡片展示包括的字段有：严重程度、攻击 IP、最新一次攻击时间、攻击来源地理位置、持续时间、攻击结果分布（攻击成功、失败、攻击未知）、以及成功的攻击手法。

## 2.4.2 攻击事件详情

用户可以通过点击攻击事件列表中的事件卡片，进行攻击事件详情切换。

攻击事件详情展示以下内容：

【事件详情卡片】：展示了当前事件的攻击来源，攻击 IP，事件 ID，以及攻击的手法，红色为成功攻击。



【热力图】根据系统检测到的本事件持续时间，在这一事件范围内绘制热力图，帮助用户判断此攻击事件的概况。



从攻击的有效性角度，热力图将事件中的告警，分为访问、敏感行为、攻击和攻击成功四种类型，用户可以直观的查看在过去 30 天内，攻击者的持续访问时间、攻击节奏以及成功攻击的时间点；

从攻击节奏的角度，热力绘制过去 30 天的告警，并将每天分为凌晨（0-6 点）、上午（6-12 点）、下午（12-18 点）以及晚上（18-24 点），并且以周的维度，区分工作日以及周末，用户可以根据攻击者的活跃时间段，攻击连续性，判断攻击行为是人还是机器，攻击者自身的作息以及所处的时区等信息。

【攻击成功】展示了此事件中，攻击成功的威胁名称，以及受影响的主机个数。

### 攻击成功



【攻击来源】展示了此事件中，攻击的来源，包括攻击 IP、攻击来源的地理位置、

微步情报、和攻击者的活跃时间段。

攻击来源

攻击IP	攻击来源	微步情报	活跃时间段
70.127.242.253	United States-Florida-Saint Petersburg	暂无情报	上午6-12时

【攻击结果】展示了此事件中，攻击结果的分布比例。

攻击结果



【TOP 受攻击域名】展示了此事件中，受攻击最多的域名。

TOP受攻击域名 | 攻击成功 | 失败 | 攻击未知



【攻击过程】TDP 智能聚合模块，将每个攻击 IP 的攻击行为，经过关联分析，以时间线的形式展示攻击过程。



首次访问：展示此攻击者的首次访问页面

威胁种类聚合：系统将相同的威胁聚合在一起展示，以时间线的形式呈现。用户可以直观的看到在这一个事件中，攻击者使用此威胁手法对某些目标发动了多少次攻击，

先后顺序如何，其中有哪些成功了。

威胁事件卡片展示了以下元素：

攻击过程 | 严重 | 高 | 中 | 低 | 信息

攻击: 3 | 成功: 3 | 70.127.242.253 → 菜刀webshell虚拟终端执行命令 → 192.168.217.129

结果	源IP	目的IP	目标地址	最近一次活动时间	操作
攻击成功	70.127.242.253	192.168.217.129	192.168.100.171/909kk.php	11/14 11:42:39	查看日志
攻击成功	70.127.242.253	192.168.217.129	192.168.100.171/909kk.php	11/14 11:42:39	查看日志
攻击成功	70.127.242.253	192.168.217.129	192.168.100.171/909kk.php	11/14 11:31:51	查看日志

最近一次告警时间、威胁阶段（包括：侦查、漏洞利用、敏感行为、控制、内网渗透、对外攻击）、告警总次数、成功次数、攻击源、攻击名称、受害者。

支持快速筛选：可以快速筛选“仅看外部攻击”、“仅看攻击成功”。

告警详情：用户点击威胁种类卡片中的“展开”按钮，可以看到具体的告警条目，包括的内容有：攻击结果、源 IP、目标 IP、目标地址、最近一次活动时间以及“查看日志”的操作。

点击“查看日志”按钮，用户可以看到告警日志的具体信息，用户可以通过告警的具体信息作进一步的判断和调查。

攻击: 1 | 成功: 1 | 102.165.30.33 → 浏览Web目录 → 192.168.177.14

漏洞利用 | 严重 | 高 | 中 | 低 | 信息

告警信息

漏洞利用: 攻击者可以利用这个特性窃取web目录下文件(S2018020036)

详细告警

攻击源: 102.165.30.33 | 攻击目标: 192.168.177.14 | 攻击名称: 浏览Web目录

HTTP

源IP/端口: 102.165.30.33:80829 | 目的IP/端口: 192.168.177.14:8081

告警资产: 192.168.177.14 | URL: 116.181.2.150:8081/

HTTP方法: GET | HTTP返回码: 200

原始报文信息

请求包

```
GET / HTTP/1.1
Host: 116.181.2.150:8081
User-Agent: NetSystemsResearch studies the availability of various services across the internet. Our website is netssystemresearch.com
```

响应包

```
HTTP/1.1 200 OK
Date: Wed, 21 Oct 2020 22:51:13 GMT
Server: Apache/2.4.41 (Ubuntu) OpenSSL/1.1.1c
Content-Length: 481
Content-Type: text/html; charset=UTF-8
```

## 2.5 内网渗透分析

内网渗透分析功能,方便安全运营人员直观地了解所监控区域的内网渗透攻击行为,聚合主机之间的攻击方向和攻击手法,清晰定位攻击来源和受影响的主机,能够全面掌握内网渗透威胁态势。

### 2.5.1 内网渗透分析概览

使用方法:

- 1.从导航菜单进入威胁页面
- 2.选择“威胁-内网渗透分析”子菜单项,来到内网渗透分析页面。



【筛选功能】TDP 支持对内网渗透的发起方、攻击手法、以及受害主机,做多种组合的筛选。同时支持筛选发起方、受害主机的资产类型。

【内网渗透时间卡片】TDP 将所有的内网渗透行为,按照渗透攻击名称进行聚合,展示在左侧。用户点击对应的卡片,则会对概览图进行筛选。

【内网渗透概览】TDP 展示内网主机之间的攻击方向,以及具体的攻击手法。图中,箭头的方向由攻击方指向受害方,箭头上会展示当前的攻击手法种类,如果只有一种,则展示攻击手法名称。

【内网主机快速查看】用户将鼠标上移到某一台主机上,TDP 将会将与该主机无关的其他渗透行为模糊化,高亮此主机,以及与其相关的渗透行为,便于用户查看单一主机的渗透行为。

【内网主机的数量限制】内网渗透概览图，默认不展示资产类型为“负载均衡”的主机，同时会将展示的内网攻击主机控制在 30 之内。

## 2.5.2 内网渗透主机、事件详情

使用方法：

在内网渗透分析页面，点击希望进一步查看的主机，弹出主机详情，如果点击主机详情中的具体事件，则会进一步展示对应的事件详情

在内网渗透分析页面，点击两主机之间的箭头，弹出内网渗透事件详情



【主机详情】点击任意一台主机，弹出主机详情弹层。展示主机相关的信息，包括资产类型、主机 IP、资产名称，以及本主机发起的攻击或者遭受的攻击。如果主机被攻击者攻击成功，或者连接恶意远控以及对外发起攻击，会将主机的颜色标红，并给出连接，点击可以查看对应的主机详情。

【发起的攻击/遭受的攻击】系统按照攻击方向，将主机相关的内网渗透事件，分为主机发起的攻击，和主机遭受的攻击。列表中展示，攻击的攻击方 IP、攻击手法和受害方 IP。事件以严重程度进行排序。

【主机内网渗透事件详情】展示攻击方 IP、资产类型以及资产名称；攻击手法，以及对应的严重等级；受害方 IP、资产类型以及资产名称。

【内网渗透事件趋势】展示了当前内网渗透事件的告警趋势，告警检出总次数。用户可以自行调整时间，查看更大事件范围内的告警趋势。

【内网渗透事件具体告警】展示了对应的内网渗透事件具体告警信息。列表中展示了具体的告警时间、源主机 IP、源端口、目的主机 IP 和目的端口。点击对应的告警，可以查看告警详细内容。

时间	源主机	源端口	目的主机	目的端口
2020/10/19 22:22:00	192.168.224.93	50581	192.168.145.132	6868

详细信息 原始记录

**告警信息**

**中危** 主动下载或传播恶意文件木马 Trojan.CobaltStrike.AS(F64a941073ebc9ee) 误报处理 白名单

192.168.224.93 (生产服务器) HTTP 6868 192.168.145.132

下载 192.168.145.132:6868/Classes/S...

**文件(HTTP)** 复制内容

源IP/端口: 192.168.224.93:50581 <b>受害者</b>	目的IP/端口: 192.168.145.132:6868 <b>攻击者</b>
告警资产: 192.168.224.93 /未分组/生产服务器	Sha256: 64a941073ebc9ee66da74c4fdcb748fa99f2f8fdb23b2954e7cda6f32c2f84 <a href="#">查看完整云沙箱结果</a>
URL: 192.168.145.132:6868/Classes/SoftManagers.exe	HTTP返回码: -

## 2.6 告警主机

### 2.6.1 告警主机列表

使用方法：

- 1.从导航菜单进入威胁页面
- 2.选择“威胁-告警主机”子菜单项，来到告警主机列表页面。

告警主机

全部业务组 | 全部主机类型 | 主机IP/名称/域名/告警名称/目标地址

全部告警主机 508台

被外部攻击成功 11台

发起内网渗透 15台

已失陷 21台

APT 0台

与远控端建立连接 4台

WebShell 2台

挖矿 2台

对外攻击 31台

阶段手法: 外部攻击和投送/漏洞利用、访问钓鱼页面、下载或传... | 严重级别: 全部 | 威胁性质: 全部 | 处置状态: 全部

严重级别	主机IP/资产属性	资产名称	主机威胁状态	检出威胁	最近告警时间	处置状态
严重	192.168.178.121 服务器	生产服务器	外部攻击或投送 内网渗透 失陷	Cobalt Strik... 连接MSSQL... SQLMAP MySQL注入...共24类告警	10/22 14:58:29	未处理
严重	120.52.185.110 服务器	生产服务器	外部攻击或投送 失陷	Cobalt Strik... SQLMAP MySQL注入 通用SQL注入...共43类告警	10/22 14:58:28	未处理
严重	192.168.178.116 服务器	生产服务器	失陷	Cobalt Strik...	10/22 14:58:27	未处理
严重	192.168.178.54 服务器	生产服务器	失陷	Cobalt Strik...	10/22 14:58:27	处理中
严重	192.168.178.79 服务器	生产服务器	内网渗透 失陷	Cobalt Strik... 木马 Trojan... MySQL注入	10/22 14:58:27	未处理

