2022

泰合网络安全管理平台
白皮书

启明星辰泰合本部

v3.0.500.5.1.0

护航数字中国，领航信息安全

目 录

1 产品综述

1.1 产品简介

启明星辰推出泰合新版网络安全管理平台是立足于公司多年信息安全领域积累的基础上，同时融合当前大数据技术和 AI/机器学习技术，面向客户最新数字化业务需求，在国家相关法律法规及最新的网络安全等级保护标准上推出的网络安全管理平台。

泰合网络安全管理平台是一套以场景化为基础，以满足实战化为目的，以威胁为驱动手段，帮助用户建立监测预警、态势评估、响应处置的安全运营平台，定位为可支撑用户“攻防实战，协同指挥，智慧运营”的平台，在传统的“监测，审计，运维，管理”维度上强化“威胁可视、智能响应”，提供集成的预测、阻止、检测和响应能力。

新版泰合网络安全管理平台进行了 2 个维度的升级：平台能力升级大幅提升平台数据采集与处理能力，业务能力升级全面匹配攻防实战的使用场景，智能驱动安全运营。

平台能力升级：采用统一的 THDK 开发框架进行开发，融合业界主流的大数据技术，采用 THBD 数据库，结合 SQL、NewSQL 和 NoSQL 技术，实现对多元、异构、海量安全数据的高效采集检索、可靠存储和负责计算。通过构建 THStore 体系，减少模块的耦合，形成高内聚，低耦合的货架式功能 APP，从底层技术架构层面解决海量资产，数据分权分域，以及高性能日志处理问题。

业务能力升级：提供智能化关联分析、自动化或半自动化编排技术、基于机器学习的行为分析，流安全分析技术，内建主动安全管理机制，通过主动的漏洞扫描和安全配置核查，及时发现业务系统隐患，并进行事前预警；结合内外部情报，提供更加准确和及时的安全分析。同时引入攻击链模型和 ATT&CK 模型分析从侦查、渗透、攻陷、控制、破坏一整套攻击流程进行事中监测，威胁定位；利用流量日志融合，提供更多攻击上下文信息，在调查和攻击溯源方面进行事后取证，案例总结。同时提供宏观视角，中观视角，微观视角为不同角色的用户提供

直观的、多维度的可视化呈现。帮助用户掌控实时安全态势，动态感知隐患与威胁，为安全分析师和决策层提供强有力的支撑。

技术上，系统采用新一代分布式计算技术架构和具有自主知识产权的非关系型数据库(NoSQL/NewSQL)技术——THDB，具有分布式、全文索引、水平弹性扩展、实时格式化数据搜索和原始数据关键字全文搜索、高可靠性等特点，同时系统采用开放平台架构设计，遵循业界通行的应用接口和管理接口，功能部件都实现了模块化装配，客户可以自由选择，并能够与客户的应用和管理环境实现良好的对接与整合。

随着指数级的数据涌入、高度持续且不断增长的攻击数量、永无止境的人才短缺以及不断增加的攻击危害度，企业通过平台构建一个新的安全运营模型，这个模型可以帮助安全运营摆脱僵化、集中的孤岛，专注于安全闭环结果，安全运营活动可以随着人员、流程和技术的演变而自然调整适应，实现自动化的运营状态。自动化的安全运营是理念、实践和工具的组合，可通过高度适应、敏捷、自动化的威胁管理方法提高组织抵御安全挑战的能力。安全运营的自动化不再是那种满屋子人观看有精美仪表板的屏幕，而是威胁检测与响应团队、安全分析团队与跨地区跨组织的职能团队的整合、自动化操作的融合。

1.1.1 网络安全管理平台总体实现思路

网络安全管理平台的建设是一个全面信息收集、融合处理感知安全状态及风险并进行态势可视化呈现的过程，该过程是动态持续的，通过连续的信息采集分析不断更新对目标网络安全态势的认知理解，掌握安全状态、了解发展规律、进行提前预警。为更好地支撑和赋能典型的安全业务场景，对于 HW 场景，平台需要具备攻防实战的能力，对于日常运营，平台需要具备智慧运营的能力，对于监管场景，平台需要具备协同指挥的能力。

基于以上场景的平台建设目标：支持安全决策者“看清全局风险、监管指挥”，又能辅助安全防护人员“防住高危威胁、威胁狩猎”，还能协助安全运维人员“补全重点漏洞、自动响应”。以场景化为基础，以满足实战化为目的，以威胁为驱动手段，帮助用户建立监测预警、态势评估、响应处置的多级安全运营平台。

泰合网络安全管理平台是构建在现有的安全防护设施之上的平台，可以兼容整合用户网络中现有的或待建设的各类安全设备、安全子系统或任何安全数据信息源，如漏扫、核查、4A、堡垒机、vpn、网站监测等中特定类型告警，防护类设备 FW、 WAF、 APT、 EDR 、IDPS、 抗 D、 防病毒等设备攻击告警，路由器交换机等网络设备的性能数据，服务器、业务系统、数据库、中间件的日志等。基于任意安全设备及数据源的对接，网络安全管理平台通过安全数据的融合分析及呈现实现态势感知能力，包括态势信息的集中采集获取、海量安全态势信息的大数据存储、面向态势感知的大数据集中分析以及态势感知的可视化呈现。

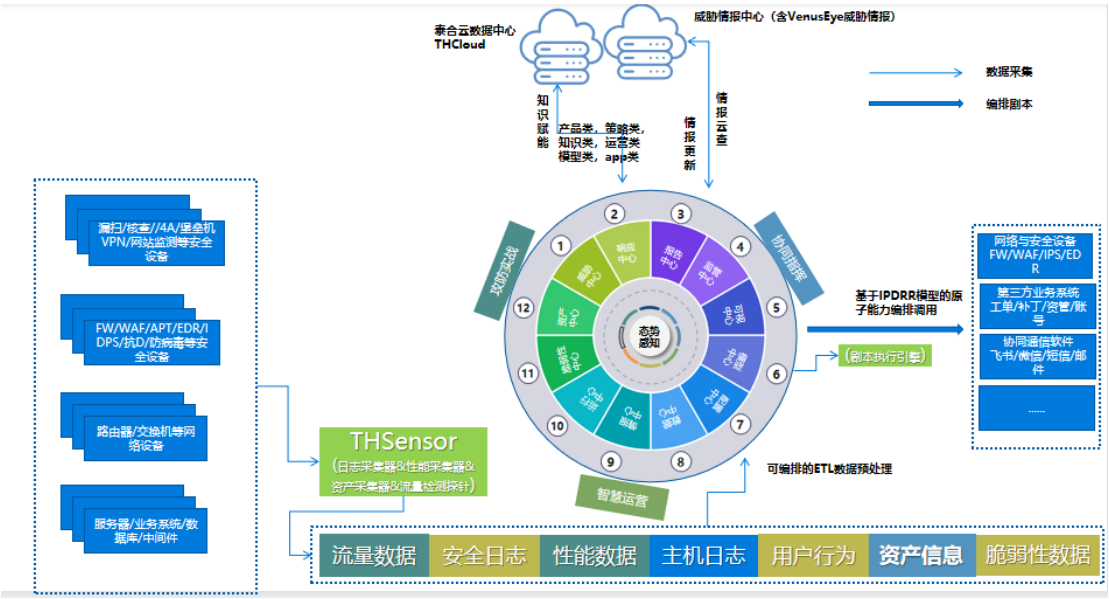

图 网络安全管理平台构成

因此网络安全管理平台要处理的是海量多维的信息，要进行多方位的关联及发掘分析，要呈现的也是多对象、多维度、多视角的安全分析与态势呈现。鉴于此，启明星辰泰合网络安全管理平台根据业务需求，平台通过对被防护资产进行安全事件研判、态势监测、自动化或半自动化编排响应形成动态的防护、精准检测、联动响应机制；平台通过内置的多分析引擎对可能影响安全的多要素进行分析：安全相关要素信息包括资产信息、运行信息、脆弱性信息、安全日志、流量信息、威胁情报、用户行为信息。安全分析引擎包括资产发现（资产发现引擎），脆弱性识别（脆弱性评估引擎），运行监控（设备监控引擎）、攻击过程溯源取证、影响分析（关联分析引擎）、攻击预测（预测引擎），风险评估（风险分析

引擎），场景分析（UEBA 引擎、AI 引擎），告警响应（SOAR 引擎），预警通告（工作流引擎），态势可视（可视化引擎）等。平台将安全态势涉及的各类安全要素和监视角度进行了梳理归纳，形成了多个维度组合构成的态势可视化：分别是资产态势、攻击态势、运行感知、脆弱性态势、风险态势、威胁态势、流量态势、网站态势以及面向综合态势监视的态势总览。

通过多个维度的感知，泰合网络安全管理平台可以为用户呈现出一幅较为通用和完整的网络安全分析与态势感知的全景图。并且在多维度的专项分析呈现和扩展外延中，用户可以聚焦整合、按需搭配，形成适合自身业务需要和安全态势监控需要的网络安全管理平台。

1.1.2 遵从态势感知经典模型与网络安全态势感知国标

网络态势感知的经典定义为：在大规模系统环境中，对能够引起系统状态发生变化的安全要素进行获取、理解、显示以及预测未来的发展趋势。

通过该定义，我们得出一个经典的态势感知应该由“态势要素获取”、“态势理解”、“态势预测”三级模型来组成。它通过态势要素获取，获得必要的数据，然后通过数据分析进行态势观察理解，进而实现对未来短期时间内的态势预测。

《网络安全态势感知通用技术要求》国标草案中网络安全态势感知定义为：通过采集网络流量、资产信息、日志、漏洞信息、用户行为、威胁信息等数据，分析网络行为及用户行为等因素构成的整个网络当前安全状态和变化趋势，获取、理解、回溯、显示能够引起网络态势变化的安全要素，预测网络安全态势发展趋势。

