泰合网络安全管理平台产品彩页

泰合网络安全管理平台基于多年来综合分析类平台系统的建设经验，面向运营、致力于为政企用户提供集中安全综合管理能力。系统应用大数据技术架构，能够实现全网海量数据规模的安全信息的采集和集中存储，在此基础上对数据进行综合处理和关联分析，从资产态势、运行态势、攻击态势、脆弱性态势、风险态势、威胁态势、网站态势、流量态势等多个方面，为用户展示面向全网业务资产防护的安全态势，帮助用户感知隐患和威胁，为安全运维提供决策支撑。

一、产品特点

全面的资产梳理：资产感知是态势感知的基础，平台能够通过多种手段帮助用户对资产进行全面梳理，提供用户以业务系统为核心的资产感知和管理能力，建立全面的资产信息态势，并为其他维度的分析和呈现提供有力支撑。

全安全要素的获取：能够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，能够充分利用用户已有的安全设备，实现了全面且灵活开放的态势感知系统架构。

面向态势感知的大数据存储能力：具备大数据平台对海量信息的存储、处理和计算能力，提供了对结构化数据和非结构化数据的数据库处理能力，其架构为泰合产品部采用当前主流的分布式大数据存储架构，经过面向安全大数据分析过程的优化改造，形成自有的盘古架构，自主可控。

先进的安全态势分析能力：平台能够综合收集到的安全信息要素，基于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

通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦　邮政编码：100193
集团总机：010-82779088　集团传真：010-82779000　售后热线：400-624-3900
售后邮箱：support@venustech.com.cn　启明星辰微信公众号：venustech_weixin
官方微信　官方微博

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，以多种分析手段支撑平台的安全态势分析。

多维度的态势感知呈现：平台通过资产感知、脆弱性感知、运行感知、攻击感知、威胁感知、风险感知、网站感知、流态势和态势总览多个维度来覆盖安全态势各个方面，来实现全方位的态势感知。

面向安全运维的预警通告及处置：平台内置了完整的预警通告及处置工作流程，并具备相应的应急处置预案，实现安全运维处置闭环。

开放的外部威胁情报接口：平台能够对接外部的开源及商业威胁情报信息，并且提供了有效的威胁情报利用和分析手段，同时支持内部情报的生产和利用。

强大的级联部署能力：平台能够提供强大的级联部署能力，非常适合总部-分中心的多级架构。

通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦　邮政编码：100193
集团总机：010-82779088　集团传真：010-82779000　售后热线：400-624-3900
售后邮箱：support@venustech.com.cn　启明星辰微信公众号：venustech_weixin
官方微信　官方微博

二、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	

通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦　邮政编码：100193
集团总机：010-82779088　集团传真：010-82779000　售后热线：400-624-3900
售后邮箱：support@venustech.com.cn　启明星辰微信公众号：venustech_weixin
官方微信　官方微博

	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	

通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦 邮政编码：100193
集团总机：010-82779088 集团传真：010-82779000 售后热线：400-624-3900
售后邮箱：support@venustech.com.cn 启明星辰微信公众号：venustech_weixin
官方微信 官方微博

	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。	

通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦　邮政编码：100193
集团总机：010-82779088　集团传真：010-82779000　售后热线：400-624-3900
售后邮箱：support@venustech.com.cn　启明星辰微信公众号：venustech_weixin
官方微信　官方微博