★完全公开

奇安信
新一代网络安全领军者

奇安信网神
网络空间安全态势感知与协调指挥系统
产品白皮书

地址：北京市西城区西直门外南路26号院1号

邮编：100044

● 版权声明

● 免责声明

本免责声明（“**本声明**”）适用于奇安信集团（包括但不限于奇安信科技集团股份有限公司、奇安信网神信息技术（北京）股份有限公司、北京网康科技有限公司，以及前述主体直接或者间接控制的法律实体）旗下推出的全部产品和/或服务（以下统称“**本产品**”）。**如您使用前述产品，即表示您同意接受本声明的一切内容。如果您不同意接受，请立即停止使用相关产品。**

奇安信集团有权随时自行决定修改、添加或删除本声明的全部或部分内容。**您有责任定期检查免责声明部分的内容**，以了解是否发生了变更。**如您在我们发布变更后继续使用本产品，即表示您接受并同意这些变更。**

1. 您明确理解并同意，**本产品按“现状”提供**，不存在任何形式的明示或暗示保证，并且在适用法律允许的最大范围内，奇安信集团不提供任何明示或暗示的陈述或保证，包括但不限于有关适销性、适用于特定目的以及不侵犯第三方权利的保证。奇安信集团不保证产品中所含的功能将满足您的全部要求，也不保证您对本产品的使用不会中断或出错。**选择本产品来达到预期结果，以及安装、使用本产品并获取结果所带来的所有责任和风险由您承担。**

2. 奇安信集团承诺致力于不断提升产品的质量，本产品是在现有技术水平基础上提供的，但奇安信集团无法保证您使用本产品将完全符合您的期望，包括但不限于不能保证您【通过使用产品能够发现所有的安全漏洞以及能检测到所有的入侵威胁，检测到的入侵威胁不保证完全正确】，**您理解并同意，出现前述不符合您对产品期望的情形不视为奇安信集团违约。**

3. 您明确理解并同意，**您在使用本产品过程中可能发生不可抗力或不可预见的情形，包括但不限于：1)被某些未经许可的个人、团体或机构通过某种渠道获得或篡改；2)因通信繁忙出现延迟，或因其他原因出现中断、停顿或数据不完全、数据错误等情况，从而使交易出现错误、延迟、中断或停顿；3)因地震、火灾、台风及其他各种不可抗力因素引起的停电、网络系统故障、电脑故障等；4)计算机系统可能因存在性能缺陷、质量问题、计算机病毒、硬件故障及其他原因；黑客攻击、计算机病毒侵入或发作等非可归责于奇安信集团的原因；5）政府管制、网络故障、国家政策变化、法律法规之变化等。如发生不可抗力或不可预见的情形，奇安信集团将尽最大努力予以补救，但奇安信集团对于因不可抗力和不可预见的情形造成的各类直接或间接损失，均不承担任何责任。**

4. **对于任何本产品的使用行为，包括但不限于您自身和/或任何第三方的行为，**

奇安信集团均不承担任何责任。

5. 对于从**非奇安信集团指定途径以及从非奇安信集团发行的介质上获得的本产品**，奇安信集团无法保证其是否感染计算机病毒、是否隐藏有伪装的特洛伊木马程序或者黑客软件。**使用此类产品，将可能导致不可预测的风险，建议用户不要轻易下载、安装、使用，奇安信集团不承担任何由此产生的一切法律责任。**

6. **上述免责声明适用于因任何性能故障、错误、遗漏、中断、删除、缺陷、操作或传输延迟、电脑病毒、通信线路故障、失窃、毁坏、未经授权的访问、篡改或使用（无论是出于违约、侵权、疏忽或任何其他诉因）而导致的任何损害、责任或伤害。**

7. 奇安信集团保留在**不发布通知**的情况下随时采取以下行动的权利： **在执行常规或非常规维护、错误纠正或其他更改所必需时，中断或修改本产品的任何组成部分的运行或功能。**

8. 本声明受中华人民共和国法律的约束并依据其解释。

9. 在法律允许的最大范围内，本声明最终解释权归奇安信集团享有。

修订记录

版本	状态	修订理由和内容摘要	修订人	批准人	修订日期
V1.0	C	新建	程涛	常月	20230222

状态：C-创建，A-增加，M-修改，D-删除

数据安全分级标注说明

■ **数据分级**错误!未知的文档属性名称	公开数据（ Y）	内部数据（）	普通商秘（）	核心商秘（）

*数据分级标注及说明：

1、文档编写前，应标注数据安全级别，默认为内部；

2、请根据文档内容评估数据安全级别，在对应数据级别（）中填写（Y）；

3、分级 TIPS：

【核心商秘】：限于个别人、小范围共享和使用的信息，例如薪酬数据、未公开的产生严重危害的样本等。如泄露将导致法律风险或者影响到社会公众利益或者严重的恶意竞争等；

【普通商秘】：限于特定人群、特定范围内共享和使用的信息，例如公司组织架构、产品样本集等。如泄露存在合规风险或者可能影响社会公众个人利益或者存在一般恶意竞争的风险等；

【内部数据】：限于在公司范围内按需使用，除去公开数据、核心商秘、普通商秘，都为内部数据。如泄露不存在法律合规风险或不存在影响社会公众个人利益的风险，但会产生轻微的恶意竞争风险等；

【公开数据】：对任何方面都无危害的、不会被任何方面进行利用的信息，例如官网上的产品简介等。如泄露对任何方面都无影响。

目录

1 产品概述 1
1.1 产品简介 1
1.2 产品定位 1
1.3 产品形态及构架 2
2 产品功能 3
2.1 综合态势功能 3
2.2 资产中心功能 6
2.3 全局检索功能 9
2.4 安全监测功能 9
2.5 分析引擎管理功能 9
2.6 分析中心功能 11
2.7 工作指挥功能 12
2.8 指令协同功能 14
2.9 报告中心功能 14
2.10 报表中心功能 16
2.11 数据中心功能 17
2.12 运维中心功能 21
3 特点与优势 23
4 产品价值 24
5 应用场景 26
6 安装部署 27

1 产品概述

1.1 产品简介

奇安信网神网络空间安全态势感知与协调指挥平台基于公司平台化战略进行构建，整合公司的全方位数据数据能力、技术能力与安全能力，实现威胁看得透，在看清威胁的基础上构建基于动态预案编排的指挥生态。形成知行闭环体系并对安全分析研判决策体系进行贴合监管的实战化升级。面向网信、公安、军队、大数据局、城市监管等监管市场提供包括监测、发现、预警、指挥、协同、处置等实战业务的新一代实战化网络空间安全治理总平台，态势感知平台基于大数据架构，联合流量采集探针和资产采集探针，运用主被动采集方式，实现海量分散安全信息采集，采集范围包括重要服务器、终端、防火墙、防病毒系统、漏洞扫描、入侵检测、核心交换机、路由器等各类网络和安全设备安全数据，实现资产入围、监视变更和退网的全流程管理。同时，通过检索、调查、场景、关联多类分析手段，实现海量安全数据深度分析，定期形成各区域全流量分析，并可从资产、漏洞、攻击、威胁、监测、处置等多个维度进行全面的态势分析展示，全面展示态势视图、威胁分布、分析预警等管理者关切的态势。

1.2 产品定位

奇安信网神网络空间安全态势感知与协调指挥平台的战略定位，是将大数据与智能化技术应用于网络安全领域，应对日趋复杂、严峻的网络安全挑战，在网络空间安全保护方面，进行社会治理体系与治理能力现代化的创新，实现网络空间的安全治理。

就顶层设计而言，平台是要配合国家监管部门建立网络安全防控体系，并与政企机构自有的安全体系形成大闭环。与此同时，平台还应能够支撑和牵引建立国家级纵横交织的监管和指挥体系，逐步做到横向到边，纵向到底。逐步实现能力的编织，从通过资产管理、安全监测、通报处置等手段，不断提高各行业、各主责单位的安全防护意识和防护能力，不断提升全社会的安全底线，破解九龙治水难题，实现多元共治，初步建立国家级安全治理体系。通过持续运营，逐渐掌

握对手的情况，包括攻击偏好、攻击习惯、常用工具、常用手段、常用资源等，从而可以从被动防御逐渐转向更有针对性的积极防御。继续通过与各职能部门的协同和信息共享，以及新的监测技术手段、管理手段的综合运用，将监测保护的对象，从网站、系统、平台，拓展到 5G、物联网、工业互联网、大数据中心、云平台等数字经济的基础设施，并与各行业建立的垂直监管平台打通，形成立体化、全息化的网络空间安全监测与保护能力。

