欺骗防御与威胁感知系统

产品简介

产品文档

腾讯云

文档目录

产品简介
产品概述

最近更新时间：2019-07-16 14:45:01

欺骗防御与威胁感知系统（Deception Defense And Threat Awareness System，DDTA），在企业内部网络中部署与真实环境类似的"诱饵"，主动诱导攻击者进入由蜜网构成的高度仿真的虚拟环境中，通过网络流量分析、自动化主机行为检测、虚拟网络仿真等技术，实现攻击发现、攻击报警、攻击隔离、攻击分析、攻击溯源、攻击延迟、攻击反制等功能。

产品功能

高价值资产伪装

在用户真实的操作系统环境中，配置高仿真的系统服务、Web 应用、脱敏数据等资产（根据内网环境添加和真实资产类似的信息，提供灵活的自定义蜜罐），深度融入内网环境，使伪装更具有迷惑性。

威胁事件感知

通过蜜罐节点实时监听已部署探针的机器，从多个维度实时感知威胁。当探测到入侵行为时，实时记录攻击事件，并将不同维度的威胁事件统一，形成完整的攻击链，实现对威胁的完整感知和溯源。

攻击欺骗转移

蜜网采用弱安全蜜罐（主动配置有安全缺陷的环境），并在用户内网环境中配置蜜标，主动诱导攻击者攻击蜜罐。同时在蜜网环境配置脱敏的价值信息，最大限度诱惑攻击者，使之将大量的时间精力投入到对高仿真环境的渗透分析中，从而延缓对真实环境的破坏，为用户获取宝贵的安全响应时间。

产品优势

最近更新时间：2019-07-16 14:45:46

多维度纵深感知

腾讯安全团队利用近10年来对样本攻防和渗透攻防经验的积累，在恶意攻击整个流程的每一步“埋点”，实现层层设点，层层包围。同时从攻击链的视角，多维监控，让攻击者无所遁形。

高度仿真蜜网

蜜网通过配置高度仿真系统服务、Web 应用、脱敏数据等资产，构建真实可变的蜜网环境，支持各种复杂场景的模拟，同时为用户提供灵活的自定义蜜罐，深度融入用户内网环境，使伪装更具迷惑性。

高度安全性

欺骗防御与威胁感知系统通过内网蜜标诱导+前端探针引流+后端蜜罐感知技术，在实现高度仿真的同时，实现蜜网和用户内网资产的高度隔离。内部从网络隔离、环境隔离、流量单向控制、IP 控制等各个维度配置了安全防护系统，保证系统自身不被攻击者识别和破坏，避免发生跳板攻击行为。