【筛选功能】TDP 支持对告警主机做多种筛选，包括以下条件：时间范围、主机状态、资产类型和处置状态。

【搜索功能】同时支持根据主机 IP、名称、域名、告警名称以及目标地址进行搜索。

【告警主机】TDP 将所选时间范围内，对应筛选条件的所有告警的内网主机，根据最近一次告警时间进行排序，包含以下信息：严重级别、主机 IP、域名/资产名称、主机状态、检出威胁、最近告警时间以及处置状态。

## 2.6.2 告警主机详情页

使用方法：

1.从导航菜单进入威胁页面

2.选择“威胁-告警主机”子菜单项，点击对应的告警主机 IP，来到告警主机详情页页面。

返回告警主机

192.168.178.54  
严重 服务器

资产名称 生产服务器

所属业务组 未分组

处理状态 处理中

威胁 威胁实体分析 处理记录 Agent

主机威胁状态

未遭受外部攻击  
该主机为遭受来自互联网的攻击

无内网渗透行为  
未发现主机的内网渗透行为

已失陷  
该主机已失陷，说明主机存在Webshell，或主机已感染恶意程序。失陷的主机会受到黑客的控制，执行挖矿、勒索、传播病毒、窃取数据、对外发起攻击等一系列恶意行为。

威胁事件列表 已处理: 0 处理中: 1 未处理: 0

阶段手法: 外部攻击和投送/漏洞利用、访问钓鱼页面、下载或传... | 严重级别: 全部 | 威胁性质: 全部 | 处置状态: 全部

威胁事件	事件类型	事件性质	严重级别	关联实体	最近发现时间	事件处理状态
Cobalt Strike远程控制(利用JQuery站点)	失陷破坏/连接远控地址	-	严重	1个外部地址	2020/10/22 15:07:20	处理中



用户可以通过点击告警主机列表中的主机 IP，来到告警主机详情页。在详情页开头，系统展示对应告警主机的主要信息，包括：严重程度、主机 IP、资产属性（服务器或终端）、资产名称以及关联域名（可能无关联的域名）、所属业务组、处理状态。

在详情页面中，系统通过以下角度呈现告警主机相关信息：

## 威胁

TDP 在“威胁”TAB 展示此告警主机相关的告警，使用威胁名称进行聚合，包含以下功能：

主机威胁状态：

主机威胁状态通过选定时间范围的威胁事件评估得出，威胁状态分为外部攻击、内网渗透、已失陷，根据主机在特点的时间展示威胁的状态。

威胁事件列表：

TDP 按照威胁事件的方式，展示出每一个事件的详细信息，包括威胁事件名称、事件类型、事件性质、严重级别、管理实体、最近发现时间、事件处理状态。我们可以将事件进行筛选来快速检索，同时也可以下载事件列表。

威胁事件详情：

操作方法：

1.从告警主机列表页面点击主机 IP 进入告警主机详情页面

2.选择一条威胁事件，点击列表中查看详情后可查看详细告警信息，详情页头部显示威胁事件名称、严重级别、事件类型、告警主机 IP、事件处理状态，下方显示威胁明细列表，展示该主机所有受到的威胁，该威胁包含时间、攻击 IP、威胁名称、严重级别、受攻击主机、协议、受攻击 URL、攻击结果，我们可以进行攻击结果及协议的筛选，也可以输入 IP 地址进行搜索，同时我们可以下载威胁明细进行内容查看。

3.点击威胁事件后，将显示该事件的详细信息，包含告警描述、示意图、行为描述图、协议详情、PCAP 查看及下载以及原始记录，不同的协议类型，展示内容有所区别。

4.分析和处置是将威胁事件进行分析，从而进一步提升威胁用户的感知。

## 威胁实体分析

在威胁实体分析模块，系统对所选的告警主机遭受的外部威胁实体进行详细描述，包括以三类：

**【攻击成功的外部 IP】**此模块展示了外部互联网侧攻击这一告警主机并且攻击成功的外部 IP，展示信息包括以下内容：

外部攻击 IP：外部攻击的 IP 地址

地理位置：外部攻击 IP 的地理位置

IP 信誉标签：此外部攻击 IP 在微步情报库中的信誉标签

最近一次攻击时间：此外部 IP 攻击产生的最近一次告警的时间

攻击手法和次数：展示了此外部 IP 攻击此告警主机的攻击手法以及次数

**【攻击当前主机的内网 IP】**展示内网中攻击当前主机的所有内网 IP，展示信息包括以下内容：

内网攻击 IP：攻击此告警主机的内网 IP 地址

资产名称：此内网 IP 的资产名称

资产属性：服务器或者主机

最近一次攻击时间：此内网主机攻击告警主机的最近一次告警时间

攻击手法和攻击次数：展示了此外部 IP 攻击此告警主机的攻击手法以及次数

**【当前主机连接的 IOC】**展示此告警主机连接的 IOC，展示信息包括以下内容：

IOC：此告警主机的连接的 IOC 地址

严重级别：IOC 的严重级别

IOC 标签：此 IOC 在微步情报中的标签

最近一次连接时间：此内网主机攻击连接 IOC 的最近一次告警时间

连接次数：此内网主机攻击连接 IOC 的次数

操作：点击“查看详细内容”可以查看此 IOC 的详情。

## 处理记录

TDP 可以进行对告警主机的状态处理, 进一步减少平台运营的人员的工作步骤, 同时我们也可以针对状态的修改进行主机处理的记录及查询。

1. 处理记录将通过时间、告警主机、威胁事件、出质人、处理结果、备注及操作进行列表的展示, 我们可以通过处理结果进行内容的筛选, 同时我也可以选择事件, 填写告警主机、威胁事件、经办人来进行内容的查询。

## Agent

展示此告警主机的 Agent 的取证结果。

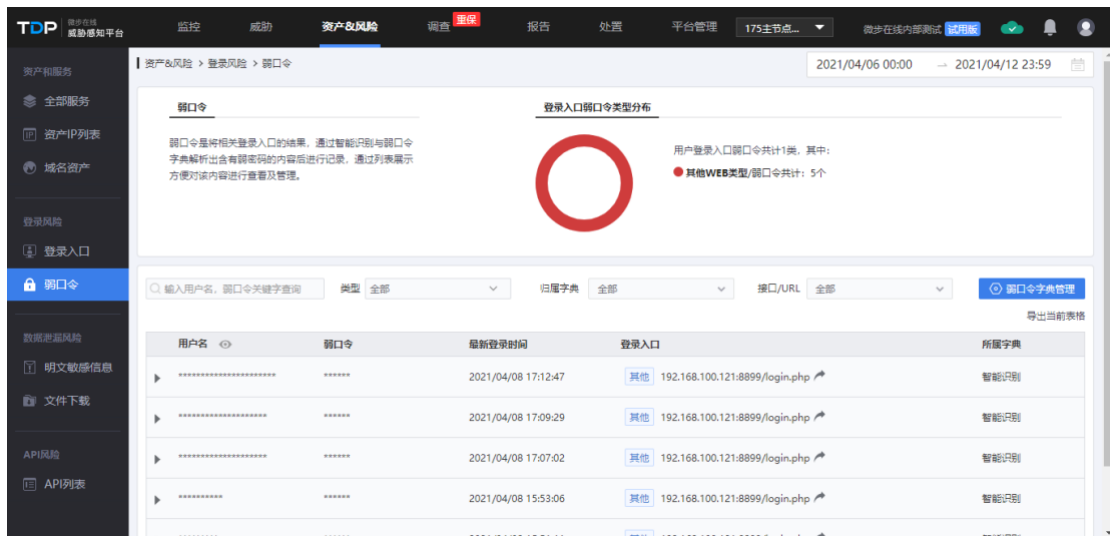
## 三、资产&风险

风险页面展示了 TDP 检测到的系统风险，包括登录风险、数据泄漏风险、API 风险和资产与服务。

### 3.1 登录风险

登录风险页面展示了系统检测到的登录风险，包括撞库风险和弱口令风险，具体功能如下：

#### 3.1.1 弱口令



The screenshot shows the TDP interface for Weak Passwords. It includes a navigation menu on the left, a top navigation bar, and a main content area. The main content area features a search bar, a table of detected weak passwords, and a summary section with a donut chart.

用户名	弱口令	最后登录时间	登录入口	所属字典
*****	*****	2021/04/08 17:12:47	其他 192.168.100.121:8899/login.php	智能识别
*****	*****	2021/04/08 17:09:29	其他 192.168.100.121:8899/login.php	智能识别
*****	*****	2021/04/08 17:07:02	其他 192.168.100.121:8899/login.php	智能识别
*****	*****	2021/04/08 15:53:06	其他 192.168.100.121:8899/login.php	智能识别
*****	*****	2021/04/08 15:53:11	其他 192.168.100.121:8899/login.php	智能识别