1.3 产品形态及构架

描述产品形态、物理组成、硬件规格及构架；

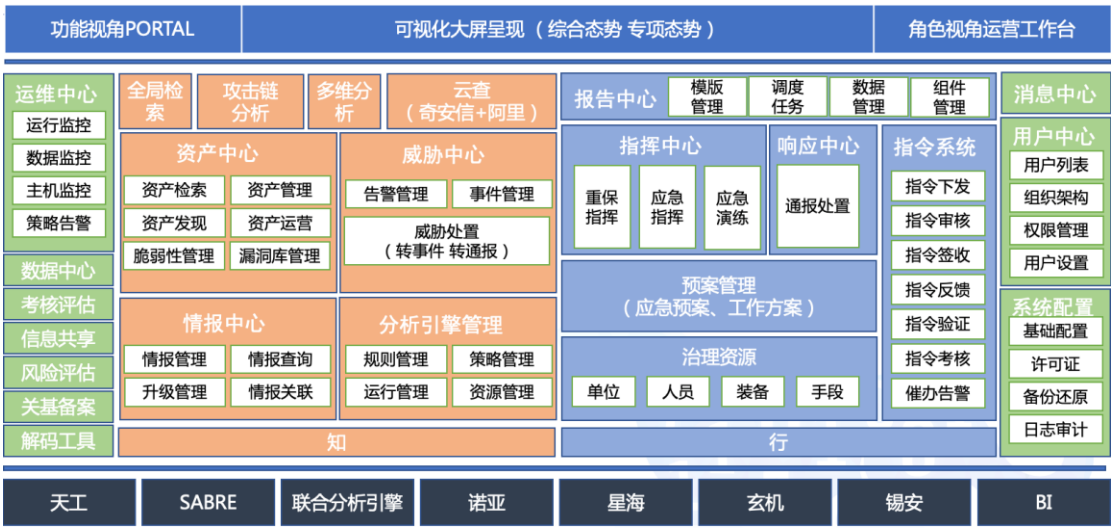


图 1-1 产品架构图

上图为网络空间安全态势感知与协调指挥平台的产品架构，分为四个部分，底部为平台的基础支撑模块，包括天工、SABRE 引擎、联合分析引擎、诺亚、星海、玄机、锡安以及 BI 支撑对上层各应用的支持。实现了能力底座、业务操作、决策支持三层解耦，并相互协同的先进架构。以公司战略平台为底座，解决奇安信及第三方安全大数据和安全能力整合利用的问题。高度整合公司现有的核心能力。以业务操作为中间层，为安全分析、业务工作、运营保障的各类用户，提供了丰富的实战化、操作型应用功能。以决策支持为顶层，为客户的高层领导提供了挂图作战、决策辅助。三层能力高效协同，使得新一代态势感知平台，同时具备了强大的安全能力、客户业务工作支撑能力、以及高层领导的决策支持能力。

2 产品功能

2.1 综合态势能力

综合态势系统基于多源数据支持安全威胁监测以及安全威胁突出情况的分析展示。综合利用多方获取的数据资源，利用大数据技术进行分析挖掘，并以数据可视化的方式呈现，实时掌握网络攻击对手情况、攻击手段、攻击目标、攻击结果以及网络自身存在的隐患、问题、风险等情况，对比历史数据，形成趋势性、合理性判断，为通报预警提供重要支撑。该模块支持对网络空间安全态势进行全方位、多层次、多角度、细粒度感知，包括但不限于对重点行业、重点单位、重点网站，重要信息系统、网络基础设施等保护对象的态势进行感知。综合态势系统分为态势分析与态势呈现两部分。态势展示功能，利用大数据分布式集群下的计算、存储和分析技术，实时对下属单位的资产状况、受威胁攻击、流量流速等情况进行全方位评估，并以地图、柱状图、曲线图、环状图等多维可视化形式进行展现，帮助本单位直观了负责的网系内整体网络安全态势，包括态势总览（综合态势）、资产态势、攻击态势、流量态势、业务态势和流量态势等态势大屏呈现，同时，态势展示系统提供了多元化的丰富的展示态势和分析组件，能够实现基于 3D 的动态攻击展示效果；同时具有大屏展示时间设置，在态势大屏中可以选取相关信息下钻跳转到对应的详细页面，在详细界面中可以具体展示该单位、部门、节点的详细信息。

图 2-1 3D 动态展示图

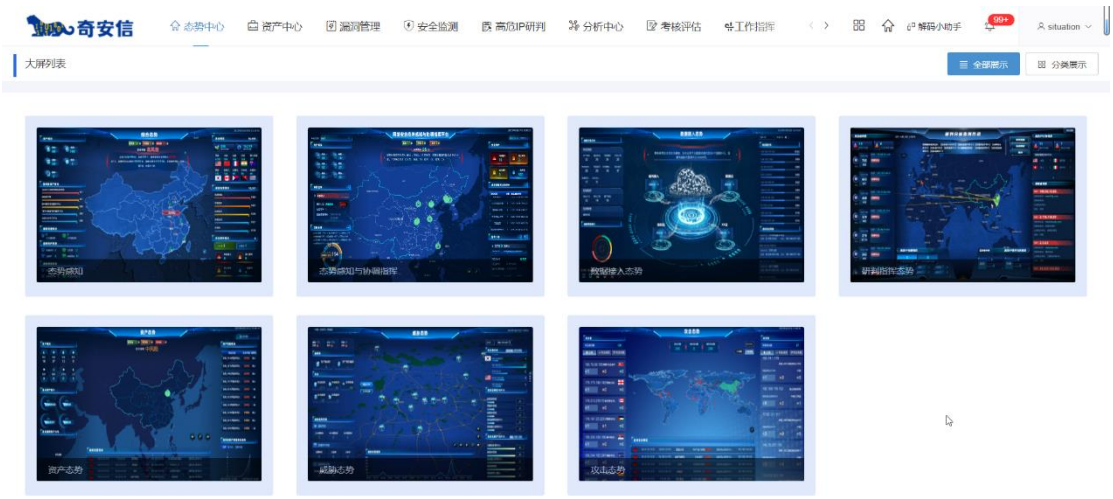


图 2-2 总体态势展示图

- 攻击态势

攻击态势展示功能，能够以攻击者和受害者的视角对遭遇到整体攻击情况进行详细展示，展示的内容包括但不限于攻击状态、攻击趋势展示当前遭受攻击的宏观现状等，在攻击详情中能够从情报命中情况、受攻击资产、攻击端口分布、攻击源 TOP 排名、攻击事件列表等展示。

图 2-3 攻击态势

- 流量态势

流量态势展示功能，通过对流量探针获取的流量数据进行整合和分析，将分析后的结果数据进行综合流量态势展示，展示范围包括但不限于现网流量总体概览和变化趋势，包括今日累计和昨日累计流量大小、今日和昨日流量峰值、平均流速等，也可以自定义选择需要展示的时间，包括 24 小时，周、月等。

图 2-4 流量态势

- 业务态势

业务态势能够对在网内收集的各类信息资产和业务系统的运行状态进行全方位的细粒度的监控和呈现。

图 2-5 业务态势

- 态势展示性能

  态势感知平台在系统能够存储的并处理好相关数据的情况下，进行数据查询，各类态势展示的时间为 8 秒。

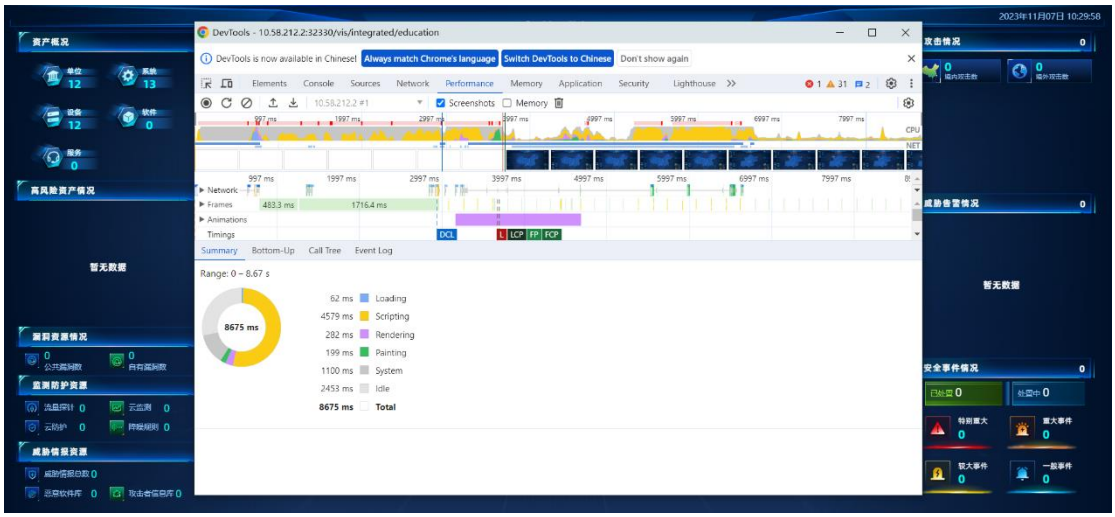


图 2-6 响应时间

2.2 资产中心能力

支持通过主动探测、流量分析、人工报送、数据导入等手段汇聚网络资产，包括关键信息基础设施以及公共空间资产，并通过统一的资产数据模型将多源异构的数据进行融合，形成以系统、网站、计算设备、软件、服务、机房、云平台为主体的网络资产库，建立关键资产和所属单位、四方单位、运营人员之间的联系，形成资产知识图谱。针对核心关键资产，提供相关运营手段，自动或半自动对资产变动进行维护。同时，完成对关键基础设施资产信息的填报管理，统一分析年度关键基础设施资产情况。资产态势功能，以网络资产（单位、系统、网站、设备软件、服务）作为切入点，为网络安全业务决策做资产相关的可视化分析，通过展示资产总体态势、今日发现资产概括、开放端口 TOP、安全域下网段信息、资产类型、操作系统 TOP 等信息，能够按照不同的维度（时间、安全事件等）对以上需要展示的相关信息进行统计性的展示，方便指战员了解所负责网系内整体资产态势信息。

