天翼云·态势感知

用户使用指南

天翼云科技有限公司

目录

1. 产品介绍

1. 1产品定义

态势感知为用户提供统一的威胁检测和风险处置平台。态势感知能够帮助用户检测云上资产遭受到的各种典型安全风险，还原攻击历史，感知攻击现状，预测攻击态势，为用户提供强大的事前、事中、事后安全管理能力。

态势感知系统通过资产管理、脆弱性评估、威胁检测等手段完成用户网络的安全检查、风险评估、可视化呈现。同时，通过与国家应急响应中心（CNCERT）权威监测平台的威胁情报、知识库对接，动态实时的完成应急协同、威胁情报接入、信息流转、防护规则更新等信息交换，做到用户安全风险的快速发现和信息闭环。

1. 2产品优势

1.2.1协同应急

对接国内最权威的网络安全监测平台，与国家应急响应中心（CNCERT）形成联动能力，及时发现用户单位网络安全威胁。

1.2.2动态评估

按照资产、威胁、脆弱性多维度的风险评估标准，动态调整各风险权重，发现和分析潜在的威胁和脆弱点，进行预防、控制和修复。

1.2.3风险可视

实时呈现网络攻击态势、资产威胁、资产漏洞、安全态势评分，同步展示国家应急响应中心发布的威胁预警、安全资讯。

1. 3功能特性

1.3.1基础版及通用功能

资产发现

通过主被动两种资产探测方式，实时精准的持续监控资产变化情况，可自动识别网络设备、主机、安全设备、操作系统、数据库、web 应用等。

资产管理

资产组件信息、变化趋势、端口分布、归属、操作系统分布自动化统计。可根据 IP、操作系统、应用组件/服务、归属部门、硬件信息等进行资产高级检索，快速统计资产信息、根据资产特征排查安全隐患。

脆弱性检测

通过漏洞扫描完成资产脆弱性评估，漏洞库可覆盖当前网络环境中主流的操作系统、数据库、web 中间件、网络设备漏洞，同时，对接国家安全监测平台的漏洞预警、安全事件通报及漏洞检测规则，完成检测规则的更新，有效应对突发安全事件，支持以资产存在漏洞及漏洞影响资产两个维展示脆弱性资产。

网络威胁检测

根据网络流量可识别丰富的网络应用层协议，通过协议分析、内容萃取等报告对应的异常事件。可检测勒索软件、恶意软件、信息泄露、C&C 通信、扫描探测、暴力破解、系统提权、web 攻击等网络威胁。同步国家能力中心下发的恶意 URL、域名等信誉数据，完成新型威胁及高级持续威胁的检测。

1.3.2高级版功能

权威情报数据

借助国内顶尖厂家共同分析的结果，快速构建威胁信誉库，将诸如僵尸木马活动、恶意代码传播、恶意攻击行为、恶意站点数据等网络安全事件及信誉数据同步至本系统，形成联动能力。

权威安全预警

定时同步国家应急响应中心（CNCERT）的漏洞预警、威胁情报、安全资讯数据，及时明晰最新安全信息。

攻击源警告

当系统检测到远端 IP 地址存在恶意入侵或者探测行为时，可以配置对应的 IP 进行告警，告警页面的内容可以自定义，当此 IP 再次连接 WEB 服务时，对其推送告警界面，以做警示。

恶意网站警告

通过国家应急响应中心信誉库自动同步恶意网站数据，在用户访问恶意网站时，给予及时告警，协助用户识别 WEB 威胁，同时运维管理员可自定义添加恶意网站。

安全态势大屏

支持 4 种态势大屏，包括全局态势大屏、资产态势大屏、脆弱性态势大屏、威胁态势大屏。

1.4应用场景

态势感知适用于安全需求较高、经常遭受个人或组织网络攻击的央企、政府、医疗、教育、金融等大型企事业单位。

1.4.1边界安全应用场景

重点行业信息系统

能源、金融、交通、教育、医疗、市政、电信与互联网、政府部门等支撑关键业务的信息系统； 态势感知将通过监控网络资产状态，结合威胁情报、脆弱性检测、威胁检测及时有效地发现网络资产是否存在挖矿勒索系统后门及告警网络攻击，通过漏洞扫描与基线扫描，直观地了解自身的安全状况，同时动态实时地监控管理业务资产。

电子政务和门户

各级党政军门户网站，教育类网站，重大活动及会议保障， 重点新闻网站等；态势感知将通过监控网络资产状态，结合威胁情报、脆弱性检测、威胁检测及时有效的发现网络资产是否存在挖矿勒索系统后门及告警网络攻击，通过漏洞扫描与基线扫描，直观地了解自身

的安全状况，同时动态实时地监控管理业务资产。

1.4.2IPV6 双栈应用场景

大型互联网平台

注册用户、订单额或交易额较大，一旦发生网络安全事故，产生较严重影响，如敏感信息泄露、基础数据泄露等；态势感知将通过监控网络资产状态，结合威胁情报、脆弱性检测、威胁检测及时有效地发现网络资产是否存在挖矿勒索系统后门及告警网络攻击信息泄露安全事件，通过漏洞扫描与基线扫描，直观地了解自身的安全状况，同时动态实时地监控管理业务资产。

生产业务类系统

政府机关面向公众服务的业务系统，或与医疗、安防、消防、应急指挥、生产调度、交通指挥等相关的城市管理系统。态势感知将通过监控网络资产状态，结合威胁情报、脆弱性检测、威胁检测及时有效地发现网络资产是否存在挖矿勒索系统后门及告警网络攻击，通过漏洞扫描与基线扫描，直观地了解自身的安全状况，同时动态实时地监控管理业务资产。

1.5规格

态势感知产品根据提供的功能不同分为两个版本：基础版、高级版。

基础版和高级版功能清单如下：

功能	基础版	高级版
安全可视化	√	√
资产发现	√	√
资产管理	√	√
脆弱性检测	√	√
网络威胁检测	√	√
国家情报数据		√
国家安全预警		√
攻击源警告		√

恶意网站告警		√
安全态势大屏		√

云主机规则参照下表：

弹性云主机（Linux）	服务器配置	设备性能	扩展性	作用	备注
一台双网卡弹性云主机	8 核 CPU/64G 内存/100G 系统盘/1T 数据盘	此配置可处理 800M 以下流量	提高硬件配置，可提高处理性能	态势感知控制器，通过资产、脆弱性、威胁多维度动态评估风险可视化	用于安装态势感知控制器
一台双网卡弹性云主机	4 核 CPU/8G 内存/50G 系统盘	此配置可处理 1000M 以下流量	不涉及	虚拟网关系统，将访问业务系统的所有流量镜像给态势感知控制器分析	用于安装态势感知虚拟网关

2. 计费说明

2. 1计费模式

提供包年/包月计费模式，最少 1 个月，最多 3 年，按照标准价格按照 6 折计算，实际价格以官网为准。收费标准根据版本（基础版/高级版）、待监控云主机 IP 数、订购周期进行收费，态势感知软件计费模式如下:

产品规格	标准价格（元/月/IP）
基础版	330
高级版	4200

2. 2续订

态势感知软件续订，使用下面的链接进入态势感知已购页面，点击“续订”按钮，进入续订界面，选择续订周期进行续订。页面截图如下：

https://www.ctyun.cn/h5/orderconsole/cnt/console/public?agencyId=0e1ba74b57029e641fe0c017c878e10c&region=cn-hbwh1&locale=zh-cn

2. 3升级

态势感知软件升级，包括升级监控云主机台数和版本，比如用户当前是基础版，可以升级至高级版，还可以选择升级新增待监测 IP 数量。使用下面的链接进入态势感知已购页面，点击“升级”按钮，进入升级界面，选择升级的版本和新增待监测 IP 数量进行升级。页面截图如下：

https://www.ctyun.cn/h5/orderconsole/cnt/console/public?agencyId=0e1ba74b57029e641fe0c017c878e10c&region=cn-hbwh1&locale=zh-cn

2. 4到期

态势感知软件到期后，无法登录态势感知页面，为避免影响使用，到期前请及时续订。

3. 快速入门

3. 1态势感知控制台登录及内网 IP 配置

3. 1. 1登录

（1）打开浏览器（支持以下浏览器：Google Chrome、firefox、Edge），用 HTTPS 方式连接内网系统部署的设备 IP 的地址，回车打开登录界面。导入授权。（授权会在购买成功后，通过邮件的形式发送到邮箱）

（2）进入下图所示的登录页，输入默认登录名及密码：Administrator/Changenow@123（首次登陆后请修改默认密码），输入验证码，单击登陆进入系统。

3.1.2内网 IP 配置

首次登录系统，或管理的 ip/ip 段变化时，需在系统管理→系统设置→内部 IP 管理菜单页面，进行 ip/ip 段的增加、编辑、删除。添加内网 IP，可以明确流量流向，明确威胁检测的异常行为阶段，明确资产扫描发现的资产的详细归属信息，方便资产扫描、漏洞扫描添加任务时选择需要扫描的资产，明确扫描范围。

ip/ip 段添加、编辑时需要填写相关信息，包括：所属公司、部门、地区、责任人、联系电话、联系邮箱，红色星号标明的字段为必填项。

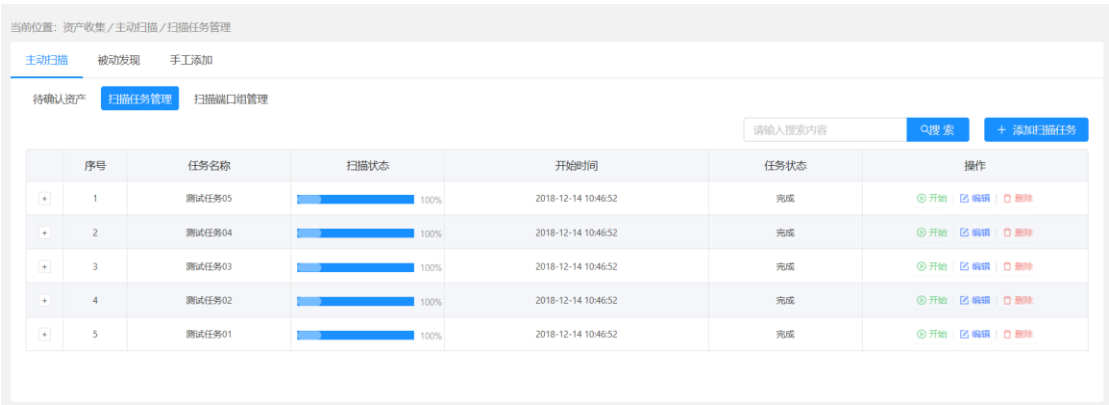
3. 2资产管理

3. 2. 1资产收集

系统支持三种方式的资产收集

主动扫描

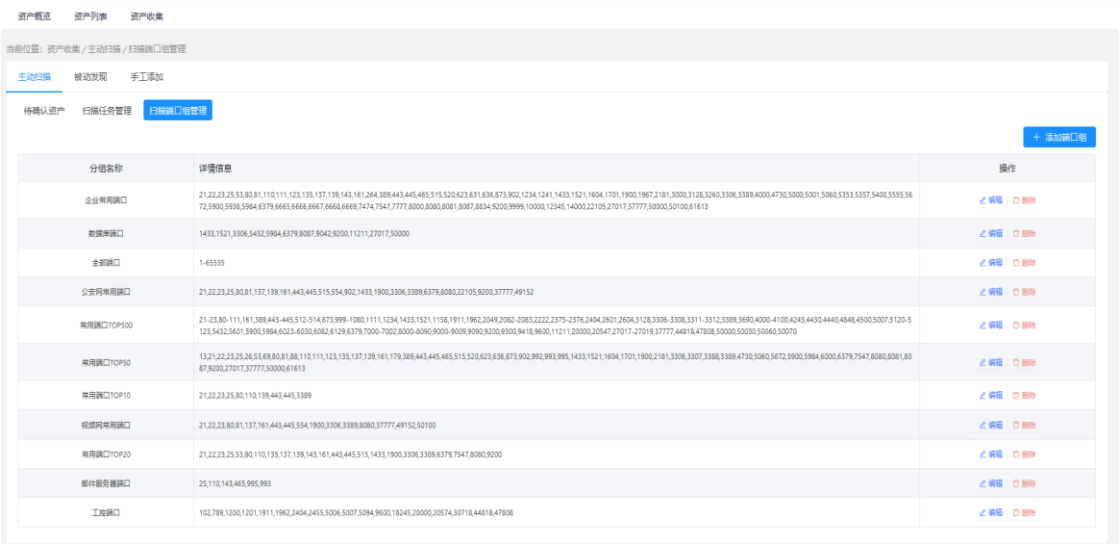
资产扫描任务管理，需在资产管理→资产收集→主动扫描→扫描任务管理页面添加、删除、编辑、开始、暂停。