协同防御支持

欺骗防御与威胁感知系统捕获的攻击数据，可以作为威胁情报输出，其它安全产品或者安全系统通过流通输出的数据，增强用户原有安全体系的防护能力。

高精度安全告警

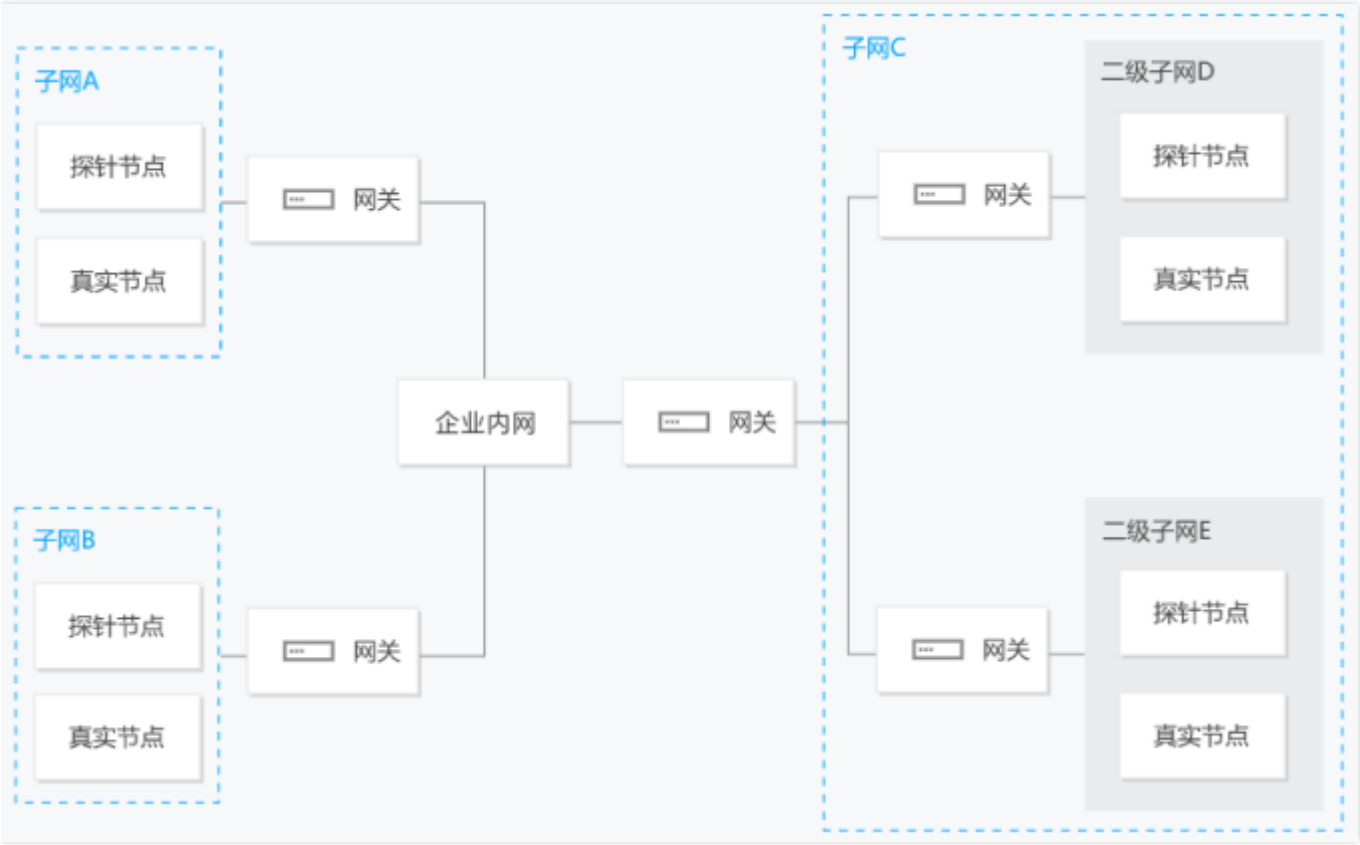
基于欺骗防御技术，欺骗防御与威胁感知系统可及时发现攻击行为，做到报警即发现。报警日志中不掺杂任何业务数据，可以极大降低安全运营的成本。

应用场景

最近更新时间：2019-07-16 14:45:58

强化威胁感知能力

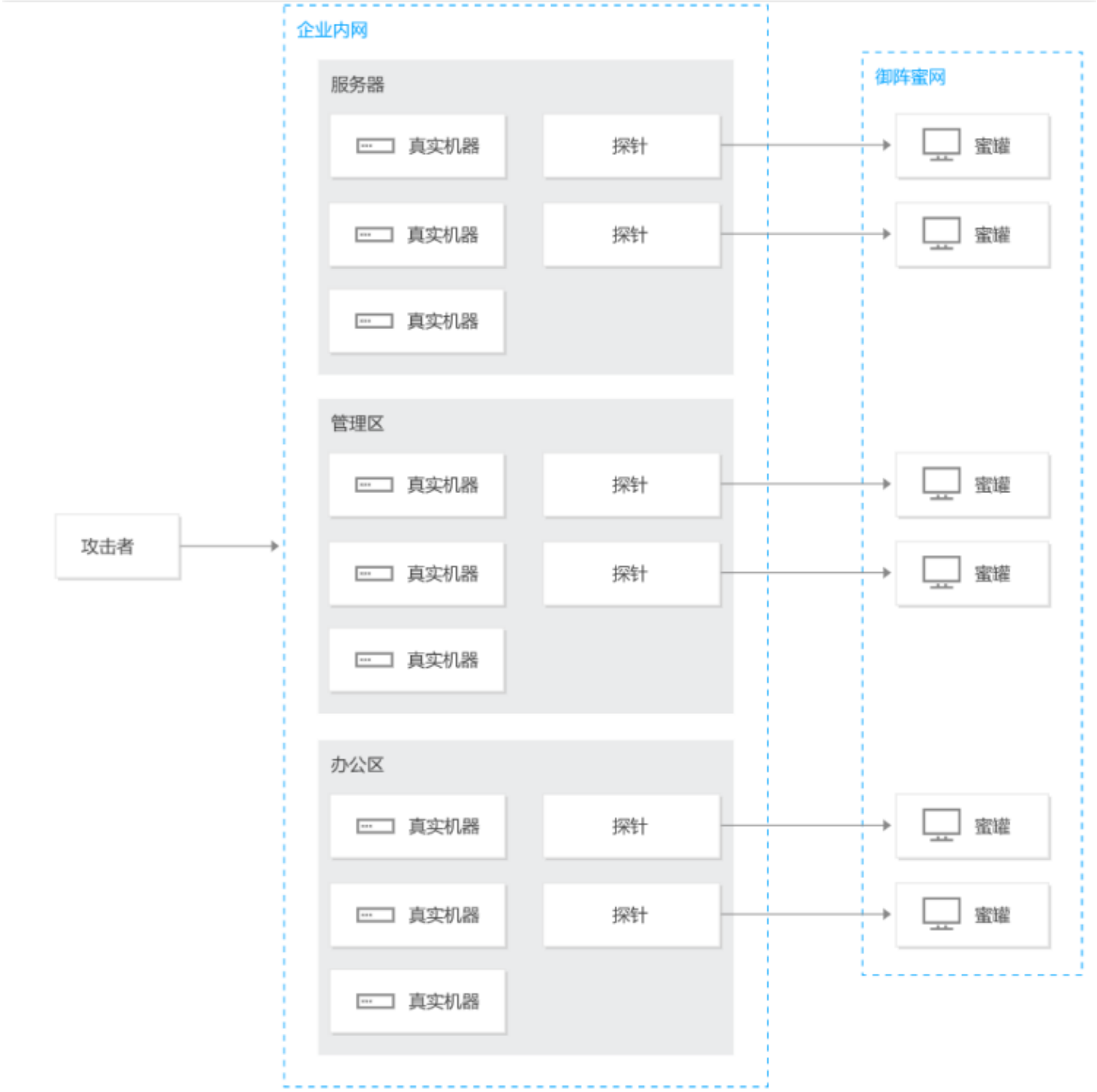
欺骗防御与威胁感知系统打破了传统安全产品基于边界或点的防护思路，将安全防护从点扩散到面。以蜜网为主体，通过探针部署的方式，将威胁感知能力映射到内网的每一个网段及每一台机器，在内部组成一个与真实业务高度融合的巨大威胁感知网络，低成本覆盖到每一个角落。



