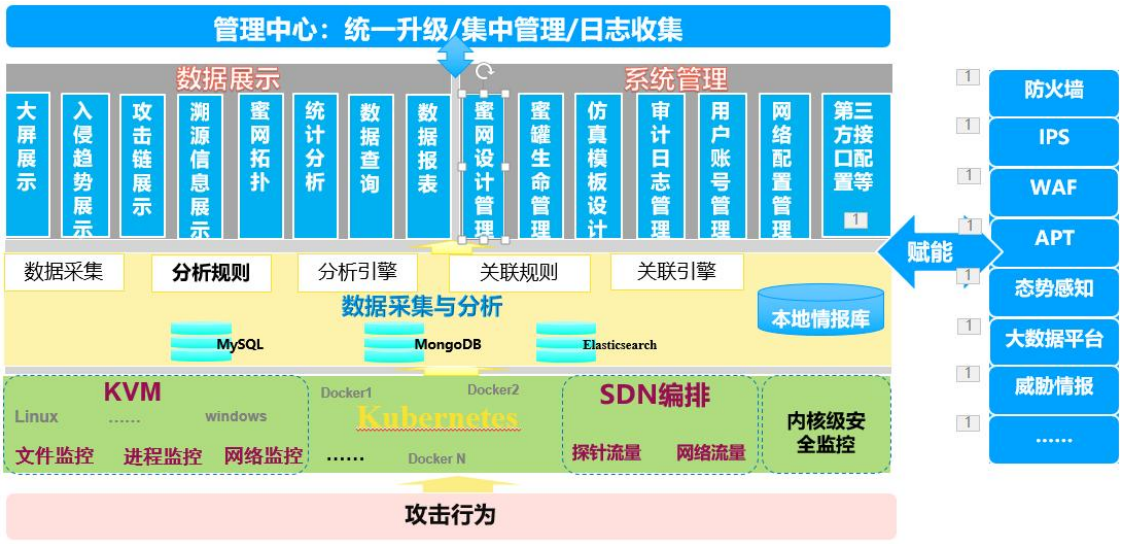
天阗欺骗防御系统 V7.0

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。

- 第三方接口

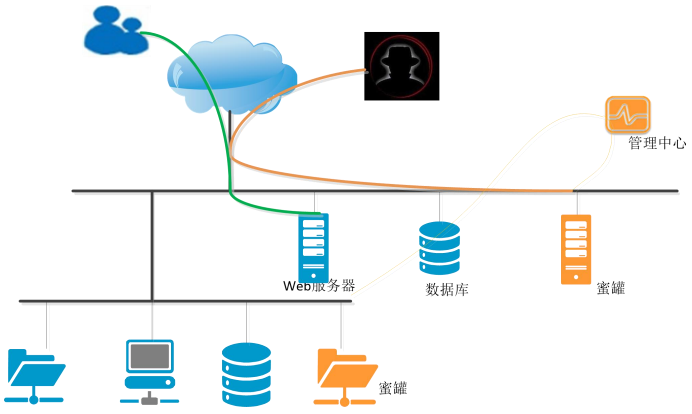
系统支持数据转发至第三方服务器，支持 syslog 和 KAFKA 两种形式，可同时配置多个第三方服务器，支持 syslog 的日志格式的选择和数据类型、编码格式的设置，支持 KAFKA 编码格式、数据类型、认证机制、日志格式的选择。

- 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
官方微信　官方微博

三、产品规格

产品名称	**天阗欺骗防御系统 V7.0**
产品型号	**CDS5888-FT-CQ**
产品用途	主要用于在网络中部署仿真主机，主动诱导攻击，记录攻击细节并产生告警，可定位攻击源，弥补网络防护体系短板，提升主动防御能力。支持国产麒麟操作系统仿真；支持 Tomcat、Apache 等主流应用系统的蜜罐；支持将攻击流量引入蜜罐，并隔离攻击流量；支持网络攻击预警，并记录攻击来源、行为等关键信息；支持监控攻击行为的网络数据包；支持低交互和高交互蜜罐的混合部署方式。
产品配置	国产化硬件设备，标准 19 英寸机架式设备，采用飞腾 D2000/8 处理器，总核数 8 个，频率不小于 2.3GHz，银河麒麟 V10 操作系统；配置 6 个业务千兆电接口，4 个千兆光口；配置 2TB 存储空间，64GB 内存容量；
产品功能	1、支持 Apache、beecms、coremail、django、drools、goby、Jenkins、joomla、Wiki、nginx、odoo、phpmyadmin、shiro、struts2、thinkphp、tomcat、webmin、VPN、weblogic、wildfly、wordpress 等主流应用系统的蜜罐。
	2、支持定制化蜜罐，包括中高交互应用类、低交互协议类、web 类以及数据库类；支持协议的端口自定义；支持自定义 web 蜜罐，用户支持配置端口、页面与标签页标题、标签页图标、页面 logo、页面背景图片、版权描述 web 仿真蜜罐；支持上传 zip 包进行 web 自定义仿真；支持数据库的数据信息自定义；

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

	3、支持操作系统类仿真，包括 centos、Debian、Redhat、Ubuntu、Windows11、统信 UOS、深度、中标麒麟、银河麒麟；
	4、具备攻击回放功能，支持基于 ATT&CK 的攻击事件回放，展示重点攻击手法及事件，同时展现攻击者对于不同蜜罐的具体攻击阶段，从持续时间、目的蜜罐、攻击阶段、攻击源、总计次数等维度进行展示；
	5、具备引流功能，支持将攻击流量引入蜜罐，并隔离攻击流量。
	6、支持管理功能，支持批量创建仿真诱捕主机，创建蜜罐时还可通过基于主动探测生成探测结果，并创建对应指纹模拟蜜罐。
	7、支持网络攻击预警，并记录攻击来源、行为、攻击报文、攻击持续时间、攻击阶段等关键信息。支持查看攻击源 IP、目的 IP、目的蜜罐、攻击次数、攻击阶段、持续时间、攻击时间范围的展示，同时支持攻击溯源反制相关信息以及捕获样本数量的展示，并支持下钻跳转至攻击者画像、溯源信息、反制信息、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。
	8、支持监控和记录攻击行为的网络数据包，支持针对攻击者会话的原始 Pcap 包下载；
	9、支持统计入侵次数、攻击流量、攻击趋势图、攻击分类统计等信息；支持查看攻击事件、首次出现 IP、持续攻击 IP 及次数、攻击源 IP、密码爆破记录的 TOP5，清晰定位攻击。
	10、支持黑名单、白名单配置，对于白名单内的 IP 不记录告警。
产品使用环境	1、工作温度 0℃~40℃

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

	2、存储温度-40℃~70℃
	3、工作相对湿度 20%~80%
	4、存储相对湿度 10%~90%
产品配套资料	产品可安装在 19 英寸标准机架，提供安装套件。
	提供纸质或电子版本的操作手册等技术资料。

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