ABT·安博通

看透安全 体验价值

4D攻击面可视化

解决方案

方案背景

近年来，网络安全事件频发，国际网络环境异常严峻。2017年勒索病毒“永恒之蓝”（WannaCry）全球大爆发，至少150个国家、30万名用户中招，造成损失达80亿美元，影响到金融、能源、医疗等众多行业，造成严重的危机管理问题。面对异常严峻的网络威胁形势，安全团队秉持着“深度防御”的策略进行安全体系建设，往往却变成了“深度消耗”。为了盲目的阻挡未知安全威胁，越来越多的设备和软件被一层一层的叠加起来，让网络结构变得一团糟。这不仅会使安全建设成本直线上升，更会使运维团队不堪重负。为了更好的保护特定数据和业务主机，企业需要更加合理高效的安全管理解决方案。

问题分析

知己不清

运维团队对自身网络了解不深，面对安全威胁无从着手，具体表现为：

- 核心数据定位不清，无法针对核心数据进行重点监控；
- 业务主机状态不清，无法保障业务系统自身安全运行；
- 网络访问路径不清，难以保障对数据与业务实施严格的访问控制；
- 用户访问行为不清，难以做到对全网用户的流量记录与深度分析。

知敌不明

安全漏洞披露的速度越来越快，基于新型漏洞的网络攻击让传统基于已知特征的防护手段束手无策。

网络攻击变得越来越专业化，攻击手段不再是单纯通过某一漏洞或技术手段实现，而是多种攻击手段复杂叠加形成的APT攻击，网络攻击表面上变得“合理化”。

目标不聚

越来越严峻的安全威胁形势催生了大量的安全产品，安全团队盲目追求对未知威胁的防护，不断在网络上叠加各种安全产品，让网络变得越来越复杂，也让自己疲于安全运维，在这个过程中迷失掉了真正的安全防护目标。

解决方案

4D攻击面可视化解决方案以可视化技术为支撑，以路径安全可视、主机安全可视、流量安全可视、数据安全可视4个维度的可视化分析为主要手段，让安全团队看清、看全网络威胁与网络攻击面，在网络攻防战中做到知己知彼。

路径安全可视

基于安全控制策略数据进行网络安全基础架构建模，分析、优化安全控制策略质量，避免策略漏洞带来的安全风险，同时监管全网的安全控制策略与业务访问路径，构造并持续维护明晰的网络安全作战路径图。

主机安全可视

围绕资产清点、风险分析、入侵监控三个方面对业务主机的安全状态进行深入的分析，根据操作系统和系统内业务的不同，自动识别不同操作系统内的关键业务服务和组件情况，周期性清点系统、中间件、进程、端口、网站、账号等资产信息，并针对各类资产进行脆弱性分析与基于行为模式的异常入侵行为监测。

流量安全可视

采集网络链路层全流量数据，全面记录网络内用户的网络行为，按字段对海量原始数据包进行解析与可视化呈现，为安全团队提供由浅及深的用户行为分析，辅以机器学习技术，即时感知异常用户行为与网络攻击事件，做到对网络异常的事中发现与事后溯源。

数据安全可视

以智能化的内容识别核心技术，对企业网络、终端、存储和应用系统中的敏感数据进行发现、监控和保护，做到敏感数据全网分布的可视、敏感数据泄露风险的可视、数据安全实现可视化呈现以及敏感数据泄露趋势的可视。

方案亮点

方案价值

网络攻击面全面清点

通过路径可视化与主机安全可视化清点内网中存在的恶意人员用来实施攻击的攻击面，认清自身状态。

网络攻击指标综合评估

综合业务访问路径与主机脆弱性进行风险评估，提供最优成本的安全防护方案，对安全威胁实施快速响应。

网络行为实时监控

通过全流量数据监控用户行为与核心数据走向，对复杂APT攻击和未知威胁提前感知。

ABT·安博通
看透安全 体验价值
北京安博通科技股份有限公司
营销中心：北京市西城区裕民路18号北环中心2602室
电话：010-80699886
研发中心：北京市海淀区上地中关村软件园二期15号楼3层
电话：010-57649050
www.abtnetworks.com