未知威胁发现方案

客户场景

在安全形势不断恶化的今天，众多企业经常面临网络攻击的威胁，虽然企业的安全管理人员已经在网络中的各个位置部署了大量的安全设备但仍然会有部分威胁绕过所有防护直达企业内部，对重要数据资产造成泄漏、损坏或篡改等严重损失。

此类威胁即包含黑色产业链驱动的高级攻击，也包含了国家驱动的APT攻击。由于这些攻击均会使用高级免杀技术以逃避传统安全设备的征检测，并寻找内部人员的安全意识薄弱环节进行社会工程学攻击，所以可以屡屡得手、很难被发现。而由于此类攻击往往具有明确的攻击目的，其对企业和单位所造成的危害也是直接而巨大的。

在这种形势下，企业和各级单位均需要一套行之有效的未知威胁检测方案来对内网已经发生或正在发生的高级攻击事件进行发现和回溯。

解决方案

360天眼新一代威胁感知系统（以下简称“天眼”）可基于360自有的多维度海量互联网数据，进行自动化挖掘与云端关联分析，提前洞悉各种安全威胁，并向客户推送定制的专属威胁报。同时结合部署在客户本地的软、硬件设备，360天眼能够对未知威胁的恶意行为实现早期的快速发现，并可对受害目标及攻击源头进行精准定位，最终达到对入侵途径及攻击者背景的研判与溯源.

1、云端情报

360基于云端海量的网络基础数据和样本文件数据，通过数据挖掘、机器学习等人工智能算法和持续的安全专家运营对互联网内每天新增的新型木马、流行木马甚至是APT攻击进行发现和跟踪，并对攻击发生的背景和源头进行挖掘。所有分析结果都将以威胁情报的形式单向推送至企业客户。

2、本地分析

360天眼可通过一整套硬件系统对企业网络中的流量进行全量检测和记录，所有网络行为都将以标准化的格式保存于天眼的数据平台，并可结合360云端发现的威胁情报对企业内网已经发生和正在发生的未知威胁进行发现。同时本地文件威胁鉴定器可以通过多种静态引擎和动态引擎对流量传感器还原后的文件进行威胁鉴定，可有效检测在网络内传输的恶意文件。

3、攻击回溯

利用云端丰富的实时威胁情报和企业本地的翔实网络行为，天眼系统可以为企业客户呈现一次攻击的完整情报，它将覆盖攻击的源头、手段、目标、氛围等相关信息，可对任何一个被发现的未知威胁进行快速的回溯和定性，轻松分辨APT攻击和普通网络攻击

客户价值

通过360天眼系统，客户可以轻松获得以下功能和价值

1. 首创使用互联网数据发掘APT攻击线索，提升企业对威胁看见的能力
2. 以威胁情报形式打通攻击定位、溯源与阻断多个工作环节，帮助企业从源头上解决安全问题
3. 高效的快速搜索技术帮助企业提升数据查找的能力
4. 基于大数据挖掘分析的恶意代码智能检测技术，提升了客户检测恶意代码的能力
5. 基于轻量级沙箱的未知漏洞攻击检测技术，提升了客户检测未知漏洞的能力
6. 专业的专家运营团队，全天候为企业保驾护航