

★完全公开



奇安信网神攻击诱捕系统

V1.0.2.3

产品彩页

地址：北京市西城区西直门外南路26号院1号

邮编：100044

1 产品概述

1.1 产品简介

在 Gartner 2020 年安全运营技术成熟度曲线报告中，分析师将“欺骗平台”这项技术放在了“期望膨胀期”，并将目前的成熟度定义为“青春期”，预计该技术会在 5 至 10 年后达到成熟并被广泛使用。护网和实战化攻防检测中证明了诱捕技术是一项极具价值的主动威胁检测技术，国际咨询机构 Gartner 的预测是 2019-2024 年的复合增长率超过 19%，全球市场规模每年超过 20 亿美金，并且保持快速增长的态势。国内市场正在起势，运营商已经开始集采，金融行业作为标配。

奇安信网神攻击诱捕系统通过主动流量牵引、攻击流量的识别、应答、攻击反制等策略构建主动的防御模式，制造了一个网络中尽是漏洞和攻击目标的假象，从而达到使攻击者疲于甄别真正的攻击目标而无法成功攻击的目的。攻击诱捕系统独创攻击流量牵引、应答、分发的重大特性，解决传统蜜罐产品诱捕效果不佳、业务仿真成本极高、攻防对抗能力不足、游离于企业防御体系之外等问题，改变了蜜罐产品的现状。

奇安信网神攻击诱捕系统是天眼产品被动威胁检测到主动威胁防御的有效补充，极大的补充了实战化和护网防护产品和解决方案的能力，也是天眼威胁检测的主动防御场景的补充。

1.2 产品规格及定位

1.2.1 产品规格

产品型号 关键指标	TSS10000-HP-D57 型号	TSS10000-HP-D3000-WS 型号	TSS10000-HP-D5000-WS 型号	TSS10000-HP-D5000-HG 型号
CPU	Intel 4214 主频 2.20 GHz 内核数 12*2	Intel 4314 主 频 2.20 GHz 内 核数 16	Intel 4314 主 频 2.20 GHz 内 核数 16*2	国产化 CPU: Hygon 5380 主 频 2.20 GHz 内核数 16*2

内存	128G	64G	128G	128G
操作系统	Cent OS	Cent OS	Cent OS	国产化麒麟操作系统
接口	4×1GE 管理口 (电)	4×1GE 管理口 (电)	4×1GE 管理口 (电)	4×1GE 管理口 (电) 2 个 USB 1 个管理口
存储	960GB SSD + 4TB SATA	960GB SSD + 4TB SATA	960GB SSD + 4TB SATA	960GB SSD + 4TB SATA
蜜罐沙箱种类	25	10	30	30
蜜罐沙箱数量	10	5	15	15
性能	低交互实例 ≥ 60 个 中交互实例 ≥ 30 个 低交互实例 ≥ 15 个	低交互实例 ≥ 40 个 中交互实例 ≥ 20 个 低交互实例 ≥ 10 个	低交互实例 ≥ 80 个 中交互实例 ≥ 40 个 低交互实例 ≥ 20 个	低交互实例 ≥ 80 个 中交互实例 ≥ 40 个 低交互实例 ≥ 20 个
尺寸	2U 机箱, 尺寸: 宽 (435mm) / 高 (87mm) / 长 (779.5mm)	2U 机箱, 尺寸: 宽 (478.8mm) / 高 (87mm) / 长 (811.7mm)	2U 机箱, 尺寸: 宽 (478.8mm) / 高 (87mm) / 长 (811.7mm)	2U 机箱, 尺寸: 宽 (482mm) / 高 (87.8mm) / 长 (760.5mm)
电源	AC 220V 550w, 冗余电源	AC 220V 800w, 冗余电源	AC 220V 800w, 冗余电源	AC 220V 550w, 冗余电源

1.2.2 攻击流量的识别和牵引

传统蜜罐依赖诱饵探针对流量进行被动捕获, 处于静默状态等待攻击进入蜜罐, 然后在罐内对攻击行为进行审计。因此, 对于传统的蜜罐、探针或者诱饵来说, 如果希望攻击者能够触碰, 要达到预期的诱捕效果, 必须保证足够的覆盖率, 此种理念限制了传统蜜罐的发展, 投入的资源 and 攻击诱捕的效果不成正比, 当到达一个临界点后, 无论再增加多少的诱饵探针或者仿真实例, 对诱捕率的提升都极其有限, 使传统蜜罐产品提供方和使用方都陷入困境。奇安信网神攻击诱捕系

统除了具备传统的被动捕获的能力外，支持引流策略的管理，支持引流防御，可将访问真实业务系统的流量引流到仿真蜜罐，使攻击无法命中真实业务系统。还可以通过主动流量牵引器，能够实现根据攻击特征或其他规则对某些特定的流量进行主动、智能化的牵引，在不增加蜜罐部署率的情况下，极大的提升的攻击诱捕系统的捕获效果，解决了传统蜜罐高投入、低产出的困境。