图 2-7 资产态势展示图

- 脆弱性管理

实现通过关联已纳管的资产数据与漏洞告警数据生成资产脆弱性数据，实现对资产脆弱性状态的管理支持已纳管资产和漏洞告警数据的关联、支持通过漏洞视角查看影响的资产情况、支持对资产漏洞告警的修复状态提示和设置、支持对各资产漏洞告警次数的统计、支持通过资产视角查看资产的漏洞告警情况、支持已纳管资产和漏洞告警数据的关联后，资产详情和漏洞告警详情的查看。通过关联已纳管的资产数据与漏洞知识库生成资产潜在漏洞数据，实现对资产潜在漏洞情况的管理、支持已纳管资产和漏洞知识库数据的关联、支持通过资产视角查看资产的潜在漏洞情况、支持已纳管资产和漏洞知识库数据的关联后，资产详情和漏洞知识库详情的查看。具有资产分类统计数据，可以直观显示每个分类（单位、系统、网站、设备、软件、服务）的资产总数，同时对相关分类的资产进行下钻详细展示，通过列表的形式展示风险资产名称、资产 IP、价值、脆弱性、威胁、处置状态等信息，同时可以对风险资产批量处置，以此来保障系统的安全性和可用性，支持对受影响资产、漏洞类型进行 TOP 排行统计，同时对漏洞危害等级进行占比统计。

图 2-8 漏洞排行

图 2-9 风险详情

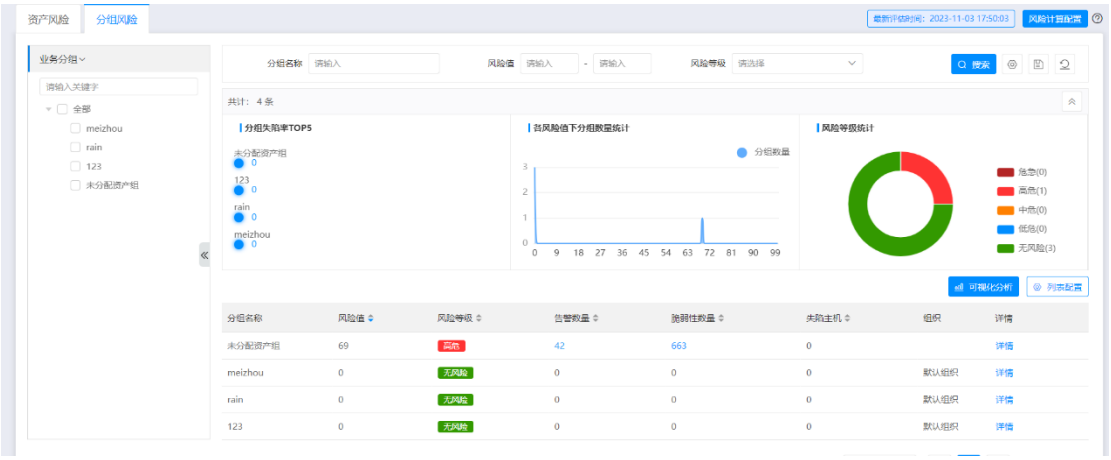


图 2-10 资产统计

- 漏洞库管理

漏洞库管理模块提供了漏洞库的管理功能，包括奇安信漏洞知识库和自定义漏洞知识库，其中奇安信漏洞知识库提供了的查看和漏洞影响面功能，自定义漏

洞知识库为用户提供了对自身维护的漏洞知识库的管理功能支持对接入漏洞知识库数据的查看和统计。支持对接入漏洞知识库数据与已纳管资产的管理、支持对接入漏洞知识库数据漏洞影响面的评估、支持对人工维护漏洞知识库的管理、支持对人工维护的漏洞知识库的新增、修改、删除、查看等基础管理功能。同时支持对人工维护的漏洞知识库数据的查看和统计、支持对人工维护的漏洞知识库数据与已纳管资产的管理以及支持对人工维护的漏洞知识库数据漏洞影响面的评估。

2.3 全局检索能力

全局检索向安全分析人员提供了对日志、告警、事件综合管理，支持全局搜索并对搜索结果进行查看，可对全局搜索到的结果信息进行分析操作，判定告警准确性支持快捷模式和高级模式两种查询模式，快捷模式中支持预定义数据字段进行快速搜索，高级模式支持分析人员按语法输入查询条件。全局检索功能支持安全分析人员利用预定义的查询条件进行快速检索，并可以保存查询条件。

2.4 安全监测能力

安全监测提供告警和事件的管理，告警管理对接入平台数据源生成的告警进行管理，支持安全分析人员对归并后的告警进行进一步研判。实现实时监测网络安全情况，及时发现攻击活动、攻击手段和攻击目标，全面监测重点单位信息系统和网络，实现对安全漏洞、安全威胁、高级威胁攻击的发现和识别，并为通报预警等业务提供强有力的数据支撑。

2.5 分析引擎管理能力

联合分析引擎是从汇聚的大量原始安全数据中提炼有价值的信息，形成告警，最终得到可处置的事件的过程。这是一个数据量缩减、数据价值提升的过程，安全分析人员在系统工具的支持下完成整个数据加工的过程。 联合分析引擎接收标准化后的日志数据，生产出告警和事件。引擎的输入日志，包括本地设备产生的日志，也包括云端提供的各种数据，引擎的输出的告警和事件为数据分析人员

提供统计后的数据进行后续处置。提供 2 类规则引擎，sabre 规则引擎（流式）和天工规则引擎（批式）。Sabre 引擎基于流式处理框架进行设计，能够在大数据量级下对各维度安全数据进行分析，发现更复杂的告警信息，并产生告警。天工引擎基于批式处理框架进行设计，能够把比较复杂的问题进行工程化。通过流量传感器、防火墙、终端安全设备、等日志数据抽象出逻辑规则，配置过滤规则，直接产生相关告警，可配置的规则包括但不限于访问使用弱团体字符串、资产开放违规端口、资产开放端口服务超出阈值数量、资产通联 ip 超过阈值、资产开放非常见端口服务超出阈值数量、资产开放远程运维类端口服务超出阈值数量、高危端口开放等，同时也可根据当前网络中的安全状态对灵活自定义配置设置规则。

图 2-11 分析规则

图 2-12 规则自定义

2.6 分析中心能力

云查向安全分析人员提供了线索数据的查询能力，包含对特定 URL、MD5 查询线索功能和在业务功能模块反查其中 URL、MD5 线索的功能，并支持多条件组合查询，能够通过导入方式获取外部相关威胁情报信息，支持平台自身发现的威胁转换为情报信息，系统能对这些威胁情报进行管理，能将这些威胁情报用于关联分析。

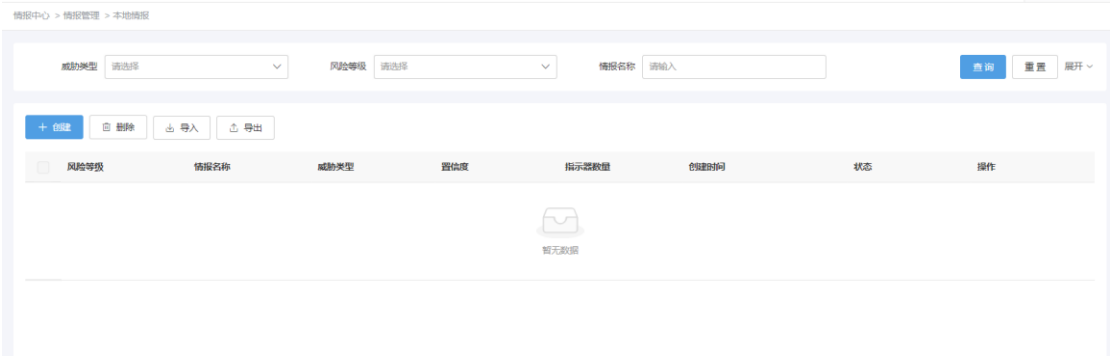


图 2-13 情报导入

多维分析通过分析流量中的行为，结合开源情报信息，挖掘网络安全事件背后的攻击者。利用流量日志、安全事件等信息，结合开源威胁情报以及网络攻防知识库，基于本体论的思想，提取关键实体并构建实体之间的关系网络，具有进出口流量、资产、ip 对会话等同比分析，能够根据自定义时间进行对比并判定偏差度来发现异常线索。

