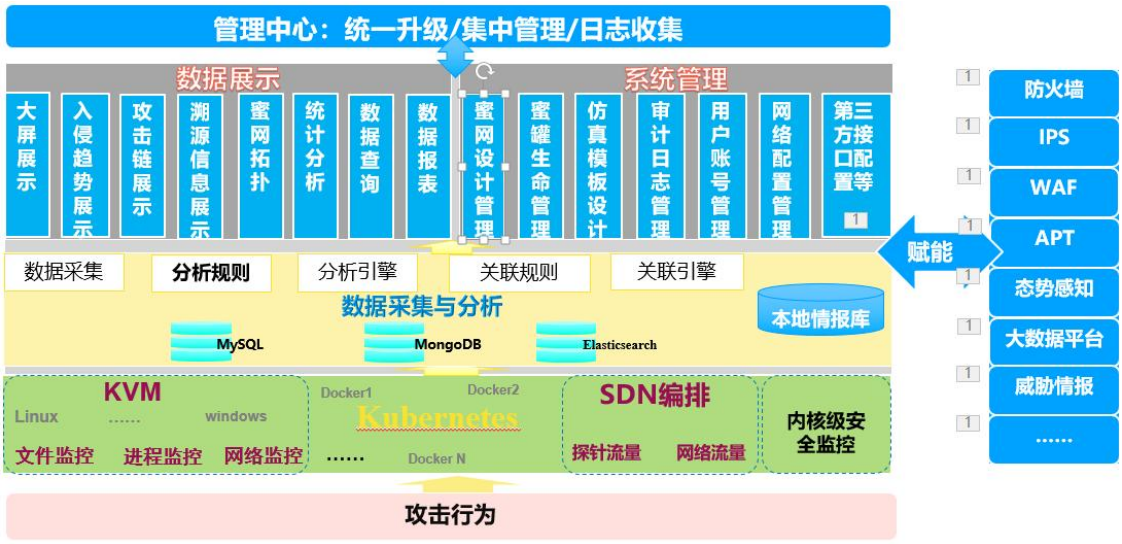
天阗欺骗防御系统 V7.0

天阗欺骗防御系统包括管理系统和业务仿真系统，系统通过虚拟化技术，集成各类仿真系统（蜜罐），通过网络设置将业务仿真系统投放到不同网段，诱骗攻击者，延缓攻击、保护真实网络资产，蜜罐捕获的攻击行为日志和数据上传至管理中心，通过管理中心分析和展示，达到溯源取证的目的。



一、产品功能

内置多种类型的仿真能力，包括应用服务类、漏洞类、操作系统类、工控类以及定制仿真。

（1）仿真能力

- 应用服务仿真

web 类：仿真类型包括 Weblogic、tomcat、thinkphp、wordpress、wiki、wildfly、wordpress、Jenkins/beescms 等；

数据库类：仿真类型包括 MySql/phpmyadmin/DB2/Redis/PostgreSQL 等；

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

通用服务类：仿真类型包括 SSH/Telnet/FTP/Extmail 等；

- 漏洞仿真

系统默认集成自身带有漏洞的高甜度蜜罐，例如 Log4j2、Shiro、Struts2 等，保障蜜罐的高仿真度和诱捕能力，可定制热点漏洞的仿真。

- 操作系统仿真

支持 windows 系列操作系统仿真，可构建办公环境、业务环境、生产环境等高仿真业务环境。

- 工业控制仿真

具备工业控制仿真能力，可支持 IEC104/IEC61850/S7/Modbus/工业 OMS 系统的高仿真能力，可进行工控系统的蜜网布设。

- 定制仿真

内置 web 框架，通过上传标签主题、标签页 icon、页面 logo、背景图等信息，可快速生产成 web 蜜罐，具备溯源社交账号等能力。另外具备高仿真定制能力，专业的安全团队支撑，基于公司多年的安全积累，可基于客户实际业务进行的高仿真定制，用于客户的专用网络或特殊场景，具有专业溯源反制能力，可通过界面直接导入天阗欺骗防御系统，实现快速高效。

（2）欺骗环境构建

天阗欺骗防御系统通过模拟三层网络、诱捕探针导流布设基础诱捕网络，通过漏洞设计、诱饵投放、仿真系统设置等构建高仿真欺骗诱捕环境。

天阗欺骗防御系统不参与真实网络业务交互，对实际业务环境无任何影响，基于用户网络的环境，通过占用空余 IP/网段、采用诱捕探针部署在已有的终端进行攻击导流进

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

行构建蜜网，攻击者一旦达到蜜网即可被吸引至仿真系统，由仿真系统完成交互，捕获攻击行为。构建蜜网时，天阗欺骗防御系统采用主动探测的技术手段主动发现 IP、端口是否被占用，提升蜜网配置效率。

诱饵投放主要以主机诱饵和互联网诱饵为主，互联网诱饵在公开的网站中设置虚假信息，在黑客收集信息阶段对其造成误导，使其攻击目标转向蜜罐，间接保护其他资产。主机诱饵需要提前投放到在真实环境中，在其预留一些连接到其他蜜罐的历史操作指令、放置 SSH 连接蜜罐过程中的公钥记录或在主机诱饵指向的蜜罐上开放有利用价值的端口，在攻击者做嗅探时，可以吸引其入侵并进入蜜罐；类如攻击者偏爱 OA、邮件等用户量大的系统，可在重点区域部署此类诱饵，并通过在真实服务器伪造虚假的连接记录诱导攻击者掉入陷阱,最后将攻击者的攻击视线转移到蜜罐之中。

