深信服全网安全感知平台方案

2017-06-01

深信服全网安全感知平台方案

网络安全现状

根据Verizon的全球安全事件调查报告显示，不计算前期侦察与信息获取的过程，攻击者从实施攻击到入侵得手仅需要花费数小时的时间。但是62%时间才能发现黑客攻击，随后还需要数天至数周的时间完成响应和补救工作。

在Mandiant最新的高级安全威胁报告中指出，企业或组织需要发现潜藏攻击者的平均时间为229天，更为严重的是，仅有33%的企业或组织是自行发构通报、曝露在暗网甚至是互联网上以后才被发现。

Ponemon Institute针对全球252个机构的1928起攻击事件的统计发现，攻击事件的平均解决时间为46天，而每延迟发现和解决攻击事件一天的成本机构Gartner更是大胆指出，到2020年，企业安全部门应该将60%的预算投资到安全检测与响应中来，以应对日趋复杂的网络安全环境。

深信服认为，企业和组织对自身业务及其对应的安全威胁的感知与发现能力不足，是网络安全问题不断、安全响应和处置严重滞后的关键短板。

深信服安全感知平台方案

深信服安全感知平台方案是一套基于行为和关联分析技术对全网的流量进行安全检测的可视化预警检测平台。方案设计体现适用性、前瞻性、可行性可视化。主要有以下技术特点：

看清业务

1、对业务系统核心资产进行识别，梳理用户与资产的访问关系；

2、对业务资产存在的脆弱性进行持续检测，及时发现业务上线以及更新产生的漏洞及安全隐患；

3、通过业务识别引擎主动识别新增业务资产以及业务访问关系；

看见内网潜在威胁

4、对绕过边界防御的进入到内网的攻击进行检测，以弥补静态防御的不足；

5、对内部重要业务资产已发生的安全事件进行持续检测，第一时间发现已发生的安全事件；

6、对内部用户、业务资产的异常行为进行持续的检测，发现潜在风险以降低可能的损失；

7、将全网的风险进行可视化的呈现，看到全网的风险以实现有效的安全处置。

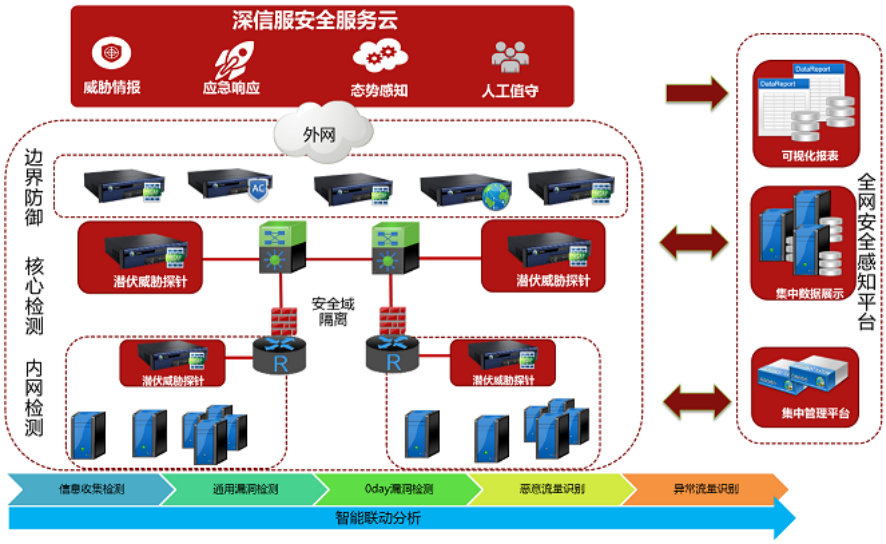
方案架构

通过潜伏威胁探针、全网安全感知可视化平台、深信服安全服务云平台构成持续检测快速响应的技术架构：

■· **潜伏威胁探针**：在核心交换层与内部安全域部署潜伏威胁探针，通过网络流量镜像在内部对用户到业务资产、业务的访问关系进行识别，基别、违规行为检测与内网异常行为识别。

■· **安全感知平台**：在内网部署安全感知平台全网检测系统对各节点安全检测探针的数据进行收集，并通过可视化的形式为用户呈现内网业务资胁；并通过该平台对现网所有安全系统进行统一管理和策略下发。

