360 天眼新一代威胁感知系统案例

某大型央企是世界 500 强企业之一 ,拥有 60 多家全资、控股子公司，业务足迹遍及世界 120 余个国家和地区 ,同时也是国外黑客攻击组织进行 APT 攻击的重点目标之一，因此及时准确地发现其内网中的 APT 攻击，提升对未知威胁发现的能力是该大型央企信息安全建设的重要目标。360 天眼新一代威胁感知系统通过国内领先的威胁情报技术、高效的快速搜索技术和灵活的大数据存储技术为该大型央企提供了对内网中的安全威胁及时发现和溯源追踪的能力，大大提升了该大型央企的安全防护水平。

某大型央企为海莲花 APT 主要攻击目标，攻击者通过渗透省分公司网站发送伪装工作邮件，感染其办公终端，因集团内部建有内网专线互联机制，以致引发整个集团大面积终端感染病毒，导致企业级重要信息存在泄露的安全隐患，总公司出台了应急解决措施，将所有被感染分公司内网专线接口实行物理隔断，集团日常业务受到了极大的影响，集团高层非常关注该事件的进展，

360 安服团队紧急介入，在该大型央企总部核心交换处旁路部署 360 天眼新一代威胁感知系统 ,抓取镜像流量 ,对此次大面积病毒感染行为进行回溯分析，帮助客户还原了整个攻击的全貌，对受害目标及攻击源头进行精准定位，从源头上解决了此次重大安全事件。

事后该大型央企决定建立全集团的未知威胁检测与防护体系 ,其中最核心的组件就是 360 天眼新一代威胁感知系统。

通过部署 360 天眼新一代威胁感知系统，该大型央企可基于 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，

获取定制的专属威胁情报。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。涉及整个集团的未知威胁检测与防护体系的建立，将使得该大型央企的信息安全防护水平得到巨大的提升。