页面路径：

- 1.从导航菜单进入资产&风险页面
2. 选择“资产&风险-登录风险-弱口令”子菜单项，来到弱口令页面。

弱口令页面展示了 TDP 检测到的所有疑似使用弱密码登录的用户，具体展示如下内容：

用户名、弱口令、最后登录时间、登录入口、所属字典。

弱口令页面支持以下功能：

【用户名搜索】可以根据用户用户名进行搜索。

【类型】可根据登录接口的类型进行筛选

【所属 API】默认展示所有登录 API 之下的使用弱密码的用户，点击可以通过下拉菜单切换对应的 API，可以根据 API 筛选所属的弱密码用户。

【弱口令字典管理】点击资产&风险>弱口令功能页面，点击弱口令管理进入该页面，进行弱口令字典的上传及管理。

### 3.1.2 登录入口

页面路径：

1. 从导航菜单进入资产&风险页面
2. 选择“资产&风险-登录风险-登录接口”子菜单项，来到登录接口页面。

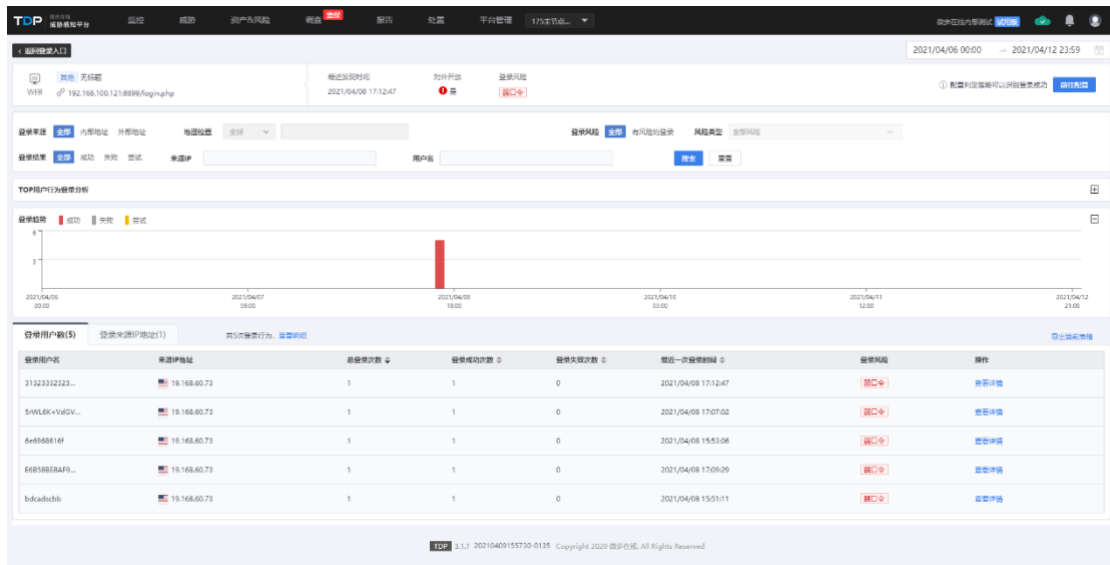


页面支持以下功能：

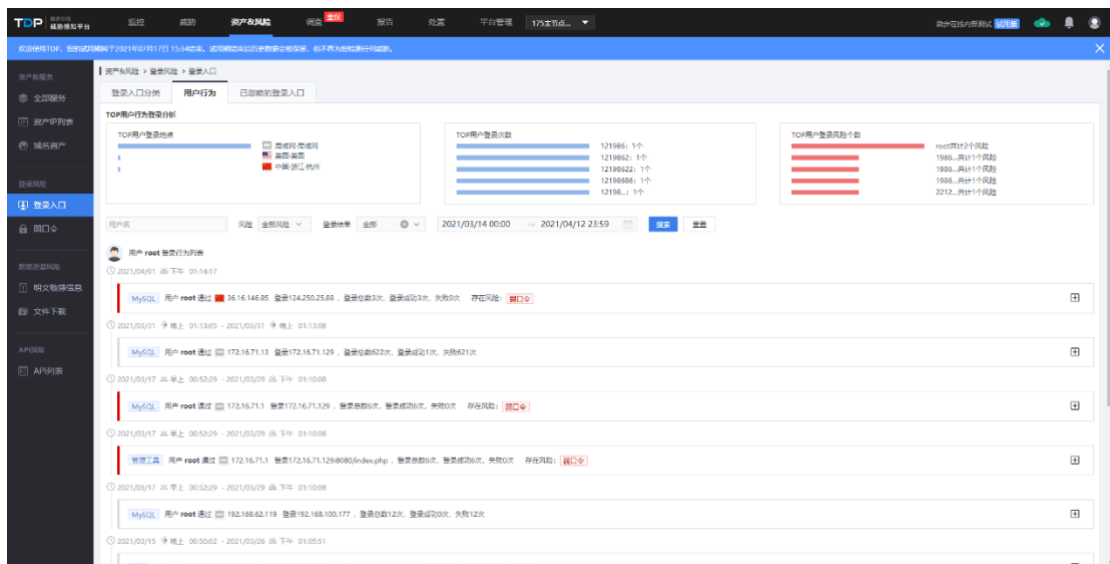
【筛选功能】可以根据登录地址、登录页面 URL、登录页面标题进行搜索

【WEB 登录配置登录规则】判断登录接口是否成功，需要用户自行配置登录成功规则。

用户点击“配置登录规则”按钮，来到登录成功规则配置页面。注意此处，用户可以根据登录风险，状态码、内容长度、关键字以及 location 进行登录成功规则的配置，配置完毕，点击保存即可生效。



【登录详情页】用户可通过登录详情页查看该登录入口下所有登录行为及风险，支持筛选



【用户行为】该页面通过用户的视角展示某个用户登录的整体行为，可查询每一个登录详情

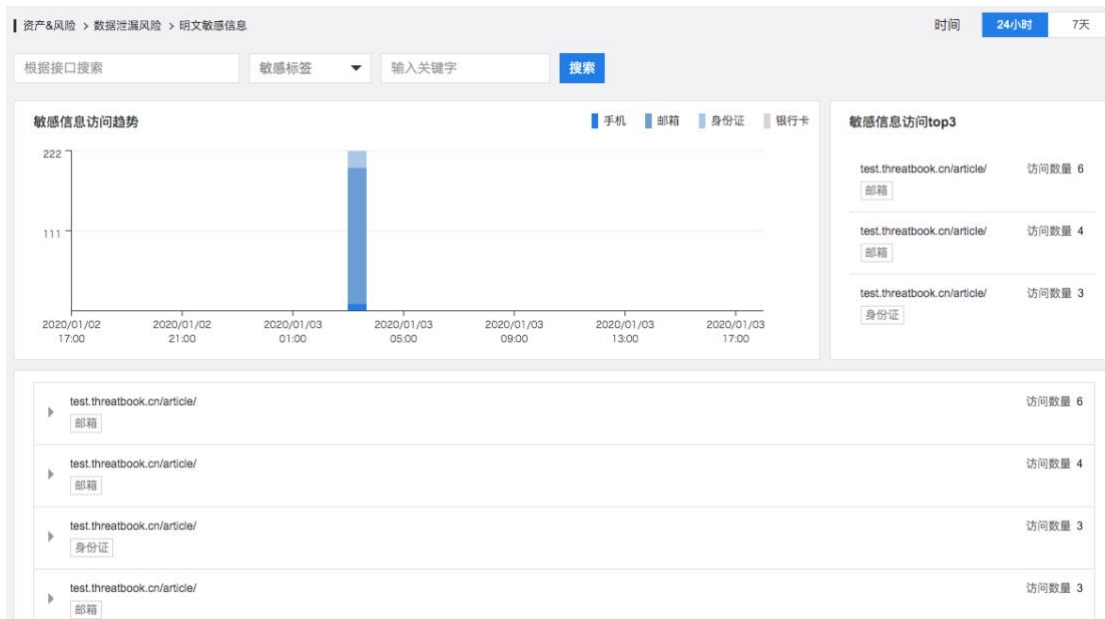
## 3.2 数据泄漏风险

TDP 可以对系统的敏感信息进行泄漏风险监测，主要包括明文敏感信息传输监测和系统文件下载监测，具体功能介绍如下：

### 3.2.1 明文敏感信息

页面路径：

- 1.从导航菜单进入风险页面
2. 选择“风险-数据泄漏风险-明文敏感信息”子菜单项，来到明文敏感信息页面。



明文敏感信息页面支持以下功能：

【时间切换】支持 24 小时和 7 天的时间切换。

【搜索功能】支持根据以下内容进行搜索：

根据接口搜索：支持根据接口关键字进行搜索

敏感标签：支持搜索敏感信息类型，包括手机、邮箱、身份证号、银行卡号进行搜索

敏感信息页面包含以下内容：

#### 1.敏感信息访问趋势：

以柱状图的形式展示了手机、邮箱、身份证号、银行卡号在所选时间范围内的趋势，鼠标滑动到对应的柱形图上，可以看到对应时间点手机、邮箱、身份证号、银行卡号的访问次数。

#### 2.敏感信息访问 TOP3:

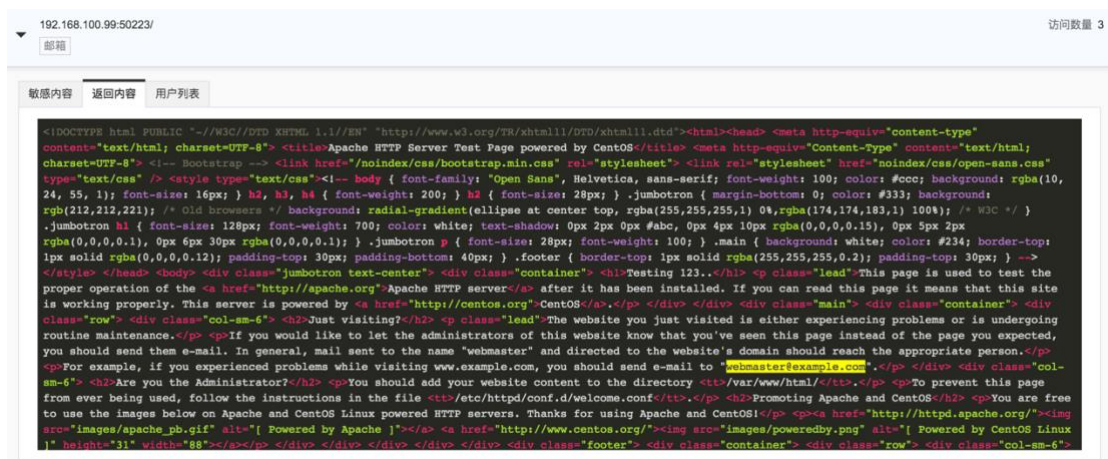
TDP 将明文传输敏感信息的接口，统计对应的访问数量，展示访问次数最多的 TOP3 接口，并且展示接口的访问数量，以及接口泄露信息的类型。