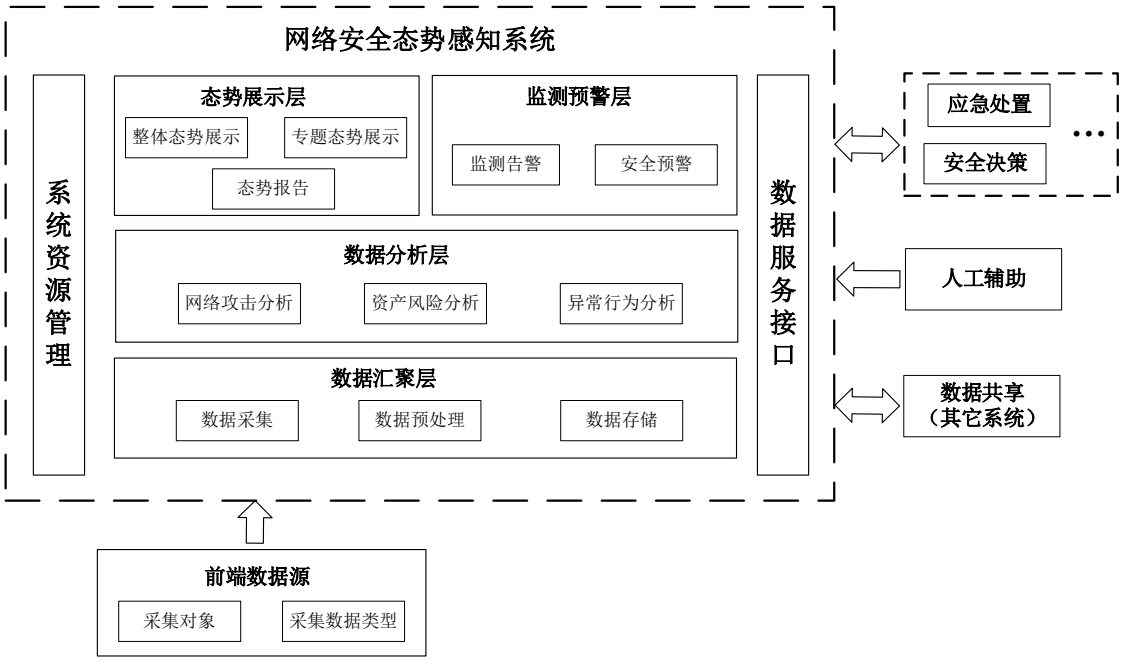

图 国标草案网络安全态势感知总体框架

如上，在国标定义中，网络安全态势感知系统主要划分为数据汇聚层、数据分析层、态势展示层和监测预警层。从前端数据源（如网络设备、安全设备等）采集数据，实现网络安全状态和趋势的分析。

启明星辰泰合网络安全管理平台是建立在大数据信息处理架构下的安全信息收集、分析与呈现的感知系统。该系统由四层架构组成，分别是安全要素采集层、安全大数据存储层、安全态势分析层和态势感知及展现层，该四层架实际上也对应了态势感知经典的三级模型：安全要素采集和安全大数据存储实现了第一级：态势要素获取，安全态势分析实现了第二级：态势理解，态势感知及展现体现了第三级：态势预测。因此启明星辰泰合网络安全管理平台具备了良好的架构基础，覆盖了实现安全管理与态势感知的各主要环节，为企业实现安全管理与态势呈现提供了有力的系统平台支撑。

1.2 系统结构

系统结构从总体上划分为五个部分，分别是：信息采集（Collection）、信息分析（Analysis）、安全处置（Action）、用户呈现视图（Presentation）与系统支撑（Supporting）。

信息采集：实现了对客户 IT 资源的资产信息、性能信息、日志与安全事件信息、流信息、脆弱性信息（配置安全信息、漏洞信息以及弱口令）、威胁信息、用户行为信息等安全要素信息的采集。

信息分析：针对采集上来的各类安全要素信息，系统实现了资产梳理、性能与可用性分析、配置符合性分析、威胁监测、流行为分析、安全与合规管理、脆弱性分析、风险发现和多维度宏观态势的计算与分析。其中，风险分析包括了资产价值分析、弱点分析、威胁分析、风险评估、影响性分析等。

安全处置：包括例行处置、例外处置以及自动化编排响应等安全事件闭环机制。例行处置主要以计划任务工单的形式体现；例外处置主要通过响应管理和告警工单处理的形式体现。自动化编排响应以多应用管理以及剧本编排的形式体现；此外，还包括了安全预警管理功能。

用户呈现视图：系统为不同层级、不同角色的用户提供了中心化的用户视图，从资产中心、脆弱性中心、运行中心、数据中心、威胁中心、响应中心、情报中心、态势中心、模型中心、报告中心等维度进行展示。用户亦能依据自身的工作需求自定义展现视图。

系统支撑：包括系统自身管理、权限管理、级联管理、知识管理、接口管理以及全局安全信息库。

1.3 系统功能组成

网络安全管理平台的功能架构由安全要素采集层、安全大数据存储层、安全模型层和场景化分析层四个层面组成，在各层中分别实现对应的系统功能。

图 网络安全管理平台功能架构图

- 安全要素采集层：提供开放式的信息采集接口，实现对用户环境内各类 IT 资产以及所采用的各厂商安全产品或安全系统进行统一的信息采集，并提供非结构化数据采集接口，可采集各类情境数据和威胁情报。
- 安全大数据存储层：实现海量安全大数据的分布式存储，提供结构化数据和非结构化数据的存储能力，并为上层的数据分析应用提供高效的数据库功能支撑；
- 安全模型层：平台综合数据处理分析的能力提供层，提供由大数据技术和架构支撑的快速检索和数据关联发掘功能。是支撑上层数据呈现和分析结果输出的计算引擎层，提供丰富的大数据统计、关联分析、数据挖掘以及态势分析能力，是系统的分析处理的核心。该层提供了基础数据处理引擎，包括流式计算引擎、复杂事件处理引擎、全文检索引擎、关联分析引擎等。基于这些计算引擎实现分析能力包括威胁目标分析、威胁源分析、攻击过程分析、影响及危害程度分析以及风险分析等。
- 场景分析层：通过下层所提供的数据采集和处理能力向用户输出场景化分析能力，包括资产中心，脆弱性中心，数据中心，威胁中心，响应中

心，运行中心，情报中心，监管中心，报告中心及安全态势总揽，服务于全网的安全态势呈现，支撑用户全局的安全防护工作。

- 外部系统：平台通过级联或 DaaS 接口可以实现平台能力的扩展以及平台能力的延伸。

1.4 产品组成部件

泰合网络安全网络安全管理平台由多个部分构成，包括网络安全管理平台、日志采集器、日志代理、性能采集器、配置核查代理、流量检测探针、AI 安全传感器和分布式数据存储索引与计算节点 9 个部件。用户通过浏览器登录网络安全管理平台即可进行各种操作。

- 网络安全管理平台

网络安全管理平台是系统的核心部件，实现了对 IT 系统集中化的性能及可用性监控、安全事件的集中管理和分析、安全风险的评估、宏观安全态势感知，以及自动化的安全响应与处理。客户通过网络浏览器即可登录网络安全管理平台，进行各种操作。

网络安全管理平台内置日志采集和性能采集功能，客户无需另行安装其它任何部件即可直接收集管理对象的日志信息和性能信息。网络安全管理平台也可以汇聚来自日志采集器、日志代理、性能采集器和流量检测探针的多源异构信息。

- 流量检测探针（**必选**）

流量检测探针（采用旁路部署方式，采集用户网络交换设备的镜像流量。在不同的环境下，NBA-CSP 实现多种解决方案。根据检测的需要，可以快速、灵活部署在网络核心、网络边界、分支机构等不同的位置。检测探针将威胁事件和元数据等信息外发至平台，做统一汇总以及二次分析展示，同时传输过程可加密处理，确保数据传输安全。网络安全管理平台可以对网络中分散的流量检测探针进行集中管理。

- **分布式日志采集器 （可选）**

日志采集器可以安装并独立运行在一台服务器上，实现对异构管理对象的日志采集，功能同网络安全管理平台的日志采集模块，用以辅助网络安全管理平台

解决日志种类繁多或管理中心与采集数据网络不直达的情况，并可以实现分布式日志采集能力。

日志采集器收集的日志可以转发给网络安全管理平台。网络安全管理平台可以对网络中分散的日志采集器进行集中管理。

- **日志代理（可选）**

日志代理用于安装并运行在管理对象上，实现对管理对象的日志采集和转发。

日志代理收集的日志可以转发给日志采集器，或者直接转发给网络安全管理平台。网络安全管理平台可以对网络中分散的日志代理进行集中管理。

- **性能采集器（可选）**

性能采集器可以安装并独立运行在一台服务器上，实现对异构管理对象的性能信息采集，包括可用性信息、运行状态信息、性能信息等，功能同网络安全管理平台的性能采集模块，用以辅助网络安全管理平台解决分布式性能数据采集的问题。

性能采集器收集的数据可以转发给网络安全管理平台。网络安全管理平台可以对网络中分散的性能采集器进行集中管理。

- **AI 安全传感器（可选）**

AI 安全传感器的威胁检测结果可以转发给网络安全管理平台。网络安全管理平台可以对网络中分散的 AI 安全传感器进行集中管理，下发 AI 分析模型。

- **分布式存储和计算节点（可选）**

CDN 节点安装并运行在独立的服务器上，分担管理中心解析、范化、入库压力。网络安全管理平台可以对网络中分散的分布式存储和计算节点进行集中管理。

添加 CDN 节点后，节点中存储组件与管理中心的存储组件组成分布式集群，实现了读写分题，提高了写入和查询速率。

2 部署方式

产品部署对于客户网络的要求比较简单，只要系统的网络安全管理平台与管理对象之间网络可达即可。

系统具备极强的伸缩性，能够通过水平弹性扩展的部署方式适应各种用户的网络环境，以及各种管理的规模。

2.1 单级部署

单级部署是指仅部署一个网络安全管理平台的模式。此时，在网络中就部署一个网络安全管理平台部件，所有的用户都登录到该网络安全管理平台进行访问，通过系统权限设置来区分不同的管理职责。

在单级部署模式下，又分为单机部署、采集器分布式部署和存储索引与计算节点集群部署。

2.1.1 单机部署

单级单机部署是最简洁的系统部署模式，也是最典型的部署模式，适用于大部分网络环境。

在单机部署场景中，用户仅需在一台服务器上部署网络安全管理平台部件。此时，网络安全管理平台可以直接采集管理对象的日志、性能和配置信息。系统使用者通过浏览器登录网络安全管理平台的 WEB 站点即可依照相关的权限进行各种管理操作。