添加扫描任务时，需要填写任务名称、扫描的资产（扫描资产可以从内网资产中选择，也可任意添加）、扫描端口（系统内置多个类型的端口组，也可以任意添加单个或多个）、

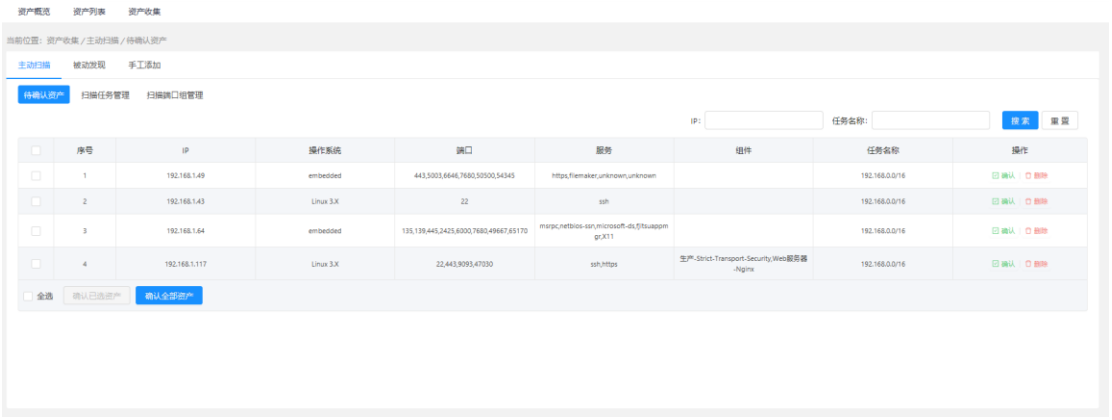
扫描类型（支持单次或周期）、扫描速度（支持慢速、中速、快速，扫描速度根据单位带宽情况选择）、允许扫描时间段。

扫描端口组管理，根据不同的网络环境，系统内置多个扫描的端口组，支持添加、编辑、删除扫描端口组。



主动扫描发现的资产，可以通过开关控制，是否需要人工确认，如不需要进行人工确认，发现的资产直接进入资产列表。如需要人工确认，扫描发现的资产进入资产管理→主动扫描

→待确认资产页，可以单个或批量确认资产，确认后进入资产列表。



被动发现

在资产管理→资产收集→被动发现页面，展示通过对流量分析发现的存活资产及操作系统。被动发现的资产，可以通过开关控制，是否需要人工确认，如不需要进行人工确认，发现的资产直接进入资产列表。如需要人工确认，在被动发现页面，可以单个或批量确认资产，确认后进入资产列表。

手工添加

在资产管理→资产收集→手工添加页面，添加资产 IP、归属信息、责任人、联系方式、硬件信息、厂商等信息后点击保存。

资产确认设置

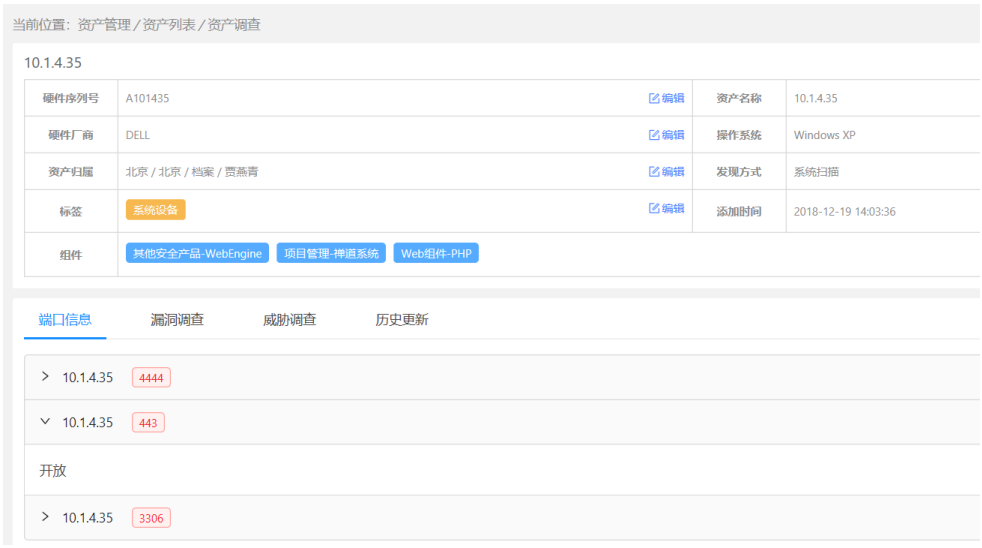
主动扫描、被动发现的资产，通过开关控制，是否需要人工确认，资产入库配置开关，在系统管理→系统设置→功能配置菜单页面，默认关闭。

3. 2. 2资产列表

资产管理→资产列表页显示确认的全部资产 IP 地址、操作系统、组件、标签、资产归属、责任人、更新时间等信息，支持高级搜索及资产导出。点击操作按钮，可以自定义显示

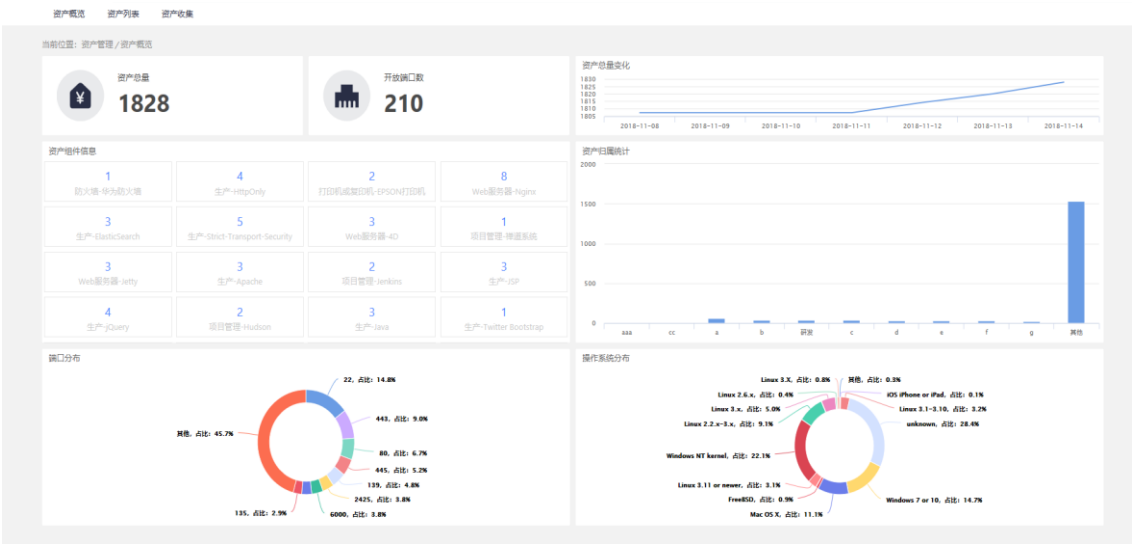
列表字段。点击列表左侧“+”按钮，可以查看资产的硬件序列号、硬件厂商、端口、服务、漏洞、威胁等信息。

点击资产详情，查看资产的属性信息，查看资产的端口开放、资产的漏洞数量、威胁数量、历史更新。



3. 2. 3资产概览

在资产管理→资产概览页面，查看资产的相关统计情况。资产总量，统计了收集到的所有资产。开放端口数，统计了资产使用的端口情况。资产总量变化，显示最近 7 次的扫描结果变化情况。设备类型分类，统计各种设备类型及数量。资产归属统计，按照部门统计资产数量。端口分布，统计端口的使用情况占比。操作系统分布，统计资产的操作系统占比。



3. 3脆弱性检测

3. 3. 1漏洞扫描

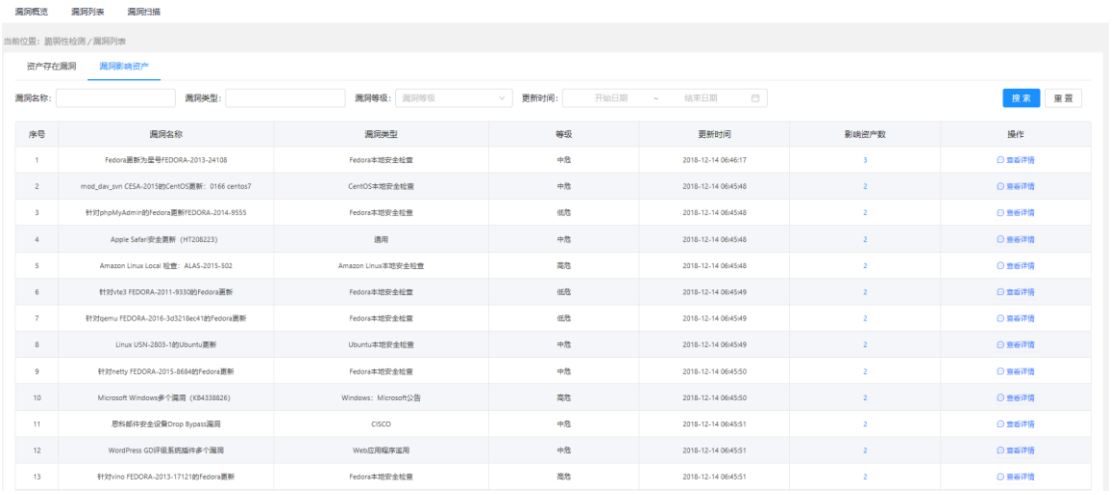
在脆弱性检测→漏洞扫描页面，对漏洞扫描任务进行管理，支持添加、暂停、编辑、删除漏洞扫描任务。

添加漏洞扫描任务，填写任务名称，选择扫描的资产即可。

3. 3. 2漏洞列表

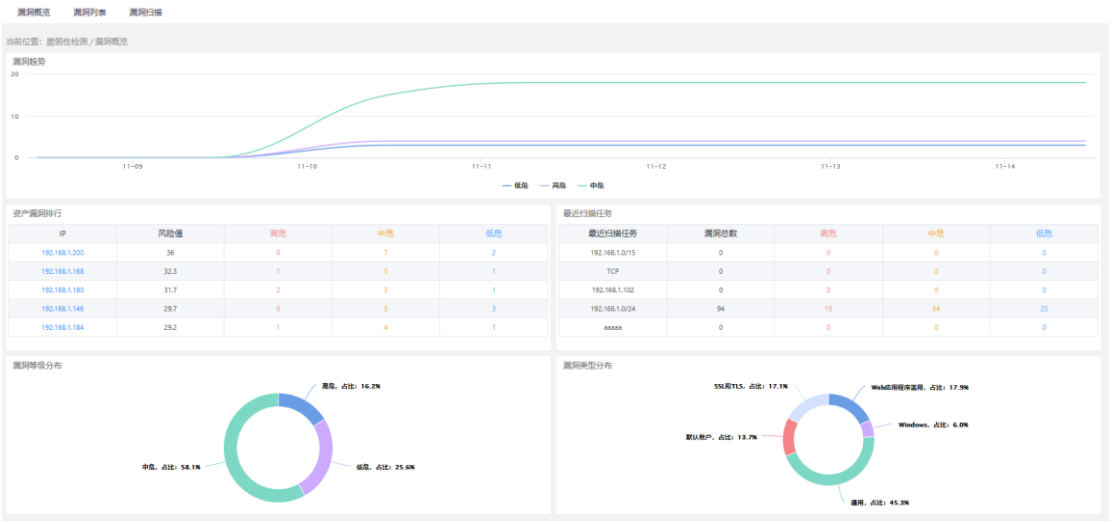
在脆弱性检测→漏洞列表页面，可以查看漏洞扫描的结果。漏洞列表以资产和漏洞维度，分别列出资产存在的漏洞列表及漏洞影响资产列表。资产存在漏洞列表展示资产 IP、漏洞名称、等级、影响组件、更新时间，点击查看详情可以看到漏洞描述、危害和解决方案信息。支持根据漏洞名称、对应资产、漏洞等级、更新时间等条件的检索。

漏洞影响资产列表，以漏洞维度展示对资产的影响情况。展示漏洞名称、漏洞类型、等级、更新时间、影响资产数量，点击查看详情可以看到漏洞描述、危害和解决方案信息。支持根据漏洞名称、漏洞类型、漏洞等级、更新时间等条件的检索。



3. 3. 3漏洞概览

在脆弱性检测→漏洞概览页面分析整体 IT 资产漏洞趋势、等级和类型分布。漏洞趋势统计最近 7 天的高危、中危、低危漏洞的数量变化曲线。资产漏洞排行，根据漏洞扫描的结果，统计漏洞风险值最高的前 5 个 IP 资产。最近扫描任务，统计最近 5 次的漏洞扫描任务结果，统计每个任务的漏洞总数、高危漏洞数、中危漏洞数、低危漏洞数。漏洞等级分布，统计高危、中危、低危每个等级发现的漏洞总数及占比。漏洞类型分布，统计漏洞数最多的前 15 种漏洞类型的数量及占比。