### 3.敏感信息接口：

敏感信息接口列表，展示接口暴露的敏感信息类型，点击“展开”按钮，可以看到“返回内容”和“用户列表”TAB。



“返回内容”TAB 展示对应的接口最近一次的返回内容，用户可以根据返回内容判断接口功能。其中，检测到的敏感信息会被高亮显示。



“用户列表”TAB 展示对应接口的访问用户，展示内容包括 IP、访问系数、QPM、访问次数、UA 和敏感数据类型。



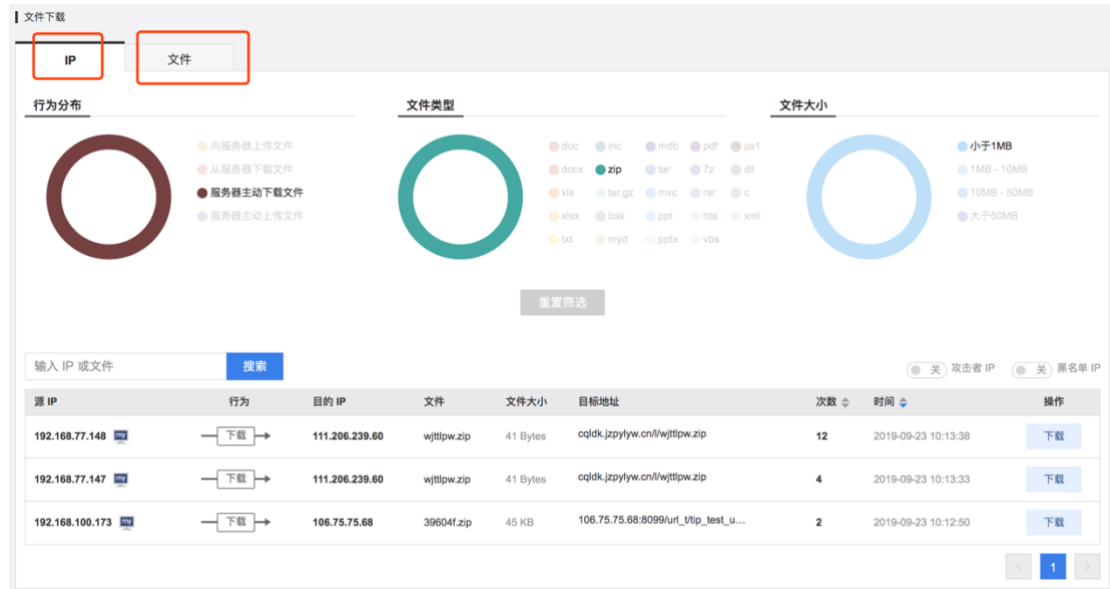
## 3.2.2 文件下载

TDP 将监测到的文件下载行为展示在文件下载页面，从下载 IP 角度和文件角度进行展示。



页面路径：

- 1.从导航菜单进入风险页面
2. 选择“风险-数据泄漏风险-文件下载”子菜单项，来到文件下载页面。



## “IP” TAB 内容如下：

点击“IP”TAB，系统以下载文件 IP 的角度，进行了下载文件行为风险的展示。

### 分布概况：

【行为分布】行为分布展示了四种下载行为，分为“向服务器上传文件”、“从服务器下载文件”、“服务器主动下载文件”和“服务器主动上传文件”四种。

【文件类型】根据文件后缀类型，展示了下载文件类型的分布。

【文件大小】将文件大小按照“小于 1MB”、“1MB - 10MB”、“10MB - 50MB”和“大于 50MB”四种类型，进行分类展示。

功能操作：用户点击对应的类型，就可以进行筛选，点击图表下方的“重置筛选”按钮，可以清空之前选择的筛选类型。

### 源 IP 列表：

【搜索功能】支持根据 IP 或者文件，进行搜索。

源 IP 列表展示一下内容：

源 IP：展示了下载文件的 IP 地址

行为：展示了源 IP 的行为类型

目的 IP：展示了下载文件的目的 IP

文件：展示对应下载的文件名

文件大小：展示下载文件的大小

目标地址：展示下载文件的地址

次数：展示此文件被下载的次数，点击可以进行“升序”或者“降序”操作

时间：展示此文件被下载最新一次时间，点击可以按照时间的“升序”或者“降序”排序

【操作】用户如果希望得到对应的文件，可以点击“下载”按钮进行下载，如果不能下载成功，则说明下载链接失效。

## “文件” TAB 内容如下：

点击“文件”TAB，系统以下载文件的角度，进行了下载文件行为风险的展示。

### 分布概况：

【行为分布】行为分布展示了四种下载行为，分为“向服务器上传文件”、“从服务器下载文件”、“服务器主动下载文件”和“服务器主动上传文件”四种。

【文件类型】根据文件后缀类型，展示了下载文件类型的分布。

【文件大小】将文件大小按照“小于 1MB”、“1MB - 10MB”、“10MB - 50MB”和“大于 50MB”四种类型，进行分类展示。

功能操作：用户点击对应的类型，就可以进行筛选，点击图表下方的“重置筛选”按钮，可以清空之前选择的筛选类型。

### 文件列表：

【搜索功能】支持输入文件，进行搜索。

文件列表展示以下内容：

文件：文件名称

文件大小：文件大小

下载次数：文件被下载的次数

文件位置：文件所处的位置

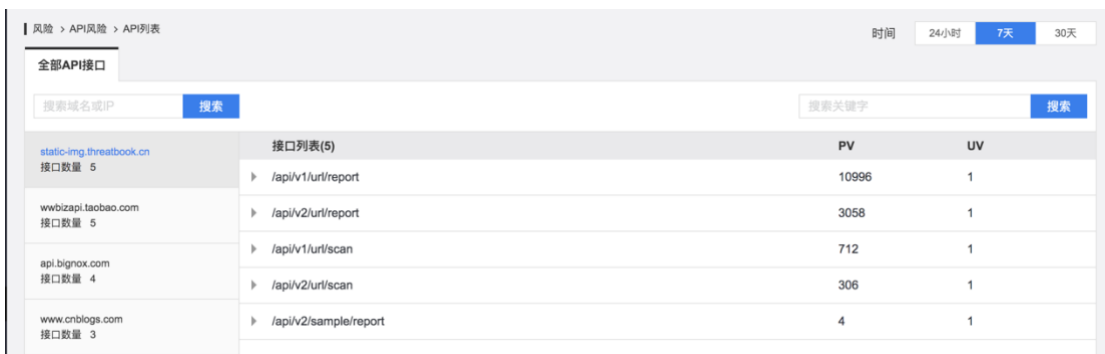
操作：点击“下载”按钮，可以下载该文件

### 3.3 API 风险

API 风险展示了 TDP 对所监控系统所有 API 的动态监控。

页面路径：

1. 从导航菜单进入风险页面
2. 选择“风险-API 风险-API 列表”子菜单项，来到 API 列表页面。



The screenshot shows the 'API 列表' (API List) page in the ThreatBook interface. It features a search bar for domain/IP and a filter for time range (24 hours, 7 days, 30 days). The main content is a table with columns for domain, API list, PV, and UV.

域名/IP	接口列表(5)	PV	UV
static-img.threatbook.cn 接口数量 5	/api/v1/url/report	10996	1
wwbizapi.taobao.com 接口数量 5	/api/v2/url/report	3058	1
api.bignox.com 接口数量 4	/api/v1/url/scan	712	1
	/api/v2/url/scan	306	1
www.cnblogs.com 接口数量 3	/api/v2/sample/report	4	1

#### 3.3.1 API 列表

API 列表在左侧展示域名或者 IP，在右侧展示所选域名或者 IP 之下的接口。

支持以下功能：

【时间搜索】支持“24 小时/7 天/30 天”的时间范围切换

【搜索域名或 IP】在左侧搜索框，输入域名或者 IP，可以进行搜索。

【关键字搜索】在右侧搜索框，输入接口关键字，可以在当前选择的“域名和 IP”之下进行接口的搜索。

## 3.4 资产与服务

资产与服务页面，展示 TDP 检测到的系统中对外提供服务的资产与服务。

### 3.4.1 全部服务

全部服务页面展示系统监测到的所有系统服务，包括数据库、Web 服务器、远程登录、邮件服务、认证服务、文件传输以及其他服务。

页面路径：

1. 从导航菜单进入风险页面
2. 选择“风险-资产与服务-全部服务”子菜单项，来到全部服务页面。



#### 按照服务分类展示：

在全部页面，选择数据库、Web 服务器、远程登录、邮件服务、认证服务、文件传输以及其他服务的按钮，会按照对应的类型展示系统内相关的服务，选中的服务类型变为蓝色。

#### IP 按照对外开放、新上线服务展示：

在全部页面，选择对外开放、新上线服务按钮，会按照对应的类型展示系统内相关的服务，选中的服务类型变为蓝色。

新上线服务定义：首次发现时间在最近三天内。

#### 服务展示：

在全部服务页面，按照“最近 7 天活跃服务”以及“近 7 天不活跃服务”两个 TAB 进行分类。

每个服务归属对应的服务类型，点击对应服务，右侧展示该服务之下的关联主机资产，资产信息包括 IP、资产类型、关联端口、关联域名、是否对外开放、以及主机最近的发现时间。

【操作】支持下载当前筛选条件下的服务以及所属资产。

### 3.4.2 资产 IP 列表

资产 IP 列表页面展示系统监测到的所有资产，类型包括终端、服务器，支持按照是否对外开放和近 3 天内新上线筛选。

页面路径：

1. 从导航菜单进入风险页面
2. 选择“风险-资产与服务-资产 IP 列表”子菜单项，来到资产 IP 列表页面。

资产 IP 数(1284)

终端: 33 服务器: 1197 对外开放: 629 近3天新上线: 4 [导出当前表格](#)

资产 <small>如需配置资产名称信息请前往 <a href="#">资产管理页</a></small>	服务	服务版本	关联域名	关联端口	对外开放	最近发现时间
172.30.150.81	服务器	Microsoft DNS	-	53	否	2019/12/24
172.30.145.33	服务器	WINS	-	42	否	2019/12/24
172.30.176.222	服务器	MSSQL	-	1433	否	2019/12/24
172.30.90.35	服务器	MySQL	-	3306	否	2019/12/24
172.30.91.176	服务器	Memcached	-	11211	否	2019/12/24
172.30.58.209	服务器	Postfix	-	25	否	2019/12/24
172.30.28.164	服务器	Qmail(pop3)	-	110	否	2019/12/24
172.30.252.101	服务器	Hmail(pop3)	-	110	否	2019/12/24

#### 资产 IP 展示：

资产信息包括 IP、资产类型、服务、服务版本、关联端口、关联域名、是否对外开放、以及主机最近的发现时间。

在列表上方，统计了资产 IP 数量，以及终端数量、服务器数量。同时统计了对外开放的主机数量，和最近 3 天内的新上线资产数量。

支持下载当前筛选条件下的所有资产。

筛选操作：

支持对 IP 地址、资产类型、服务名称、服务版本、关联域名、关联开放端口、是否对外开放、近 3 天新上线这些条件进行组合筛选。

### 3.4.3 域名资产

对于企业客户，TDP 支持对于企业内网的域名资产进行检测和展示，支持以下功能：

梳理系统内所有二级域名以及二级域名之下的子域名，展示二级域名的注册人信息以及最近一次的注册人变更信息；展示子域名对应的具体 IP 地址等信息。

支持查看子域名的业务属性，包括子域名之下的登录接口、API 接口（含敏感信息的 API 接口）、文件下载行为等。

能够对子域名的变更信息做监控展示，包括近 3 天内对外开放、近 3 天上线、新增管理后台。

能够对于域名进行快速搜索和筛选。

页面路径：

选择“资产&风险”导航，选择“域名资产”子导航

即可以看到域名资产页面。

## 查看所有域名

在域名资产页面左侧，展示了系统内检测到的所有二级域名，点击对应的二级域名，可以查看此二级域名之下的子域名。对于每个二级域名，会统计此域名之下的子域名个数进行展示。

二级域名如果存在注册人，会展示对应的注册人信息。

是否对外开放: [全部](#) 是 否    是否近三天内上线: [全部](#) 是 否    输入域名/IP    [筛选](#)    [重置](#)

是否存在敏感信息接口: [全部](#) 是 否    是否存在管理后台: [全部](#) 是 否

全部域名: 2345    二级域名: 27    [导出当前表格](#)