2.1.2 采集器分布式部署

采集器分布式部署是指将日志、性能或配置信息采集功能分别采用分布式采集器部件进行部署的模式。通常，用户如果遇到如下几种情况时，需要考虑采集器分布式部署：

1. 需要进行管理的节点规模较大，且分散在物理网络中的多个位置。

此时，大量的性能、日志和配置数据透过网络汇总到网络安全管理平台，会给网络带宽造成一定的影响。通过在被管理节点处就近部署分布式的性能采集器、日志采集器，将信息就近送给这些采集器，采集器获取数据后通过压缩加密方式传输给网络安全管理平台，降低网络负载。分布式日志采集器还支持归并、

过滤和定时上传日志功能，有助于进一步降低网络带宽的占用。通过这种部署方式，将一部分信息预处理的工作压力分散到了分布式采集器上，也能提升网络安全管理平台的信息处理吞吐量。

2.有的被管理节点与网络安全管理平台不在同一个逻辑网络中，例如之间有安全网关、防火墙、网闸隔离，或者有 NAT 地址转换。

由于被管理节点与网络安全管理平台之间网络不通，可以通过部署分布式采集器节点进行信息中继。此时，分布式采集器节点必须具备跨两个网络的能力。

3.有的被管理节点与网络安全管理平台所在网络是跨广域网连接的，且广域网接入的带宽容量有限。

此时，被管理节点虽然与网络安全管理平台之间是网络可达的，但由于广域网带宽容量有限。为了降低对广域网带宽的占用，可以在远端部署分布式采集器，然后由分布式采集器将压缩后的数据透过广域网传递给网络安全管理平台，降低广域网带宽负载。

2.1.3 存储与计算节点集群部署

分布式存储和计算节点（后简称 CDN 节点)用于日志处理规模大及高可靠数据存储的需求场景。随着日志规模的扩大，集中的网络安全管理平台无法满足数据存储和分析需求时，可通过增加 CDN 节点进行水平扩展，CDN 节点可支持弹性扩展，节点数量灵活方便，可根据数据规模灵活增减，并提供数据冗余存储，可根据数据可靠性需求，在不同的节点保存数据的多份备份，配置灵活简单。

2.2 多级部署

多级部署是指部署多个网络安全管理平台，并构建起一个总部平台连接若干个分中心平台的部署模式。此时，在网络中就部署了多个网络安全管理平台部件，各个分中心平台的管理员通过浏览器登录各自的分中心平台对所辖网络进行安全管理和态势呈现，总部平台的管理员则通过浏览器登录总部网络安全管理平台进行全网的统一管理、集中态势展现，并可以监督各个分中心平台的管理工作。

该模式适用于对于具有分支机构或者垂直管理下属机构的企事业单位，以适应用户多级管理的体制。系统通过上下级节点的注册来实现级联，下级平台可向上级平台上报风险数据、告警数据、运行状态数据、报表文件数据。

3 产品特点

3.1 面向场景化、实战化、运营化的构建思路

启明星辰泰合网络安全管理平台通过对接网络中现有或未来可能扩容的各类安全防护系统引擎，实现了全面且灵活开放的态势感知系统架构。在这种体系下，任何类型任何厂商的安全设备或系统都可以作为用户网络或业务上各环节的安全监测传感器，这些传感器所产生的安全监测信息都将作为数据源由网络安全管理平台统一获取，这样不但平台可以尽可能全面的采集安全要求信息，同时也可以最大限度的利用用户网络中已有的安全监测防护手段，保护用户已有投资，实现资源优势整合。

现有安全资源的引擎化整合是全面获取安全要素信息的基础，在此基础上，平台通过资产感知、攻击感知、运行感知、脆弱性感知、风险感知、威胁感知和态势总揽这些维度来覆盖安全态势各个方面并用来实现全方位的态势感知。

基于泰合网络安全管理平台进行全方位态势感知的实现流程大致包括 3 个关键步骤，分别是各类安全要素信息的获取、面向实战和场景化的威胁分析、自动化运营。

3.1.1 多安全场景下多安全要素信息的获取

网络安全管理平台通过对接网络中的各类安全设备、子系统、安全数据源来获取影响网络环境安全态势的各类安全要素信息，这其中包括有系统日志类、攻击类告警、对象弱点类信息、系统运行类信息、网络流量类、资产信息类信息以及外部威胁情报信息。

启明星辰网络安全管理平台为开放型的平台架构，任何安全设备或子系统都可作为安全监视的数据源或引擎，通过平台丰富和高兼容度的信息采集接口实现

安全数据的广泛采集，不限安全设备的厂商或型号，最终都将整合到平台的统一安全要素信息分析展现体系中，形成完整全面的一站式态势感知能力。

系统安全要素采集层的下方是组织网络中各类各厂商的安全设备和系统，以及大量要被防护监控的 IT 资产。这些设备和资产所能产生的海量安全监控数据和运行日志，包括外部的威胁情报信息都将通过泰合网络安全管理平台开放的各类信息采集接口进行采集汇总。这实现了网络安全管理平台-态势感知中对可能影响安全态势要素信息获取的重要环节，即合理的整合了环境中已有或将建设的各类安全防护资源形成安全信息源，这也是完整的全方位态势感知系统的实现基础。

3.1.1.1 支持多种监控对象

系统支持对大部分主流 IT 软硬件资产的监控，部分监控对象如下表所示：

设备类型	厂商或产品
交换机	所有支持 SNMP 协议（包括 V3）的交换机，例如 Cisco、Extreme、Juniper、博科、华为、H3C、神州数码、锐捷等
路由器	所有支持 SNMP 协议的路由器，例如 Cisco、Extreme、Juniper、华为、H3C、神州数码、锐捷等
防火墙/UTM/USG	启明星辰、网御星云，以及支持 SNMP 协议的安全网关类设备，例如 Cisco、Juniper Netscreen、飞塔、Checkpoint、Nokia、天融信、东软、网御神州、H3C、迪普、山石等
VPN	只要支持 SNMP 协议即可，例如启明星辰、网御星云、天融信
网闸	只要支持 SNMP 协议即可，例如网御星云
IDS/IPS/IDP	只要支持 SNMP 协议即可，例如启明星辰、网御星云
Anti-DDoS	只要支持 SNMP 协议即可，例如启明星辰、网御星云、绿盟
WAF	只要支持 SNMP 协议即可，例如启明星辰、网御星云
服务器	IBM AIX 、HP-UX 、Microsoft Windows、SUN Solaris、Linux

	等
虚拟化系统	VMware
数据库	Oracle、SQL Server、DB2、MySQL、Informix、Sybase 等
中间件	Weblogic、WebShpere、JBoss、Apache、Tomcat、Domino
存储系统	HP、IBM、VERITA
应用服务	SMTP、POP3、HTTP、FTP、TELNET、SSH、SSH2、DNS、DHCP、WINS、LDAP、URL
其它	只要支持 SNMP 协议（包括 V3）即可

数据采集模块负责采集获取网内被监护资产对象以及作为监测管控引擎的安全设备所产生的各类安全信息。

数据采集模块实现了系统数据采集的开放性，其提供了丰富的数据对接接口，除了可采集各类设备或安全子系统上报的异构事件日志外，还可并行实现对结构化以及非结构化海量安全信息的采集。其中结构化数据由一系列标准日志及结构化信息的采集服务接口实现对接，包括但不限于 Syslog、SNMP Trap、WMI 等，可采集的安全要素信息包括安全事件、运行日志以及性能数据等信息。非结构化数据由一系列文档或文件采集 API 组成，可采集脆弱性结果、WEB/XML/文本等信息以及各类情报数据。

3.1.1.2 高适应性日志采集

系统综合采用多种技术手段，充分适应用户实际网络环境的运行情况，采集用户网络中分散在各个位置的各种厂商、各种类型的海量日志。系统内置了对业界大部分常见厂商和设备类型的日志支持，对于目前暂不支持的管理对象，系统还提供了方便灵活的扩展机制。只要获得管理对象的日志样本以及通讯协议方式，编写一份 XML 格式日志解析文件，导入系统，即可获得对该管理对象的日志采集能力，无需编码。

为了最大程度地采集各种厂商、各种类型的日志信息，系统没有强求管理对象必须具备什么日志协议，而是支持通过多种协议方式采集日志。这些协议包括

并不仅限于：Syslog、SNMP Trap、FTP、OPSEC LEA、NETBIOS、ODBC、WMI、Shell 脚本、VIP、Web Service 等等。

系统自带日志采集功能，同时也支持在用户网络中分布式部署多个日志采集器，就近采集管理对象的日志信息，并进行日志的范式化、分类、过滤和归并，然后汇聚到管理中心，从而实现对分散管理对象的日志采集，并有效降低网络中日志流的带宽占用。

3.1.1.3 业界领先检测引擎和流采集技术

流检测引擎具备高性能、高安全性、高可靠性、高稳定性、高易用性、高有效性六大特性，内置业界领先的检测引擎和流采集引擎，同时具备深度包解析，双向检测，全流量分析，流行为学习模型等多项功能，满足安全场景下的入侵分析。凭借多年来基于威胁检测技术领域领先的研究成果与技术积累，在原有病毒、木马、蠕虫、僵尸网络、缓冲区溢出攻击、拒绝服务攻击、扫描探测、欺骗劫持、SQL 注入、XSS 攻击、漏洞利用、暴力破解、非授权访问、挂马攻击等威胁检测技术的基础上，加入了业界领先的全流量双向检测技术，有效提升了检测能力。同时，规则检测引擎完美兼容 snort 规则，支持子写、开源、商用 snort 规则的导入使用，同时兼容 LUA 脚本，通过脚本高级分析功能可检测规则集中无法检测的内容；探针内置 1+1 病毒监测引擎，通过病毒检测引擎结合深度解析还原算法对被检测文件的内容进行检测，支持文件片段的检测还原、多协议文件的检测还原、深度解析还原算法对多层加壳压缩文件进行检测防止恶意文件绕过行为，对病毒文件进行深度检测的同时进行完整还原提供文件下载功能从而支持进一步研判；通过对全流量建立全量 FLOW 表，利用标签标记会话，通过自主可控算法对历史应流量进行分析学习，多维度对比流行为，发现敏感访问行为；

检测探针通过智能协议分析和基于流量特征的识别等关键技术，对流量数据进行高效、完整、准确的协议类型识别和解析，系统支持常规协议、5G 协议、物联网协议、工控协议的深度解析。系统支持 SSL/TLS 加密流量卸载以及加密流量的安全监测，防止了客户安全盲区。为提升平台的追踪溯源能力，探针具备威胁事件的数据包存储和转发功能，加快了安全事件的响应，提供了取证的证据。