1.2.3 高仿资产的自动生成

仿真环境或者诱饵的仿真性，直接影响蜜罐的成效，蜜罐在部署期需要对用户的业务系统进行调研，根据业务系统重要性、仿真的工作量，必要性等维度挑选出需要仿真的系统，协议类型将不同的攻击流量引入不同的蜜罐实例，然后蜜罐的供应商会投入人力对需要仿真的系统进行定制化，这个过程非常耗时，且成本较高。奇安信网神攻击诱捕系统内置了大量基于各类网络资产和应用制作的仿真蜜罐，并支持低成本的自定义仿真，降低了蜜罐系统对仿真的依赖的同时也降低了蜜罐系统的部署成本和运维成本。

1.2.4 协同防御

攻击诱捕系统是企业纵深防御、协同防御中极其重要的环节，传统蜜罐非常依赖于罐内行为的审计能力，容易游离在企业的防御体系之外，如果长时间没有明显的诱捕效果，极有可能在企业的安全体系中被边缘化。奇安信网神攻击诱捕系统不仅在系统层面集成了天眼的实战化能力，对宿主机及虚拟机进行全方位安全监控，检测容器层面的恶意程序逃逸行为，保证蜜罐系统整体安全。利用流量数据对 HTTP 等协议数据进行回放，还能和企业已经部署的天眼的流量传感器和分析平台进行联动，实现整体的协同，对天眼的未知威胁的检测能力是极大的补充。

1.3 产品形态及构架

奇安信网神攻击诱捕系统产品功能架构如下：

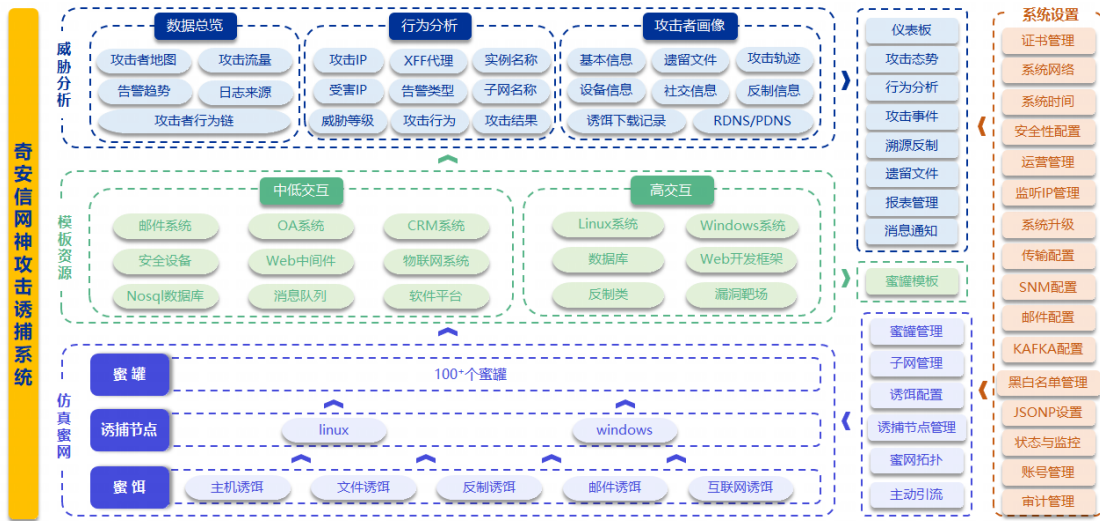


图 1 产品架构图

攻击诱捕系统分为了仿真蜜网、模板资源、威胁分析和系统设置。

仿真蜜网：由蜜饵、诱捕节点、蜜罐共同构成，其中蜜饵包括了：主机诱饵、文件诱饵、反制诱饵、邮件诱饵和互联网诱饵；诱捕节点可以部署在 Linux 操作系统和 Windows 操作系统的客户端中；系统也支持构建多个蜜罐实例。

模板资源：系统内置了 100+的蜜罐模板供用户构建蜜罐，以高中低三种交互方式展示在蜜罐模板中，支持 IPV4 和 IPV6 协议。

当用户完成蜜罐构建、部署诱捕节点、布撒蜜饵后，系统能够实现欺骗伪装的效果，贴合真实环境的仿真蜜网，大大提升欺骗环境的复杂性和真实性。

威胁分析：当攻击者被诱导至蜜网中进行嗅探和扩展时，系统就可以更全面的感知威胁、溯源信息、反制攻击者。通过“灵境”实现威胁分析，仪表盘上的攻击者地图、攻击者行为链等展示告警数据总览，行为分析上的攻击 IP、受害 IP 和实例名称等记录攻击行为，攻击事件中将遗留文件、设备信息、攻击轨迹、社交信息等汇总描绘形成攻击者画像，对攻击者的威胁标签分析，判断是否有 APT 攻击、勒索攻击、挖矿行为。