域名	解析IP	对外开放	登录接口	API接口(含敏感信息接口)	文件下载	近期变更
threatcook.com 子域名: 1234	注册人: xfhgkgk@threatbook.cn 上次变更: 注册人由xfh@threatbook.cn变更为xfhgkgk@threatbook.cn, 变更时间: 2020/02/17 18:00					
tzt.threatbook.cn XXXX管理平台	111.206.218.124	是	1	1000+ [345]	12	<a href="#">近三天对外开放</a>
tzt.threatbook.cn XXXX管理平台	111.206.218.124	是	1	988 [345]	12	近期无变更
tzt.threatbook.cn	111.206.218.124	是	1	66 [12]	12	<a href="#">近三天上线</a>
tzt.threatbook.cn	111.206.218.124 111.206.218.124 111.206.218.124	是	1	988 [345]	12	近期无变更
tzt.threatbook.cn XXXX管理平台	111.206.218.124 111.206.218.124 111.206.218.124 ...等13个	是	1	1000+ [345]	12	<a href="#">新增登录接口</a>

< 1 2 3 4 5 6 >

## 查看域名的业务属性

点击登录接口、API 接口（含敏感信息接口）、文件下载对应的数字，可以查看此域名之下对应的信息。

## 查看域名对应的变更信息

在表格变更信息列，会展示域名对应的变更信息。包括域名三天内上线，域名新增管理接口和域名三天内对外开放。

## 域名的快速筛选

支持对域名和对应的 IP 进行筛选。

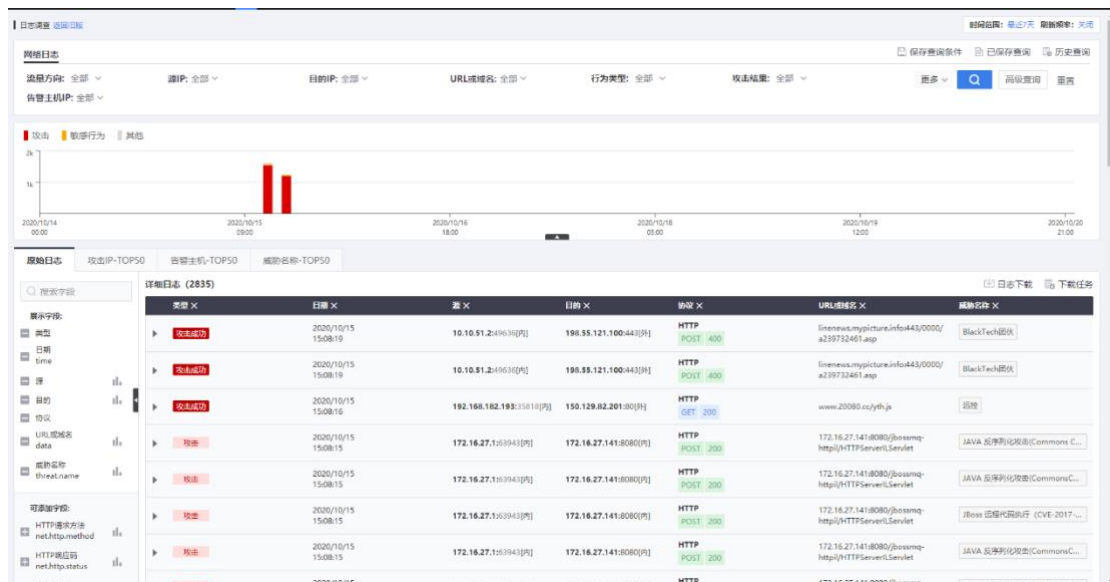
## 四、调查

调查模块为用户提供高级的调查分析能力，包括日志调查，终端取证和命中情报三个功能；同时通过攻击 IP、告警主机、威胁名称视角展示相关内容。

### 4.1 日志调查

#### 4.1.1 新版网络日志

TDP 新版日志调查页面，为用户提供更友好的交互方式，更全面的字段说明与提示，以及更加灵活的告警日志展现方式。



页面路径：调查-日志调查

#### 调查-简单筛选

用户可以通过平台日志筛选区域进行字段选择，选择后进行查询。

- 1) 如果字段的值为固定的值，则系统会将所有选项呈现出来，供用户选择；
- 2) 如果字段值不固定，系统支持模糊搜索和精确匹配，同时模糊搜索与精确搜索都支持匹配多个值。
- 3) 如果用户希望搜索更多的字段，而不是默认的字段，则可以通过“更多”按钮，



获取更多支持检索的字段, 进行添加; 字段支持根据字段名称以及字段值进行模糊搜索;

## 调查-高级搜索

用户可以通过 sql 语句进行日志的检索, TDP 提供友好的提示:

- TDP 对于用户输入时, 会提示可搜索的字段, 并根据输入内容匹配对应的字段
- 用户输入或者选择字段后, TDP 会继续提示运算符
- 选择运算符后, TDP 会自动将匹配的值加上引号, 并将输入光标放在引号之内。
- 用户输入匹配值后, 进行搜索, 如果满足转换条件, 高级检索可以和简单搜索切换。(当用户先进行简单查询条件筛选后, 点击高级查询, 则简单查询的条件将直接展示在高级查询输入框内, 多条件将默认通过“AND”连接, 如有需要可以自行修改, 修改后不可再进行查询方式的修改。)

## 调查-增加日志条件记录

当用户进行日志查询时, 可以通过选择不同的字段进行日志的筛选, 为了方便用户长期的使用, 调查筛选增加了保存查询条件、已保存查询、历史查询功能。

- 保存查询条件: 当用户选择完筛选条件后, 可以点击保存查询条件, 输入语句名称进行条件保存, 我们同时也将展示检索语句及日志展示列, 点击确定后可进行保存;
- 已保存查询: 点击已保存查询, 将展开通过保存查询条件后的列表, 用户可以通过在此处选择检索条件进行日志查询; (提供搜索框、检索、删除)
- 历史查询: 点击可以查看历史 7 天查询记录, 同时展示检索语句。(提供检索按钮可再次查询)

## 调查-告警日志展示列支持自定义

调查页面, 为了便于用户查看原始告警, 默认展示日志类型、日期、源、目的、协议、URL 或域名以及威胁名称六列, 如果用户希望看到更多, 可以自行在可展示字段中添加列; 同时告警日志表格列的顺序可以自行调整。

## 调查-支持自动刷新

调查页面，支持根据设置的频率进行自动刷新，以便于用户了解最新的告警。刷新的告警将在日志列表中展示带有“NEW”标识，若刷新频率较为频繁，建议时间选择尽量短，以免系统开销过大。

## 调查-行为类型可视化

通过可视化列表展现在一定的时间范围内，受到的行为记录，通过图表展现。（目前分为攻击行为、敏感行为、其他）

## 调查-日志分类展示

针对日志列表将其以不同的视角进行展示，进一步展示为用户进行内容查询及汇总。

- 攻击 IP-TOP50：通过攻击者视角展示其行为，在详情页中针对攻击手法、活跃程度及熟悉资产均进行分析描述。
- 告警主机-TOP50：通过告警主机维度展示主机被威胁的情况汇总，针对威胁次数、威胁方式、威胁事件均进行罗列。
- 威胁名称-TOP50：针对威胁进行列表展示，展示威胁方式整体分析威胁行为。

### 4.1.2 网络日志（旧版）

旧版日志调查分为网络日志和终端日志两种，可以通过下拉选择框进行切换。



网络日志展示系统监测到的所有镜像流量的网络告警日志，包括搜索功能、检索聚合功能、日志趋势图以及日志详情列表。

## 搜索功能

【时间搜索】网络日志支持时间精确搜索，以及“1 小时”、“24 小时”、“今天”、

“近 7 天” 和 “最近 30 天” 的快捷选择。

**【语法说明】** TDP 提供快速检索语句，包括以下语句：

所有告警：检索网络日志中所有的告警

外部攻击：检索互联网对内网的攻击

来自某 IP 的 SQL 注入攻击：检索来自某 IP 的 SQL 注入攻击，用户可以自行替换 IP 以及攻击手法，进行搜索

内网反连某远控地址：检索网络日志中国，所有的对外反连地址

HTTP GET 访问某 URL 返回 200:用户可以按照需求修改返回状态码 “200”，以及对应的 “URL” 进行检索

**【语句搜索】** 网络日志检索支持以下语句检索：

类别	字段名称	搜索语句
实体相关	我方资产 IP	machine = '192.168.100.175'
	我方资产名称	machine_name = ''
	我方资产端口	machine_port= '80'
	外部资产 IP	external_ip='11.11.11.11'
	外部资产端口	external_port='12345'
	流量方向	direction = 'in '
	网络访问目标地址 (IP/ 域名 /URL)	data= 'www.threatbook.cn'

HTTP 相关	<p>HTTP 请求方法</p> <p>HTTP 请求体</p> <p>HTTP 响应体</p> <p>HTTP 请求域名</p> <p>HTTP 用户代理</p> <p>HTTP 响应码</p> <p>url</p> <p>http 来源地址</p> <p>HTTP 请求端真实IP</p>	<pre>net.http.method = "GET" net.http.reqs_body LIKE '%"%' net.http.resp_body LIKE '%"%' net.http.reqs_host = 'www.baidu.com' net.http.reqs_user_agent = "elastic/5.0.74 (darwin-amd64)" net.http.status = "200" net.http.url = "/static/js/26.cde9b1f3.chunk.js" net.http.reqs_referer = "" net.http.xff = ''</pre>
外部攻击相关	<p>外部 IP</p> <p>来源国家</p> <p>来源省份</p> <p>来源城市</p> <p>标签 (取威胁名称)</p> <p>攻击</p>	<pre>external_ip = "192.168.1.168" geo_data.Country = "局域网" geo_data.Province = "局域网" geo_data.City = "局域网" threat.name = "查询 json 接口" threat.msg = '查询 json 接口' threat.tool = 'SQL 注入'</pre>

	攻击工具	
	敏感行为名称	threat.level = 'action'
	敏感行为描述	and threat.name = '查询 json 接口'
	ip 信誉	threat.level = 'action' and threat.msg = "查询 json 接口"
		ip_reputation = "bogon"
传输层协议相关;	传输层源 ip	net.src_ip = '180.120.94.175'
	传输层目的 ip	net.dest_ip = '180.120.94.175'
	传输层源端口	net.src_port = '80'
	传输层目的端口	net.dest_port = '80'
	传输层协议	net.proto = "TCP"

在输入框中，输入搜索语句后，鼠标失焦后，会将输入的语句标签，用户想去掉其中一项时，点击对应标签的“X”关闭按钮以后，搜索语句会自动去掉这一条件，点击搜索后会按照新的语句进行检索。