探针覆盖百、千、万的高性能硬件处理平台，具有业界领先的高性能架构、高绩精准的入侵检测能力、强大的会话跟踪和流重组、IP 分片重组能力、全流量分析和取证能力、高度灵活的规则自定义能力、丰富的元数据外发字段（350+），为网络安全管理平台的攻防实战、安全运营场景提供准确的告警数据以及详实的上下文信息。

3.1.1.4 脆弱性数据采集

弱点信息采集：系统能够通过远程评估产品收集整个网络的弱点情况并进行统一管理，对收集的信息进行统一的范式化处理后，对脆弱性信息提供查询和展现功能，使得管理人员可以清楚的掌握全网的脆弱性。

3.1.1.5 威胁情报数据采集

情报数据采集：提供开源情报采集能力，集成第三方威胁情报服务商数据接口，通过导入或者主动自动抓取的方式获取外部相关威胁情报信息，可将通过平台发现的威胁转换为内生情报。

3.1.1.6 资产数据采集

资产信息采集：它通过主动发现、导入或创建的方式来识别和梳理目标网络中要被防护的资产及业务对象，发现方式包括 agent 代理，配置核查结果识别，资产采集器，漏扫结果识别，手动添加，日志或事件中获取。

3.1.2 面向实战和场景化的威胁分析

在汇集了海量多方位安全要素信息的基础上，网络安全管理平台将综合这些数据，面向总体安全态势的认知和监测进行数据的融合、关联分析和发掘分析。这其中包括对资产及业务对象收到攻击威胁和自身风险程度的分析、复杂攻击的攻击过程及攻击目标分析、攻击的危害及影响范围分析、攻击威胁溯源分析、外部威胁情报与内部安全信息比对分析等。这些分析处理工作将为上层态势呈现提供数据和计算任务的支撑。

美国洛克西德·马丁公司于 2011 年提出攻击链模型，指网络空间攻击行为分为七个步骤。包括侦查探测（Reconnaissance）、制作攻击工具

（Weaponization）、将工具投送到目标（Delivery）、释放代码（Exploitation）、成功安装并控制（Installation）、主动外联（Command &control）、远程控制及扩散（Actions onObjectives）。

1 侦查探测：也叫踩点，攻击者通过社交网络，社会工程学等方法了解目标组织的防御措施，IT 架构以及人员信息。

2 制作攻击工具：基于侦测结果，购买或者编写针对攻击目标现存漏洞的恶意代码，为绕过目标防御进行逃避测试。

3 传递到目标：也叫投放，通过钓鱼网站，邮件等方式发起攻击，诱导用户点击，下载恶意代码

4 释放代码：也叫漏洞利用，恶意代码被成功植入失陷主机，并利用漏洞获取主机更高的执行权限

5 安装成功：也叫下载植入，利用恶意代码和高的执行权限，控制失陷主机下载功能更丰富的恶意软件，并安装与启动

6 主控外联控制端：也叫 C&C 命令控制，失陷与控制服务器建立远程连接，并接收控制指令

7 远程控制及扩散：攻击者控制失陷主机发起进一步的恶意行为，如扫描内网其他主机的漏洞，入侵新目标，窃取有价值数据并外传等等。

在攻击链模型中，七个环节为防御方提供了一个防护机会：在第一环节中发现有刺探行为，可以加强防御，在边界防护策略或主机安全上加固，将攻击者挡在第一道防护线外，在第三、四、五环节发现攻击，可以防止造成更大的损失。在第六环节中，发现控制通道，可以斩除失陷主机和远程控制的连接。在最后一个环节，可以防止威胁的进一步扩散，同时在已造成损失时，也能明确损失程度。

网络安全管理平台按照防御方情况将平台中的攻击链分析按同样将将攻击分为如上七个阶段，通过在告警分析中对特定阶段的攻击事件数量分布情况，向用户提供可供参考的分析数据。对全网业务资产被攻击情况进行全程监控呈现；掌控实时攻击进程趋势，进行及时有效的响应处置；记录攻击上下文信息，保存

证据，同时了解攻击者的攻击规律，攻击手法，攻击意图，为后续的防御、诱捕、反制提供理论支撑。

3.1.3 高度自动化响应的智能运营

泰合网络安全管理平台通过态势分析以及态势呈现所发现的安全问题及相关预警可通过平台内置的运维支撑模块进行事前预警和事中工单处置。对于任何的告警、预警或安全事件的发生，网络安全管理平台都支持通过工单流处理的方式，将安全问题放在定义好的处置流程中，由指定的人员和规范的步骤来操作。每类告警、预警或安全问题都可以设定对应的处理流程，工单流程自动处置流转，直至问题的解决。通过工单系统，有助于协助用户利用标准化、流程化、自动化的方式来处理安全问题。

网络安全管理平台内置有响应中心模块，平台中使用安全编排与自动化响应（SOAR）技术，通过数字化的工作流定义事件分析和响应过程，安全运营人员可根据标准化的事件响应流程，实现自动化的进行事件分析和优先级排序，帮助企业和组织在面临威胁时提供预测、防御、检测和响应能力。

3.2 数据平台与智能平台双驱动，构建安全能力中台

3.2.1 多安全能力中台成为高效安全运营的基石

传统的安全建设方式导致安全设备烟囱化泛滥，安全团队需要面对十多个安全厂商的几十甚至上百款安全设备。这些设备使用界面都不一样，里面的资产信息、人员信息大多数时候没有同步，导致管理与运营效率低下。这些安全设备统一管理无法开展、安全策略的统一管理无法开展，想要完成安全管理与运营的闭环，还缺少一个关键点，也就是安全能力中台。

随着全面在线化、广泛的远程办公场景、在线会议等，安全运营还要与 IT 运营、内控、人力资源等完成更紧密的协作与融合，安全管理与运营需要进行跨职能部门的资源协调，需要能整合企业内各应用系统，支持与保障企业的数字化战略。随着安全管理与运营的成熟，以及网络安全的常态实战化，**安全建设理念正朝着一体化安全迈进**。同时，由于网络信息安全的基础性和泛在性，任何一个组织都无法独立应对网络安全威胁，必然需要政企、行业、国家多层面的协调联动。**这种多层次的协调联动，必然产生安全能力标准化和互操作的要求**。综上内外多个因素，**安全能力中台将成为企业网络安全的核心枢纽，以资源化、能力化、服务化、标准化的方式，打通组织内外和职能边界，让安全“四通八达”**。

要想实现高质量的安全编排、自动化和响应(SOAR)，首先要打通组织内外的安全经脉；安全能力中台就是企业的网安枢纽，打通了任督二脉，安全建设才能跳出堆叠的泥沼，实现一体化的飞跃。

打破原有安全系统“烟囱式”架构，融聚安全共性能力下沉至中台，个性化功能作为应用插接在中台之上，轻量化按需部署，对共性安全能力统一编排调用，实现便捷、高效、随选的安全能力提供与扩展。

安全能力中台具体应该包括以下内容：

- 为安全能力的实现统一标准。我们需要制定某种标准，让安全能力以某种约定形式进行封装，就像标准服务一样。

- 异构集成，满足安全能力无缝对接。异构集成是安全中台的核心能力之一，也是降低创新成本的关键。异构集成能够快速融合新安全能力，提高兼容性。分别实现安全能力的快速集成和前台应用的快速调用。
- 提供安全流程及规范化能力。企业内部很多工作，例如开发、运维、数据管理等需要协调多个安全功能，完成一系列流程。如何让这些业务很好的协同工作，也需要一个标准的流程。

THBridge 应用集成的目的在于通过半标准化的方法提供统一的应用集成，从而对上提供标准化接口，对下进行非标准化对接，以此支持面向异构接口的联动协同互操作能力。**THBridge 是实现安全能力中台的重要底座。**

数据即服务（Data-as-a-Service，DaaS）是指与数据相关的任何服务都能够发生在一个集中化的位置，如聚合、数据质量管理、数据清洗等，然后再将数据提供给不同的系统和用户，而无需再考虑这些数据来自于哪些数据源。

企业 DaaS 策略以及基础架构成为 CIO 和业务部门最为关注的话题之一，这体现在：企业数据仓库(EDW)越来越倾向于 DaaS 策略结构化与非结构化数据增长促使了 DaaS 的发展应用孤岛中的数据越来越集中化管理，DaaS 基础架构就变得更加重要。要做企业级的数据分析就必须先推行 DaaS 策略。DaaS 解决方案的优势：

- ✓ 敏捷性：通过数据访问的整合，客户能够更加快速地对其进行移动，而无需再去考虑底层数据的来源。如果客户需要稍微不同的数据结构或者调用特定位置的数据，DaaS 通过最小程度的变更能够非常快速满足需求
- ✓ 成本效益：服务提供者找数据专家来建好底层架构，表现层可以外包给别人(报表和仪表盘用户界面等)，同时使得任何变更需求都能更灵活的满足
- ✓ 数据质量：通过服务来控制数据的访问，这对数据质量改进非常有帮助，因为更新点只有一个。当服务彻底测试之后，如果下一次部署不发生变化，那么他们只需要进行回归测试就好了。

- ✓ 效率、高可用和弹性：这些优势来自于虚拟化，物理服务器资源共享将提升效率，跨多个物理服务器的集群可以提高可用性，动态调整和实时迁移集群节点到不同的物理服务器能够增强弹性

DaaS 技术方案尤其适合安全数据中台的建设需求。近两年，包括政府、金融、运营商、交通、能源等多个行业主管部门已经意识到，打通行业内部各个孤立的态势感知平台，通过数据上报、情报下发形成行业合力，发挥行业主管部门的协调指挥作用已经成为不可逆的趋势，通过网络安全管理平台的 DAAS 接口来快速支撑上下级联的行业级态势感知平台体系建设。

3.2.2 支撑安全大数据业务的数据支撑平台 THBD

安全大数据存储层实现对所采集海量数据信息的预处理和存储，该层提供了结构化数据和非结构化数据的数据库处理能力，在数据库架构上采用当前主流的分布式大数据存储架构，并经过面向安全大数据分析过程的优化改造，采用自研 THBD 大数据安全分析底层架构，系统综合运用 Hadoop、Spark 等大数据底层货架技术，结合自主知识产权的 THMQ 消息总线和 THBD 非关系数据库技术，并在之上构建了流式分析引擎、持续聚合引擎、交互分析引擎、全文检索引擎、回放引擎、批处理引擎等高性能计算框架和分布式资源调度与集群运维管理，为平台实现数据治理，数据服务奠定了基础。大数据分析技术特有的特点，为大规模网络安全事件监测分析提供计算支撑力量，同时对海量的基础数据进行深度挖掘及分析处理，及时监测发现网络安全事件，实现对整体网络安全态势的感知