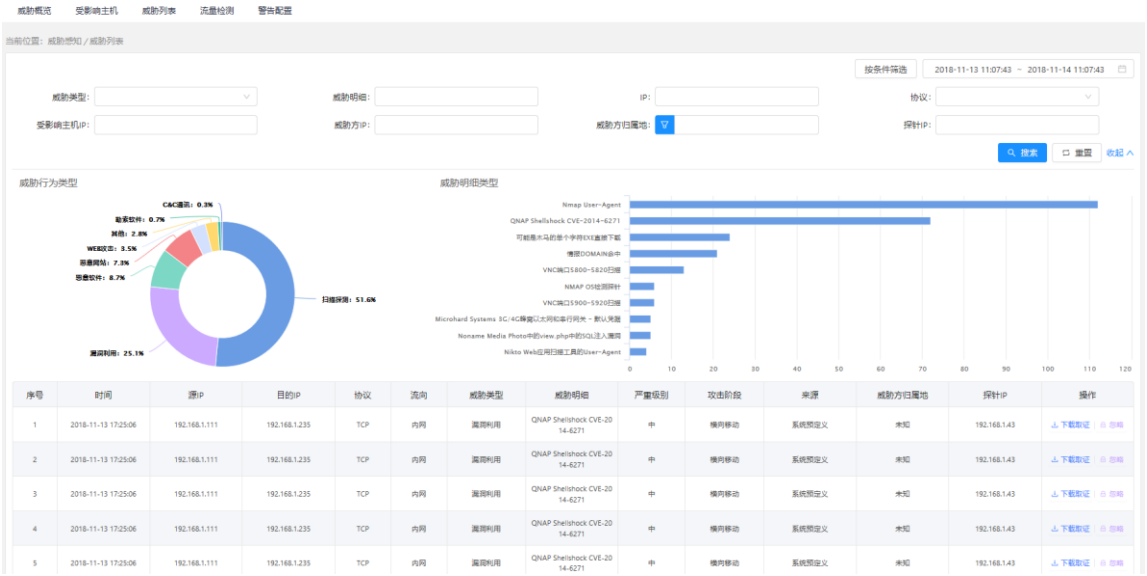
3.4威胁检测

3.4.1威胁概览

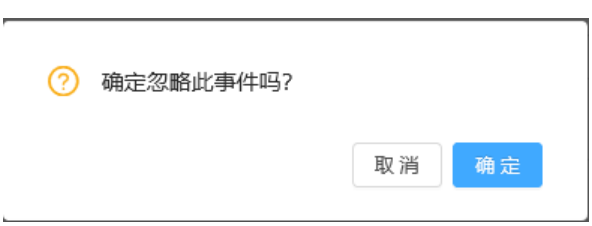
在威胁检测→威胁概览页面，主要统计分析当前用户环境所面临的威胁情况。具体包括异常行为的总量及高危异常行为类型 TOP3。统计最近 24h 的异常行为类型及数量。根据最近 24h 的异常行为数量，统计受影响主机 TOP5，表格展示资产 IP、资产归属、异常行为数。根据威胁数量统计最近 24h 的威胁方排行，国内、国际分别统计 TOP5，表格展示威胁方 IP、所在地、异常行为数。威胁方归属地统计异常行为数最多的威胁方所在地，国内、国际分别统计 TOP10。

3.4.2威胁列表

在威胁检测→威胁列表页面，列表详细记录了威胁事件发生的时间、源 IP、目的 IP、协议、流向、威胁类型、威胁明细、严重级别、攻击阶段、来源、威胁方归属地、探针 IP。威胁事件支持按照时间、按照事件的属性进行筛选。威胁事件根据威胁类型和威胁明细统计，影响最多的前十类。列表右侧操作项，威胁事件支持下载数据包取证。



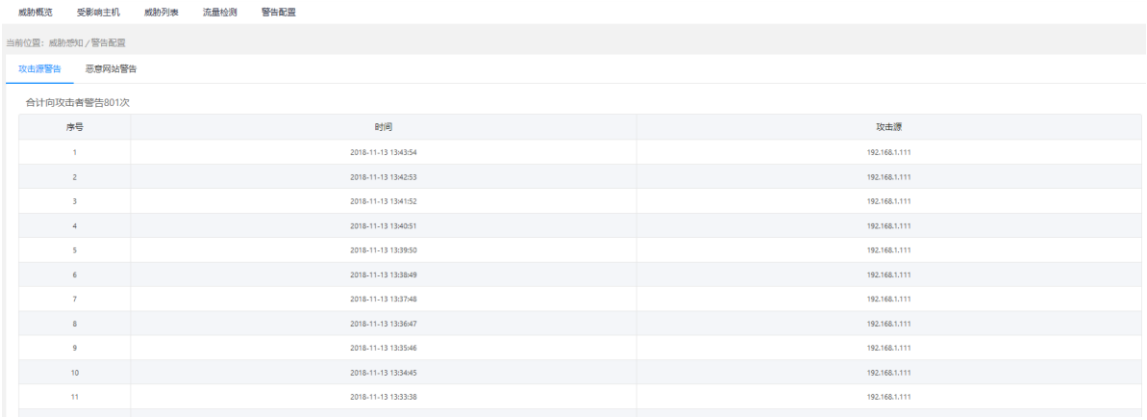
列表右侧操作项，威胁事件支持针对事件和规则的忽略。忽略事件，仅忽略当前一条事件日志。忽略规则，包括忽略此条检测规则和此资产 IP 相关的事件。



忽略的规则，通过系统管理→系统设置→忽略规则管理页面管理，将已经忽略的规则删除后，规则继续生效。

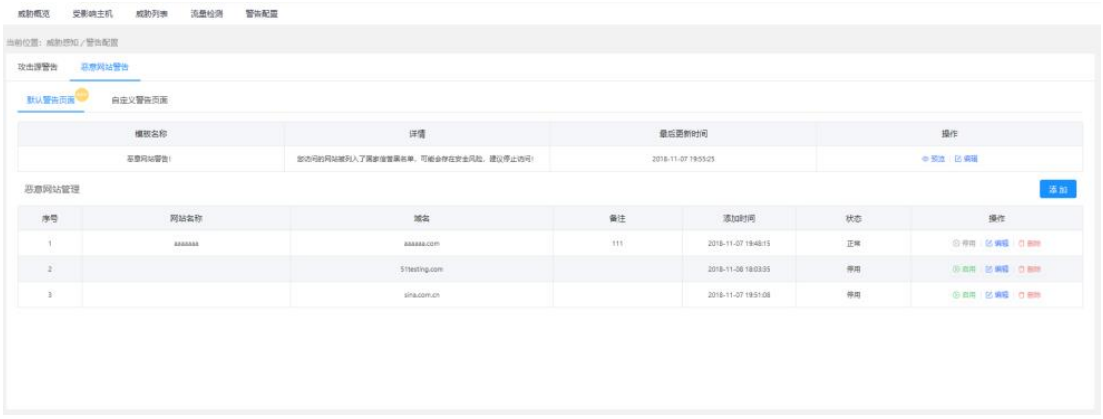
3. 4. 3警告配置

威胁检测→警告配置页面的攻击源警告，用于对攻击源警告。当系统检测到远端 IP 地址存在恶意入侵或者探测行为时，可以对相应的 IP 进行告警，对其推送告警界面，以做警示，并记录告警事件时间和攻击源 IP 地址。



威胁检测→警告配置页面的恶意网站警告，用于对系统用户警告。当系统用户访问恶意网站时，对自己的用户推送提示页面，可以使用默认的提示内容，也可以自定义提示页面，自定义页面仅支持上传 html 的文件包。

恶意网站的数据，来源于国家能力中心。也支持用户自定添加，用户将自己整理的恶意网站的名称、域名添加到系统中，系统支持对自定义添加的恶意网站的编辑、删除、停用、启用。



恶意网站检测的功能开关，在系统管理→系统设置→功能配置菜单页面，默认关闭。

3.5国家能力中心

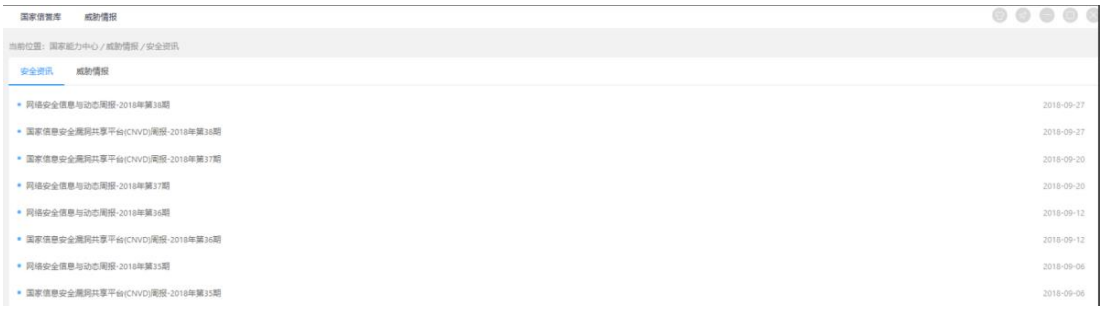
3.5.1国家信誉库

基于国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称CNCERT或CNCERT/CC)拥有的国内最为先进且独一无二的公共互联网网络安全监测平台，能够将诸如僵尸木马活动、恶意代码传播、恶意攻击行为、恶意站点数据等网络安全事件及信誉数据同步至本系统，与国家级监测平台形成联动能力，及时发现用户单位网络安全威胁。

国家中心云平台配置，在系统管理→系统设置→功能配置菜单页面，统计数据上传云平台开关默认关闭，国家信誉库自动更新开关默认开启。

3.5.2威胁情报

对接国家中心的威胁情报和安全资讯，及时更新，包括：网络安全信息与动态周报、国家信息安全漏洞共享平台周报、CNCERT 互联网安全威胁报告、突发漏洞安全公告等。

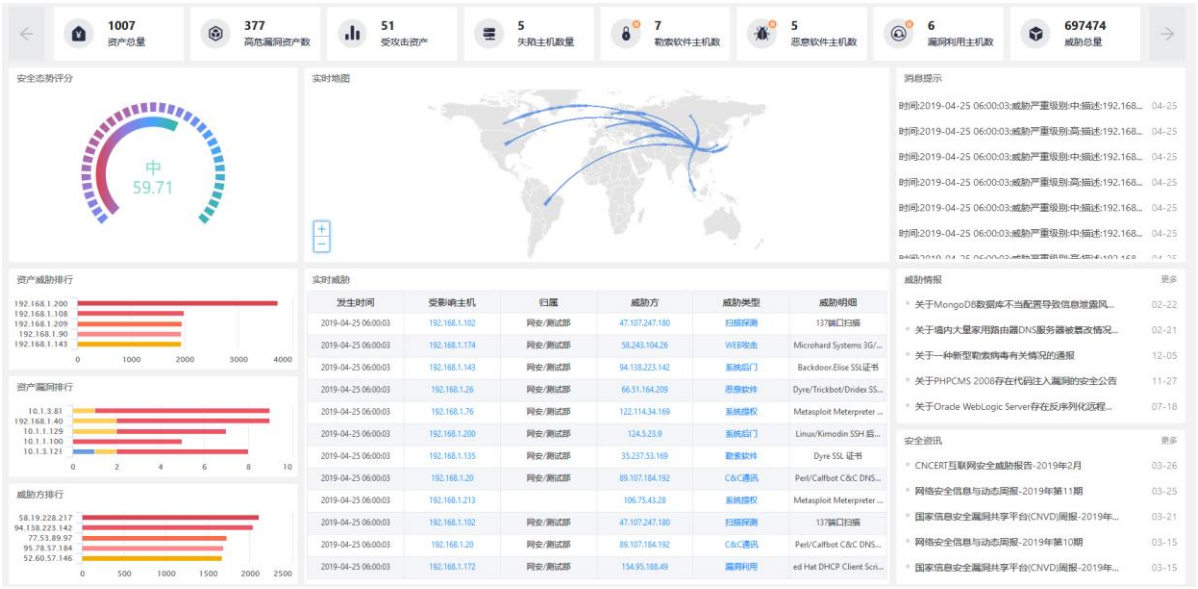


3.5.3规则库

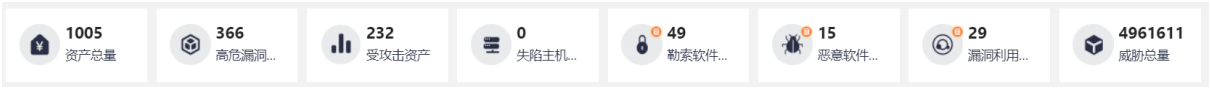
为了保障威胁检测能力，我方会每个月更新一次威胁规则库，规则文件会以邮件的形式发送到用户邮箱，用户只需要在此界面点击上传，将文件上传至设备即可。

3. 6控制台

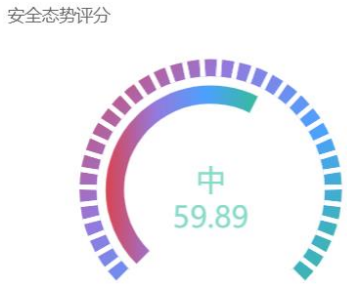
控制台用来统计分析用户单位的资产情况、所面临的威胁情况、单位整体的安全态势评分、威胁资产、漏洞资产、威胁方、实时消息提示及威胁情报。



控制台首行数字贴，统计显示资产总量、高危漏洞资产、受攻击资产、失陷主机、勒索软件主机、恶意软件主机、漏洞利用主机、威胁总量。

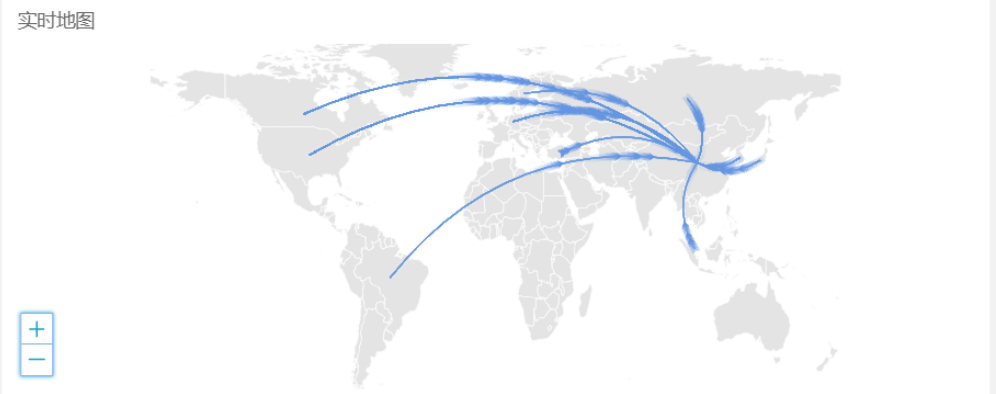


安全态势评分，是系统基于当前单位的资产情况、漏洞情况、威胁情况量化出来的一个分值。分值越高，表示系统安全系数越高，系统的安全级别分为：优、良、中、差、危五个级别。