系统设置：由证书管理、系统网络、系统时间、系统升级、黑白名单管理、账号管理、审计管理等模块共同组成，方便用户可视化管理系统的基础设置。

2 产品功能

2.1 主动流量牵引

基于 SDN 技术的网络编排和天眼的实时威胁检测能力，对链路中指定威胁流量牵引至目标蜜罐及蜜网。流量牵引工作在网络层，不破坏攻击 IP 与受害 IP 间的联网结构，引流的白名单，包括对源 IP、目的 IP、域名的过滤。

攻击 IP 在扫描或渗透真实受害 IP 过程中，支持自动策略和手动策略，自动策略模式下支持和流量检测分析设备进行联动，将指定告警类型告警流量引入到蜜罐系统中。手动策略可以配置需要引流的源 IP 和目的 IP，天眼检测到威胁行为，触发 SDN 联动，对目的 IP 进行主动爬取，并对爬取后的页面进行了自动化的容错处理，包括对资源的引用问题等。实时牵引后续威胁流量至指定蜜罐及蜜网，网络牵引过程对于攻击者无感，有效的解决了直接暴漏蜜罐给攻击者欺骗能力不足的问题。

2.2 多设备仿真

信息收集是实战化攻防中必不可少的一步，如何在信息收集这步实现“诱敌深入”，模拟和仿真多种设备是一种重要方法。

从蜜罐产品实现的角度来看，如何尽可能多的仿真各类网络设备是共同的难点。我们结合云端大数据收集的数百种协议构建了设备指纹（banner）库。

通过模版的方式导入蜜罐模版，可以配置蜜罐模版名称、服务名称、端口，类型，包括高交互蜜罐、中交互蜜罐和低交互蜜罐。提供多种取证技术手段，还原黑客攻击入侵蜜罐的过程，形成黑客攻击链；

多设备仿真的目的在于如何欺骗攻击链的侦察阶段，或者说攻击者的信息收集阶段。针对攻击者的一些自动化的工具探测（如 Nmap 的端口扫描）可以较好的进行欺骗，提供 HTTP 攻击流量进行诱骗，涵盖的 Web 攻击类型包括：文件读取、目录遍历、命令执行、代码执行、SQL 注入、XSS 等能够欺骗过工具扫描行为。将攻击行为沿着攻击链向前推进并停留在平台内，是多设备仿真的初衷。多设备蜜罐会自动将该攻击 IP 引到漏洞靶场或开源蜜罐，进行后续的高交互操作。

2.3 场景化攻击反制

对于步入攻击诱捕系统的攻击者，提供反制技术，可对攻击进行精准有效的反制，支持浏览器漏洞反制技术，获取攻击者信息如果能对他们进行一定程度的反制，那么这也是实战化攻防演练的加分项。攻击反制的方法有很多，奇安信攻击诱捕系统支持包括但不限于通过 JSONP 反制、文件下载欺骗反制、MySQL 反制等多种反制手段。攻击反制可以获取的信息，包括但不限于攻击者的桌面截图、文件目录、浏览器指纹、主机账号、主机 IP 及端口开放情况、个人应用账号等等。我们可以通过升级的方式来更新反制策略并不断增强。系统内置的交互反制 exe 文件可以直接反制攻击者的电脑进行远程控制，同时在特殊期间也会可以提供加载 Shellcode 用于用户上传的反制文件进行远程控制的方式。

2.4 实战化漏洞靶场

内置多种漏洞靶场环境或重点应用系统。结合实战化攻防演练经验，对攻击队关注的且可能存在 0day 或 Nday 漏洞的重点应用，对漏洞使用的攻击诱捕，包括对已知漏洞、未知漏洞利用的完整攻击行为事件、系统、CMS 或网络设备等进行虚拟化安装，让攻击队误以为是真实的系统，内置常见漏洞的靶场，包含 weblogic、Struts2、tomcat、thinkphp 等。

2.5 安全设备联动

攻击诱捕系统提供开放接口，实现对接联调，支持与天眼流量传感器、天眼分析平台分析进行联动，推动企业的防御体系从积极防御向进攻防御演进。

- (一) 天眼流量传感器：设备部署方式为主动引流时，需要与天眼流量传感器联动使用，基于天眼流量传感器侧的告警日志下发主动引流策略。
- (二) 天堤流量传感器：设备部署方式为主动引流时，需要与天堤流量传感器联动使用，基于天堤流量传感器侧的告警日志下发主动引流策略。
- (三) 天眼分析平台：攻击诱捕系统支持将威胁告警发送到天眼分析平台上，

方便告警日志集中管理。

- (四) 天眼文件威胁鉴定器：攻击诱捕系统支持将攻击者遗留在蜜罐沙箱中的文件发送至天眼文件威胁鉴定器进行文件鉴定，并接收文件鉴定结果展示在【威胁感知】-【遗留文件】和攻击者画像中。