盘古数据平台（简称 THBD)定位于简化大数据应用开发中的数据接入、数据处理、数据存储、资源调度、数据管理、数据统一服务等安全大数据业务的系统支撑平台。提供了网络安全管理平台在安全监测、威胁分析和态势分析过程中所需要的大数据分析计算能力。该平台向安全管理与态势感知产品提供数据收集、处理、存储、计算等通用型便捷、高效、易用的大数据支撑环境，可以实现大数据技术与态势业务解耦、业务无感知的底层技术迭代，提供配置式大数据业务开发环境，高效利用大数据资源。

该模块基于大数据架构的数据处理技术，采用分布式的信息处理及索引节点，可将繁重的分析处理任务分摊负载到若干个处理节点并行运算，并由管理中心节点对处理结果进行统筹和调取。该架构可根据数据分析的规模动态的拓展或缩减节点，具有良好的伸缩性，可根据实际的需求完成海量数据的分析处理。

- 数据采集与处理

THBD 基于分布式数据采集器对异构数据源的结构化数据、非结构化数据进行采集与预处理，**引擎以 DAG（有向无环图）的理念进行配置和运行，方便扩展与自定义开发**。支持实时数据采集与离线数据采集，通过对海量数据采集任务的智能调度，**引入高性能内存无锁队列(disruptor)，将数据接收、解析、存储等各个环节通过消息队列进行解耦，大幅提高了并发性能**。

- 数据分析

利用 Clickhouse 与 Elasticsearch 联合构建新的大数据分析引擎，使 THBD 数据平台分析性能大幅提升。采用了分布式多主架构提高并发性能，对多个数据块来说，大大减少了命令执行次数，缩短了计算时间。**THBD 数据统一查询服务基于 CK 和 ES 两种数据库技术，统计计算使用 CK，全文检索使用 ES 服务为其他子系统提供统一服务的接口，**将数据平台复杂的能力封装为易于使用的实时数据服务、批处理服务和交互式分析服务。

- 数据存储

数据湖和数仓融合架构，湖仓一体（Lakehouse）作为一种新兴架构，湖仓一体在扩展性、事务性以及灵活度上都体现出了独有的优势。THBD 实现统一的 DaaS 数据服务接口。THBD 采用存算分离架构，并且是可分可合的。用户根据不同的场景诉求，既可以同一进程启动存储和计算的功能，也可以将两者分开部署。

3.2.3 支撑分析运算的智能平台 THBRAIN

为应对各类的分析运算场景，THBrain 智能平台继承了传统的规则关联引擎和情境关联引擎，同时借助机器学习和 AI 分析技术构建了一个 AIsec 分析引擎，模块化 AI 模型算法同时标准化模型服务接口，实现标准化的 AI 对外赋能；通过 UEBA 分析引擎对用户异常行为轮廓的刻画来识别异常，为安全分析师提供高价

值线索。该分析层可根据需要提供一系列数据分析处理引擎，包括流式计算引擎、CEP 引擎、挖掘分析引擎、全文检索引擎、关联分析引擎、行为分析引擎、情境计算引擎和回溯引擎。在此基础之上可进行具体的大规模数据统计以及威胁隐患分析和态势分析，包括批量统计分析、风险计算分析、实时/历史关联分析、趋势分析、全文检索分析等。该层所提供的各类分析引擎和分析处理能力是实现系统态势感知的重要运算分析支撑。

- 分布式关联分析引擎

在网络安全领域中，关联分析是指对网络全局的安全事件数据进行自动、连续分析，根据用户定义的、可配置的规则来识别网络威胁和复杂的攻击模式，从而可以确定事件真实性、进行事件分级并对事件进行有效响应。关联分析可以用来提高安全操作的可靠性、效率以及可视化程度，并为安全管理和应急响应提供技术手段。关联分析引擎已经是态势感知系统或安全管理系统的必备组件

分布式关联分析引擎，是 CEP（Complex Event Processing，复杂事件处理）技术在大数据领域的一个具体实现，关联分析是 SIEM 领域的老话题，也是一个正当其时的关键技术。随着用户侧网络数据规模越来越大，对关联分析引擎的性能要求是目前该技术的关键点。

大数据流式分布式关联分析引擎需要满足至少三个要求：

1) 支持接入全量数据，从而保证分析结果的准确性，这一点对 APT 攻击的发现和溯源至关重要；实际项目中的数据规模已经达到 20 万 EPS 级别。

2) 关联分析引擎可实现实时计算和实时统计，比如，在 IT 系统中，防火墙会持续过滤数据包，公司办公系统会持续被访问，只有计算速度够快才能保证实时输出结果；

3) 快速建模，安全分析师可借助关联分析引擎，可以用可视化配置的方式，就能把自己想要检测场景转化成对应的检测规则，下发到分析引擎运行。

- 行为分析引擎

UEBA 通过对用户和实体（如主机、应用、网络流量和数据集）基于历史轨迹或对照组建立行为轮廓基线来进行分析，并将那些异于标准基线的行为标注为

可疑行为，最终通过各种异常模型的打包分析来帮助发现威胁和潜藏的安全事件。

UEBA 技术可以帮助政府企业，有效检测内部信息系统的安全问题。UEBA 可使用机器学习实现账号变更、行为变更等异常操作行为进行快速检测，常见的如账号的异常登录、服务器上用户的违规操作和终端上的异常动作等等。UEBA 通过与大数据驱动、人工智能等技术相结合，能够将内部的违规操作、窃取数据、非法删除等非正常行为和正常行为区分并精准地进行描述，从而以极高的准确率命中异常事件，使得内部的威胁浮出水面。并在安全漏洞可能发生之前主动预警，帮助企业止损，同时为企业降低在诉讼中浪费的时间和金钱，降低公关危机。

内部人员的越权或风险行为能引起严重的网络安全威胁事件。所以通过 UEBA 机器学习模型建立行为基线，实时发现预警各类账号的异常行为，是最后一道关键防线。

UEBA 关键技术点：

- ✓ 支持自定义模型的行为分析引擎技术，灵活适配单机环境与分布式环境
- ✓ 基于 CEP 的关联分析引擎技术，灵活适配单机环境与分布式环境
- ✓ 支持反馈机制的多维行为基线模型
- ✓ 成熟稳定的行为分析算法库：包括行为聚类算法、行为预测算法、STL 时序算法、伴生行为算法、信息熵算法等
- ✓ 多层次关联的异常行为降噪技术
- ✓ 支持策略反馈的用户/实体打分模型
- ✓ 用户可扩展 APP 的行为分析计算框架
- ✓ 可解释、可追溯的异常行为调查技术

4 产品功能

安全态势分析层提供了网络安全管理平台在安全监测、威胁分析和态势分析过程中所需要的大数据分析计算能力。该模块基于大数据架构的数据处理技术，采用分布式的信息处理及索引节点，可将繁重的分析处理任务分摊负载到若干个处理节点并行运算，并由管理中心节点对处理结果进行统筹和调取。该架构可根

据数据分析的规模动态的拓展或缩减节点，具有良好的伸缩性，可根据实际的需求完成海量数据的分析处理。

为应对各类的分析运算场景，该分析层可根据需要提供一系列数据分析处理引擎，包括流式计算引擎、CEP 引擎、挖掘分析引擎、全文检索引擎、关联分析引擎、情境计算引擎和回溯引擎。在此基础之上可进行具体的大规模数据统计以及威胁隐患分析和态势分析，包括批量统计分析、风险计算分析、实时/历史关联分析、威胁 KPI 分析、趋势分析、全文检索分析等。该层所提供的各类分析引擎和分析处理能力是实现系统态势感知的重要运算分析支撑。

4.1 数据中心

数据中心提供系统日志数据以及流量等多类型安全数据的统一存储和快速整合，快速整合多源异构数据，并实现统一的分析检索，提供基于多种时间粒度、多种时间周期的存储检索，也就是说，数据中心是用户分散的日志数据信息聚合的中心。在这里提供数据的交互式管理界面，方便用户对数据进行实时监测和梳理。

数据中心提供不间断的数据存储。系统提供从 TB 级存储容量，保障全部安全数据，应用协议数据，流量数据的长期存储。经过 ETL 数据处理，包括数据收集，数据标准化，数据标签化和数据补齐以及数据融合，数据中心是各类安全数据，业务数据，流数据在平台的第一个集成汇聚点，这里提供了数据的集中存储，检索并为其他应用提供良好的数据准备。

数据中心存储的各类安全数据，业务数据属于摘要类信息，一方面，透过此类事件难以还原攻击/违规的事发现场；另一方面，出于各种原因，事件记录可能不全，导致难以作出准确的研判。因此，对于安全管理和态势感知平台而言，仅仅分析事件以及与事件相关的情境信息是不够的。要进行更加全面的安全分析，还需要对网络中的流量类信息进行分析。流（Flow）是 IP 节点之间会话信息的记录。流信息能更加详实地再现攻击/违规的事发现场，流分析可以作为事件分析的有力补充。

系统可以直接接收并分析网络中的流信息，也可以主动的抓取并生成流信息。而系统的智能化流安全分析主要体现在以下几个方面：

流分布分析：支持对流信息的统计分析，譬如重要业务系统或者服务器的进出流量、各协议流量分布和流量趋势、到办公区的工作日进出流量，以及重要资产的业务流量等等。

流与日志的协同分析：通过将流安全分析技术与日志分析技术有机地整合到一起，系统能够实现从关联告警事件到原始事件的钻取，再到原始事件发生时段的原始流信息的回溯分析，甚至到原始包数据的回溯。

4.1.1 基于策略的各类日志分析

用户可以通过丰富的日志事件分析策略对全网的日志进行全方位、多视角、大跨度、细粒度的实时监测、统计分析、查询、调查、追溯、地图定位、可视化分析展示等等。每条事件分析策略就像是地图的图层，或者是 Photoshop 的滤镜，只展现出用户关心的信息，帮助用户快速从海量日志中筛选出重要的事件。借助这种分析过程，用户从传统的“条件编辑”式的分析体验转变为“策略选取”式的分析体验，大大提升分析效率。