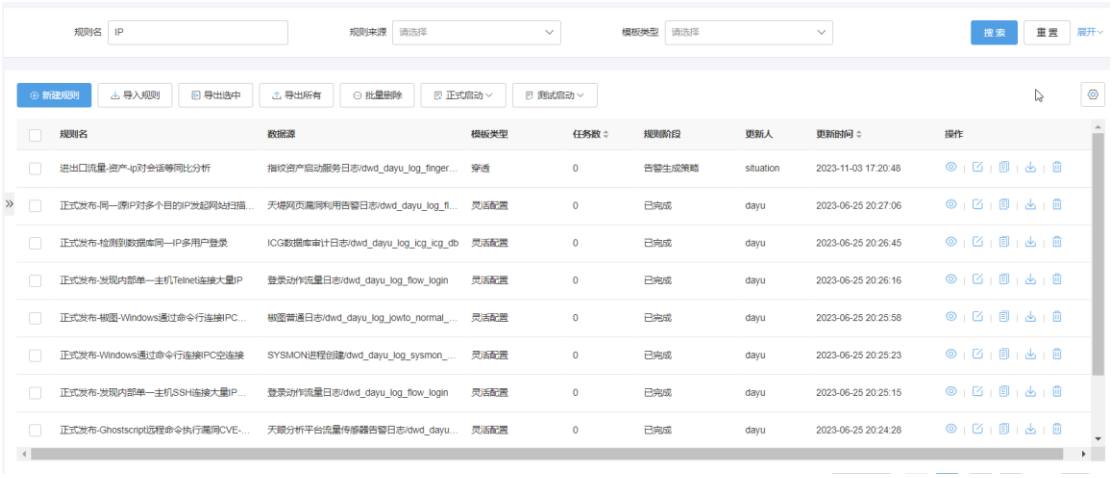


图 2-14 同源分析

攻击链分析基于监测的网络攻击告警信息，针对攻击源和受害地址，利用网络流量日志、网络安全告警以及人工取证的信息，对攻击过程进行还原。图谱式

事件分析能力，图谱模式可以清晰的展示攻击 IP 和被保护系统间的关系，还可以展示攻击者所属的场景及攻击次数，通过攻击 IP 可以查看攻击者更多信息，例如地理位置、恶意行为类型、攻击者详情等。支持展示不同时间段的攻击柱状图，了解攻击趋势分布情况，图谱分析页面实现以 IP、端口、服务、告警、MD5、URL 等任意维度的信息查询，并对查询节点相关的告警、攻击、弱点信息进行扩展查询。

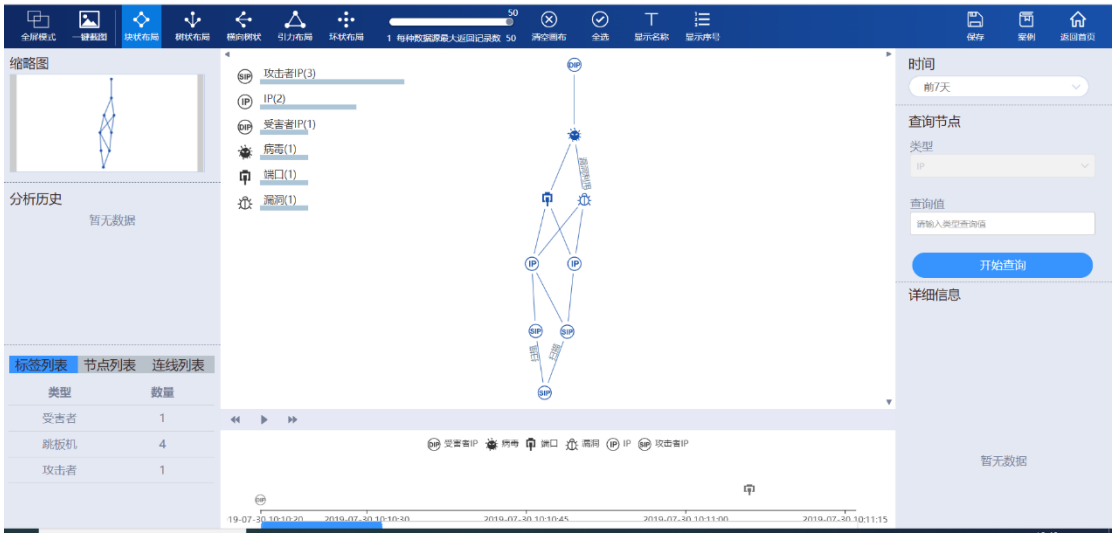


图 2-15 多维分析

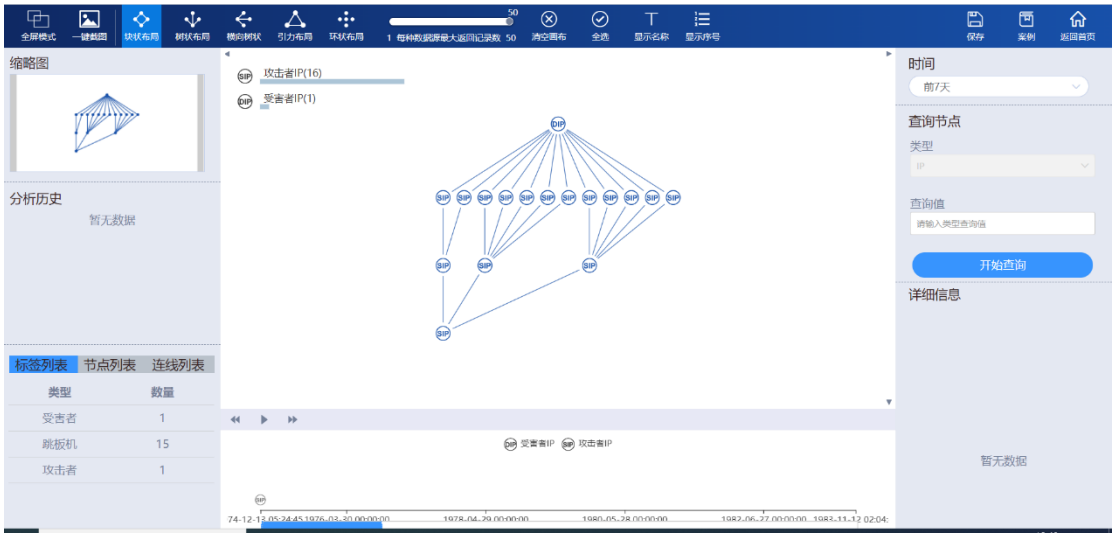


图 2-16 多维分析

2.7 工作指挥能力

工作指挥中包括对流程预案的管理，包括工作方案和网络安全事件应急预案。支持对原子手段的编排形成预案，灵活应对当前由于业务工作需要造成的流程变

化，态势感知平台支持工单功能，工单功能，能够对告警事件和预警事件派发处理。由管理员指定工单处理人和工单处理周期及告警处理建议。

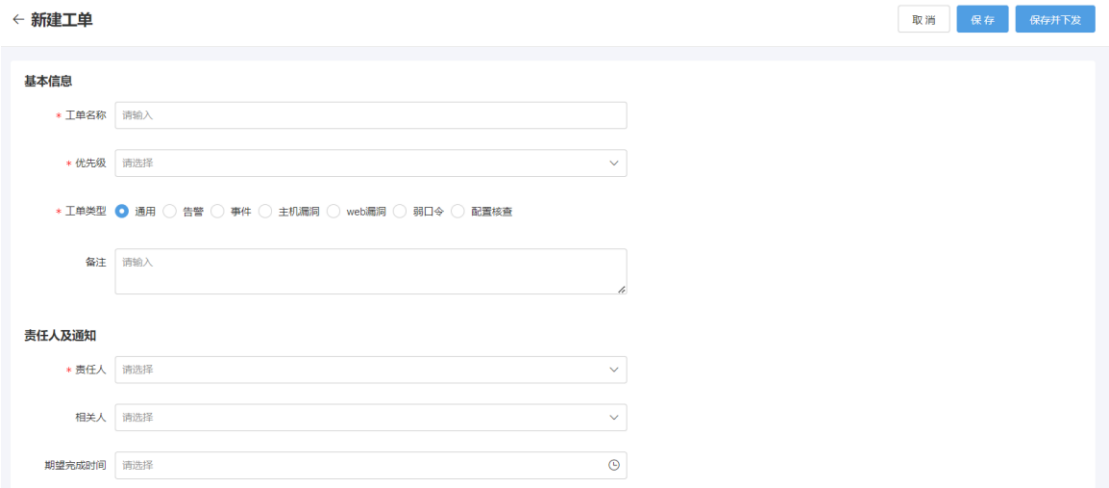


图 2-17 工单管理

重要活动保障在重要会议或重大活动期间，加强网络重保人员调度，全方位全天候掌握重保单位、系统和网站安全状况，协同多家技术支撑单位、互联网安全厂商及网络安全专家保障整个过程的网络安全和数据安全，通过重保期间全方位、全天候的指挥调度，对网络安全威胁、事件、进行通报预警，快速处置重大网络安全事件，实现全要素采集、全要素监控、扁平化指挥，提升重大活动的安全保障能力。个人工作台功能，在该功能下工作台能够展示含待办工单数、建单数量、已办数量、紧急任务数量，同时能够展示出总体威胁告警数和变化趋势以及当前安全事件数量级变化趋势，管理员，支持工单列表管理功能，支持跟踪工单的流程图和审批记录。

