泰合信息安全运营中心系统

TSOC-AEM5600-PAP1

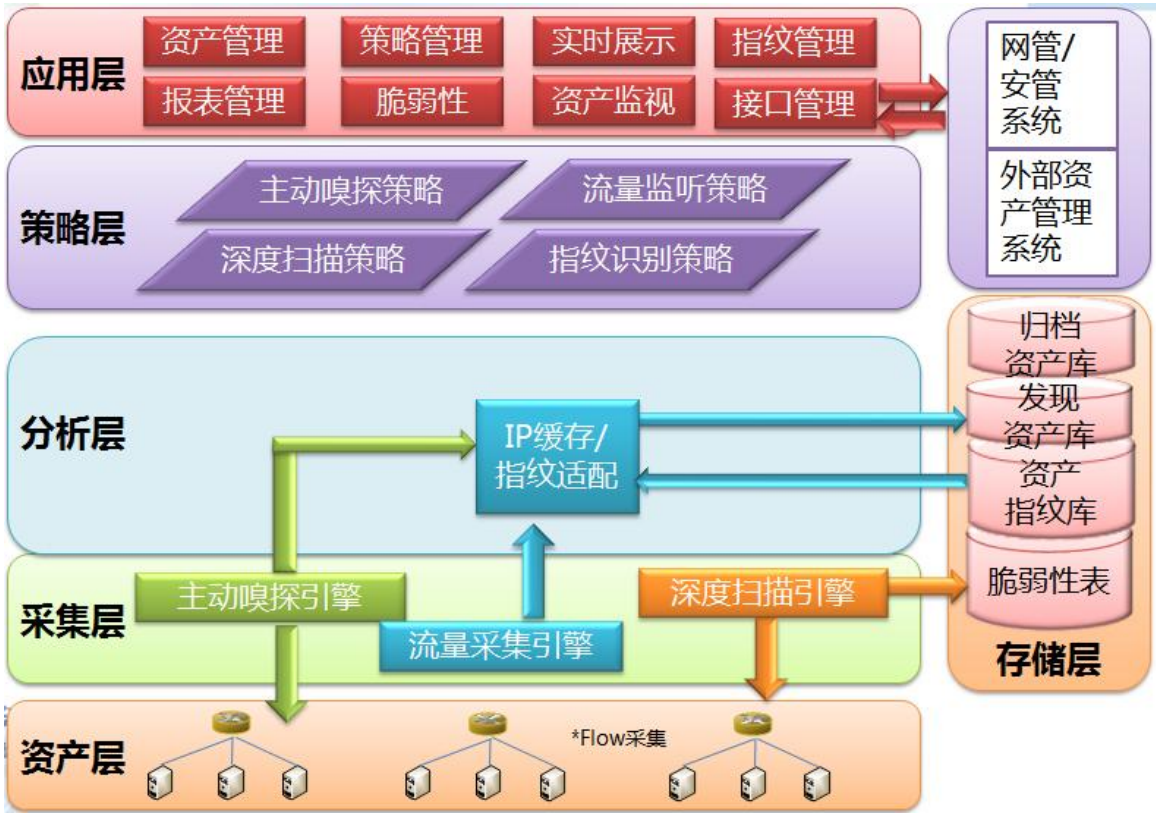
泰合信息安全运营中心系统是一款致力于网络安全资产管理的平台，采用分布式组件化设计，主被动相结合的多种资产发现与采集方式，实现全网资产的全面测绘梳理和资产问题的监测预警与闭环监控。帮助客户测绘现网 IT 资产状况，监测预警资产问题，辅助决策并规范资产治理,提高安全建设水平。

设备照片（图片仅供参考，以实际供货设备为准）

一、 系统架构

资产自动发现与管理系统整体架构设计可满足多种复杂网络情况，支持分布式部署方式；支持资产扫描策略的灵活定义；从总体业务逻辑架构由下至上划分为采集层、分析层、策略层、应用数据展示层，输出三大功能模块；系统的整体架构如下图所示：

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



主动嗅探引擎通过 Nmap 方式主动建立扫描任务目标区域，将发现的资产 IP 及开放端口等信息，被动监听将 flow 信息进行分解，发现资产源 IP、目标 IP、端口信息，两者都将结果保存到 IP 缓存对比模块，此模块负责对发现到的资产信息进行汇总、去同，并与系统中内置的资产指纹库进行对比，最终将发现的资产信息及属性发送给管理中心。使用 flower 的被动方式存在实时性高、发现属性相对较少的情况，而主动扫描方式则是发现资产属性多，但实时性不高，系统将两种方式有机的结合在一起，当被动扫描发现新的资产时会通知主动嗅探引擎进行扫描，既解决了发现实时性又能够尽可能的补全更多的资产属性。