## 检索统计

TDP 在左侧展示筛选条件下的所选择的网络日志的聚合结果，包括以下内容：源 IP、目的 IP、HTTP 请求域名、传输层协议、应用层协议、攻击名称、敏感行为名称和 HTTP 返回码。

所选择的网络日志，均会统计相应的字段，按照每个项的占比暂时在左侧中，点开  
后，支持搜索功能，点击下载按钮可以下载相关的内容。

## 日志趋势图

日志趋势图展示了所选择告警日志，在对应时间内的告警趋势，鼠标浮动在趋势图  
上后，浮动展示当前时间的告警次数。

时间快速选择：用户将鼠标移入趋势图的时间轴之下，可以看到鼠标变成十字选择  
按钮，用户可以使用此时间选择控件，快速缩小时间范围。

## 日志详情列表

日志详情列表展示每条告警的基本信息，点击展开后可以查看详细日志。

基本信息包含以下内容：

告警时间、源 IP 和端口（如果网络日志中存在 XFF 的 IP，并且来源于可信任 IP，  
XFF 的 IP 会展示在源 IP 之下）、方向、目的 IP 和端口、协议、HTTP 方法和返回码、  
URL 以及攻击标签

详细信息包含以下内容：

详细内容：展示了此告警 HTTP 以及 DNS 的请求和返回协议

JSON：展示了这条告警在存储中的原始记录

### 4.1.2 终端日志（旧版）

终端日志展示了 Agent 的所有上传日志。

在调查-日志调查页面，切换下拉选择器，将“网络日志”选项，切换成终端日志，

就可以

查看系统内安装的 Agent 日志。

点击具体的日志告警，可以查看日志具体信息。

## 4.2 终端取证

---

终端取证页面展示了系统中所有已经安装的 Agent，主要功能如下：

【时间控件】：支持“24 小时/7 天/30 天”的时间切换

【搜索功能】：支持根据主机名称、网络地址、取证结果、分组、在线状态和操作状态进行搜索。

【下载 Agent】点击下拉菜单，可以下载 linux 版本的 Agent 安装包。

【终端列表】包括以下信息：主机名、分组、网络地址、取证结果、开启功能、采集模版和 Agent 版本。

【终端详情】点击列表中对应的“查看详情”按钮，系统可以查看对应 Agent 的终端取证详情页面。

## 4.3 自动以情报

---

自定义情报中，展示用户导入的情报，通知支持用户在此页面导入自定义情报。支持以下功能：

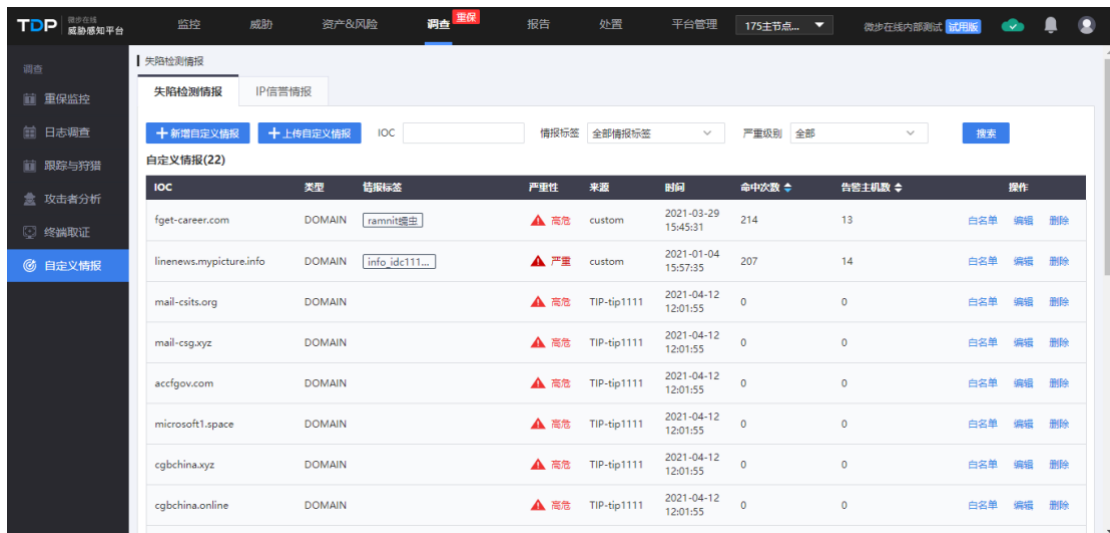
### 4.3.1 自定义情报

自定义情报分为失陷检测情报、IP 信誉情报

### 失陷检测情报：

- 【搜索功能】可以根据 IOC 进行搜索
- 【情报标签】可根据情报标签进行筛选
- 【严重级别】可根据严重级别进行筛选
- 【新增情报】支持用户自定义上传单条情报。
- 【上传情报】支持用户上传自定义情报。

【失陷检测情报列表】：展示 IOC 名称、类型、情报标签、严重性、命中次数、告警主机数。



IOC	类型	情报标签	严重性	来源	时间	命中次数	告警主机数	操作
fget-career.com	DOMAIN	ramnit域名	▲ 高危	custom	2021-03-29 15:45:31	214	13	白名单 编辑 删除
linenews.mypicture.info	DOMAIN	info_idc111...	▲ 严重	custom	2021-01-04 15:57:35	207	14	白名单 编辑 删除
mail-csits.org	DOMAIN		▲ 高危	TIP-tip1111	2021-04-12 12:01:55	0	0	白名单 编辑 删除
mail-csg.xyz	DOMAIN		▲ 高危	TIP-tip1111	2021-04-12 12:01:55	0	0	白名单 编辑 删除
acfgov.com	DOMAIN		▲ 高危	TIP-tip1111	2021-04-12 12:01:55	0	0	白名单 编辑 删除
microsoft1.space	DOMAIN		▲ 高危	TIP-tip1111	2021-04-12 12:01:55	0	0	白名单 编辑 删除
cgbchina.xyz	DOMAIN		▲ 高危	TIP-tip1111	2021-04-12 12:01:55	0	0	白名单 编辑 删除
cgbchina.online	DOMAIN		▲ 高危	TIP-tip1111	2021-04-12 12:01:55	0	0	白名单 编辑 删除

### IP 信誉情报：

- 【搜索功能】可根据 IP 地址、情报标签进行搜索
- 【情报来源】可根据情报来源进行筛选
- 【新增 IP 信誉】支持 IP 信誉情报导入
- 【IP 信誉列表】：展示 IP 地址、情报标签、情报来源、更新时间



The screenshot shows the TDP interface with the '自定义情报' (Custom Intelligence) section active. The page title is '失陷检测情报' (Compromised Detection Intelligence). There are two tabs: '失陷检测情报' and 'IP信誉情报' (IP Reputation Intelligence). The 'IP信誉情报' tab is selected, showing a list of IP addresses with associated tags and sources.

1. 录入自定义IP情报后, TDP会自动将情报标签与对应IP地址的告警/行为日志相关联, 提供更丰富的上下文展示。  
2. 如果您同时使用了微步在线威胁情报管理平台(TIP), 则可通过配置与TIP联动, 自动从TIP同步IP信誉情报。 [点击前往配置](#)  
3. 如果您没有开启全流量记录模式, 命中自定义IP信誉情报的流量日志默认不会记录, 如果您希望记录, 可在设备配置功能中进行设置。 [点击前往配置](#)

Table data:

IP地址	情报标签	情报来源	更新时间	操作
188.166.164.164	exploit.HW2021	TIP-tip1111	2021-04-12 12:01:55	<a href="#">编辑</a> <a href="#">删除</a>
183.141.61.119	exploit.HW2021	TIP-tip1111	2021-04-12 12:01:55	<a href="#">编辑</a> <a href="#">删除</a>
173.208.153.34	exploit.HW2021	TIP-tip1111	2021-04-12 12:01:55	<a href="#">编辑</a> <a href="#">删除</a>
178.62.78.40	exploit.HW2021	TIP-tip1111	2021-04-12 12:01:55	<a href="#">编辑</a> <a href="#">删除</a>
178.62.72.12	exploit.HW2021	TIP-tip1111	2021-04-12 12:01:55	<a href="#">编辑</a> <a href="#">删除</a>
122.190.43.149	exploit.HW2021	TIP-tip1111	2021-04-12 12:01:55	<a href="#">编辑</a> <a href="#">删除</a>

## 4.4 攻击者分析

攻击者分析页面, 列出所有 TDP 检测到的攻击 IP, 通过微步情报, 历史攻击/访问行为, 微步云端数据等, 对攻击者特征进行综合计算, 为企业安全运营团队在日常安全运营和重保防御过程中提供参考。

## 4.4.1 攻击者分析列表

攻击者分析列表，将系统检测到以及云端共享的所有攻击者展示出来，以便于企业安全人员了解攻击来源，明确威胁水平，提高应对能力。

The screenshot shows the 'Attacker Analysis' (攻击者分析) page in the ThreatBook TDP interface. The page is divided into several sections:

- Search and Filter Section:** Includes input fields for 'Attacker IP' (攻击者IP), 'Attack Method' (使用攻击手法), and 'Geographic Location' (地理位置). There is also a slider for 'Attack Visit Ratio' (攻击访问占比) ranging from 0 to 100. Filter buttons include 'Active' (活跃度), 'Attack Level' (攻击水平), 'Targeted' (针对性), and 'Control Assets' (掌握资产). A 'Clear' (清空) button and a 'Search' (搜索) button are also present.
- System Detection and Cloud Sharing:** Two tabs at the top of the main content area: 'System Detection' (系统检测) and 'Cloud Sharing' (云端共享).
- Attacker List Table:** A table displaying detected attackers with columns for 'Attacker IP', 'Latest Attack Time', 'Status', 'Attack Visit Ratio', 'Attacker Characteristics', 'Attack Methods', and 'Actions'.
 