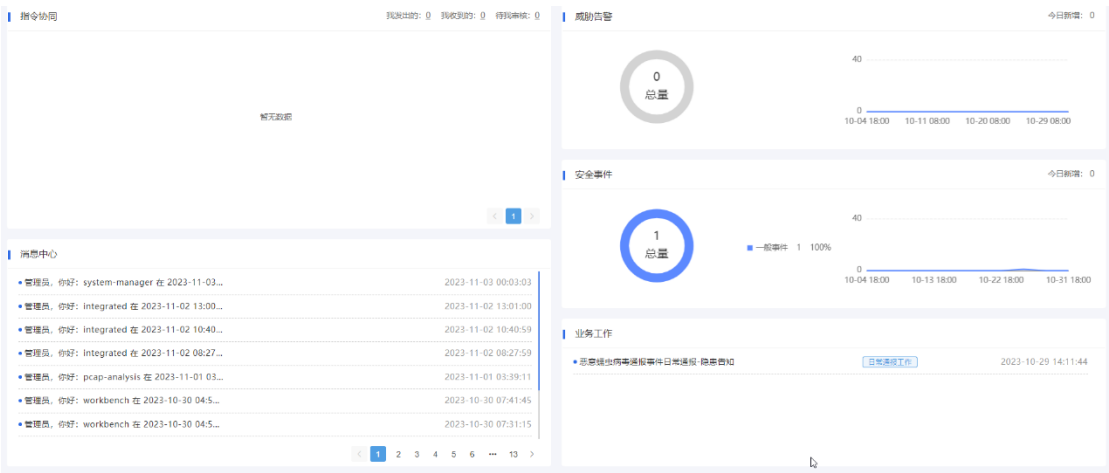


图 2-18 个人工作台

突发事件应急指挥系统，通过可编排的数字化应急预案，结合事前应急演练，针对重大网络安全突发事件，实现对预警响应流程和应急指挥流程的全方位支撑，对各类资源的统筹调度、协同联动，对安全事件定义个性化监控指标和视图，对事态发展进行实时监控，提高网络安全突发事件的应急指挥能力。

日常通报工作针对关键信息基础设施运营单位，就该单位发生的网络安全事件进行通报，确保问题得到及时整改，形成威胁发现、通报、整改、反馈的闭环。

2.8 指令协同能力

针对日常通报、突发事件应急、重大活动保障、应急演练等工作场景，提供统一的资源协调、指令下达、反馈响应机制，对指令传播通道、指令类型、指令内容进行统一管理。并对各级单位的响应率、响应速度、响应质量进行评估。

2.9 报告中心能力

报告中心通过配置功能和图形化的操作界面，帮助用户轻松制定专业水准的数据报告，通过所见即所得式操作引导用户像搭建乐高积木一样来快速组装不同需求场景下的数据报告。系统支持多源异构数据的接入，内置多种布局模板，在页面布局模板中可根据不同需求预定义报表，也可根据不同需求构建展示报表。通过灵活配置各类分析报告，实现将态势中心、资产中心、威胁中心、分析中心等多个业务子系统的数据结果经由处理后输出为 Excel、word、PDF 等多种文件格式，支撑系统运营人员完成整体安全态势、相关安全事件以及业务工作情况的分析报告，并支持将构建的报表以邮件和短信等前转方式进行推送通知和告警。系统内置综合分析报告、安全风险报告、资产与脆弱性报告、安全威胁分析报告等报告模板，同时也可根据使用需要进行自定义创建相关报告，报告具有周期性（每日、每周、每月、每年）自动生成报表并通过下载、导出等方式获取。

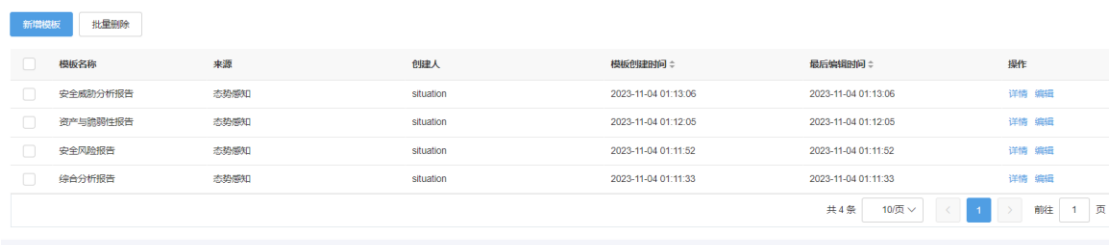


图 2-19 报告模板

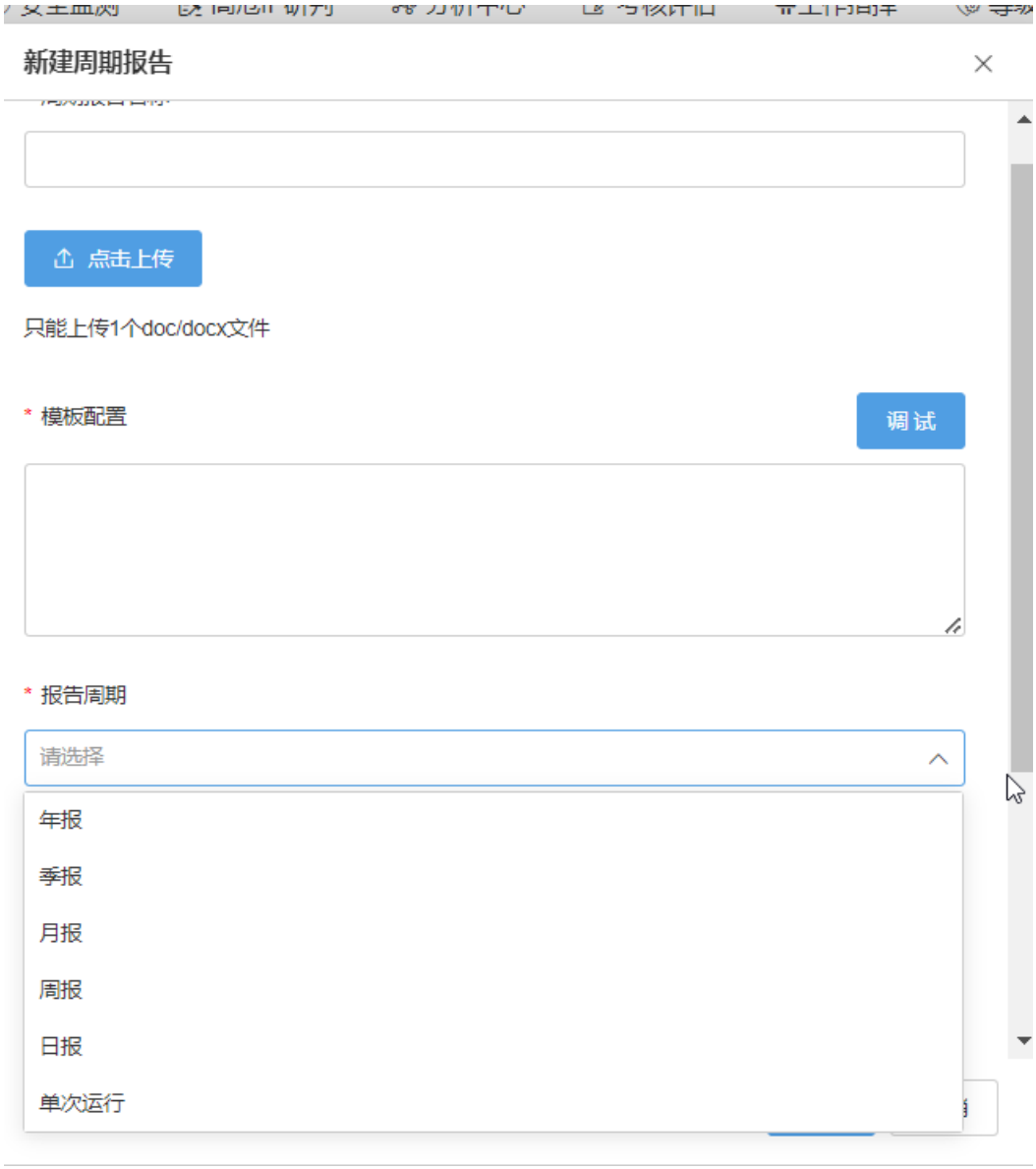


图 2-20 周期报告

报告总览支持对系统中生成的报告进行管理，包括查询、搜索、删除以及下载等工作。

快速报告支持选定模版和周期性的报告创建。可以坚持添加、删除以及搜索功能。

调度管理支持对查询数据量比较大的任务创建调度任务。包括任务的名字、使用的模版、报告生成周期等功能。可以对调度任务进行查询、删除、新增以及编辑等基本操作。

报告管理支持对报告列表进行搜索、下载、删除、预览等操作。其中预览只

支持 pdf 类型的报告。

数据源支持多种数据查询的链接。包括 Excel、CSV、ES、MySql、Oracle、PG 等。通知支持创建数据查询模型，可直接用于报告中的查询。

模版列表支持支持对模版的基本增删改查的操作。维护内容包括模版名称、来源、创建人、创建时间以及最后编辑时间。新建模版后支持图表、文字标题等内容的拖拉拽操作。支持图层位置的边界等功能。

2.10 报表中心能力

报表中心支持对系统数据源以及分析视图和仪表盘的创建和管理功能。数据源管理实现对分析所需数据源进行读取及管理。支持从数据库中读取相关数据表结构、表数据信息，支持数据库物化视图并按照指定周期、频次更新数据；支持文件数据源导入及校验；支持接从接口中读取数据；支持数据预览以及数据搜索。