攻击欺骗转移

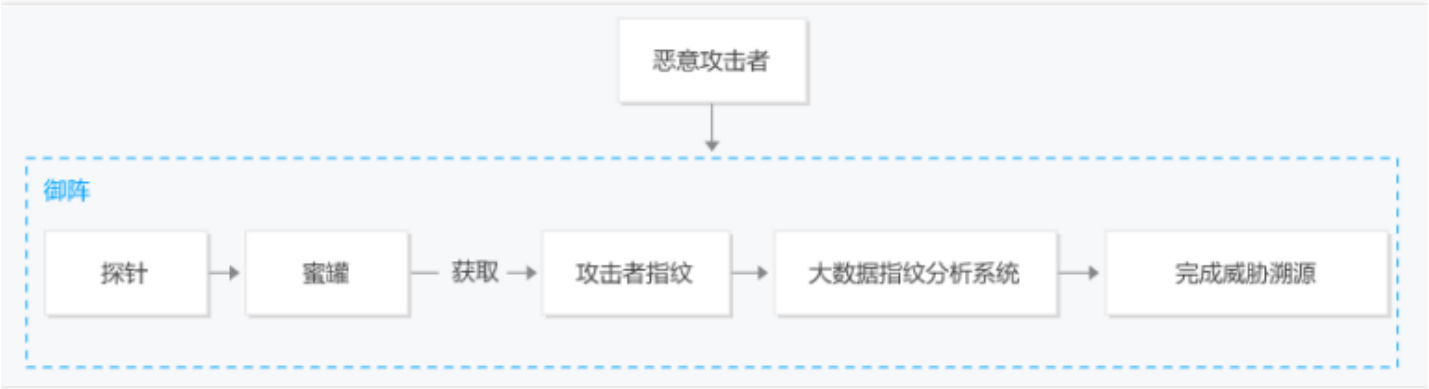
欺骗防御与威胁感知系统在蜜网中配置高度仿真的用户资产，并通过部署探针的方式深度融入真实环境中，干扰攻击者对攻击路径的判断，将攻击流量转移至蜜网中，延缓入侵者对真实环境的破坏，为用户赢得宝贵的应急响应时

间。



攻击者行为溯源

当欺骗防御与威胁感知系统探测到入侵行为时，将攻击事件实时记录，并将各维度的威胁事件统一，形成完整的攻击链。通过基于大数据的设备指纹系统分析攻击链，实现对威胁的完整溯源。


恶意攻击者
御阵
探针
蜜罐
获取
攻击者指纹
大数据指纹分析系统
完成威胁溯源