攻击者IP	最近攻击时间	情报标签	攻击访问占比	攻击者特征	攻击手法	操作
61.160.247.70 中国 江苏 常州	刚刚	IDC服务器	18%	手法多样 IP绑定了域名	b374k WebsHELL连接成功 扫描黑客WebsHELL后门 ...等17种	查看详情   +关注   +阻断
52.196.17.52 日本 东京都 东京	刚刚	IDC服务器	79%	IP绑定了域名	利用ngrok进行内网穿透	查看详情   +关注   +阻断
3.15.53.92 美国 俄亥俄州 都柏林	刚刚	-	73%	IP对外开放端口 IP绑定了域名	利用ngrok进行内网穿透	查看详情   +关注   +阻断
70.127.242.253 美国 佛罗里达州 坦帕	刚刚	Dynamic IP	71%	新发现的攻击者，正在分析中...	扫描黑客WebsHELL后门(base64传输) 暴力websHELL模拟终端执行命令 ...等4种	+关注   +阻断
208.51.206.168 美国 美国	刚刚	-	36%	新发现的攻击者，正在分析中...	MySQL注入 预测管理后台 ...等3种	+关注   +阻断

页面路径：

- 1.从导航菜单进入调查页面
2. 选择“调查-攻击者分析”子菜单项，来到攻击者分析页面。

This screenshot shows the filter section of the Attacker Analysis page. It includes input fields for 'Attacker IP', 'Attack Method', and 'Geographic Location'. A slider for 'Attack Visit Ratio' is set to 0. Filter buttons include 'Active', 'Attack Level', 'Targeted', and 'Control Assets'. A 'Clear' button and a 'Search' button are also present.

【攻击者筛选】系统支持用户使用以下字段进行攻击者筛选，包括攻击者 IP、攻击者使用手法、攻击者所在的地理位置以及攻击者攻击/访问占比。

【攻击者特征筛选】系统定义了以下特征，同时支持用户根据进行对攻击者筛选。

攻击者特征	攻击者名称	含义
活跃度	攻击时间长	说明攻击者的攻击天数大于 3 天。
攻击水平	手法多样	攻击者使用多种手法进行攻击。

	手法高级	攻击者使用了高水平的攻击手法, 体现出了较高的能力水平。
针对性	攻击多个系统	攻击者针对多个系统进行攻击。
	手动攻击	攻击者使用非自动化等攻击手法, 说明是针对性很强的攻击者。
	攻击过同行	攻击者近期攻击过当前客户同行业的客户。
掌握资产	与其他 IP 共同攻击	攻击者使用多个 IP 共同攻击。
	IP 对外开放端口	攻击者 IP 对外开放了端口。
	IP 绑定了域名 (可溯源)	攻击者 IP 绑定了域名, 可通过 whois 进行溯源。

【只看关注的攻击者】勾选“已关注”选项, 可以只查看用户关注的攻击者。

【攻击者列表自动刷新】支持攻击者列表的自动刷新, 用户可以选择自动刷新的时间间隔。

【系统检测中攻击者列表】展示攻击者的攻击 IP、地理位置、最近攻击时间、情报标签、攻击访问占比、攻击者特征、攻击手法以;

攻击者列表支持下载;

点击“查看详情”, 可以查看次攻击者的具体内容;

点击“关注”, 则用户对此 IP 进行了关注;

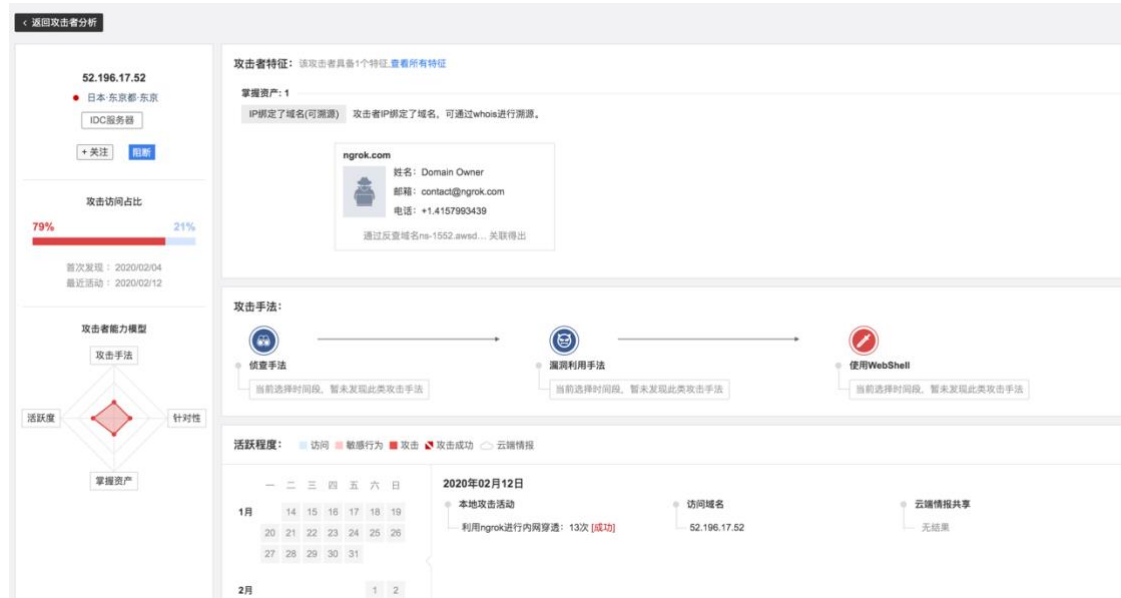
点击“+ 阻断”, 用户可以将这个攻击者 IP 添加至阻断列表。

攻击者IP	最近攻击时间	情报标签	攻击访问占比	攻击者特征	攻击手法	操作
61.160.247.70 中国 江苏 常州	刚刚	IDC服务器	18%	手法多样 IP绑定了域名	b374k WebsHELL连接成功 扫描黑客WebsHELL后门 ...等17种	查看详情 + 关注 + 阻断
52.196.17.52 日本 东京都 东京	刚刚	IDC服务器	79%	IP绑定了域名	利用ngrok进行内网穿透	查看详情 + 关注 + 阻断
3.15.53.92 美国 俄亥俄州 都柏林	刚刚	-	73%	IP对外开放端口 IP绑定了域名	利用ngrok进行内网穿透	查看详情 + 关注 + 阻断
70.127.242.253 美国 佛罗里达州 坦帕	刚刚	Dynamic IP	71%	新发现的攻击者, 正在分析中...	扫描黑客WebsHELL后门(base64传输) 菜刀websHELL虚拟终端执行命令	+ 关注 + 阻断

【云端共享中攻击者列表】展示攻击者的攻击 IP、地理位置、最近攻击时间、情报标签、攻击访问占比、攻击者特征、攻击手法以; 点击“+ 阻断”, 用户可以将这个攻

击者 IP 添加至阻断列表。

## 4.4.2 攻击者详情



页面路径：

点击系统检测中某个攻击者 IP 的“查看详情”按钮，来到对应的攻击者详情页面。

【攻击者基本属性】展示攻击者的 IP、地理位置、云端情报标签；同时展示用户的攻击访问比，首次发现时间和最近活动时间；展示攻击者的能力模型，包括攻击手法、针对性、掌握资产和活跃度。

【攻击者特征】展示攻击者的所有特征，默认会将不具备的攻击者特征隐藏，点击“查看所有特征”会展示全部。如果攻击者可溯源，则会展示溯源到的攻击者真实信息，展示绑定的域名，以及注册域名时的姓名、电话和邮箱。

【攻击手法】展示攻击者的所有攻击手法，按照侦查手法、漏洞利用手法和使用 webshell 进行区分。

【活跃程度】展示了近 30 天内，攻击者的活跃程度，以及每天的具体行为。行为主要包括：访问、敏感行为、攻击、攻击成功和云端情报。点击日历中具体的某一天，

可以查看对于天的本地攻击活动、访问的域名，以及当天此 IP 的云端共享情报。

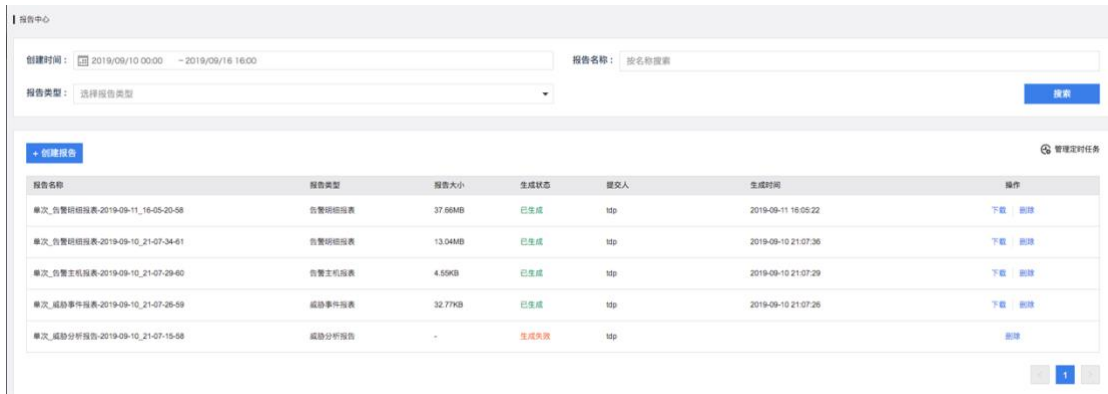
【掌握资产】展示了此攻击者使用的攻击 IP 个数、掌握的域名个数、浏览器 User-Agent 个数和攻击使用的 cookie。Cookie 的 key 和 value 的值会以列表的形式呈现。

## 五、报告

### 5.1 报告中心

页面路径：

- 1.从导航菜单进入报告页面
2. 选择“报告-报告中心”子菜单项。



报告中心，支持用户导出以下四类报告：

告警明细报表 (.csv) :最细粒度的报表，每一行代表一次告警

威胁事件报表(.csv)：每一行统计相同主机相同告警行为发生次数，和最近一次完整告警信息

告警主机报表(.csv)：每台告警主机一行数据，聚合展示威胁事件，统计告警次数

威胁分析报告(.doc)：综合性报告，多角度完整地描述了组织内的威胁情况

创建报告方法：

- 1.从导航菜单进入报告页面
2. 点击页面上“创建报告”按钮，弹出“编辑报告”弹窗，选择需要创建的报告类型，选定时间范围、生成周期，点击确定就可以说生成。

报告列表如下：

报告名称	报告类型	报告大小	生成状态	提交人	生成时间	操作
单次_告警明细报表-2019-09-11_16-05-20-58	告警明细报表	37.66MB	已生成	tdp	2019-09-11 16:05:22	下载 删除
单次_告警明细报表-2019-09-10_21-07-34-61	告警明细报表	13.04MB	已生成	tdp	2019-09-10 21:07:36	下载 删除
单次_告警主机报表-2019-09-10_21-07-29-60	告警主机报表	4.55KB	已生成	tdp	2019-09-10 21:07:29	下载 删除
单次_威胁事件报表-2019-09-10_21-07-26-59	威胁事件报表	32.77KB	已生成	tdp	2019-09-10 21:07:26	下载 删除
单次_威胁分析报告-2019-09-10_21-07-19-58	威胁分析报告	-	生成失败	tdp		删除