实时地图和实时威胁，展示系统检测到的实时异常行为情况，攻击线表示威胁方针对资产的异常行为，箭头代表了攻击方向。

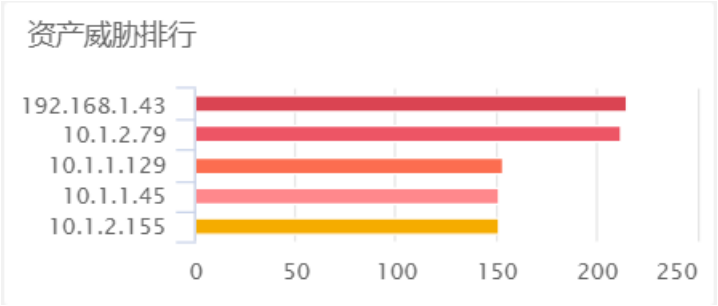
实时地图



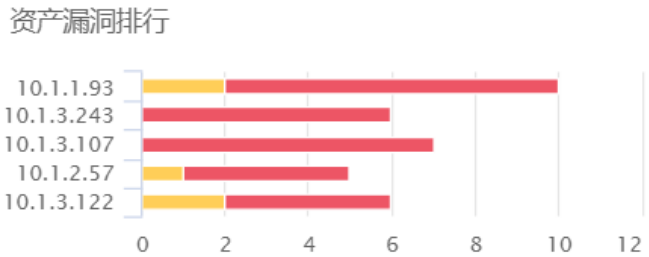
实时威胁

发生时间	受影响主机	归属	威胁方	威胁类型	威胁明细	检测源
2019-03-20 06:...	192.168.1.27	北京分公司/安...	58.42.242.58	其他	SSL指纹黑名单...	系统预定义
2019-03-20 06:...	10.1.2.77	北京分公司/安...	58.19.228.217	WEB攻击	XML外部实体...	系统预定义
2019-03-20 06:...	10.1.1.113	北京分公司/安...	117.23.2.58	暴力破解	Anuna PHP 后...	系统预定义
2019-03-20 06:...	10.1.1.56	北京分公司/安...	124.5.23.9	系统后门	Linux/Kimodin ...	系统预定义
2019-03-20 06:...	10.1.2.218	北京分公司/安...	35.237.53.169	勒索软件	Dyre SSL 证书	系统预定义
2019-03-20 06:...	10.1.3.249	北京分公司/安...	121.32.129.253	其他	SSL指纹黑名单...	系统预定义
2019-03-20 06:...	10.1.2.162	北京分公司/安...	47.107.247.180	扫描探测	137端口扫描	系统预定义
2019-03-20 06:...	10.1.2.199	北京分公司/安...	47.107.247.180	扫描探测	137端口扫描	系统预定义
2019-03-20 06:...	10.1.3.99	北京分公司/安...	47.107.247.180	扫描探测	137端口扫描	系统预定义
2019-03-20 06:...	10.1.2.73	北京分公司/安...	58.19.228.217	WEB攻击	XML外部实体...	系统预定义
2019-03-20 06:...	10.1.3.120	北京分公司/安...	58.19.228.217	WEB攻击	XML外部实体...	系统预定义

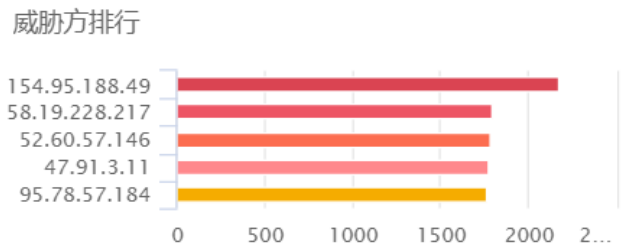
资产威胁排行，根据最近 24 小时的异常行为次数统计了风险资产的 top5。



资产漏洞排行，根据最近 24 小时的漏洞数值统计了风险资产的 top5。



威胁方排行，根据最近 24 小时的攻击情况，统计了威胁方 top5。



消息提示，展示系统产生的操作提示，高危漏洞、威胁等检测结果，动态滚动提示。

威胁情报，对接国家中心的威胁预警，包括：漏洞公告、恶意代码通告等。

安全资讯，对接国家中心的安全态势报告，包括：网络安全信息与动态周报、国家信息安全漏洞共享平台周报、CNCERT 互联网安全威胁报告等。

3.7系统管理

3.7.1系统设置

系统状态

显示系统当前的使用状态。包括：IP、CPU、内存、硬盘、管理口、检测口，点击查看详情。

Thinkflow 管理

系统支持对接多个流量探针，支持探针的添加、编辑、删除。

内部 IP 管理

管理内网的 IP/IP 段，及 IP 的归属信息。通过内网 IP 管理添加 IP 后，可以明确流量流

向，明确威胁检测的异常行为阶段，明确资产扫描发现的资产的详细归属信息，在资产扫描、漏洞扫描时明确扫描范围，方便快速添加扫描资产。

白名单管理

全局白名单，包括威胁检测、违规外联检测、攻击源警告等，支持添加 IP 和 URL。

忽略规则管理

威胁检测→威胁列表，忽略的规则，在此页面统一管理，删除规则后，在威胁检测中忽略的规则继续生效。

功能配置

系统各配置功能的开关，包括：系统与云平台配置、资产入库配置、违规外联配置、威胁检测→警告配置→恶意网站警告→恶意网站检测配置。

3.7.2用户管理

用户管理

系统支持用户分权分级管理，可以创建不同的用户，分配不同的角色，进行系统的管理。用户管理显示登录名称、用户名称、邮箱、角色、备注、状态，支持登录用户的添加、编辑、删除、锁定。

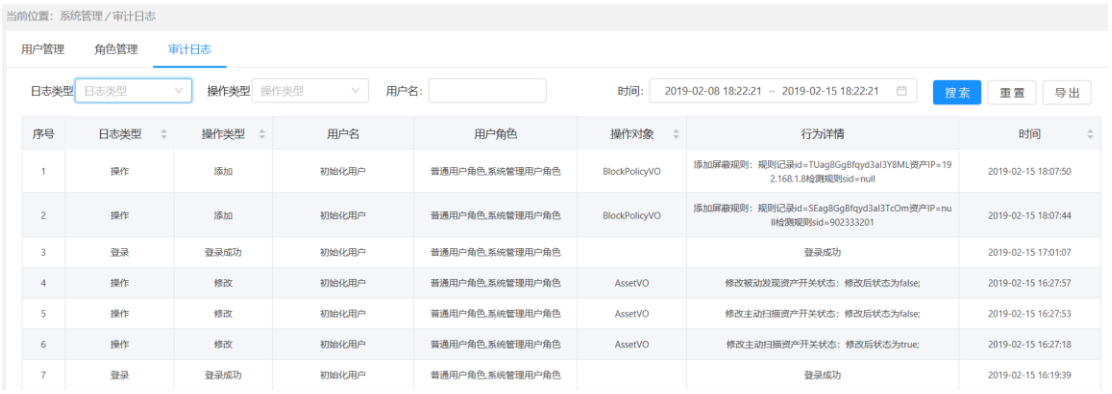
添加用户时，填写登录名称、用户名称、邮箱、设置密码、选择用户角色（支持多选）、填写备注，点击保存即可。

角色管理

用户角色的添加、编辑、删除、权限管理。系统包括三种用户角色：普通用户、系统管理员、安全管理员。系统管理员全功能。普通用户只可以查看数据，没有系统设置、用户管理的功能权限。安全管理员，只能使用安全检查功能模块。

审计日志

只有系统管理员可以查看审计日志，审计日志页面记录包括：日志类型、操作类型、用户名、用户角色、操作对象、行为详情、时间。审计日志页面支持按照日志类型、操作类型、用户名、时间的日志检索，支持日志的导出、重置。

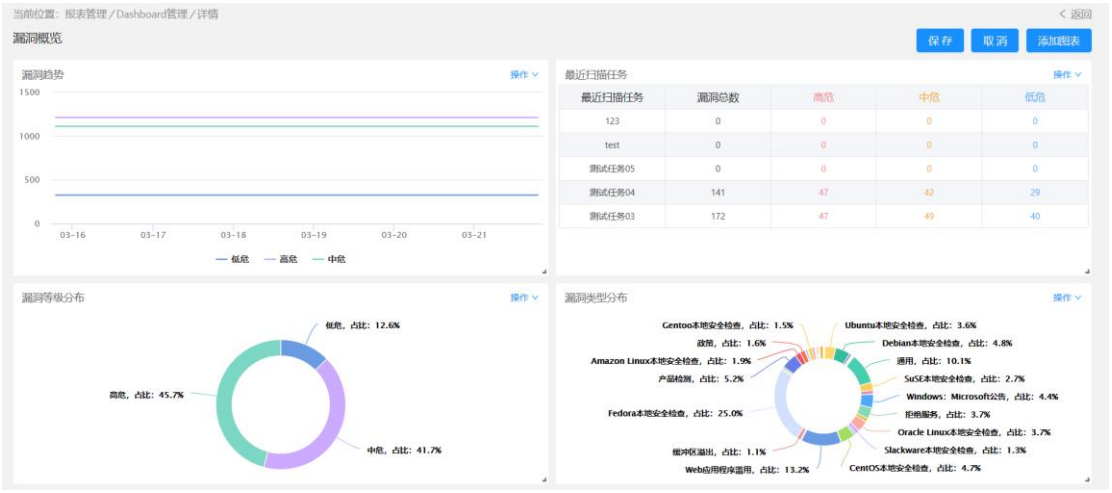


3. 7. 3报表管理

控制台、概览页管理

控制台、资产概览、漏洞概览、威胁概览四个概览页面，可以通过页面来管理数据图表的展示，点击编辑，进入相应概览页面的可编辑状态。

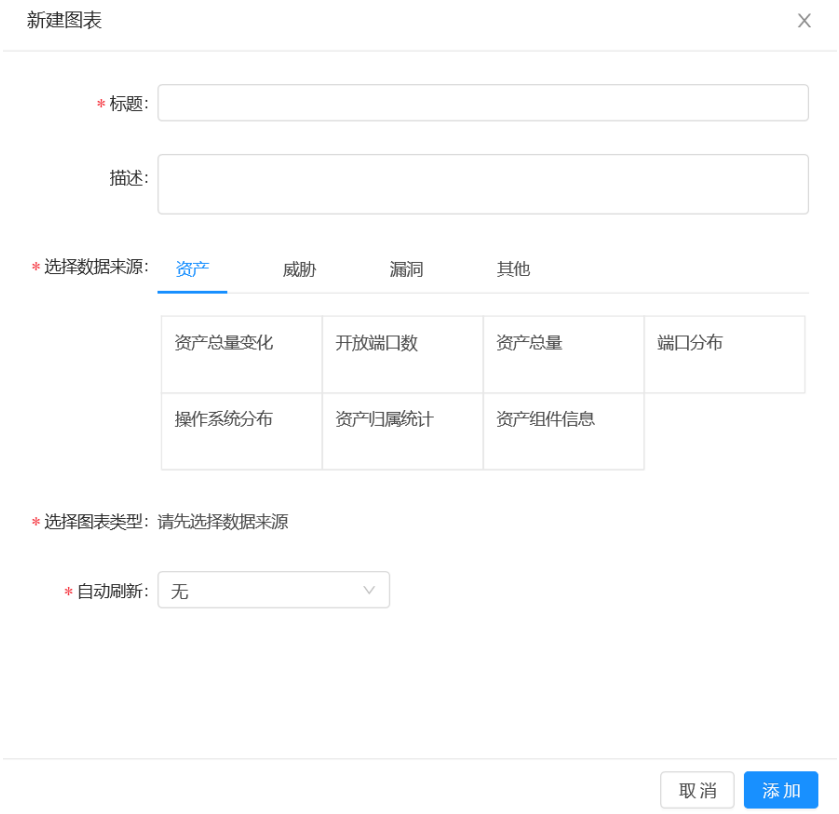
进入到编辑状态后，点击选中的数据图表，可以将图表拖拽到任意位置，可以拉伸图表的高度和宽度，重新对页面排版。重新排版后，顶部会出现保存、取消按钮，点击保存后，所有修改生效，点击取消按钮，修改被重置，页面数据不变。