数据集管理根据分析需要构建数据集，数据集来源于单个已加工处理好的数据表或者多个数据表关联构造数据集；支持基于数据库表、SQL 语句、文件数据源、接口数据源创建数据集；支持对数据集进行编辑，包括数据复杂条件过滤、新建计算字段、关联其他数据表、数据行权限设置等；支持维度、度量管理，包括字段名、字段类型、数据字典绑定、层级、显示隐藏、显示格式（度量）、聚合方式（度量）等设置；支持数据目录管理以及数据目录权限设定；支持对数据集进行授权。

分析视图持根据分析需求构建视图，支持构建交叉表、明细表、分组表、以及饼图、柱图、条形图、双轴图、指标卡、矩形树图、词云图等图形分析；支持视图的复制，复制后进行编写可生成新的视图；支持视图编辑功能，通过拖拽方式配置视图数据，支持对数据排序、显示格式配置；支持视图统计指标高级计算，包括同环比分析、累计值、占比分析；支持视图数据直接使用日期维度的不同时间粒度；支持视图数据下钻、数据 TOPN、颜色标记、参考线等；支持对视图数据进行复杂条件过滤；支持自定义视图功能，满足个性化视图样式渲染；支持视图目录管理。

2.11 数据中心能力

数据中心包括元数据管理、数据仓库和数据服务。提供一个一站式、标准化、可视化、透明化、可运营化大数据资产全生命周期智能管理平台，为实现原始数据资产化、数据资产价值化、业务数据化提供合法、合规、安全、高效的技术支撑。

元数据管理将安全业务数据化，建立上下文关联信息，为内生数据应用提供支撑能力。支持管理业务元数据、数据业务类型、信息分类编码标准、规则和质量管理。管理业务元数据确定共同认可的词汇和对应的信息资产，确保领域知识的共同理解；管理数据业务类型与不同数据源类型中数据物理类型的映射关系，实现技术元数据和业务元数据的统一定义；管理信息分类编码标准，支持信息分类编码标准增加、删除、查询、编辑等功能；基于数据质量规则库，配置不同的质量检测规则以满足满足数据质量的时效性、准确性、完整性、一致性、有效性检测。

数据仓库对业务系统数据进行统一管理，以便于应用，数据仓库包括明细层和汇聚层。明细层基于强大的数据预处理能力，将各业务系统、各类型的数据抽取加载至目标数据库，实现各类业务数据的同步与集成，为后续进一步加工数据奠定基础。汇聚层基于全局定义的项目空间、明细层，根据业务数据需求，提供灵活高效的可视维度建模能力，支持雪花模型和星座模型，将数据资产价值化，为内生数据应用提供支撑能力。

数据服务提供 API 数据消费方式，帮助用户更好地进行数据资产应用以实现价值化。

- 数据采集能力

态势感知平台通过内置的采集器实现对网络安全设备、网络设备和重要服务器的进行性能与可用性信息的周期性采集，采集器包含了日志采集器、流量采集器以及第三方采集器信息的查看与管理功能，方便用户更清晰的了解采集器的具体信息，以及在线/离线状态，使得用户对于采集器的使用情况一目了然，具有采集协议包括但不限于 SNMP、TELNET、SSH、SSH2 或 ODBC 等常用协议。

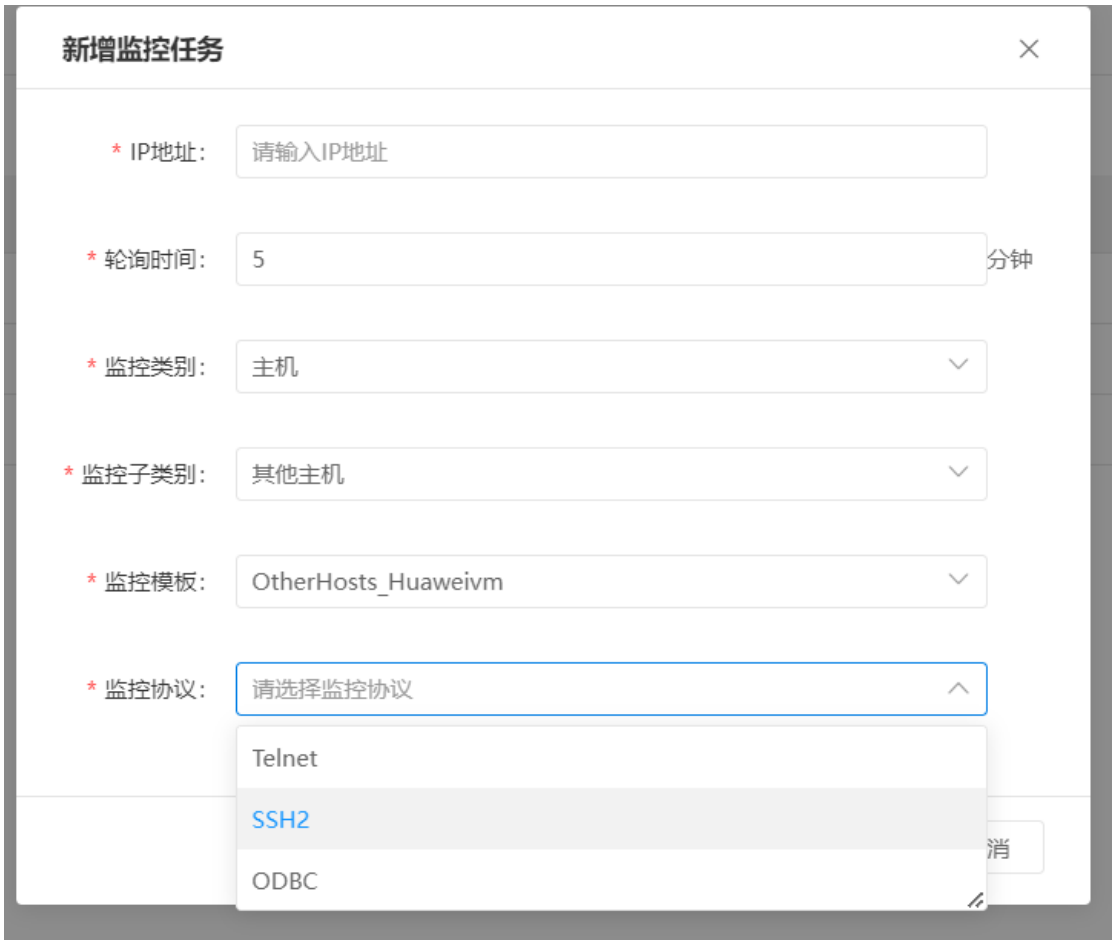

新增监控任务
* IP地址：
请输入IP地址
* 轮询时间：
5
分钟
* 监控类别：
主机
* 监控子类别：
其他主机
* 监控模板：
OtherHosts_Huaweivm
* 监控协议：
请选择监控协议
Telnet
SSH2
ODBC
消

图 2-21 数据采集

图 2-22 数据采集

- 设备接入能力

态势感知平台，能够接入各类设备和应用系统，包含但不限于主机、服务器、防火墙、IPS/IDS、WAF、其他网络设备、其他安全设备等，能够对相关系统产生的系统日志和告警日志进行收集。

图 2-23 设备接入

- 日志采集

具有数据采集功能具有主动、被动采集/收集目标日志，包括但不限于以下几种日志采集方式，Syslog 日志、SNMP 日志、文本格式日志、JDBC、数据库日志、WMI 日志、Netflow 日志、HTTP 日志、Script 日志、FTP 或 SFTP 等多种方式完成日志采集/收集功能，支持客户端代理采集，支持对 KAFKA 数据源采集，等多种采集方式在采集过程中具有限流功能，方便用户对采集日志配置的统一管理。

