欺骗防御与威胁感知系统

常见问题

产品文档

腾讯云

常见问题

最近更新时间：2019-07-16 14:46:29

什么是欺骗防御？

让入侵者相信内网中存在有价值且可利用的安全弱点，并具有值得攻击窃取的资源（伪造的或不重要的），从而将入侵者引向这些蜜标。允许防护者跟踪入侵者的行为，在入侵者入侵窃取重要信息之前修补系统可能存在的安全漏洞。

在真实环境中，如何诱导攻击者攻击蜜罐？

- 蜜罐上会部署一些弱安全的服务，例如弱口令或者漏洞，来吸引攻击者攻击。
- 在攻击者容易发现的地方放置蜜标，例如账号密码，证书等等。

蜜罐如何感知恶意攻击？

蜜罐通过监控攻击者的网络流量和进入蜜罐后的异常行为，来获取攻击者。

探针可以部署在哪些系统上?

探针可以部署在任意系统，包括但不限于 Windows、Ubuntu、Centos、Macos。

部署探针是否会存在安全隐患？

探针在部署机器上只起到代理作用，用于流量转发，攻击者无法对部署机器进行任何操作，可以保证部署机器的安全性。基于 SSL 加密的探针和中控交互，可以保证通信的安全性。

如何部署蜜罐？

蜜罐高度集成在御阵中心，蜜罐无法直接和用户环境通信，与外部环境通信需要通过欺骗防御与威胁感知系统中心配置。

客户内网环境中每个区域建议部署多少探针？

探针的数量不受蜜罐数量限制，可以实现多对一，建议机器与探针的比例是3：1，3台机器可以部署1个探针。该比例可以保证欺骗防御与威胁感知系统对内网节点的全面覆盖。

如何实现探针的最佳部署？

- 根据探针与蜜罐的绑定与选择，可以有针对性地部署探针。欺骗防御与威胁感知系统分为两种蜜罐，报警蜜罐和主机蜜罐，报警蜜罐成本低，方便扩容，主机蜜罐成本高，但是可以实现对攻击数据的细粒度感知。
- 针对公司的核心资产区（如数据，运维区域），可以多部署主机蜜罐，并在不同区域绑定不同蜜罐。例如在数据区、生产资料区，可以多绑定数据库蜜罐和中间件蜜罐。在办公区，可以多绑定 Windows 系统蜜罐。在服务器区，多部署 Linux 系统蜜罐。
- 非重要区域可以多部署报警蜜罐，在节省成本的同时，做到对内网的全覆盖。

欺骗防御与威胁感知系统如何收费？

目前处于内测阶段，用户 申请试用 并通过审核后可以获得试用权限，具体说明请参见 购买指南。