对页面的数据图表进行管理，可以添加图表、删除图表、编辑图表标题。

编辑图表标题后，页面顶部出现保存、取消按钮，点击保存后，所有修改生效，点击取消按钮，修改被重置，页面数据不变。

添加图表，需要填写图表的标题、描述、选择数据来源、选择图表类型、是否自动刷新等设置项。



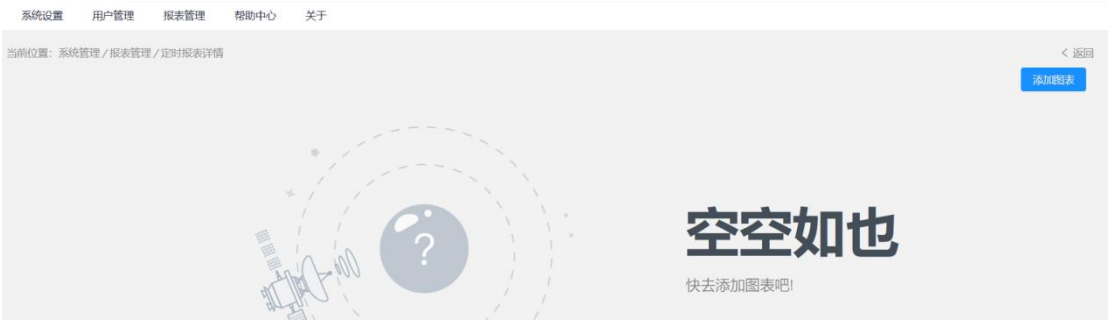
删除图表，会有弹窗提示是否真的删除。

定时报表

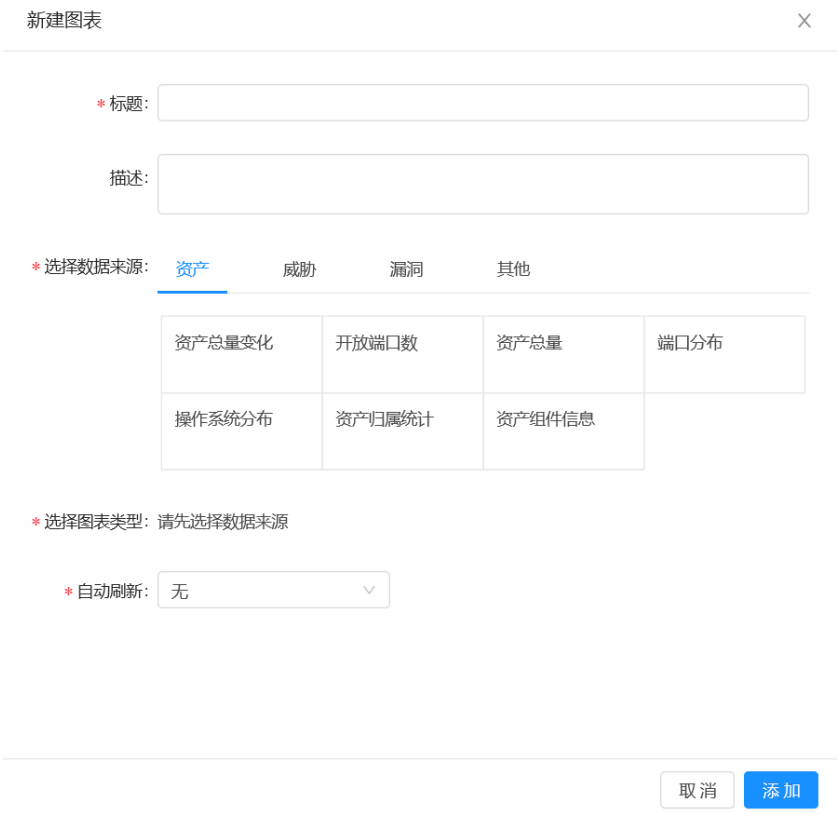
定时报表，用户可以根据实际需求，选择特定时间段生成报表，报表类型主要包括：日报、周报、月报。定时报表的列表显示定时报表名称、描述、定时生成时间、创建时间、操作项。支持定时报表的添加、编辑、删除，编辑查看报表详情。

创建一个新的定时报表，填写报表名称，选择报表类型、定时生成时间，保存。

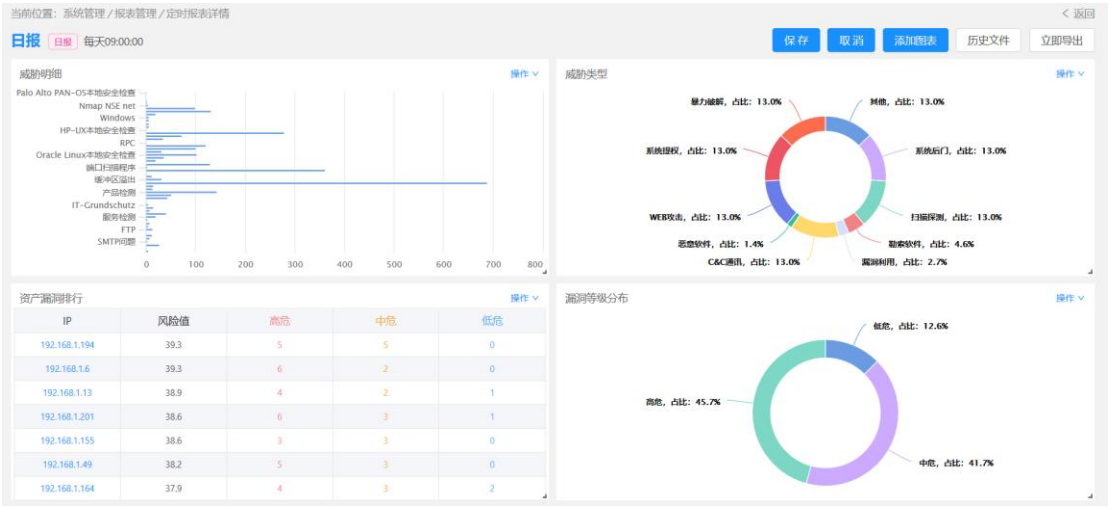
创建一个报表后，点击详情，进入报表内容编辑页面，新创建的报表没有图表，需要添加图表。



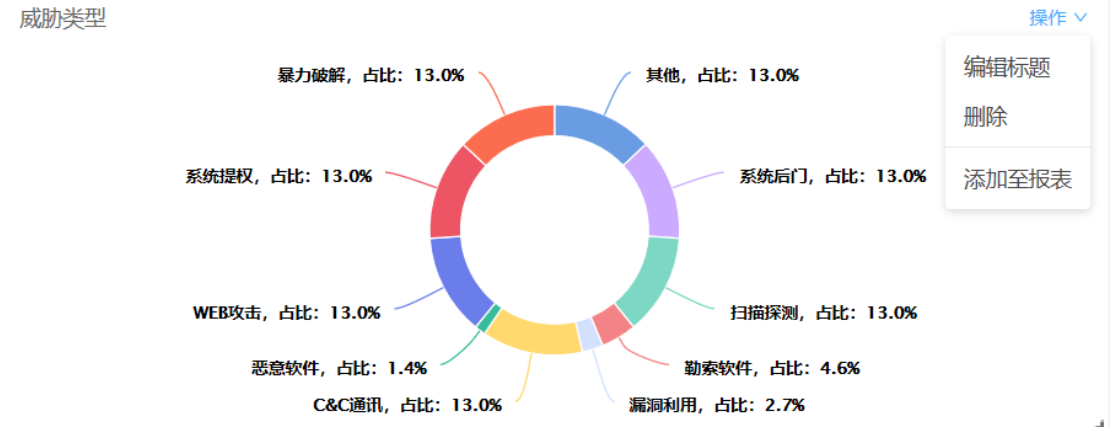
添加图表，需要填写图表的标题、描述、选择数据来源、选择图表类型、是否动刷新等设置项。



添加图表后，点击选中的图表，可以将图表拖拽到任意位置，可以拉伸图表的高度和宽度，重新对页面排版。重新排版后，顶部会出现保存、取消按钮，点击保存后，所有修改生效，点击取消按钮，修改被重置，页面数据不变。

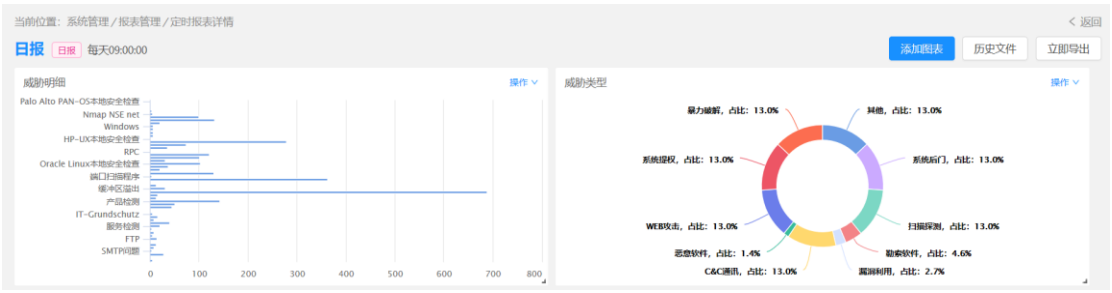


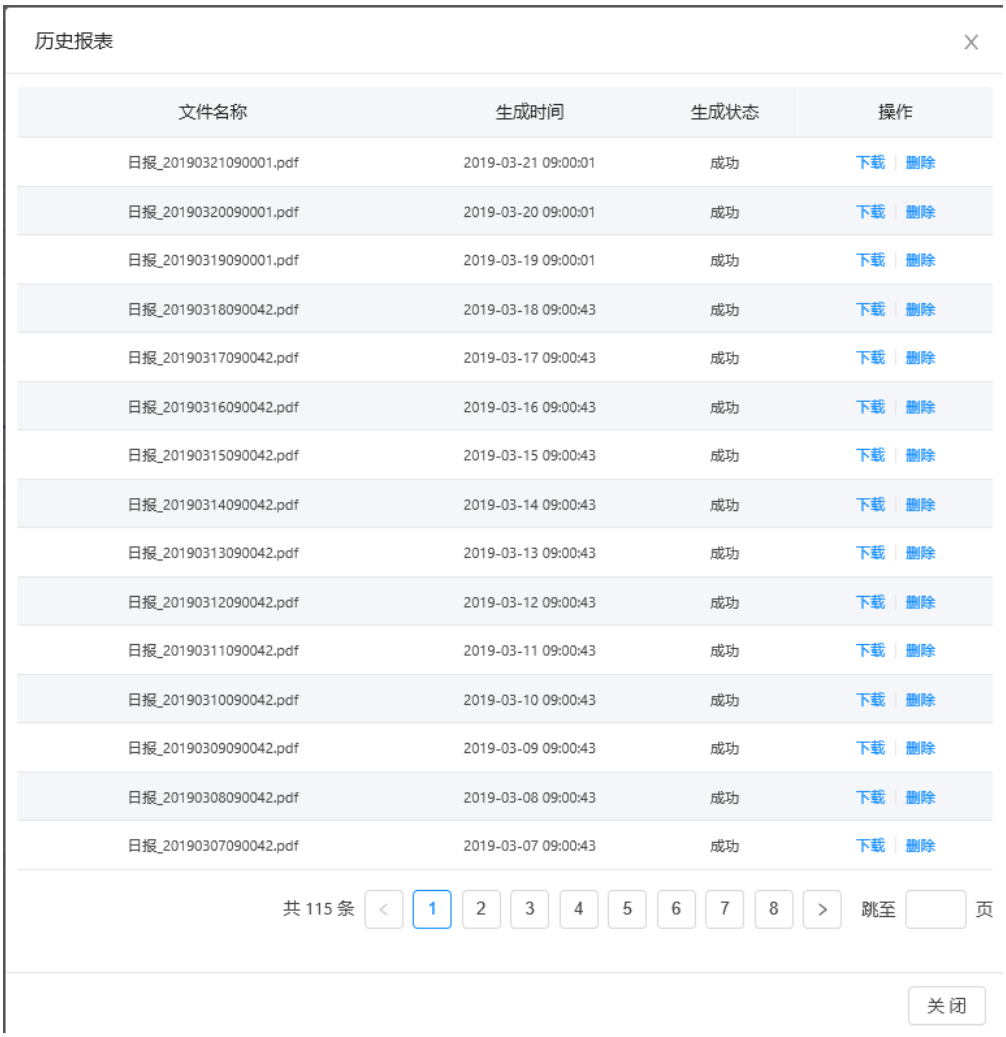
可以删除图表、编辑图表标题、添加至其他报表。



编辑图表标题后，页面顶部出现保存、取消按钮，点击保存后，所有修改生效，点击取消按钮，修改被重置，页面数据不变。

历史文件，就是此定时报表的生成记录。点击历史文件，可以看到生成列表，显示文件名称、生成时间、生成状态，支持下载、删除操作。





立即导出，就是立即生成定时报表，在历史报表列表可以马上看到记录，显示生成时间是当前时间。可以下载、删除。

3.8安全态势大屏

3.8.1 全局态势大屏

全局态势大屏，从资产、脆弱性、威胁视角，全面展示用户单位的整体安全态势。

3.8.2 资产态势大屏

资产态势大屏，从资产视角，展示在线资产的变化趋势、各部门的资产漏洞威胁情况、端口、组件、系统的分布状态等，帮助关键信息基础设施运营单位快速实时掌握网内资产态势。

3.8.3 脆弱性态势大屏

脆弱性态势大屏，从脆弱性视角，直观展示漏洞总数、影响资产数和已验证漏洞数，资产脆弱性风险排行、部门脆弱性风险排行、漏洞影响资产排行等，快速发现高脆弱性风险的资产和部门、及影响最严重的漏洞，不仅能够帮助运营单位快速实时掌握资产脆弱性态势，还能够实现漏洞影响资产的快速排查，大大缩减了面对新漏洞时快速响应时间。

3.8.4 威胁态势大屏

威胁态势，从威胁视角，展示威胁动态攻击路径，威胁告警实时滚动播放，受攻击资产和受攻击部门 TOP 排行，帮助关键信息基础设施运营单位快速定位到受影响最严重的资产和部门，使威胁无处遁形。