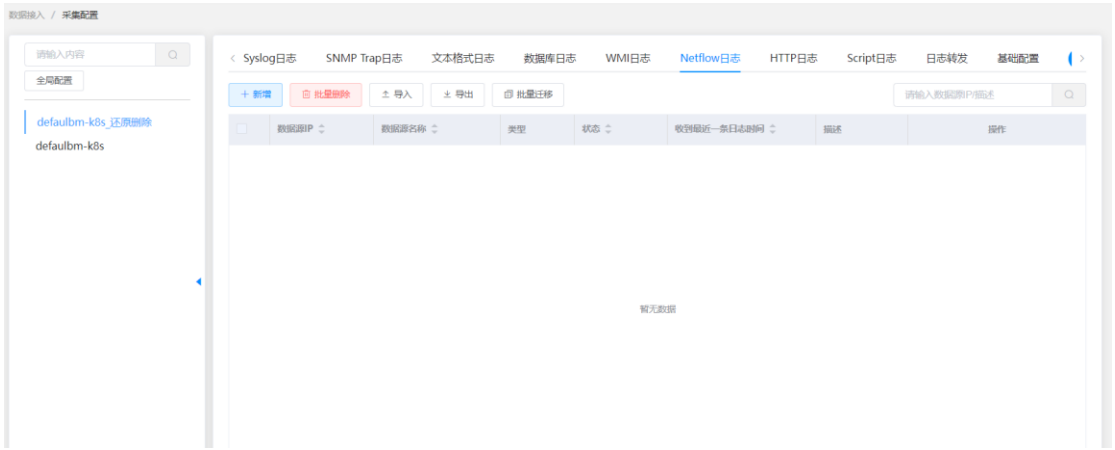
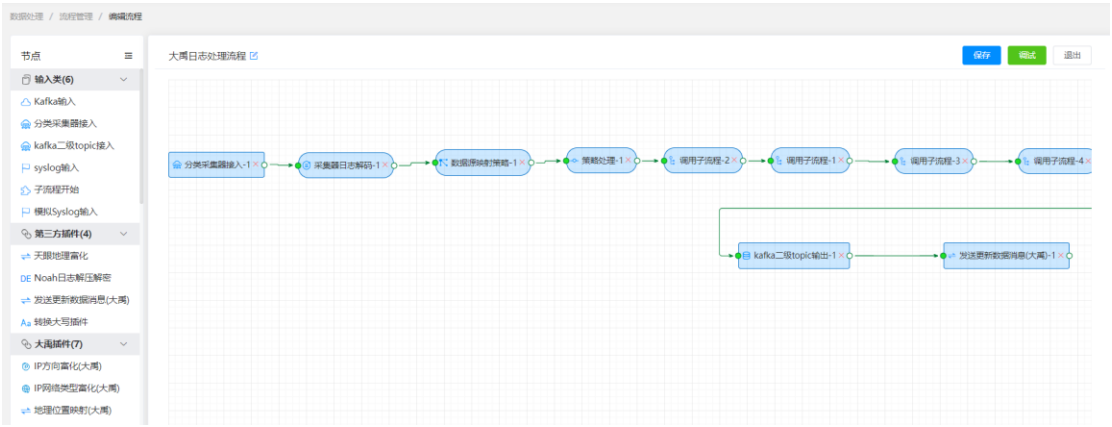


图 2-24 数据接入

- 日志范化能力

具备对日志范式化功能，实现对异构日志格式的统一化，支持现有主流大厂设备，自动识别日志数据匹配规则，自动生成框架，配置相关解析规则、过滤规则、富化规则，实现对于多源异构数据的输入、处理、输出的加工全过程，包括流程管理、规则管理、部署管理等系统功能，不需要手动配置规则和日志类型，从而实现数据处理的数据抽取、清洗、富化和加载工作。



2.12 运维中心能力

实现对部署节点的状态、指标、资源等进行监控。单机部署：对硬件资源使用情况进行监控；集群部署：对集群节点状态、资源使用情况进行监控。以及对平台系统组件、业务支撑组件、业务组件状态进行监控。系统组件：系统组件为系统运行底层组件（例如：redis、pg、kafka、ES 等），主要对系统组件运行状态、关键指标参数进行监控；业务支撑组件：业务支撑组件为支撑平台业务运行的支撑组件，主要对各业务支撑组件状态、各业务支撑组件下业务服务运行状态进行监控；业务组件：平台开发的微服务业务组件（例如：uae-alert-server（安全监测-告警详情）等），主要对各组件运行状态及该组件关键运行参数进行监控。对各类数据接入流（例如：日志采集器、流量采集器状态等。）、业务流（例如：平台接收器等。）进行可用性监控。态势感知平台，支持添加流量监测和资产采集探针，能够将流量监测设备和资产探针的相关系统性能进行实时显示，同时对本地采集器的运行时长、CPU 和内存，内置的跳转链接能够实现一键跳转至流量监测探针和资产采集探针页面，方便管理人员对接入的相关设备进行灵活管理。

有对流量采集探针和资产探针的统一管理和日志采集分析功能；内置的统一升级中心具有相关特征库，能够对全流量检测探针和资产探针提供特征库升级服务。

图 2-25 探针管理

图 2-26 探针详情

图 2-27 统一管理

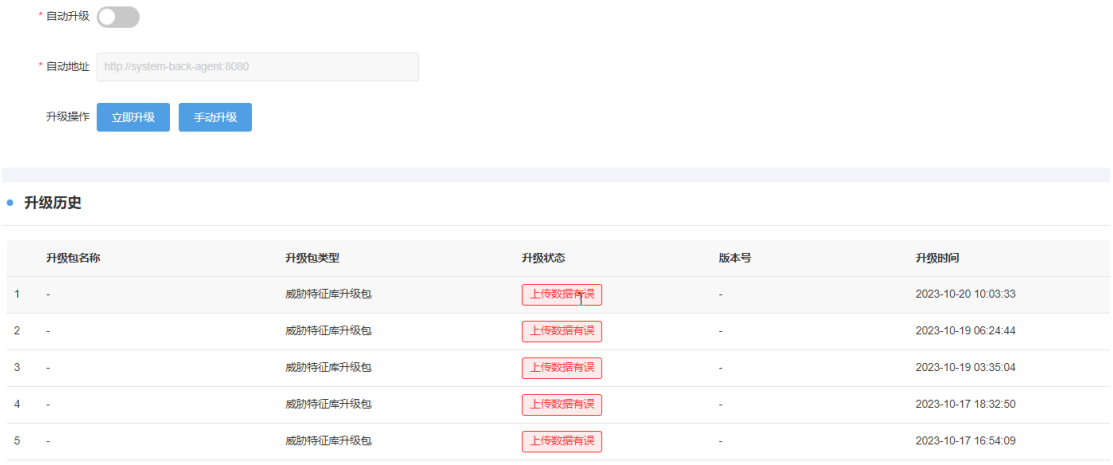


图 2-28 特征库升级

3 特点与优势

- 安全能力

可以网站遭受目录遍历攻击，此规则可有效降低探针对于目录遍历相关的告警

通过监控攻击来源 IP 使用攻击手段的数量、攻击目标的数量以及攻击次数，筛选出那些可能导致重大风险的攻击源进行优先处置

可以识别出地址扫描通常会配合端口协议扫描、漏洞扫描等行为

可以识别单一 IP 来源对 SSH 服务器尝试高频登录，多次失败后登录成功，用以检测爆破结果，此规则可有效降低探针对于暴力破解的告警量

可以识别单一 IP 来源对 RDP 服务器尝试高频登录，多次失败后登录成功，用以检测爆破结果，此规则可有效降低探针对于暴力破解的告警量

可以检测出攻击者利用 MSF（MetaSploit Framework）工具对此漏洞的扫描和利用行为

可以检测到 Webshell 上传告警后，如果马上出现同一源和目的 IP 的 Webshell 利用告警则可判定 Webshell 上传后被利用的行为

通过探针网络攻击日志和探针网页漏洞利用日志，检测在发生 Redis 敏感操作之后出现可疑下载行为的内部主机

通过探针网络攻击日志和探针网页漏洞利用日志，检测在发生 Redis 敏感操作之后出现可疑下载行为的内部主机

通过分析 DNS 流量数据中识别域名，并且能够区别疑似的 DGA 生成的域名以及相关的 IP 情况，能够给客户进行及时的预警。

- 动态预案编排

针对不同类型的业务提供对应的业务手段进行支撑。影响范围包括态势感知产品涉及所有流程业务。原流程类业务设计研发需整体从设计到研发实现至少需要 60 人天做需求设计以及研发测试工作。采用统一的设计框架后设计按照标准手段进行设计后使用编排引擎支持编排和流程的运行。用户可通过在界面拖拽节点机连线关系来完成流程编排，系统生成工作流引擎支持的标准工作流程定义文件，降低了工作流引擎使用的难度。通过阶段将流程划分为多个阶段，每个阶段内支持节点的并发、顺序、选择执行。

4 产品价值

经过近 6 年的研究与实践，奇安信将态势感知与协调指挥平台的核心能力，归纳为 7 ＋ 1 的能力体系，即：数据能力、技术能力、服务能力、安全能力、业务能力、呈现能力、交付能力，以及将以上能力进行有机整合的平台化能力。

- 数据能力

奇安信的数据能力，包括：多源异构数据积累、采集、治理、监测、存储、计算的综合能力。就数据源而言，包括：开源数据（如：云监测、云测绘、云防护、云端情报）、重点资产、单位信息、网络链路、暴露面、漏洞、重点单位流量、重点单位网络拓扑、城域网流量、政务云 / IDC 出口流量、供应链信息、本地情报、重保检查、渗透测试、等保测评、应急预案等数据源，以及集成第三方安全机构的数据源、通过共享平台交换的数据源。通过与安全中心合作，还可拓展到省口、国际口流量。

与此同时，奇安信还专门打造了星海平台、诺亚平台、玄机平台，来解决海量数据高性能采集、处理、计算，高效存储，数据资源高效组织的问题，为进一步的数据分析和深挖奠定基础。

- 技术能力

奇安信在态势感知与协调指挥平台中使用的技术能力，主要指各种安全引擎的能力，包括：流量探针、流式处理引擎、高性能关联分析引擎、离线批处理引擎、开放式的大数据智能建模平台（内置了多种深度学习框架、机器学习算法、异常发现模型）、高交互性的数据检索引擎、SOAR 引擎等，通过这些引擎，极大地提高了数据处理的自动化程度和性能，尽可能把存在规律的工作，让机器来处理，在此基础上，通过人机结合的方式，发挥人的专业能力和创造性。

