态势感知与安全运营平台(NGSOC)解决方案

客户场景:

在安全形势不断恶化的今天，众多用户经常面临网络攻击的威胁，虽然用户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，但仍然会有高级威胁绕过所有传统防护直达组织网络内部，对重要数据资产进行窃取、篡改或破坏，给组织带来重大损失。即便攻击者能够得逞，也往往会在网络中留下攻击的痕迹，这样的痕迹通常就隐藏在网络的流量和各种各样的设备和系统的日志中。对流量数据和日志进行深入分析就有可能发现攻击行为、追溯攻击者。但随着网络规模和数据量越来越大，使用传统的技术手段无论是在数据采集、实时分析、数据存储与快速检索、历史数据统计、可视化展现方面都存在严重的不足，同时，传统仅依靠本地数据采集去发现攻击行为的检测手段也很难发现使用0Day、NDay漏洞的APT攻击，设备间缺乏有效联动也使得无法利用检测的结果快速响应处置，最大程度降低攻击造成的损害。如何实现更加广泛维度的海量数据采集、处理、展现，并将综合检测的结果，与快速响应处置，及深入的调查分析进行结合，形成业务闭环，成为新一代安全管理与运营的关键。

新一代的安全管理与运营需要采集用户的全量原始数据，结合云端的威胁情报，进行全方位持续监测，以及挖掘分析。这要求本地具备海量数据采集能力、存储能力、检索能力和多维度关联能力，同时需要持续获得高质量的威胁情报。大数据与威胁情报的驱动成为新的核心驱动力。利用威胁情报、安全大数据搜索、数据挖掘、自动化关联分析、统计计算、机器学习等新的技术手段，对传统手段进行革新与丰富，将成为发现本地安全威胁与异常的新利器。同时可视化分析技术也将用户内外部安全态势，进行整体的呈现，使得用户的管理者能够实时掌握用户的安全态势状况，保障业务的顺畅运行。

解决方案:

360NGSOC态势感知与安全运营平台是基于360威胁情报和本地大数据技术，对用户本地的安全大数据进行快速、自动化数据分析，全方位监测、发现威胁和异常、快速处置与响应，并针对安全事件进行深入调查的平台。同时，通过可视化技术将企业总体安全态势呈现给用户。并且能在日常的安全管理工作中提供各类工具，帮助提升安全运维效率。

在平台架构上，NGSOC分为数据采集，大数据存储与检索、数据分析引擎工具、安全应用、态势感知多个层面，再结合360多年积累的云端威胁情报，给用户的安全管理运营提供了新的“大脑”与智慧协同的平台。

NGSOC支持与多类安全产品的协同，尤其是与终端响应与检测（EDR）、网络响应与检测（NDR）的配合，拓展网络与终端的传感器，将网络流量与终端文件级、进程级数据进行汇总分析与协同响应。将威胁情报与数据的能力贯穿监测与防御体系，达到智慧协同。

客户价值:

1 威胁情报监测高级威胁

由于APT攻击的复杂性和背景的特殊性，仅依赖用户本地数据已经无法有效发现APT攻击，难以做到真正的追踪溯源。360利用强大的互联网安全数据采集能力和安全研究团队的分析能力，建成了具有很高覆盖的安全数据库，及时提供高时效威胁情报。360态势感知与安全运营平台充分利用360云端提供的威胁情报，结合本地数据，能够有效提高针对用户网络的APT攻击的检出率。

2 以数据驱动打通攻击定位、溯源与阻断多个工作环节，提升了客户对攻击回溯的能力

传统的防护体系在多台设备间进行联动往往需要通过特别开发的接口对一种或几种特殊类别的告警或信息进行分发和通知，这种设计往往会制约多种不同设备或系统之间的信息传递。同时由于对于消息接口缺乏一个系统化的规范化的描述，很难对复杂的攻击行为进行准确定义。360态势感知与安全运营平台的一大创新点在于用威胁情报的形式对各种APT攻击中常出现的特点和背景信息进行记录和传输，而威胁情报将通过统一的规范化格式将APT攻击中出现的多种攻击特征进行标准化，可满足未来扩展APT攻击特征以及后续扩展联动设备的需要。

3 使用搜索技术对企业信息进行记录和检索，提升了客户在海量数据中快速查找所需数据的能力

360态势感知与安全运营平台创新性的采用分布式搜索引擎技术作为本地数据存储和检索核心技术，极大地提高检索性能，同时相比传统架构也能够降低大量接口上的开发量。可为企业本地的大规模数据保存、攻击证据留存和查询、实时关联分析提供坚实的技术保障。

4 基于数据处理与计算分析的自动化关联技术，提升客户发现本地异常行为的能力

360态势感知与安全运营平台通过基于数据处理与计算分析的自动化关联技术自主研发的SecStream流式计算引擎，对各类数据按照预定的流程进行流式处理，保证了数据实时处理的高性能。360态势感知与安全运营平台使用SecCEP作为关联分析引擎，利用内置的多种分析规则，对数据进行多维度的关联分析，有效发现攻击行为和违规访问，降低安全预警事件的误报和漏报。

5 基于可视化技术，使得用户网内的威胁和异常清晰可见

通过可视化技术的利用，将原本碎片化的威胁告警、异常行为告警、资产管理等数据结构化，形成高维度的可视化视图，以便于用户理解。大数据的存储与实时运算能力保证了360能够实现数据的实时推送，配以可以实时交互的3D可视化界面，与其美观的3D展示效果相得益彰。可视化技术的利用使得用户可以更直观地感受到网内的安全态势，使得安全由不可见变为可见，不但带来了更好的用户体验，同时还有效地提高了安全监控的效率。

6 告警与处置中心，使安全管理工作真正做到闭环

通过高效的关联分析引擎对事件的实时分析以及利用360的威胁情报对本地采集数据的快速查寻匹配，360态势感知与安全运营平台可快速发现当前对网络的攻击行为、违规访问以

及对网络的APT攻击，发现网络中受控主机，及时产生告警，并可采取多种响应方式，既可以邮件、短信方式通知管理员采取必要措施，也可与360的防火墙产品和终端管理产品进行联动（网络检测与响应-NDR，终端检测与响应-EDR），自动阻断有害连接，终止有害进程，最大程度保护用户IT资产。

7 可视化追踪溯源，发现攻击背后的黑手

通过海量的本地数据，结合360庞大的云端安全信息数据库，利用360的海量数据检索能力和可视化展现技术，可以帮助安全分析人员对安全事件进行深入的源源分析，还原攻击的整个过程，定位安全事件背后的攻击者，为更好地抵御未来的攻击提供有效的技术支撑。