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、 产品特色

主被动结合的资产测绘方式：采用这两种方式，可有效覆盖管理和时间上的盲区，拓宽纳管的资产范围。

基于技术安全与管理安全并重的合规分析：技术安全与管理安全并重齐考核，持续监测与度量。

资产测绘与监测预警处置闭环一体化：从摸清资产到掌握合规状态，并进行处置闭环的监控。

快捷高效的全文检索：提供全文检索功能，可快速定位资产。采用 ElasticSearch 全文检索引擎，使得资产搜索更快速高效，并能对搜索结果二次分析。

资产数据分级存储：系统将资产信息基于不同的阶段，分为发现库和归档库两部分存储。发现库用于存储新发现和新增资产；归档库用于存储已经确认的资产。在资产测绘任务执行后，数据自动对比，识别和感知资产变化。

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

三、 部署方式

➢ 单级部署

单级部署模式又叫路由或网桥部署模式，该部署模式对客户网络的要求比较简单，只要系统的管理中心以及资产扫描器（AC）与管理对象之间网络可达即可。对于网络拓扑结构简单，规模较小以及安全级别相同的客户网络来说，通过产品的简单部署即可实现，即在服务器上部署管理中心并架设一台资产扫描器（AC），管理中心就可以正常工作，实现对全网的资产发现和管理。对于网络拓扑结构复杂、物理位置分散、安全级别有差异的网络，建议采用单级的分布式部署方式，即在中心服务器部署管理中心，在其他多个网络位置部署多台分资产扫描器。如上图所示，显示了系统的一个单级分布式部署场景。

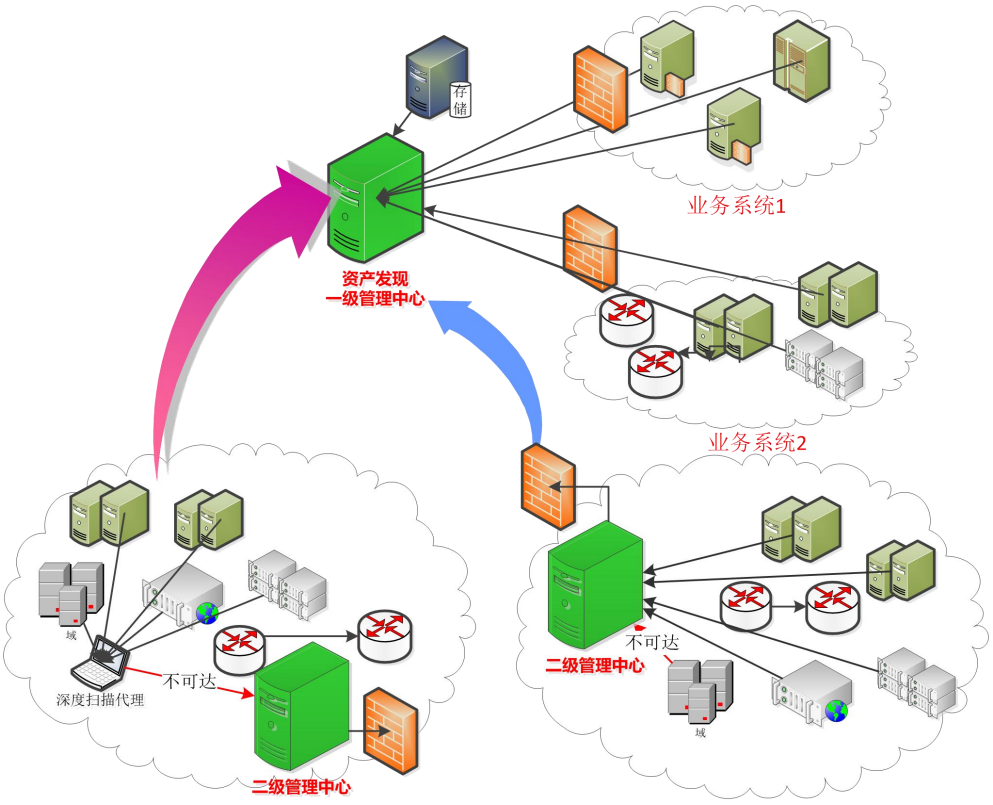
通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦 邮政编码：100193
集团总机：010-82779088 集团传真：010-82779000 售后热线：400-624-3900
售后邮箱：support@venustech.com.cn 启明星辰微信公众号：venustech_weixin
官方微信 官方微博

在这个单级部署场景中，管理中心可以直接制定资产管理任务，资产的扫描发现通过 AC 完成。

系统使用者通过浏览器登录资产数据采集探针的 WEB 站点即可进行各种管理操作。

➢ **多级部署**

对于具有独立管理功能的分支子机构或者垂直管理下属机构的大型企事业单位，系统支持级联部署，以适应用户多级管理的体制。如下图所示，展示了一个系统多级级联部署的典型场景。