包含内容有：

报告名称、报告类型、报告大小、生成状态、提交人、生成时间。用户可以点击操作这一列，进行报告的下载和删除。

定时任务管理：

用户点击“管理定时任务”按钮，就会来到定时任务管理页面，可以对定时任务进行编辑、修改和禁用。

报告名称	报告类型	状态	创建用户	创建时间	生成周期	下一次生成时间	操作
定时_告警明细报表	告警明细报表	启用	tdp	2019-09-23 14:03:40	每周-1:00	2019-09-30 01:00:00	编辑 禁用 删除
定时_告警明细报表	告警明细报表	启用	tdp	2019-09-11 16:08:17	每周三1:00	2019-09-25 01:00:00	编辑 禁用 删除
定时_告警主机报表	告警主机报表	启用	tdp	2019-08-30 00:21:40	每周-0:00	2019-09-30 00:00:00	编辑 禁用 删除
定时_威胁事件报表	威胁事件报表	启用	dd	2019-08-29 20:16:51	每月1日1:00	2019-10-01 01:00:00	编辑 禁用 删除
定时_告警明细报表	告警明细报表	启用	dd	2019-08-29 19:57:58	每周二3:00	2019-09-24 03:00:00	编辑 禁用 删除
定时_告警明细报表	告警明细报表	启用	dd	2019-08-29 19:57:17	每周-2:00	2019-09-30 02:00:00	编辑 禁用 删除
定时_告警明细报表	告警明细报表	启用	dd	2019-08-29 19:48:04	每周-2:00	2019-09-30 02:00:00	编辑 禁用 删除
定时_告警明细报表	告警明细报表	启用	dd	2019-08-29 19:35:15	每周三2:00	2019-09-25 02:00:00	编辑 禁用 删除
定时_告警明细报表	告警明细报表	启用	dd	2019-08-29 19:22:12	每周四1:00	2019-09-26 01:00:00	编辑 禁用 删除
定时_威胁事件报表	威胁事件报表	启用	dd	2019-08-29 19:08:33	每周三1:00	2019-09-25 01:00:00	编辑 禁用 删除
定时_告警明细报表	告警明细报表	启用	dd	2019-08-29 19:00:48	每周二1:00	2019-09-24 01:00:00	编辑 禁用 删除

## 六、处置

### 6.1 阻断

阻断功能是为用户提供处理外部攻击的一种方式，当前支持旁路阻断或联动阻断，用户可自定义配置阻断方式进行阻断。

旁路阻断：



联动阻断：



#### 6.1.1 阻断策略

##### 旁路阻断

通过旁路部署，向攻击方和被攻击方双向发 reset 包来实现，要实现封禁需要确保 tdp 的包能发出去，否则无效。

【阻断列表】IP、添加时间、过期时间、状态、添加来源、阻断次数、备注

【新增阻断】支持手段添加 IP、自动阻断策略配置

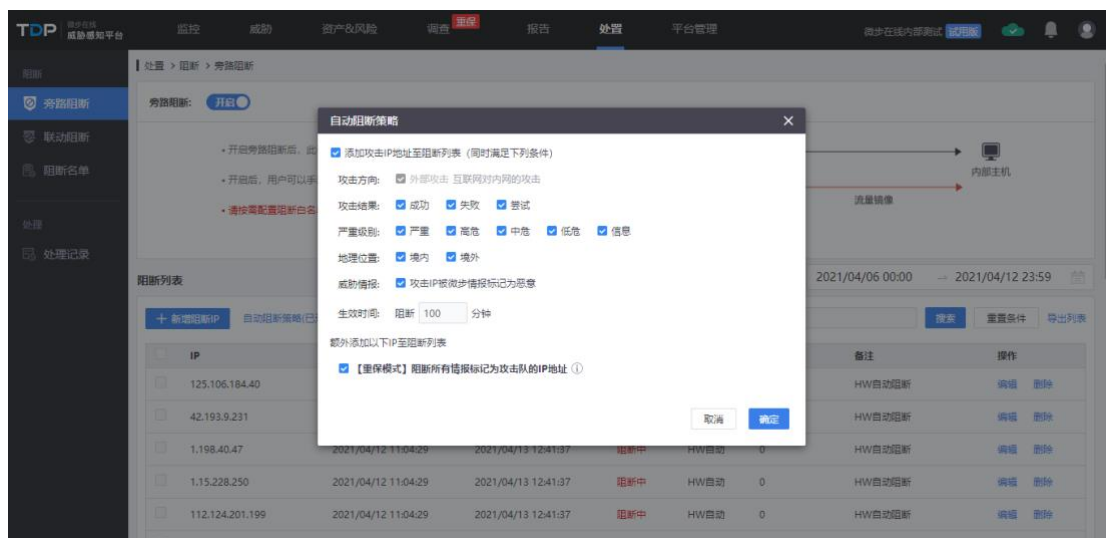
【筛选条件】可根据来源、状态、IP 进行筛选及搜索

##### 自动阻断

用户可以选择自动阻断策略配置，发生外部攻击的 IP，将会被自动添加至阻断列



表。用户可以自定义这些 IP 的阻断时间，时间范围限制在 10 分钟到 30 天内。



## 联动阻断

通过策略生成阻断 IP List 与第三方设备联动从而达到阻断的效果



【阻断策略配置】进行阻断 IP 策略配置，可进行相关配置生成阻断 IP List

【阻断 IP】通过阻断策略生成 IP List 展示该链接

## 阻断白名单

IP 白名单

用户可以添加阻断的白名单，支持单一 IP、网段和 IP 区间。

情报、规则、模型 ID 白名单

在白名单中的情报/规则/模型 ID 关联的攻击 IP 不会被阻断

## 阻断黑名单

在阻断黑名单中的威胁 ID，均会被阻断。

## 6.2 处理

### 处理记录

TDP 在处置中增加了处理记录，用来记录用户在威胁中将告警主机进行过处置的内容整理，方便与处置结果的查询。

【筛选】可根据处理结果、事件范围、告警主机、威胁事件、经办人进行查询筛选

【下载】可以进行处理列表的下载

【列表展示】包含处理时间、告警主机、威胁事件、处置人、处理结果、备注



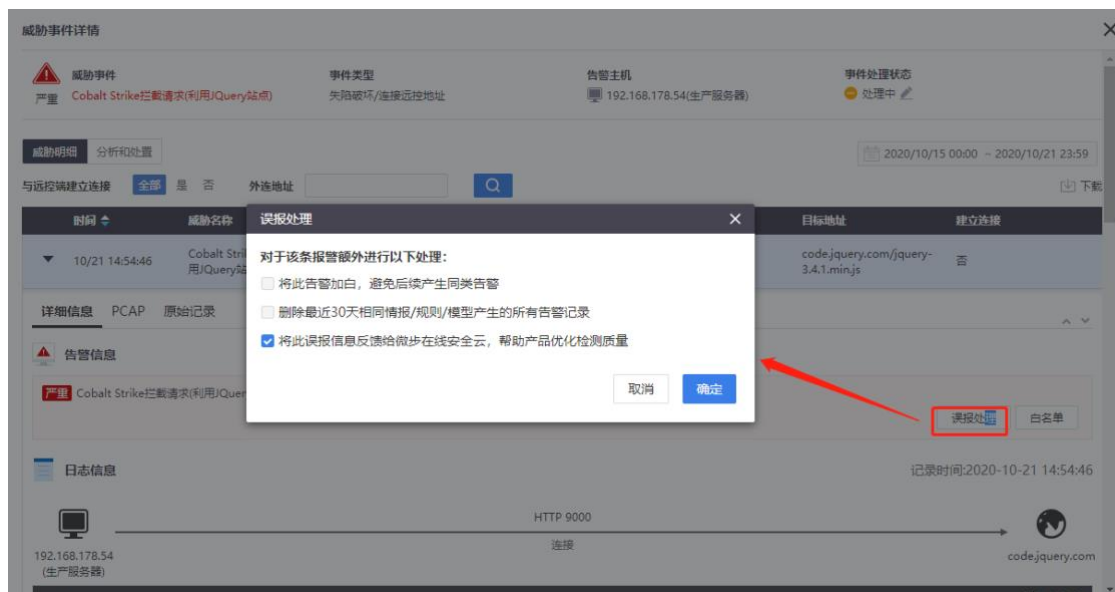
处理时间	告警主机	威胁事件	处置人	处理结果	备注	操作
2020/10/22 13:45:24	192.168.178.54(生产服务器)	Cobalt Strike拦截请求(利用/Query站点)	tdp	处理中	测试信息	删除
2020/10/22 11:41:29	192.168.178.54(生产服务器)	Cobalt Strike拦截请求(利用/Query站点)	tdp	未处理		删除
2020/10/22 11:41:29	192.168.178.54(生产服务器)	Cobalt Strike拦截请求(利用/Query站点)	tdp	已处理/无需处理		删除
2020/10/20 17:41:38	192.168.178.121(生产服务器)	全部威胁事件	tdp	未处理		删除
2020/10/20 17:41:12	192.168.178.121(生产服务器)	利用struts2漏洞	tdp	处理中		删除
2020/10/20 17:41:03	192.168.178.121(生产服务器)	全部威胁事件	tdp	已处理/无需处理		删除
2020/10/20 17:40:46	192.168.178.121(生产服务器)	Struts2 远程代码执行漏洞(CVE-2017-5638)	tdp	已处理/完成处理		删除
2020/10/20 17:40:35	192.168.178.121(生产服务器)	Cobalt Strike拦截请求(利用/Query站点)	tdp	处理中		删除

## 七、误报反馈

TDP 支持用户将系统产生的误报告警反馈至云端，同时用户可以删除同类型的告警，并按照自定义规则加白。

页面路径：

在任意告警的详细内容模块，点击“误报处理”按钮，即可进行误报反馈



选择“将此告警加白”时，用户可以选择将同类型的告警删除；同时也可以选择删除最近 30 天相同情报/规则/模型产生的所有告警记录；也可以进行将误报信息反馈给微步在线安全云，帮助产品优化检测质量。

## 误报反馈



以上误报已收到，感谢您的反馈！后续核实后会及时联系您。

对于该条报警额外进行以下处理：

针对此类告警进行加白，加白后不再产生告警

白名单策略：

匹配字段	匹配策略	匹配内容	
规则/情报/模... ▼	属于	S2019010046	✓ ✕
<a href="#">+ 新增条件</a>			

- 支持对规则/情报/模型IP, url, 文件HASH加白
- 多个条件组合, 则每个条件都命中时才生效
- uri支持匹配字符串或者正则表达式

生效时间：

永久

延长  分钟

生效至

删除近30天相同规则/模型/情报产生的所有告警

取消

确定