4. 用户指南

4. 1申请双网卡弹性云主机

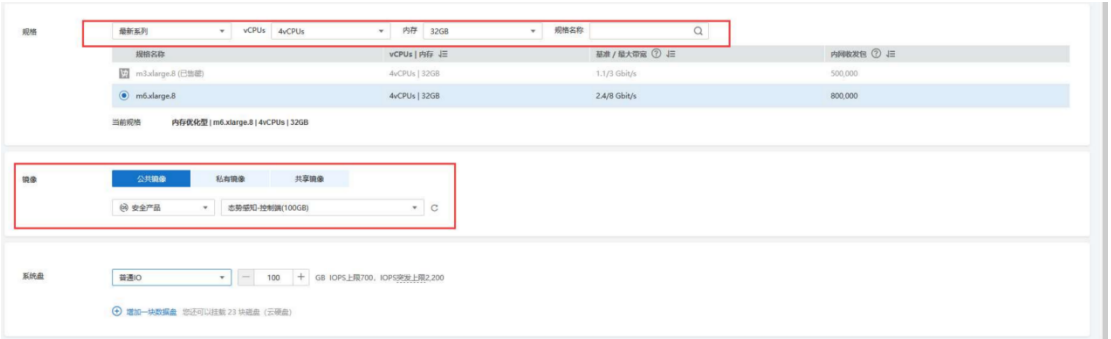
开通态势感知服务需要开通 2 台双网卡弹性云主机，其中一台云主机为态势感知控制端，最低配置建议为 8 核 CPU/64G 内存/100G 系统盘/1T 数据盘。另外一台云主机为虚拟网关,最低配置建议为 4 核 CPU/8G 内存/50G 系统盘，（场景 A、B、C 则需要 2 台虚拟网关主备）。

需要单独在天翼云控制中心下的虚拟私有云中去申请一个态势感知的子网。态势感知的网段和防火墙、业务、负载均衡的网段不在同一网段。如果有多余的网段，就不用去申请。

4. 1. 1开通态势感知弹性云主机

在天翼云官网下的控制中心下的弹性云主机中创建弹性云主机 。

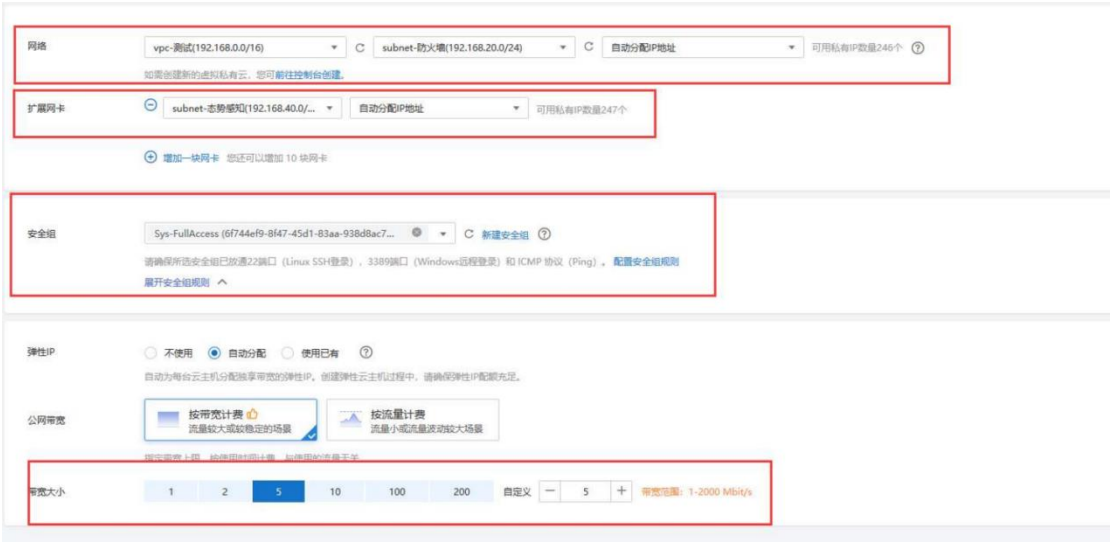
态势感知云主选择的镜像在公共镜像下->请选择操作系统下拉选择安全产品，请选择操作系 统版本下拉选择态势感知-控制端（100GB）。



态势感知的 eth0 网段和业务是同一个网段，ip 地址可以自己手动分配或者自动分配 。

态势感知的 eth1(扩展网卡)网段是态势感知的网段，和业务不同网段，建议新建子网用于镜像流量接收使用。

安全组入方向中放行 22 端口以及 18443 端口，弹性 ip 的带宽建议 5M 。



设置密码并同意相关协议即可开通态势感知云主机，等待创建即可。

4.1.2开通态势感知虚拟网关云主机

态势感知网关 eth0 的网段设置:

A. 网络环境中有云下一代防火墙。则态势感知网关的 eth0 网段和防火墙的外网出口（即防 火墙做目的 NAT 的内网 ip）同一个网段。如果是多个外网出口的防火墙 ip，需要更改防火墙为同 一个外出口。不清楚的请与态势感知厂家联系确认后联系防火墙厂家更改。

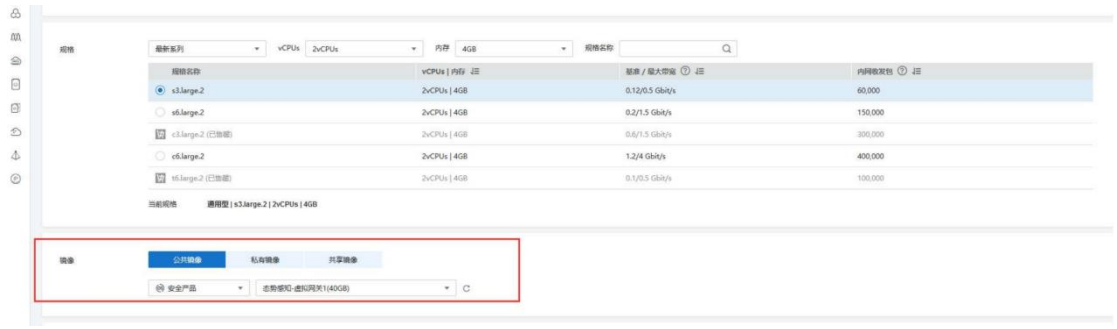
B. 网络环境中没有云下一代防火墙，有负载均衡器。则态势感知网关的 eth0 网段和负载均衡器的 ip 同一个网段。

C. 网络环境中没有云下一代防火墙和负载均衡器，则态势感知网关的 eth0 网段和业务同一 个网段。

D. 网络环境中有云下一代防火墙和负载均衡器，则态势感知网关的 eth0 网段和云下一代防 火墙的外出口同一个网段。如果是多个外网出口的 ip，需要更改防火墙为同一个外出口。不清楚 的请与态势感知厂家联系确认后联系防火墙厂家更改。

态势感知网关 eth1 网段是态势感知网段，和业务防火墙负载均衡不在同一个网段。

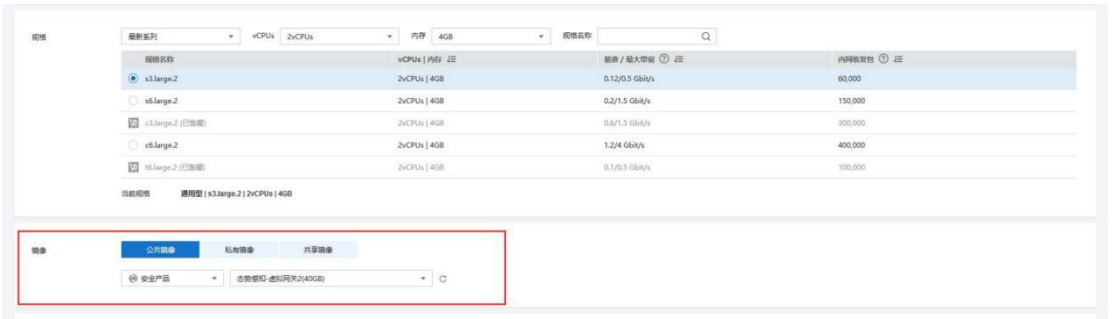
态势虚拟主网关选择的镜像在公共镜像下->请选择操作系统下拉选择安全产品，请选择操作 系统版本下拉选择态势感知-虚拟网关 1（40GB） 。



态势感知主网关 eth0 网段根据网络环境中是否有云下一代防火墙、负载均衡器配置，eth1(扩展网卡)和态势感知是同一个网段。安全组入方向方向 22 端口，弹性 ip 带宽建议 5M 。

设置密码并同意相关协议即可开通态势感知云主机，等待创建即可。

态势虚拟备网关选择的镜像在公共镜像下->请选择操作系统下拉选择安全产品，请选择操作 系统版本下拉选择态势感知-虚拟网关 2（40GB）。



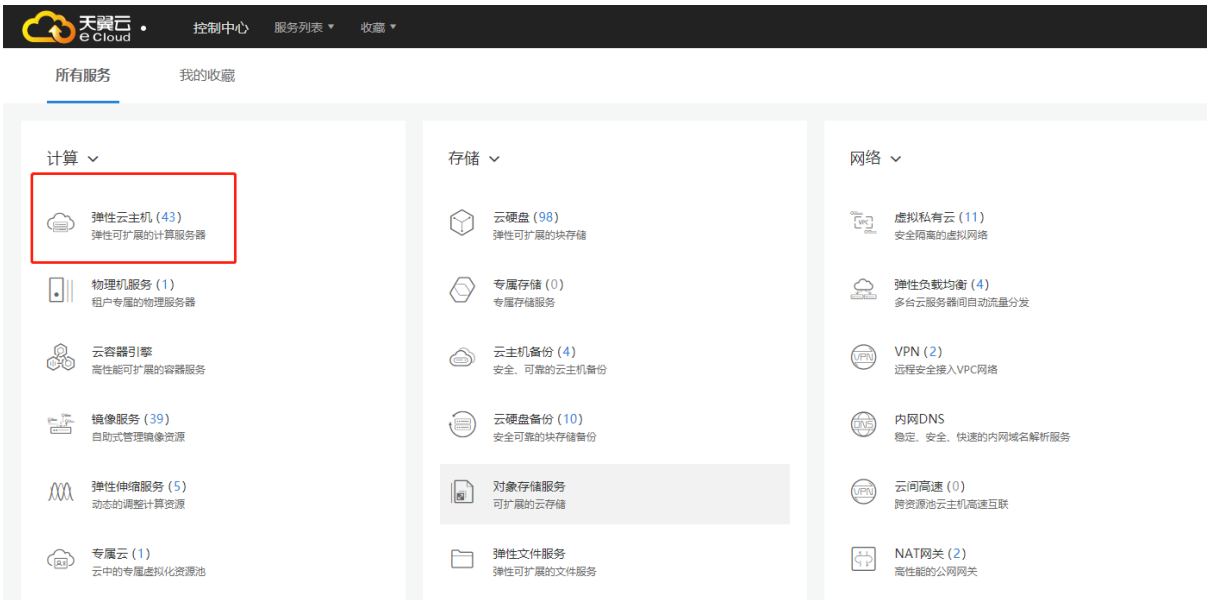
态势感知备网关 eth0 网段根据网络环境中是否有云下一代防火墙、负载均衡器配置，eth1(扩展网卡)和态势感知是同一个网段。安全组入方向放行 22 端口，弹性 ip 带宽建议 5M。

设置密码并同意相关协议即可开通态势感知云主机，等待创建即可。

4. 2申请虚拟 IP

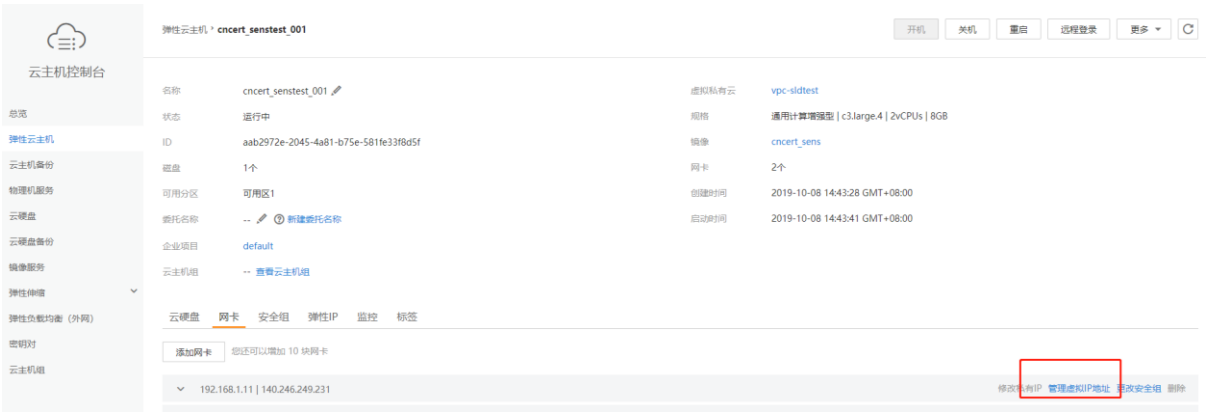
双网卡弹性云主机开通完成后申请虚拟 IP，并且绑定虚拟网关系统（场景 A、B、C）。流程如下:

步骤一: 在天翼云控制中心所有服务下的计算中找到弹性云主机，点击开通的弹性云主机。



步骤二: 在态势感知网关弹性云主机网卡 eth0 选项中点击管理虚拟 IP 地址。特别注意: 这里的 eth0 是和态势感知网段不同的哪个网段。具体的网段是根据网络环境中是否有云下