安全分析师进行日常分析时，可将分析过程中选择的条件组合保存为策略，这样以后需要做类似分析时就可以直接选择该策略，提高了分析效率。系统内置了策略库供用户选择，用户也可以分析策略进行再编辑和保存，包括定义筛选的机制和展示的方式。不同的日志分析策略可以任意组合成为仪表板视图，在系统工作台中予以集中展示。

4.1.1.1 交互式查询

系统使用了大数据交互式查询技术，满足安全分析师的日常工作需要。安全分析师可以通过自定义的仪表盘与系统所存储的所有日志进行交互，实时显示查询到的数据，查询时间缩短到秒级。系统支持任意嵌套查询，并可随意回退，通过仪表板可视化处理数据，真正做到所见即所查。系统可将查询条件保存为策略，支持策略的导入导出，供后期使用，为安全分析工作提供便利。安全分析师通过

仪表板可任意选择需要显示的字段和信息，并可对查询结果随时进行统计分析、可视化分析，包括地理定位、多维分析、TopN 分析，支持关键字和正则表达式的全文检索。系统的交互式分析功能为安全审计和分析人员在进行日志调查和威胁分析时提供了一个强有力的武器。

4.1.1.2 事件混合检索技术

传统的日志分析技术主要包括两种常见的方式，一种方式是日志进行范式化描述，转化成标准化的统一格式后基于标准化字段进行审计。这种审计的能力主要局限于范式化字段的多少，在范式化过程中字段数据越多从日志中提取的信息就越多，审计能力就越强。对初级使用者来说非常方便，但它存在的问题是对范式化能力要求高，需要审计人员可以根据需要修改范式化脚本或者需要长时间的积累。这种产品的代表有上一代泰合信息安全审计系统和 HP 公司的 ArcSight 等；另一种方式是对采集的原始日志不进行范化，直接对原始日志进行保存，同时做一些全文索引，形成日志数据仓库。高级安全审计员可根据自己的需要进行搜索和查找，并在此基础上进行人工分析。这种方式的特点是非常灵活，它为水平较高的安全审计人员提供了一个数据分析平台。安全审计员可以根据自己的审计需要随意进行查询并统计，但它的最大的不足是对日志审计人员的专业技术水平要求非常高，受限于资金和人力的投入，一般组织很难招募到优秀的高水平分析师，所以这类数据搜索工具很难为组织的安全审计提供有效帮助。这样的产品的典型代表为 Splunk。

基于以上日志审计的两种方式，系统提供的混合检索技术属于交互式分析技术。它完全融合了两种日志审计方式的优点，它的特点就是不仅提供了基于范式化后的格式数据内容的实时关联分析和统计报表，同时还提供强大的全文搜索能力。混合式检索技术包括通过对范化后的字段值进行全部日志记录的搜索，其功能完全等同于传统关系库中的 SQL 查询，查询出包含搜索值的所有的日志记录，并分行显示。同时，支持全文检索技术，它不局限于几种或几十种固定的字段，不需要指定数据的格式，可以结合时间与关键词进行搜索，实时展现搜索结果，并对关键字进行高亮显示，使用上就和 Google 一样直观易用，用户可以输入关

键词或正则表达式进行任意搜索，提供即时的在线查询，立即产生长时期结果；采用交互式对比查询，可以逐渐收敛事件范围；可以用事件、关键词和复杂流程拼接关联事件。

4.1.1.3 可视化的数据中心

系统为用户提供了丰富的可视化数据分析视图，充分提升了分析效率。

针对日志，用户可以对其源目的 IP 地址进行追踪，并在世界地图上标注出来。安全分析人员也可以对一段时间内的日志进行行为分析，通过生成一幅事件拓扑图形象化地展示海量日志之间的关联关系，从宏观的角度来协助定位安全问题。系统能够实时地绘制事件分时图，动态显示不同时段内各种等级日志的数量分布，点击每个分时柱子都能够进行日志钻取和过滤。系统提供了针对日志的多维分析图，可以通过平行坐标轴显示大量日志相对于多属性的聚合关系，分析人员还能够对分析维度进行自定义。系统提供了针对日志的视网膜分析图，可以形象地展示日志源目的 IP 之间的关系和事件数量。系统提供了日志分析图，可实时展示日志的各类摘要信息和详细信息，可以对用户指定区域或类型的日志进行可视化展示，帮助安全分析师发现行为异常。

4.2 资产中心

随着大云物智移等技术的发展，资产类型越来越多；资产的部署越来越简易，且不易被感知；资产面临的脆弱性和暴露面越来越难以感知；多数企业和组织并未建立有效的资产管理或治的有效措施，导致了问题资产的存在，又缺乏技术措施进行有效的治理，导致一系列问题的发生。

在建设网络安全管理平台时，需优先关注客户的资产纳管情况，资产管理主要是指对于 IP 化软硬件资产提供安全管理，其管理范围包括主机、网络产品、安全设备、数据库、中间件、企业应用系统、机房设备，大数据或虚拟化系统等。

资产管理是安全管理的基础，首先它通过主动发现、导入或创建的方式来识别和梳理目标网络中要被防护的资产及业务对象，发现方式包括配置核查结果识别，资产采集器，漏扫结果识别，手动添加，日志或事件中获取。所获得并维护的被防护对象信息将在资产的纳管过程中被新增和更新，多种来源同时发现资产

的情况下会存在大量重复资产，为减少重复数量，需要进行重复资产的判定，由程序自动进行合并，以便减少运维人员人工确认的情况。被纳管的资产将被其他多个能力中心所利用，成为面向安全对象安全态势分析的基础。

资产视角的资产中心将从资产纳管、资产标签管理等角度来审视资产的整体安全防护状态。具体如下：

- 资产发现：

资产来源目前有 6 类，分别是流量被动发现资产、日志识别资产、脆弱性（配置核查发现资产，漏扫发现资产）识别资产，手动添加或批量导入资产，资产适配器插件，资产采集器；在多种来源同时发现资产的情况下会存在大量重复资产，为减少重复数量，系统支持重复资产的判定，由程序自动进行合并，以便减少资产管理与运维人员人工确认的情况。

发现后的资产会根据安全域 IP 段设置情况自动分配到对应的安全域，安全域是指同一环境内有相同的安全保护需求、相互信任、并具有相同的安全访问控制和边界控制策略的网络或系统。每个安全域具有基本相同的安全特性，如安全级别、安全威胁、风险等，依据这些特性，将资产纳管到不同的安全域中，实施不同的安全保护。

纳管后资产可基于 ES 全文搜索引擎，可以对资产数据进行精确检索、模糊检索、全文检索等各类搜索方式，并且可以自定义查询表达式进行灵活的数据过滤筛选。对查询到的结果通过进行分类统计以 ECharts 图表可视化展现。

- 资产基础画像和高级画像：

系统支持统一的页面呈现资产的基础属性，扩展属性，安全属性。宏观层面，提供告警数量，日志数量，风险值指标值，通过脆弱性计算资产的安全评分。提供趋势分析：日志趋势，告警趋势，漏洞数量趋势，设备运行状态监控趋势；对资产信息被采集，更新记录以时序图的形式展示。从日志，核查，漏洞，监控，告警，风险，端口，访问情况，端口情况 10 个维度进行资产高级画像。

- 资产标签视角

通过配置位置标签，部门标签，业务标签，系统支持对资产多维度分类和展示。

- 资产建模

随着应用环境的扩展，内置的资产属性无法达到所有应用环境的属性要求，系统提供了资产动态建模能力。可以动态的配置资产的属性、类型，资产建模配置好之后，资产以及涉及到资产的部分则会以配置好的属性和类型呈现资产。资产建模包含了属性管理、类型管理，属性管理即属性的动态配置。

- 资产异常分析

系统基于内置的异常资产规则，可分析异常资产，异常类型包括。

4.3 脆弱性中心

脆弱性是安全对象本身固有的，可被威胁利用、引起安全对象的损失。脆弱性中心是系统全网各区域以及各资产业务的脆弱性问题的统一呈现模块。脆弱性中心综合了漏洞扫描、基线核查所扫描的全网漏洞弱点进行脆弱性呈现，使用户统一把控全网各区域各资产业务类型的弱点暴露。资产的脆弱性包括资产系统漏洞和配置弱点。系统能够通过远程评估产品收集整个网络的弱点情况并进行统一管理，对收集的信息进行统一的范式化处理后，对脆弱性信息提供查询和展现功能，使得管理人员可以清楚的掌握全网的脆弱性。

脆弱性分析解决了以下问题：

全场景化资产问题集中管理问题：主机漏洞、web 漏洞、配置不合规、资产运维使用不合规全面统一纳管。脆弱性全生命周期闭环管理 ，从脆弱性扫描发现、分析评估、派发处置、整改归档实现四位一体跟踪记录。

海量漏洞应该优先处置哪一个，内置漏洞处置优先级评估推荐模型，支持模型影响因子权重灵活配置保存，更有人工关注漏洞可纳入计算模型中，满足用户多场景下的模型评估需要。

以运维视角，深化周期性运营报告，资产脆弱性分布、分类分析、处置数据一应俱全，一张报告全覆盖，提供给用户最有价值的最为关心的资产脆弱性数据结果。

脆弱性中心功能通过自动化下发扫描任务以及对弱点问题处置跟踪进行全生命周期管理。通过多引擎的高效并发管理能力、全场景的脆弱性发现能力、脆弱性全生命周期管理能力、细粒度的权限划分能力解决用户资产纳管难、脆弱性跟踪处置难的问题。同时采用“分权分域”管理机制，实现各部门各业务系统的资产脆弱性自洽管理，从根本上解决漏洞难以追踪、自动化扫描难以实现、大规模场景难以梳理的问题，为安全研判、应急处置、资产全量纳管、漏洞修复提供优秀的解决方案。

系统的脆弱性中心内置了同厂商扫描引擎的升级与授权进行统一维护、监控与配置集中管理，扫描任务能作为定期任务再次启动和复用，有效降低运维精力，让运维工作精简化。具备超强性能保障，内置 ES、CK 和 Mysql 数据库集群综合应用查询检索和统计分析，保障百万级资产和脆弱性数据管理页面数秒内完成响应。内置最新的漏洞情报、漏洞库、POC 知识、补丁关联关系，既能作为知识应用查询检索和详情查看，又能与资产安全属性碰撞分析，梳理出最热漏洞的资产影响范围。按区域划分或业务系统划分视角进行资产与脆弱性管理，做好责任人划分，各司其职，有效应对漏洞监督检查和数据保密分化要求。

