火眼金睛--态势感知攻击检测

中国xxx集团有限公司 张三 182xxxxxxxx

# 一、背景与目标

网络安全监测预警与态势感知的重要性不言而喻，态势感知作为网络安全监测预警和信息通报的基础平台，可以实现对整体安全形势的事前预警和事后溯源。【客户名称】网络安全态势感知平台对网络流量进行监测，切实掌握公司自身风险特征，探索构建坚实可靠的网络安全体系，利用智能化分析实现安全监测服务的转变提升，利用自动化响应实现安全事件的高效闭环。在重大活动、重大事件中有能力对企业突发情况进行准确的研判和对重点部位、重要情况进行预警，保障公司关键信息基础设施安全可靠运行。

# 二、态势感知部署思路与功能

态势感知系统利用日志探针采集海量数据，进行多维关联分析和自动化挖掘，对受害目标及攻击源头进行精准定位，并结合威胁情报，提前洞悉各种安全威胁，结合安全编排与自动化响应技术，实现IP快速封禁与事件快速协同处置。

【客户名称】态势感知平台采用分布式部署模式，将网络探针采集到的数据分散的部署在网络关键节点，采用可扩展的系统结构，利用多台存储服务器分担存储负荷，利用位置服务器定位存储信息。采用双重防护模式，进行入侵检测。通过旁路采集、分析和存储所有网络流量，利用威胁感知系统检测已知威胁。借助全流量存储分析能力，进行回溯展示。通过回溯分析数据包特征、异常网络行为，加强对潜伏已久的高级未知攻击的检测。

# 三、态势感知监测实施方法

在此次专项行动中，【客户名称】态势感知平台使用多种监测方法，一是使用云端数据拓展威胁情报，优化攻击模型，提升对威胁看见的能力；二是关联各类告警挖掘攻击线索，明确攻击链条，提升对威胁洞悉的能力；三是联动多类工具响应安全事件，有效处置闭环，提升对威胁响应的能力。

# 四、攻防实战

1.修筑流量监测纵深异构防御战线

“纵深异构”指的是构建纵深的流量监测防御体系，并采取异构部署模式，实现对攻击路径的全覆盖，实现监测能力的相互验证、补短。

演习前，充分了解各流量监测安全产品的优缺点，并对现有流量镜像网中各流量镜像节点的流量情况进行摸排，随后统筹规划了不同流量监测系统流量探针的流量分配方案，通过重做map、去重、过滤等手段解决了“安全设备丢包、流量镜像网带宽占满”的问题，形成外到内、内到内、内到外的流量监测纵深防御战线，全面覆盖互联网边界、安全域边界、重要应用，以最终达到提升安全设备有效性的效果。

此外，基于流量监测系统的告警内容，收敛对外暴露或跨域暴露的高危端口、弱密码、管理后台等，清理内网失陷机器及违规行为。

## 2.修筑重要系统防御战线

安全态势感知平台收集5大类数据，即网络日志、安全日志、应用日志、资产信息、威胁情报，具体包括防火墙日志、反向代理日志、流量监测告警、邮件沙箱日志、蜜罐日志、LDAP日志、SVN系统日志、DNS日志等。同时，编排数据源监控面板，每类数据源依据历史基线定义收取频率，一旦在定义的时间间隔内未收到该日志，则标红显示并短信告警。将重要系统（如堡垒机系统、域控服务器、VPN、数据交换系统等）、重要账号加入重点监控范畴，不断完善网络侧、应用侧、主机侧的核心防御战线。在条件允许的情况下，对其进行攻击测试，保证对其进行攻击或者变更，能触发流量监测告警、终端审计日志、EDR告警。

## 3.构建协同预警体系

整合实景化攻防技战术的深入研究成果以及强对抗环境下防御手段的创新应用，以智能化的方式实现海量攻击日志数据的自动关联分析，实时监测HW高危事件，如0day利用、OA账号爆破、恶意邮件钓鱼、webshell文件上传成功、交互异常（主动外联、隐蔽信道）、提权类告警及其前置行为等。其中，安全态势感知平台通过API对接威胁情报管理平台，对访问【客户名称】资产的全量互联网IP进行威胁情报匹配，若仅匹配高危情报标签但未触发攻击模型告警，则加入重点关注清单，一旦产生可疑行为则自动告警；若匹配高危情报标签且触发攻击模型告警，则立即封禁。此外，安全态势感知平台通过对接蜜罐系统，对攻击者的攻击行为进行捕获，通过IP情报及指纹情报，查看攻击者身份、标注、攻击者轨迹及黑客危险等级、操作系统、地理位置等信息，提升预警的精准度。为提升安全态势感知平台的预警能力，一方面，需要对攻击模型不断迭代，减少误报率和漏报率。根据安全大环境以及行业态势，实时扩展攻击模型，如0day攻击以及来源于fofa、zoomeye等网络空间探测引擎的真人攻击。另一方面，需要提升安全态势感知平台中的数据质量，精准匹配数据模型，以解决“重要字段缺失或无法匹配、某些攻击模型无法产生事件、机器学习模型无法生效”的问题。

# 五、应用效果

中国【客户名称】在本次专项行动中通过态势感知平台监测处理安全问题日志xx条，其中重点安全事件xx条，监测到的恶意攻击总数为xx次，恶意攻击者（攻击ip）xx个。日志数据全部可查询，可分析，可追溯。

在15天的实战演习行动中，网络安全态势感知平台主动捕获一起0day攻击事件并告警，有效防止攻击者对其他机器的横向攻击，遏制攻击者的攻击行为，并提供详细日志记录对分析攻击者行为和手法，进行分析和回溯，发现cookie中密码明文传输，某系统存在任意文件下载等潜在漏洞，成功定位失陷主机和漏洞的所在位置，做到早发现早整改早处置，减少安全隐患。

# 五、后续工作

下一步，【客户名称】将增加探针部署与各个网络节点，并与二级单位态势感知平台互联互通，建设中国【客户名称】网络安全态势感知一张图，全面利用安全态势感知平台将SIP、情报、沙箱等多维安全产品集中管控，重点做好以下两个方面：

1. 防守对抗自动化

智能分析与自动响应通过安全态势感知平台，构建演习相关攻击分析场景，快速发现安全事件根源，确定攻击手段及评估攻击损失，实时、精准生成待封禁IP清单；结合安全技术自动化编排与响应，将封禁/解封IP清单下发至两地三中心以及子公司的互联网墙进行实时封禁，有效遏制了攻击态势。

2. 安全态势可视化

实时风险动态展示通过在安全态势感知平台设置多维度的安全风险指标，构建了安全运营、安全运维为一体的安全态势总览。借助可视化程度高且细粒度、高精度的风险监测模型，安全人员能及时发现和处置网络中的可疑事件。通过动态描绘攻击及防守趋势图，实现了安全风险及态势的全景可视化管控。