一代防火墙、负载均衡器配置的，在最前面的就是 eth0 网卡。



步骤三：在虚拟 IP 选项下申请虚拟 IP 地址，可以自动分配或者手动分配。

完成虚拟 IP 申请后。在操作选项下的绑定服务器中绑定 2 台虚拟双网关云主机。一次只能绑定一台态势感知网关，操作两次即可。弹性 ip 先暂时不绑定。后面配置的时候配合态势感知技术人员操作绑定。

4.2.1订购态势感知基础版/高级版

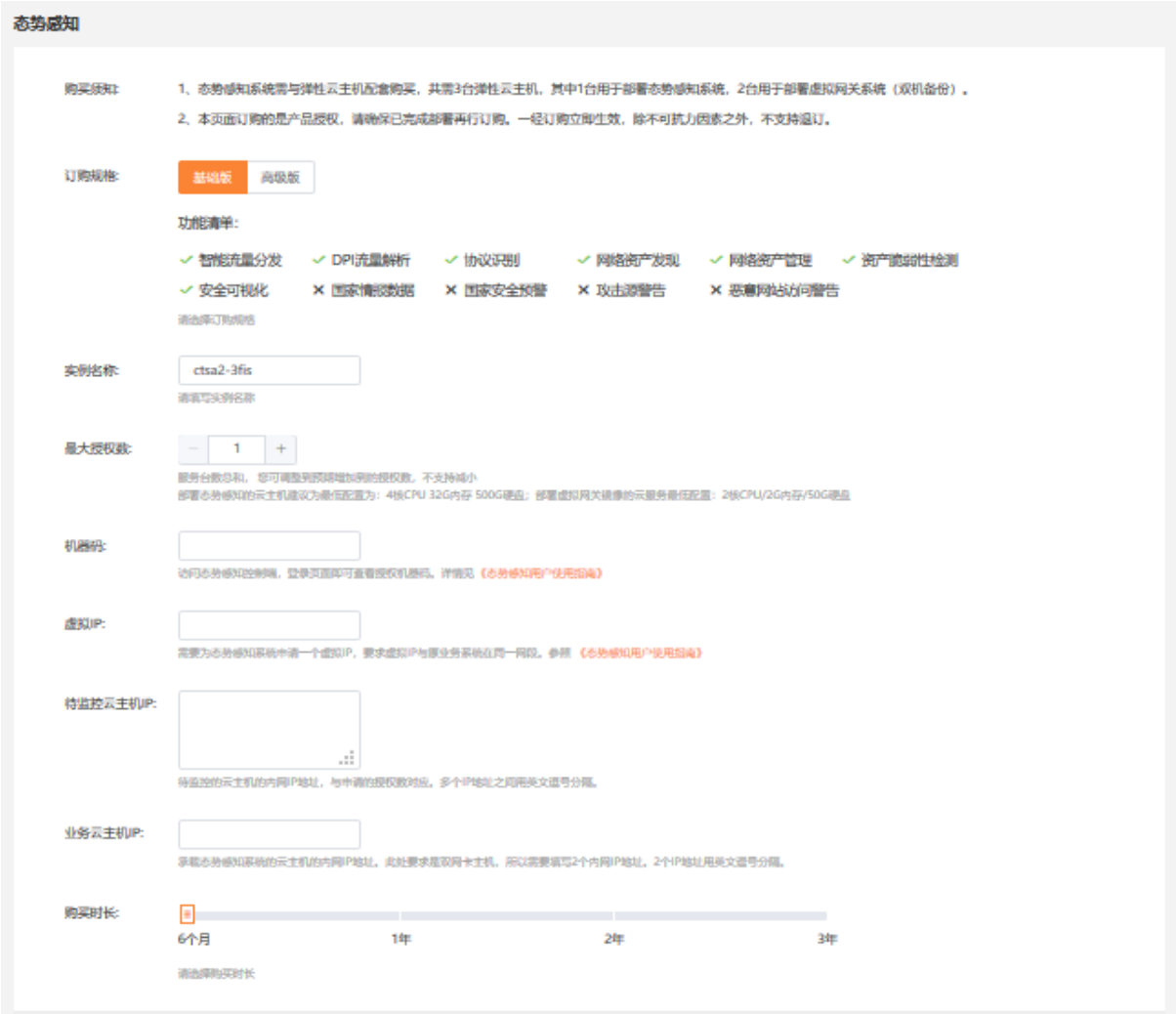
通过天翼云控制中心下的安全选项下的态势感知进入订购态势感知授权页面，订购页面如下，填写对应的信息。态势感知网络配置的场景：