- 服务能力

奇安信拥有 2000+人的安全服务团队，能提供从基础安全运营，到深度安全分析、追踪溯源、蜜罐诱捕、反制配合、深度综合报告、重大事件专项分析报告等综合安全服务。态势平台根据业务场景的需要，将其与数据能力、技术能力有机集成起来，形成体系化的安全能力输出，供态势平台的上层应用消费。

- 安全能力

平台通过整合数据、技术、服务三方面的能力，建立了一系列的安全能力，

如：网络空间深度测绘、资产画像、系统画像、漏洞监测、暴露面监测、威胁情报（机读威胁情报、高级威胁人读报告、威胁雷达、威胁判定支持、威胁分析武器库等）、骨干网的大规模网络威胁感知、告警监测、告警智能归并与关联分析、安全事件自动化和半自动化识别并将其与上层的业务应用相结合，为监管机构提供强大的安全能力支撑和业务支撑。

- 业务能力

业务能力方面，奇安信态势平台紧贴监管行业的业务需求，系统化梳理业务场景，以知行合一、平战结合、攻防兼备、智能开放为设计原则，将其实现为一系列的功能模块，并以通过动态预案的编排，对业务应用进行开放式管理，使其非常易于扩展，可以随着业务需要的变化，快速调整。

- 呈现能力

从大量的实战情况看，呈现能力，并不等同于可视化能力、或者说仅仅是漂亮的大屏，而是业务能力、数据能力、安全能力、服务能力、可视化能力综合在一起，形成的能力。也就是说，光有炫酷的大屏是远远不够的，更需要回答的问题是：在什么场景下，让什么人看到什么内容，并使其易于理解、使用和作出判断。特别是在高层领导指挥决策的场景下，呈现能力更加重要，也更具挑战性。奇安信经过长期摸索，已经形成以 3D 技术和地理信息图谱技术为支撑，以 C2 为框架的态势呈现体系，专门服务于高层领导指挥决策，使态势平台的价值易知、易懂、易用。

- 交付能力

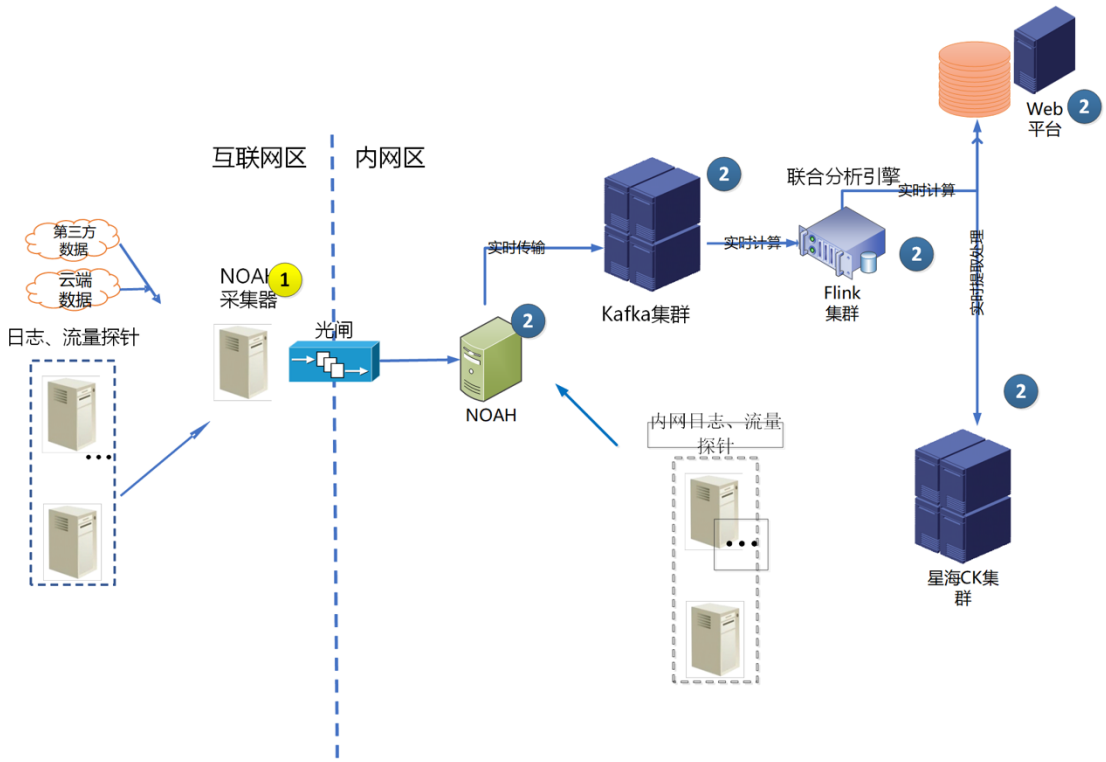
实践证明，态势感知与协调指挥平台的建设与运营，是一个复杂的系统工程，需要高度工程化的组织保障、流程制度、强有力的项目管理、强大的运营服务能力，才能保障系统建设和使用的成功。态势平台不仅仅是个 IT 系统，更是个 DT 系统，系统上线之日不是终点，而是起点。奇安信在此方面进行了大量实践，并总结了大量的经验教训，从而能够较好地完成工程交付和实战化运营工作。

- 平台化能力

以上 7 大能力，如果散碎地罗列在一起，将会非常难以管理，也很难协同一致，形成一盘棋。为此，奇安信以平台化思路，推出态势感知 3062 版本，将数据、技术、服务、安全能力进行整合，使其有机衔接起来，系统化地输出各种安

全能力，供上层应用使用。

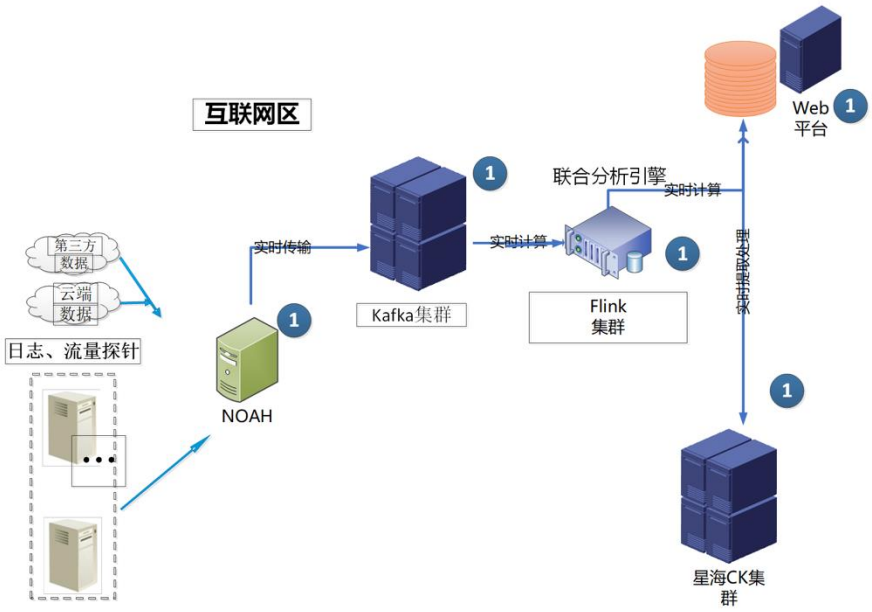
5 应用场景



应用场景 1：适用于内网应用场景、需要穿光闸的应用场景。

编号 1：外网侧，noah 采集器，需要单独占用 1 台机器。

编号 2：内网侧，编号 2 可以共用机器，以集群的方式提供服务。至少需要 3 台物理机组集群



应用场景 2：适用于互联网场景。

编号 1：内网侧，编号 1 可以共用机器，以集群的方式提供服务。至少需要 3 台物理机组集群

6 安装部署

1、该型号平台和采集设备，支持 X86 架构与 ARM 架构硬件服务器，平台为必选，采集设备可选。

2、该型号平台和采集设备，支持软件交付和软硬一体交付，软硬一体交付自带服务器。软件交付相关配置参考见下表。

3、该型号平台为集群方式安装，且支持集群模式安装。

4、采用推荐服务器配置时最少服务器台数为 3 台（高性能配置）。

5、采用最低服务器配置时最少服务器台数为 8 台（低性能配置）。

6、操作系统要求：Centos7.6 Minimal

7、操作系统根目录/所在分区的大小要求：大于 600G

平台推荐服务器配置：

CPU	Intel 4214 主频 2.20 GHz 内核数 12 缓存 16.5 MB L3 X 2（或 48 核或以上 CPU）
内存	256G
硬盘 1	960G SSD X 2 ，组 raid 1（用于安装系统用）
硬盘 2	4T SATA 机械磁盘 X 12，每个磁盘单独组 raid 0（数据盘）
RAID 卡	LSI 9361/3108 缓存 1G 或 2G （2 块磁盘 1 做 raid 1，磁盘 2 每个盘单独组 raid0）
网卡	万兆网卡

注意：数据盘容量可以不达到 4T，但是容量小对数据存储的时间范围有影响。数据盘的数量必须满足最少 4 块。

采集设备推荐配置：

CPU	Intel 4214 主频 2.20 GHz 内核数 12 缓存 16.5 MB L3 X 1（或 24 核或以上 CPU）
内存	64G
硬盘	4T 机械磁盘 X 1
网卡	千兆网卡