总部部署资产发现一级管理中心，根据需要可部署分布式资产发现采集器，实现了对一级管理中心的安全管理。而各下属各分支机构为了实现对各自信息系统的资产管理，分别部署各自的二级管理中心。总部与分支机构的管理中心进行通信，实现总部对分支机构资产数据采集探针的查看和管理。

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

四、 产品规格

产品名称	泰合信息安全运营中心系统 V3.0	备注
型号	TSOC-AEM5600-PAP1	
品牌	启明星辰	
产地	北京	
详细配置（单台的详细配置）		
主要用途	系统主要实现全网资产全面测绘梳理和资产问题的监测预警与闭环监控。测绘现网 IT 资产状况，监测预警资产问题，辅助决策并规范资产治理。	
基本配置	标准 2U 机架式设备，具备 6 个千兆电口，4 个千兆光口（含光模块），2 个万兆光口（含光模块），有效存储 4TB，双冗余电源。	
性能指标	至少支持 10 万个 IP 每周一次的资产属性探测 安全配置检查性能：每分钟可核查设备数至少 5 个 IP；快速扫描策略可满足，24 个 C 类地址/小时； 资产存活探测性能：至少 2500IP/分钟;资产属性探测一个 C 类网络不超过 3 分钟； 支持 150 个并发用户数	
功能指标	1. 主动嗅探：探测网络上的主机，主动的端口探测扫描，硬件特性及版本信息，主要包括以下功能。探测网络上的主机：例如列出响应 TCP 和 ICMP 请求、开放特定端口的主机。 2. 端口扫描：探测目标主机所开放的端口。版本检测：探测目标主机的网络服务，判断其服务名称及版本号。系统检测：探测目标主机的操作系统及网络设备的硬件特性。 3. 具备可视化呈现功能，支持资产数量与 Ip 设备数的总量与同比环比分析展示；展示全网资产数量、IP 设备数量，资产类型、端口分布、操作系统的 Top 分布。	

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

	4. 具备资产测绘功能，支持主被动结合的方式进行资产扫描发现 5. 具备资产测绘功能，支持 Agent 方式采集资产属性，可在 Windows、Linux、AIX、HPux、Solaris 等环境中部署，免安装，支持周期采集资产的属性，包括操作系统版本、厂商、IP、MAC、开放端口、服务、数据库中间件等版本、安装路径、实例名等信息。 6. 被动监听：通过采集或镜像 NetFlow、NetStream、jfow、ipfix 等协议监听网络上的主机及开放的端口。 7. 具备资产测绘功能，具备扫描任务管理功能，支持 IP 和域名方式的资产探测；支持立即扫描及周期扫描，周期扫描可按分钟及小时方式周期执行。 8. 具备资产指纹管理，具备资产发现指纹库，并支持指纹库升级功能。 9. 具备资产指纹管理，内置主流 IT 设备及系统组件、BY0D 与大数据、虚拟化组件指纹； 10. 具备资产指纹管理，指纹信息包含：端口指纹、OS 指纹、WEB 指纹等信息；指纹更新无需二次开发，支持自定义。 11. 具备资产管理与全生命流程管理，对于发现的资产和需要归档的资产能够区分管理，具备处理相同 IP 的资产的能力，应显示的体现资产属性的填充率、发现资产类型及其来源。 12. 具备资产管理与全生命流程管理，支持查看资产的生命流程记录，包括操作人、修改时间、修改详情等信息； 13. 具备资产全文检索功能，支持基于条件的查询，如基于 IP、资产类型、开放端口、开放服务、资产状态等条件的检索。 14. 具备资产全文检索功能，支持对查询的结果可进行二次分析，内容包括资产问题分布、资产对应的责任人分布、资产类型分布； 15. 具备检测预警功能，实现对资产问题的全面跟踪与监视，提供问题的发现、通知、整改、验证、归档完整流程，并对响应时间进行排名统计。 16. 具备监测预警功能，可识别和发现典型问题：疑似资产被替换、发现未知资产、发现影子资产、发现资产宕机、发现移动设备接入、使用不安全协议、开放违规端口、发现失陷主机、开放 FTP 服务、资产存在中高危漏洞、资产安全配置不合规、使用弱团体字符串等。 17. 具备资产画像功能，支持以时间轴方式展示资产生命周期内的指纹信	

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

	息变化，变化范围包含：操作系统类型变更、新增开放端口和服务、中间件信息等信息的新增或变更等。	
其他	随机提供配置手册、用户手册，含纸质版 1 套和光盘 1 张	

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