场景 A：态势网关作为网络出口，直挂业务主机（网关主备监控同公网 IP 下资产）

场景 B：态势-网关下挂负载均衡（网关主备监控 1 资产）

场景 C：态势-网关下挂云防火墙（网关主备监控 1 资产）

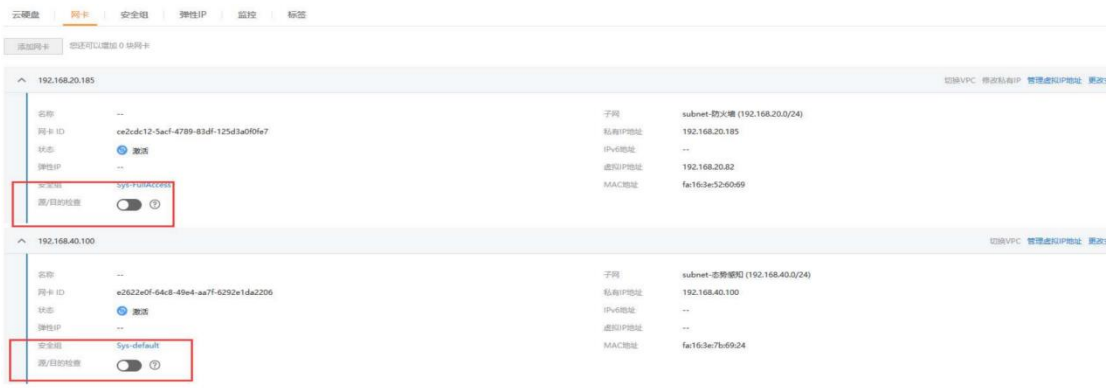
场景 D：态势-网关上挂云防火墙（多资产监控）



在订购完成后会有态势感知技术人员联系对接网络配置，请确保联系方式顺畅。

4.2.2虚拟网关配置

确保态势感知网关的安全组放行 22 端口，所有态势感知云主机网卡下关闭源/目的检查。虚拟网关的配置需要配合态势感知技术工程师。由态势感知技术工程师配置。



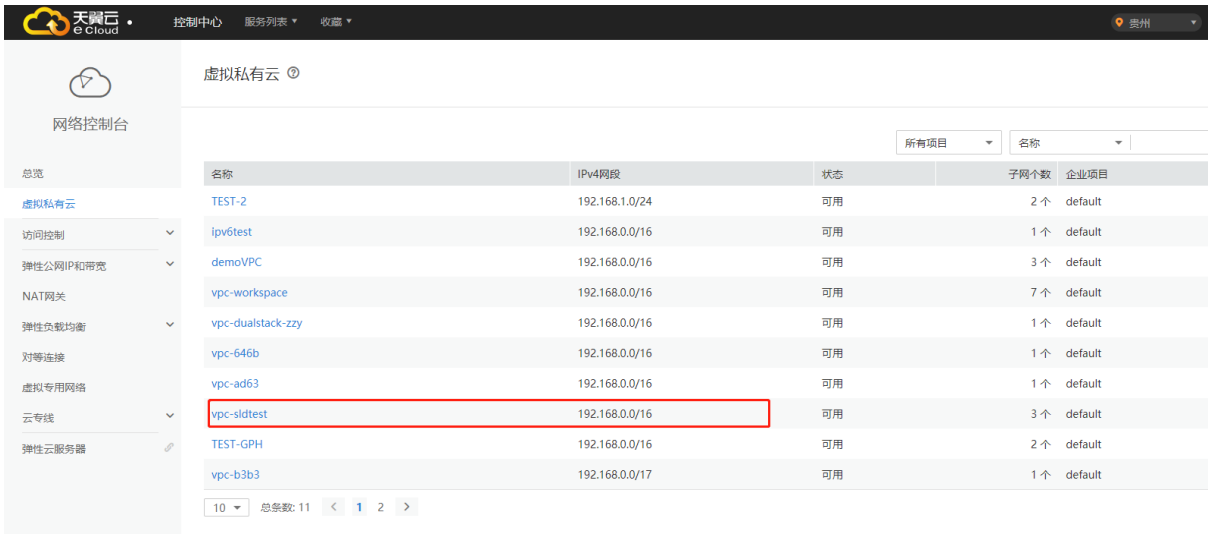
4.3网络配置

4.3.1场景 A

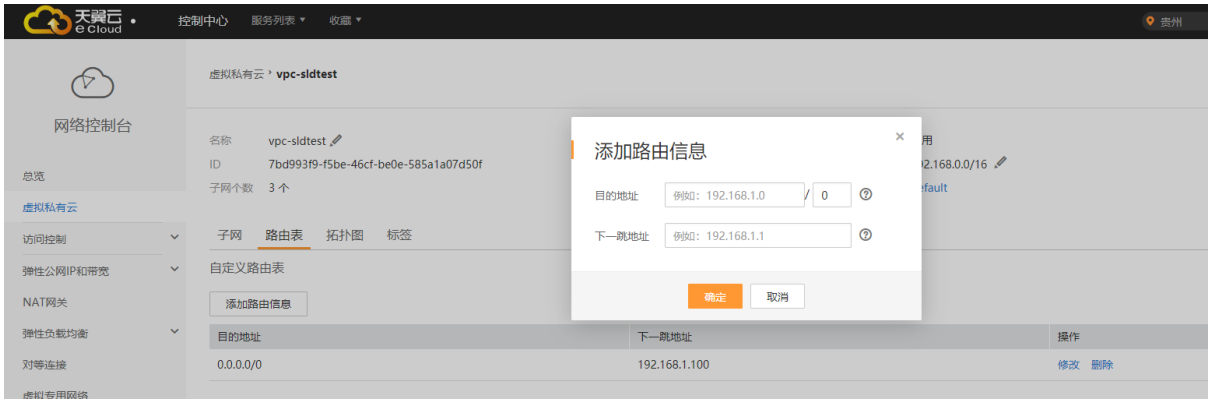
态势-网关，直接下挂业务场景，网络配置步骤：

步骤一：在天翼云控制中心所有服务中点击网络下的虚拟私有云。

步骤二：在虚拟私有云中找到对应开通的云主机网段，点击进入。



步骤三：点击路由表选项下添加路由信息，配置路由，下一跳的 IP 地址为虚拟 IP 地址。

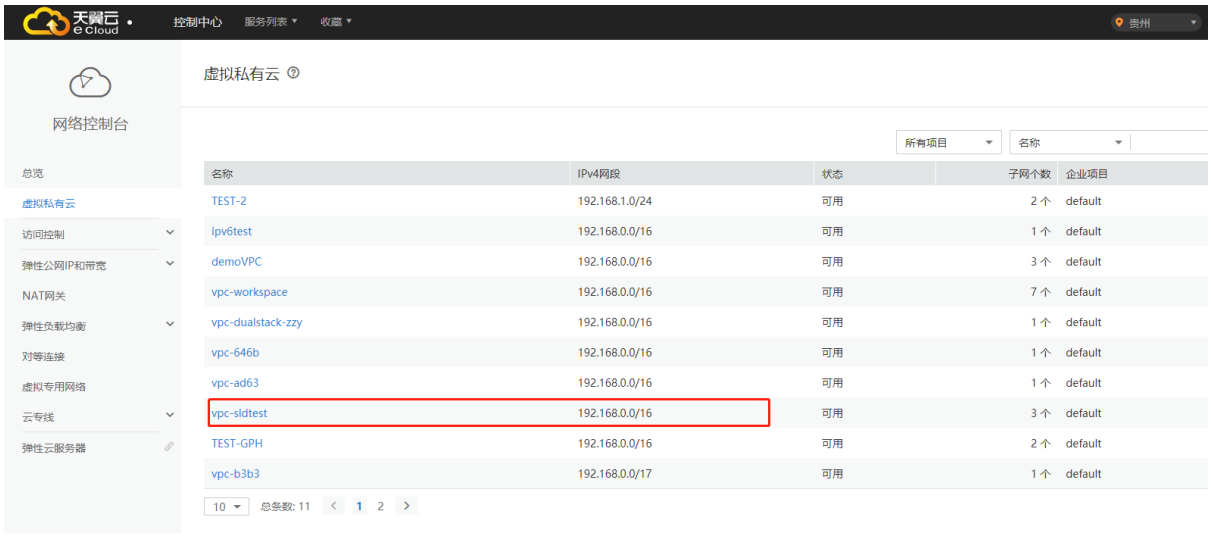


4. 3. 2场景 B

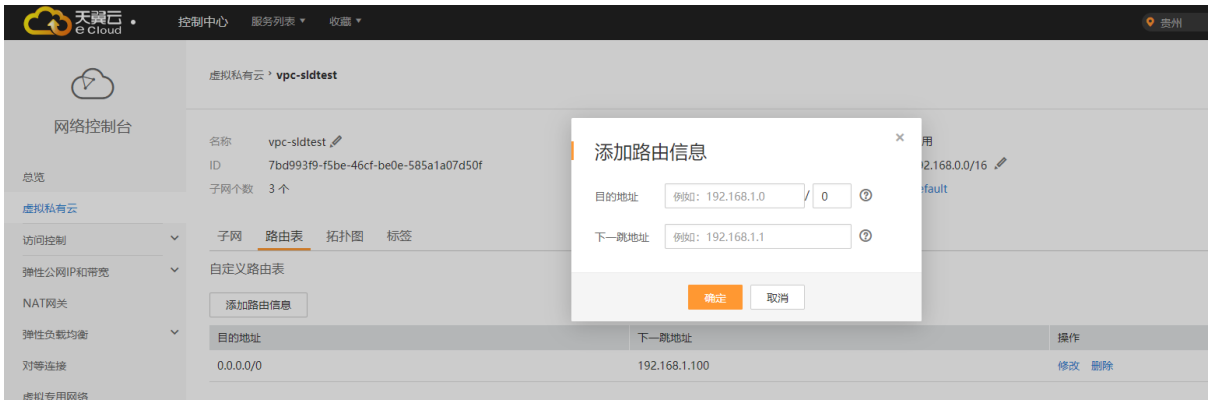
态势-网关下挂负载均衡器场景，网络配置步骤：

步骤一：在天翼云控制中心所有服务中点击网络下的虚拟私有云。

步骤二：在虚拟私有云中找到对应开通的云主机网段，点击进入。



步骤三：点击路由表选项，配置路由，下一跳的 IP 地址为虚拟 IP 地址。

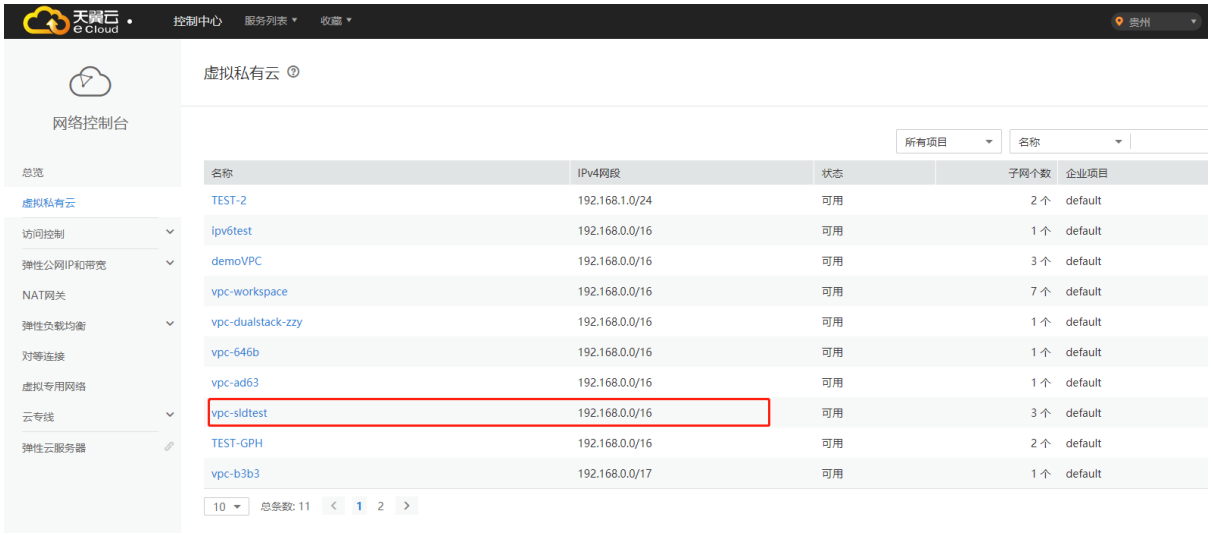


4.3.3场景 C

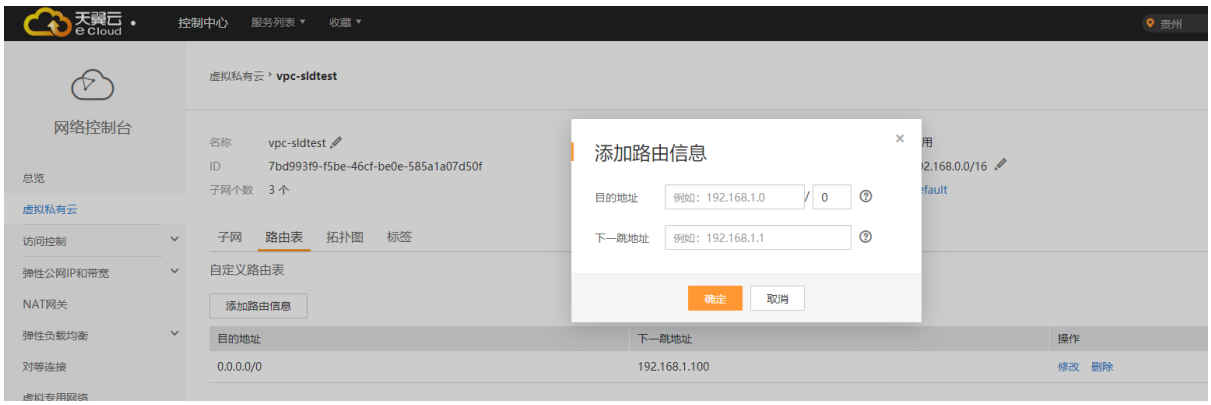
态势-网关下挂防火墙，网络配置步骤：

步骤一：在天翼云控制中心所有服务中点击网络下的虚拟私有云。

步骤二：在虚拟私有云中找到对应开通的云主机网段，点击进入。



步骤三：点击路由表选项，配置路由，下一跳的 IP 地址为虚拟 IP 地址。



步骤四：防火墙所在的网卡上关闭 源/目的检查。

4.3.4场景 D

态势-网关上挂防火墙，网络配置步骤：

步骤一：先配置好云下一代防火墙割接业务没问题

步骤二：态势-网关部署在云墙的内侧业务主机的外侧

步骤三：防火墙配置目的路由将流量转发至态势-网关

步骤四：内网业务主机修改网关地址为态势-网关地址

4.4部署完毕

部署完毕并测试。首先在分析器看是否有流量、是否可以进行分析。

其次看业务是否受影响。态势-网关采用透明传输方式，不影响在负载均衡器和防火墙上的设置。

5. 最佳实践

5.1威胁聚合分析最佳实践

背景信息

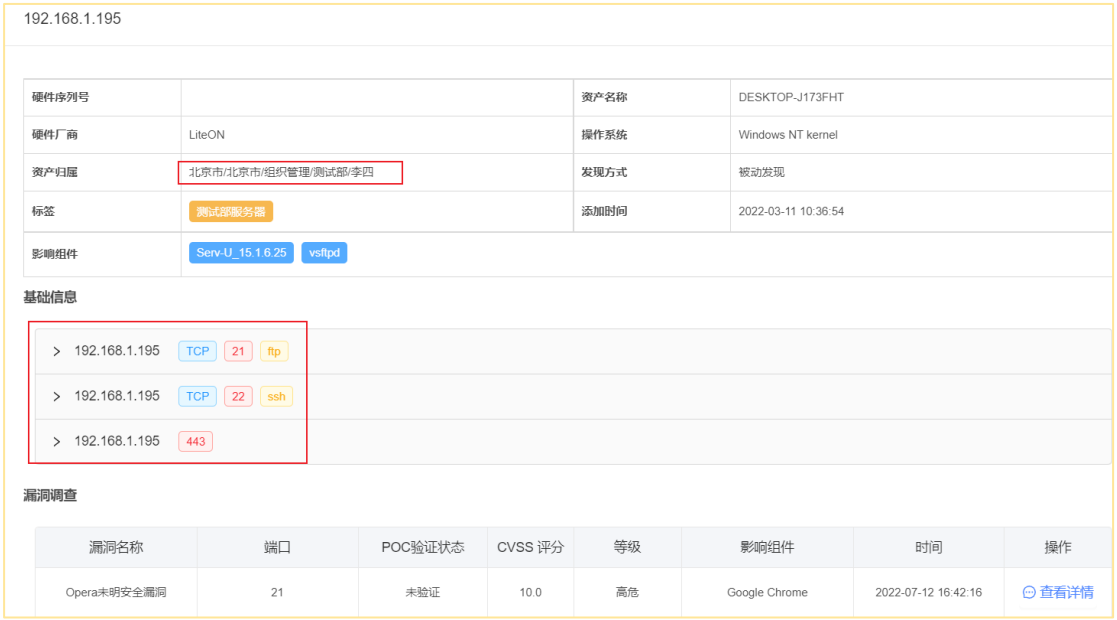
网络攻击事件是指通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的信息安全事件。所以当安全产品检测到一条威胁事件时，我们除了要分析威胁事件本身，还要分析威胁事件影响的资产情况，为处置决策提供全面准确的依据。

威胁聚合分析

我们分析一下“ssh 暴力破解”这个事件，在威胁聚合页面，我们用 “事件名称” 作为聚合条件进行检索，查找到一条数据，显示威胁事件“ssh 暴力破解”中受影响资产数有 3 个，下钻继续分析，查看到具体这 3 个资产 IP，继续下钻分析，查看其中一个资产的详情和存在漏洞情况，查看详情可查找到漏洞解决方案。

通过聚合分析我们找到了该威胁事件受影响的所有资产，下面截图中可以看到 3 个资产 IP 。

通过下钻查找资产 IP 开放的服务，用户自行比对是否是预期开放的服务，通过资产归属信息，可以立即找到该资产的负责人，为后续处置提供依据。



同时我们也可以查找到资产存在哪些漏洞，通过查看详情，用户可以快速找到漏洞修复的解决方案，为后续处置提供依据。

处置建议

基于聚合分析提供的数据，有以下处置建议：

1） 受攻击资产 IP 立即修改密码；

2） 受攻击资产 IP 关闭非预期开放的端口；

3） 受攻击资产 IP 基于漏洞修复方案完成全部漏洞修复；

4） 使用态势感知弱口令检测功能排查网内资产存在的弱口令风险；

6. 常见问题

6.1计费类

态势感知计费如何计算？

态势感知采用包年/包月计费，最少订购 1 个月，最多可订购 3 年。这里的态势感知计费指的是态势感知软件计费，所需弹性云主机资源需另行购买。

包年/包月是一种预付费方式，按订单的购买周期计费，影响价格的因素包括购买周期、待监控 IP 数量、版本（基础版/高级版），举个例子：

基础版单价： 198 元/月/IP

购买基础版 1 年、3 个待监控 IP 的总价 = 12 * 198 * 3 = 7128 元

态势感知基础版和高级版有什么区别？

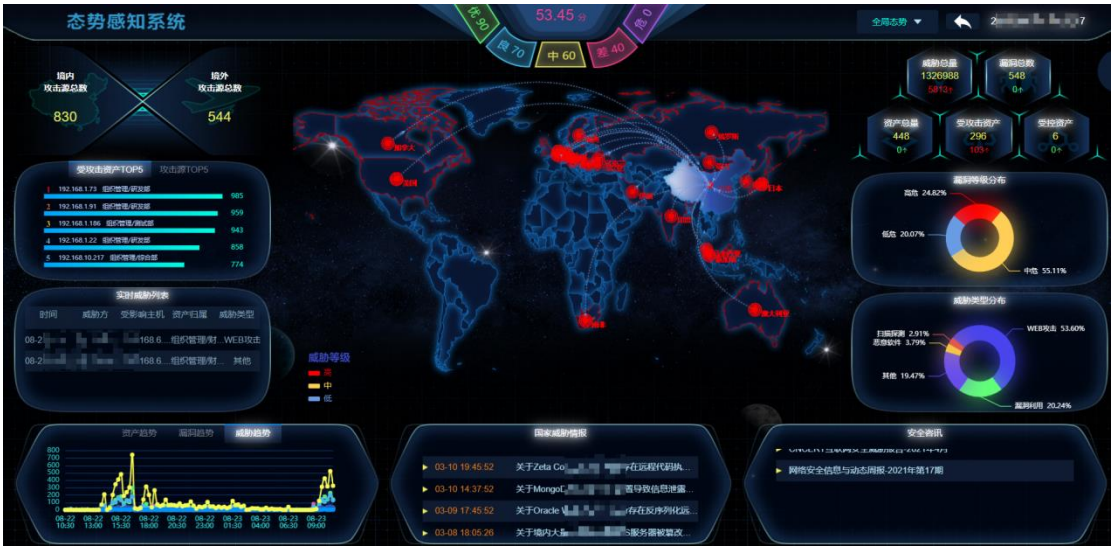
基础版包含资产发现、资产管理、网络威胁检测、脆弱性检测、可视化呈现功能；

高级版包含国家情报数据、国家安全预警、攻击源警告、恶意网站告警、安全态势大屏；

主要区别：高级版增加国家情报和预警能力，同时安全态势大屏只有高级版才有，基础版的可视化呈现主要是指控制台运维页面，下面用两个截图来做对比。

✓ 基础版可视化呈现页面截图：

✓ 高级版安全态势大屏截图：



6. 2操作类

为什么检测口没有流量?

1）确认在虚拟网关已经进行了镜像，且能看到流量;

2）确认接入系统的端口是设置了检测口;

3）确认 thinkflow 组件是否正常运行;

4）查看 thinkflow 日志;

5）根据日志信息再进一步排障。

为什么威胁检测没有数据?

1）确认检测口是否有数据;

2）确认知识库是否正常加载。

为什么国家信誉库没有同步?

1）确认同步开发是否开启;

2）确认同步配置是否设置正确;

3）确认与国家信誉库平台连接是否正常。