在脆弱性管理方面，从脆弱性统计、脆弱性发现、脆弱性清单、脆弱性追踪和脆弱性配置形成一个脆弱性生命周期的管理闭环业务。

4.3.1 脆弱性统计

系统从以下维度进行了脆弱性识别以及整改情况的统计和趋势分析：漏洞整改率、弱口令整改率、web 漏洞整改率、配置核查整改率、各类漏洞清单发现趋势、各类漏洞清单等级分布、发现漏洞数 IP 地址 TOP5、影响 IP 地址漏洞名称 TOP5、漏洞清单状态分布。

4.3.2 脆弱性发现

系统提供导入文件和主动调度引擎任务两种方式发现资产脆弱性。提供弱口令识别、系统漏洞扫描、WEB 漏洞扫描、基线漏洞扫描任务，驱动引擎启动进行

在线或离线扫描任务。脆弱性文件（漏洞扫描文件或配置核查结果）导入或扫描结果返回后，漏洞信息便与系统中的资产进行了关联。

4.3.3 脆弱性清单

维护脆弱性信息的当前最新的状态变化情况，状态变化依赖于处置情况，支持清单的处置，查询。清单包括系统漏洞清单、弱口令清单、web 漏洞清单、基线漏洞清单。

4.3.4 脆弱性追踪

脆弱性审核主要是脆弱性处置操作，重要是对发起整改要求的漏洞进行管理，对漏洞的状态可以进行状态维护（已整改、无法整改、延期和误报），最终可以进行归档。

4.3.5 脆弱性配置

系统内置了多引擎的配置能力，包括系统漏扫引擎、web 引擎、配置核查引擎、弱口令引擎。通过引擎的授权管理，升级包管理，策略查看与配置、弱口令字典的自定义下发等深度管理能力完成与脆弱性引擎的无缝对接。

4.4 威胁中心

通过事前的预防（完善的安全机制对内部人员的威慑）、事中的发现和阻断、事件响应和事后取证和追溯这四环节的紧密合作，可以构建强大的权限管控和威胁发现能力的安全体系，从而切实降低企业在安全事件中的损失。威胁中心内置风险识别、告警分析、图谱分析、UEBA、攻击预测等多个功能模块来实现威胁的发现，攻击的分析，告警事件的研判。

4.4.1 风险

风险管理模块负责维护资产的价值、弱点、威胁、风险相关信息。资产弱点管理实际管理资产的弱点，资产的弱点信息可能来自于扫描器，系统提供扫描结果导入功能。当要对资产的安全风险进行评估时，系统根据资产的价值、它的弱

点和所受威胁的信息，根据业界认可的经验公式，经过计算可以得到资产的安全风险值。系统提供对资产弱点、威胁、风险的统计信息，给出统计图。

- 风险总览

风险统计功能主要是对当前安全域下的资产弱点，风险，威胁进行分析后，以图形化界面展现出来，包括通过统计值显示当前安全域下的资产价值、数量、风险等级。通过矩阵图展现当前风险的可能性及影响性，点击矩阵节点会进入查看当前风险影响的应用进行查看。通过曲线图展现风险值最高的五个资产的风险趋势，在安全域上可以通过右上角资产或子域按钮来切换显示当前安全域或当前安全域的子域，在时间上可以通过点击右上角的当前、24 时、7 天、30 天、365 天来查看不同时间段内的风险趋势。具体资产的风险可以通过点击相应资产的柱状图进入点击资产进行进一步的查看。

- 资产风险

展示当前安全域下风险主机总数，风险复现主机数、今日新增主机数、高风险主机数、高威胁主机数、高脆弱性主机数等指标信息安全域中的资产按照列表展现，展示字段有资产名称、资产 IP、资产价值、脆弱性值、威胁值、风险等级、风险来源、风险最近发生时间、风险最近处置时间等信息。并提供风险主机处置功能。

资产列表是以非常直观的形式展现每个资产的属性和当前状态。选中一个资产可展现安全属性、风险趋势、脆弱性分布、威胁分布信息。同时通过告警处置和脆弱性处理实现风险主机的进一步处理，并记录风险处置记录。

4.4.2 图谱分析

图谱分析汇总了资产、告警、脆弱性、监控四个模块的数据并构建出对应关系，通过图谱的方式进行展示这四个维度之间的关联关系。系统的图谱分析已检索页面为查询入口，以图谱拓扑方式展示对应条件下的分析结果，可针对指定类型（告警、资产、漏洞、服务）的关键字进行检索和分析。图中节点支持扩展和隐藏，节点或连线显示对应的属性值。系统可通过进入聚焦模式，包括对地址、

告警、开放服务、弱点、攻击者的聚合，聚焦模式下可查看节点和关系以及基础信息的详情。

4.4.3 告警

➢ 告警查询

攻击视角的告警：从攻击者视角来查看用户网络攻击情况，按照目的资产 TOP10 图、失陷状态图和 ATT&CK 进行展示被攻击情况。网络安全管理平台按照防御方情况将平台中的攻击链分析分为侦察跟踪、武器构建、载荷投递、漏洞利用、安装植入、命令控制、目标达成七个阶段，通过各阶段事件的源 IP、目的 IP、事件类型、事件数量等信息，向用户提供可供参考的分析数据。对全网业务资产被攻击情况进行全程监控呈现；掌控实时攻击进程趋势，进行及时有效的响应处置；记录攻击上下文信息，保存证据，同时了解攻击者的攻击规律，攻击手法，攻击意图，为后续的防御、诱捕、反制提供理论支撑。

防守视角的告警：从防护视角来看攻击者的信息，攻击源国家 TOP10、安全类型 TOP10、告警等级、告警地图数据 4 个维度呈现告警防护方情况。

告警溯源：如何在入侵之后快速定位攻击源以及入侵原因，已经成为网络安全防护工作中的重中之重。告警溯源正是基于上述背景，通过访问关系、攻击上下文日志、流量、pcap 包信息来快速定位入侵原因、制定应急决策。

告警详情查询：告警可通过四类信息进行分组查询，包括基本属性，IP 属性，安全属性和知识属性。对每条告警的原始告警以及每个原始告警的原始日志信息可进行追溯查询。

告警智能分析：根据攻击源 IP 对数据进行同源分析，根据目的地址对告警进行相似度分析。并且按照告警出现的时间轴进行展示。

➢ 告警处置

告警状态变更：修改告警的处置状态。

加入工单：生成工单，把这条告警指派给相关人员处理

剧本响应：把告警指派给相应的剧本进行处理

动作响应：把告警指派给相应的动作进行处理

- 告警分诊

系统能够基于预定义或自定义的研判策略和生成策略自动化地聚合告警信息，生成高质量的告警信息，减少管理员需要查看的告警数量，通过告警模型自动地推荐告警的处置优先级，加快安全响应速度。

- 告警调查

安全运营人员可以对告警信息进行检索查询，可以以时间线的方式显示不同时间切片下不同等级告警的数量信息，并可以自定义各种告警统计图表，能够以曲线图、面积图、柱状图、饼图等形式可视化呈现统计结果。

安全运营人员可以修订告警的状态，可以针对具体的告警信息产生工单，或者添加到案例中去。在将告警信息添加到案例的时候，可以指明将告警的哪些属性值作为痕迹加入该案例中。

针对每条告警，可以进入告警调查页面，对告警信息进行全面呈现和调查分析。在告警调查过程中，可以对告警信息进行追溯，可以调用剧本和应用动作，并查看执行结果。

- 告警处置

告警状态变更：修改告警的处置状态。

加入工单：生成工单，把这条告警指派给相关人员处理

剧本响应：把告警指派给相应的剧本进行处理

动作响应：把告警指派给相应的动作进行处理

系统支持基于规则的自动化响应，自动触发并执行相应的剧本或者应用动作，告警响应规则包含告警条件、告警响应剧本或者应用动作。同时，系统允许安全运营人员对每个告警的处理过程进行记录，修改告警状态，还可以针对告警派发工单，或者送到案例管理中进行后续响应。

4.4.4 攻击预测

攻击事件分析预测的建模对象是用户的整个网络中带有 ATT&CK 的攻击 TTP 字段的告警，建模目标是根据过去时间窗口内的攻击行为来预测未来网络中可能发生的攻击模式，给出概率值，也就是说采用历史数据进行统计，计算出已知条件下的概率表，以查表的方式基于已经发生的条件得到未发生事件的概率。

4.5 响应中心

4.5.1 工单

管理员可以生成周期性任务工单，也能够根据安全事件和告警触发一次性工单，并派发给指定的处理人。工单处理人在接收到工单后可以记录工单的流转信息和状态信息。管理员可以查看所有的工单及其流转的全过程，能够对工单的数量、状态（处理情况）等进行统计分析。

通过工单的建单趋势统计、建单类型统计、工单状态统计，处置完成率，处理及时率分析为管理员提供一个工单的综合分析视角，针对不同的角色提供各自权限范围内的工单信息，并为特定权限用户提供个人工单工作台。系统通过工作流机制实现工单的流程管理，包括工单的创建、审批、驳回、签收、反签收，办理，撤销等。

4.5.2 预警

用户可以通过预警管理功能发布内部及外部的早期预警信息，并与网络中的 IP 资产进行关联，分析出可能受影响的资产，提前让用户了解业务系统可能遭受的攻击和潜在的安全隐患。系统支持内部预警和外部预警；预警类型包括安全通告、攻击预警、漏洞预警和病毒预警等；预警信息包括预备预警、正式预警和归档预警三个状态。

4.5.3 作战室

作战室以自然语言交互和智能推荐技术为核心，提供安全事件多人协同处置、安全指令下发、剧本执行交互功能。在安全事件处置的交付页面中，可完成安全人员交互、安全人员下发安全指令以及安全剧本调用功能。内置的协同机器人可实现 7*24 自动化响应，提供图片智能识别、图片文字内容提取、协助下发或解析安全指令、智能推荐相关知识库和处置动作的功能，大大提升了安全事件的响应处置效率。