深信服安全服务云：通过深信服云平台，提供未知威胁、威胁情报、在线咨询、快速响应等安全服务。

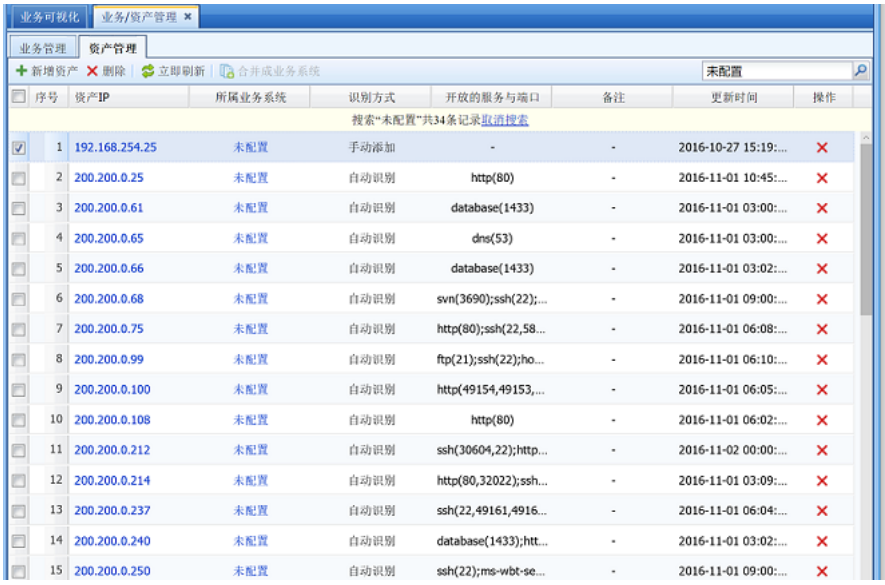


安全感知平台方案特性

■· 全网业务资产可视化

主动识别资产：通过安全检测探针可主动识别业务系统下属的所有业务资产，可主动发现新增资产，实现全网业务资产的有效识别；

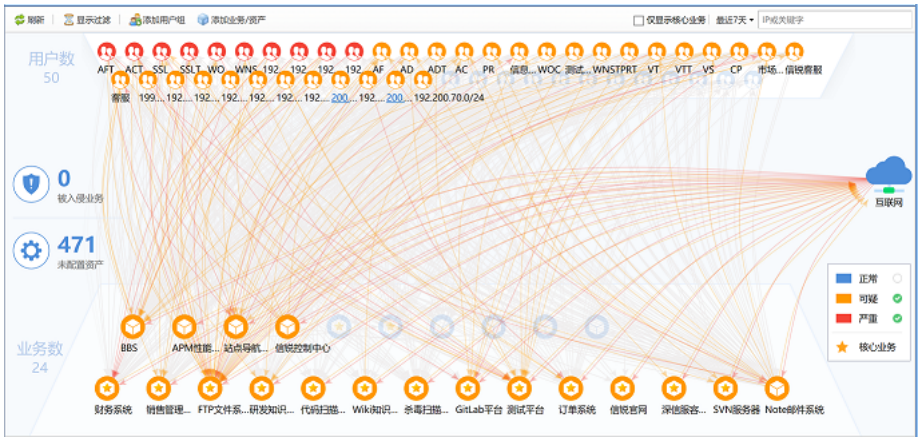
资产暴露面可视化：将已识别的资产进行安全评估，将资产的配置信息与暴露面进行呈现，包括开放的端口、可登录的web后台等。



■· 全网业务访问关系可视化

业务系统访问关系：通过访问关系学习展示用户、业务系统、互联网之间访问关系，通过颜色区分不同危险等级用户、业务系统，可视化的呈现以证

业务系统应用及流量可视化：业务系统的应用、流量、会话数进行可视化的呈现，并提供流量趋势分析。



■· 内部攻击可视化

内部横向攻击行为检测：对越过边界防护，或以内部主机为跳板的横向攻击，进行实时检测与报警，包括对内扫描、对内利用漏洞进行病毒传播、对

■· 违规操作可视化

违规访问行为检测：结合全网的资产及访问关系可视，将违规访问业务系统的行为进行可视化的呈现，防止进一步可能存在的攻击，并向管理员预警

■· 异常行为可视化

业务资产异常行为检测：包括业务资产在非正常时间主动发起的请求、业务主动向外发起非正常请求（如DNS请求）等异常行为预警可能存在的安全

潜在风险的访问路径：将可能失陷的终端对业务系统的访问路径、存在异常流量及行为的终端/服务器的访问路径进行预警，帮助管理员及时响应安

■· 全网安全态势感知

整体安全态势：结合攻击趋势、有效攻击、业务资产脆弱性对全网安全态势进行整体评价，以业务系统的视角进行呈现，可有效的把握整体安全态势

全网态势感知：展示内网服务器被外网攻击的实时动态图，实现全网安全攻击态势大屏展示；

有效的攻击事件：通过旁路镜像的方式可将攻击回包状态进行完整的检测，结合业务系统的漏洞信息，可以识别攻击成功的有效安全事件；

失陷业务系统/资产：通过外发异常流量、网页篡改监测、黑链检测等检测技术确定业务系统/资产是否已被攻击，并将资产存在的后门进行检测，并

安全事件关联分析：将下一代防火墙及安全检测探针的安全事件进行关联分析，结合黑客攻击链进行关联分析，并确定更加高级的安全威胁。

我们在客户全网发现的攻击

非法接入数据库

潜伏威胁探针识别出公司的数据库服务器正在接受来自办公区一台电脑的频繁访问，该电脑并没有接入数据库的业务需求。潜伏威胁探针的分析结果显示关键数据和数据库结构的非法访问是内网遭受攻击的一个明显信号。

内网端口扫描

潜伏威胁探针发现公司内网的一台电脑正在向内网IP段进行端口扫描，似乎在侦测内网特定服务端口。这台电脑是一台苹果电脑，但是安装了旧版本的W常工作不需要进行端口扫描操作。最终发现该电脑已经被黑客控制，并在进行进一步渗透前的侦测行为。

异常内部文件传输

在分支机构的其中一台电脑从共享空间上持续下载了1GB的共享文件，从过往的行为模型看该用户间或会从共享文件夹下载文件，而如此大的下载量是首合法接入权限。

勒索软件感染

某天早上公司一位内网用户访问了一个归类为恶意链接的网站，从该网站下载的可执行文件绕过了边界防病毒引擎和沙箱的检测。几小时后，潜伏威胁探网络共享的文件系统进行大量的读写操作，稍后的响应和取证证实该用户遭受了勒索软件的攻击。

与僵尸网络相关的远程控制接入流量

潜伏威胁探针发现网络中其中一台电脑正在使用远程接入工具（RAT），而该工具与知名的僵尸网络Zeus相关。很明显这是一个僵尸网络中毒事件。Zeus是账号及信用卡信息。该病毒通过变种、加壳、rootkit、沙箱逃逸的方式躲过了众多边界防御措施。然后潜伏威胁探针通过全网行为异常监控发现了这一僵

上一篇：无