（2）攻击者画像

天阗欺骗防御系统，可记录攻击者的 IP 地址、所在区域、攻击时间、攻击手段等，通过进一步溯源获取到攻击者的设备指纹、虚拟身份等。天阗欺骗防御系统根据攻击时间、攻击目标、攻击过程、设备指纹等进行汇聚处理，深度分析，溯源攻击者信息，以攻击者为单位展示攻击过程、攻击阶段，展示攻击路径和攻击手段。

（4）系统管理

- 三权分立

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

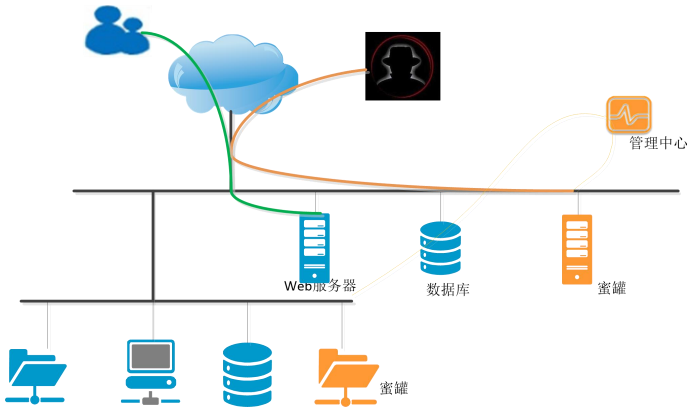
系统设备的管理员用户使用三权分立的原则对设备进行管理和配置，所谓“三权分立”是指的将用户管理，配置管理和审计三种不同的操作分派给三种管理员用户：用户管理员、配置管理员和审计管理员来进行，实现管理员用户之间的各司其职，符合信息安全相关规范要求。

- 管理与运维

系统具备通过界面升级的能力，通过界面升级至最新版本，记录个版本更新情况和升级结果。方便维护，支持系统配置备份、恢复，恢复出厂设置，磁盘超过阈值的自动清理等功能。运维方面，支持 ping、traceroute、arp 等工具，可及时诊断系统网络情况，便于运维。

二、产品部署

天阗欺骗防御系统采用旁路接入模式，不改变客户网络架构，无需镜像流量，适用于多种网络环境，支持单机部署、分布式部署。



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

三、产品规格

产品名称	**天阗欺骗防御系统 V7.0**
产品型号	**CDS5600-FT-CQ**
产品用途	主要用于通过业务仿真构建蜜网，诱惑攻击行为进入蜜网，实现攻击捕获，延缓攻击者对实际业务网络的攻击，实现攻击行为的快速取证溯源，保护真实网络资产。
产品配置	国产化标准机架式设备，高度 2U，采用 FT-2000+/64 处理器，银河麒麟 V10 操作系统；配置 6 个千兆电口，4 个万兆光口，5 个接口扩展槽位，冗余电源，64G 内存。
产品性能	支持高交互蜜罐并发数量为 150 个；
产品功能	1、支持展示系统内配置的事件规则及规则详情，包括威胁等级、事件类型、攻击手段等信息，系统支持的内置规则不少于 20000 种。
	2、具备溯源及反制能力，反制信息界面支持查看到攻击者指纹、攻击 IP、用户名、计算机名、系统详情信息(CPU、CPU 型号、bios 版本、内存、硬盘、显卡、声卡)、系统启动时间、主机制造商、主机型号、系统分辨率、系统语言、时区、IP 信息、端口开放表、WLAN 信息、机器截屏、桌面文件名、系统进程信息、浏览器历史、书签、账号保存、下载记录等信息,获取到的浏览器信息支持打包下载。
	3、支持下载通过各种方式上传到蜜罐内部的可疑样本文件,支持查看文件上传源 IP、来源蜜罐、捕获时间、更新时间、文件大小、文件类型、文件哈希、文件物理路径。

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、探针支持接收 windows 和 linux 系统产生的事件日志，可将安装探针主机的事件日志发送到蜜罐系统，用于辅助研判失陷情况。支持通过配置流量转发，将检测到的潜在威胁实时引导至蜜罐环境。
	5、支持查看攻击事件总数、触发诱饵、攻击者、攻击溯源、攻击反制、捕获样本数量，并支持下钻跳转至攻击者画像、溯源信息、样本文件，并支持根据全链条 ATT&CK 分析查看对应阶段攻击事件，并支持点击后查看详细事件。
	6、支持 WEB 应用类蜜罐，包括但不限于：beecms、coremail、django、drools、goby、Jenkins、joomla、Wiki、nginx、odoo、phpmyadmin、shiro、struts2、thinkphp、tomcat、webmin、VPN、weblogic、wildfly、wordpress。
	7、支持操作系统类:包括 centos、Debian、Redhat、FreeBsD、Ubuntu、Windows11、统信 UOS、中标麒麟、银河麒麟。
	8、支持蜜网配置，包括绑定服务、安全策略、编辑蜜网、删除蜜网操作；支持设置蜜网出网，可设置流量阈值及可访问网段，实现蜜网出网流量控制。
	9、支持在线制作感知型文件蜜饵，支持格式种类包括但不限于 doc、xls、ppt、pdf，部署在操作系统中，一旦攻击者触碰蜜饵，系统将产生相应告警。
	10、蜜罐节点具备定时重置和一键重置功能，可快速恢复至初始状态，扰乱攻击者认知。同时支持对蜜罐做快照，保存攻击环境状态；

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

	11、支持系统平台的资源管理与监控，包括 CPU 使用率、CPU 使用详细表、CPU 核数、内存总数及使用率、磁盘读写速率、网络连接信息，各网卡的上下行流量，以便发现异常行为。
产品可靠性	平均故障恢复时间≤30 分钟
配套资料、配件	提供完整的用户手册，含纸质版 1 套和光盘 1 张。
	配件含万兆光纤 2 根，普通直连网线 2 根，电源线两根。

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