4.6 可视中心

4.6.1 态势中心

态势感知不仅在“419”讲话中被提及，而且被写入《“十三五”国家信息化规划》的十大任务，再次体现了态势感知的重要性。安全态势感知已开始逐渐为人们所熟知，随着《网络安全法》的出台，各大网络安全厂商纷纷发布网络安全态势感知解决方案，安全态势感知也成为网络安全的热点。态势中心基于系统下层安全要素的采集和分析，负责向用户呈现态势感知能力，根据安全防护的重点和影响安全态势的几个重要方面，网络安全管理平台的态势中心提供包括通用态势以及自定义态势能力，通用态势包括：态势总览，资产态势，攻击态势，运行态势，脆弱性态势，风险态势，情报态势，系统将通过这几个维度使用户对网络的安全态势进行把握和感知。

4.6.2 通用态势

经过全面的安全要素获取和数据信息的集中处理分析，平台将为用户呈现多个中心：资产中心，脆弱性中心，数据中心，威胁中心，响应中心，报告中心，监管中心，运行中心，模型中心，情报中心以及态势中心，在态势中心中我们将通过资产态势、攻击态势、运行态势、脆弱性态势、风险态势、威胁态势这六个主要维度和安全态势总揽作为态势感知的直观呈现，通过这些维度有助于把庞大复杂的态势感知信息处理体系进行切片的理解和构建，所有的安全要素信息的采集和处理都可以围绕这些维度展开。

4.6.2.1 态势总览

态势总览从全局维度展现被监管对象的安全态势情况，总体安全态势的呈现效果：态势总览从全局维度展现被监管对象的安全态势情况，会根据资产态势，运行态势，攻击态势，脆弱性态势，运营态势等指标计算出全网总览得分，各个态势会根据得分给出定性的状态描述，比如脆弱性态势的状态指标描述为优秀，良好，合格，一般，待改进。

在态势总览中会从告警处置状态，攻击趋势 ，脆弱性统计，被攻击资产，被攻击区域，攻击预测等角度进行宏观趋势分析。

4.6.2.2 资产态势

资产感知是态势感知的基础，首先它通过主动发现、导入或创建的方式来识别和梳理目标网络中要被防护的资产及业务对象。所获得并维护的被防护对象信息将在整个态势分析呈现过程中，被其他维度的感知所利用，成为面向安全对象安全态势分析的基础。

以资产为中心对全网资产和安全域进行梳理，从被防护对象的角度审视资产安全。通过此维度可以实时了解全网资产的安全状况，资产发现、补全、纳管情况，资产发现来源，价值分布，资产类型分布、互联网暴露资产、开放端口等因素，对当前全网资产态势进行分析呈现。

4.6.2.3 运行态势

运行态势基于各类信息资产和业务系统的性能与可用性信息，通过对各种监控对象进行全方位细粒度的监控，提供丰富的可视化图表；系统会自动计算业务的整体性能指数，系统同时会自动计算业务的脆弱性指数和业务的威胁指数，连同业务性能指数，综合计算业务的健康度，并绘制出健康度随时间变化的业务健康曲线。

运行态势从支撑生产业务的系统运行角度感知相关安全态势，对全网设备数、设备可用率、性能情况进行监控。包括内存、CPU 的异常波动，磁盘的异常使用，磁盘的异常暴增，各种设备 CPU、内存的负载情况，重启次数等指标，感知业务运行态势，对影响系统运行的风险和威胁进行提前的预防处置。

4.6.2.4 攻击态势

攻击感知基于汇总全网相关的攻击行为相关信息，通过统计分析、关联融合等手段对攻击信息进行处理，从而获得全景式的攻击态势监视。攻击感知从遭受攻击、攻击的类型、分布、攻击关系、趋势、攻击结果等维度进行攻击态势的呈现。攻击感知的主要功能内容：感知所有攻击行为的来源、目标、规模、影响和

结果。在地图上进行动态攻击情况展示，对攻击类型趋势进行分类描绘，展示攻击端口 top5/攻击源 top5/受攻击安全域 top5 排名。利用攻击事件的名称、攻击次数、事件量等因素进行列表分析，对当前攻击态势进行评估分析。

4.6.2.5 脆弱性态势

综合漏洞扫描、基线核查、弱口令发现的全网漏洞弱点进行弱点态势呈现，使用户统一把控全网各区域各资产业务类型的弱点暴露。所呈现的态势包括漏洞的分布 TOP 统计、影响的资产 TOP 情况、各类型脆弱性问题的发现态势以及复现态势等。

4.6.2.6 情报态势

情报态势页面主要以内外部情报为基础，依托强大得情报源接入为支撑，不仅支持自己的 VenusEye，还支持其它情报厂商和开源情报、内部情报的接入。通过情报数据的使用情况统计（实时匹配、历史管理、云端云查、云端溯源、情报上传、情报下达），情报的命中情况（命中类型，命中列表）等因素的分析呈现，同时呈现外部情报和内部情报的更新趋势，从情报数据本身和情报消费两个维度进行情报态势呈现。

4.6.2.7 风险态势

风险感知综合资产价值、安全属性、脆弱性、攻击威胁等风险要素，基于风险模块内置的风险计算模型，进行全网、各安全域及各业务系统的风险量化评估和风险赋值。风险感知是从风险的角度来衡量被防护对象的安全态势，在平台的态势呈现过程中，风险感知存在于资产感知、漏洞感知和态势总揽当中，通过在各维度中为对应的目标给定风险值来帮助用户把握安全态势，例如在资产感知中，通过风险视图呈现各资产类型、安全域及业务系统的风险值，在态势总揽中通过风险视图给出全网的风险等级。

以全网的安全状况为中心，对影响业务正常的运行的风险态势全局感知。资产的脆弱性、威胁信息图呈现攻击入侵，信息泄露，恶意代码等威胁关系图，同时对安全域，资产脆弱性，资产风险 TOP5 进行排序呈现。

4.6.2.8 网站态势

网站态势给出了网站安全评级情况，包括高危网站、中危网站、低危网站、安全网站数量。根据网站监测的范围分别统计了漏洞的等级分布情况，网站可用性情况，以及网站监测任务的分布情况、高危网站 TOP5、网站异常行为 TOP5。

4.6.2.9 流量态势

流量态势从流量大小、流量协议趋势和类型分布、流量访问关系维度、全网端口流量 TOP、IP 流量 TOP 等维度呈现全网的流量态势。流量可关于网络层的安全事件 TOP 以及攻击者，受害者 TOP 呈现流量分析维度的攻击情况。

4.7 报告中心

出具报表报告是网络安全管理平台的重要用途，系统内置了丰富的报表模板，包括统计报表、明细报表、综合审计报告，审计人员可以根据需要生成不同的报表。系统内置报表生成调度器，可以定时自动生成日报、周报、月报、季报、年报，并支持以邮件等方式自动投递，支持以 PDF、Excel、Word 等格式导出，支持打印。

系统内置运营报告和统计报告，运营报告包括综合安全风险评估报告、资产与脆弱性报告、安全威胁分析报告。统计报告内置综合分析报告。

报表也按照日志、资产、风险、监控、预警、告警、工单等分类内置模板，同时支持灵活的报表定制功能，用户可以自行设计报表，包括报表的页面版式、统计内容、显示风格等。

5 产品规格

产品名称	泰合网络安全管理平台	**备注**
型号	TSOC-CSA-PG	
品牌	启明星辰	
产地	北京	
详细配置（单台的详细配置）		
基本配置	软件形态交付，国产化自主研发，支持国产化自主安全云平台部署。	
性能指标	（1）日志处理速度≥15000EPS。 （2）在存储空间容量 48BT 下，安全数据存储时间≥1 年。	
功能指标	（1）具备日志采集功能：支持主动、被动采集/收集目标日志；支持对网络设备、安全设备、主机系统、数据库等安全日志、网络流量以及业务信息等多种数据源的采集。 （2）具备日志范式化功能：实现对异构日志格式的统一化，范式化字段至少包括事件接收时间、事件产生时间、事件持续时间、用户名称、源地址、源 MAC 地址、源端口、操作、目的地址、目的 MAC 地址、目的端口、事件名称、网络协议、网络应用协议、设备地址、设备名称、设备类型、文件大小、命中威胁情报、功能码、攻击类型等内容。 （3）具备日志分析功能：支持场景化分析，实现特定业务场景的综	

	合分析研判；能够预置基于网络安全设备日志、原始流量分析的告警分析规则；具备包括信息收集、内容安全、威胁情报命中、威胁活动、异常事件等；支持对日志事件依据其源目的 IP 和端口等各类字段信息进行深入的日志事件追踪调查。 （4）具备态势展示功能：能够通过系统的分析规则实现安全威胁的监测和结果呈现，形成威胁告警信息；能够展示攻击者数量、攻击者 IP、攻击者活动时间、指向性、攻击手段数量、攻击成功以及失陷的数量；支持展示受害者 IP 数量、受害单位数量以及受害网站数量，支持展示受害 IP 地址、受害 IP 所属区域、受害 IP 所属单位以及受害 IP 遭受尝试攻击、失陷攻击以及成功攻击的数量。 （5）具备资产管理展示功能：能够按设备类型展示各类型下资产数量、威胁数量、漏洞数量以及安全事件数量；能够展示各安全域的风险情况，包括安全域的资产数量、威胁 数量、漏洞数量、安全事件、高危资产数量、中危资产数量、低危资产数量；能够展示资产漏洞整体情况，包括漏洞总数、累计修复数、受影响资产数情况；能够展示漏洞威胁的分析情况，包括低危、中危、高危、危急的数据分布；支持以资产为中心的多维数据统计分析大屏展示。 （6）具备威胁攻击分析功能：能够展示选定时间范围内威胁告警、攻击者、受害者的数量；能够对选定时间范围内的威胁类型、攻击者、受害者进行统计分析，能够对告警进行实时监测，能够支持实	

	时推送监测到的告警，支持以图谱的方式展示攻击者与受害者之间的关系。 （7）具备关联分析功能：持基于规则的安全事件实时关联分析，能够对不同的事件进行相关性分析，发掘潜在的信息；平台内置不少于 150 关联分析规则，包括但不限于以下关联分析场景：信息搜集、攻击利用、命令控制、违规操作、异常行为、内容安全和设备故障类。 （8）具备监控基本指标功能：支持通过丰富的可视化图表查看监控指标信息；可以对监控指标设置告警阈值；可以将监控指标的数据保存起来，进行历史分析；可以进行基于指标的横向对比分析和基于时间的纵向对比分析。	