

奇安信网神威胁监测与分析系统

奇安信网神威胁监测与分析系统(SkyEye, 以下简称天眼系统)是以攻防渗透和数据分析为核心竞争力, 聚焦威胁检测和响应, 为客户提供安全服务与产品解决方案。天眼基于网络流量和终端EDR日志, 运用威胁情报、规则引擎、文件虚拟执行、机器学习等技术, 精准发现网络中针对主机与服务器的已知高级网络攻击和未知的新型网络攻击的入侵行为, 利用本地大数据平台对流量日志和终端日志进行存储和查询, 结合威胁情报和攻击链分析对事件进行分析、研判和回溯, 同时结合边界NDR、终端EDR以及自动化编排处置可以及时的阻断威胁。

用户价值 CUSTOMER VALUES

高级威胁的精准检测

与传统的检测方案相比, 天眼系统可以快速并精准发现网络威胁攻击, 准确率高, 误报率低。

重大安全事件的快速响应

基于威胁情报的上下文, 天眼系统可以帮助安全运营人员发现、研判和处置重大安全事件, 如: 永恒之蓝、APT事件、NotPetya、BlueKeep、Sodinokibi。

网络攻击的回溯和分析

天眼系统还原和存储网络流量的元数据, 可以帮助用户回溯已经发生网络攻击行为, 分析攻击路径、受感染面和信息泄露状况。

满足新等保的合规要求

天眼系统满足了新等保2.0对网络攻击检测和分析要求, 特别是针对新型网络攻击和APT攻击。

产品功能 PRODUCT FUNCTIONS



高级威胁检测

运用威胁情报、文件虚拟执行、智能规则引擎、机器学习等技术, 天眼系统可以检测和发现高级网络攻击和新型网络攻击, 涵盖: APT攻击、勒索软件、WEB攻击、远控木马、僵尸网络、窃密木马、间谍软件、网络蠕虫、邮件钓鱼等高级攻击, 并基于可视化技术, 清晰的展示网络中的威胁。



异常行为检测

基于网络流量数据, 天眼系统运用大数据分析和机器学习技术建立网络异常行为检测模型, 内置非常规服务分析、登录行为分析、邮件行为分析、数据行为分析等数种场景, 实现对新型攻击和内部违规的检测和发现。



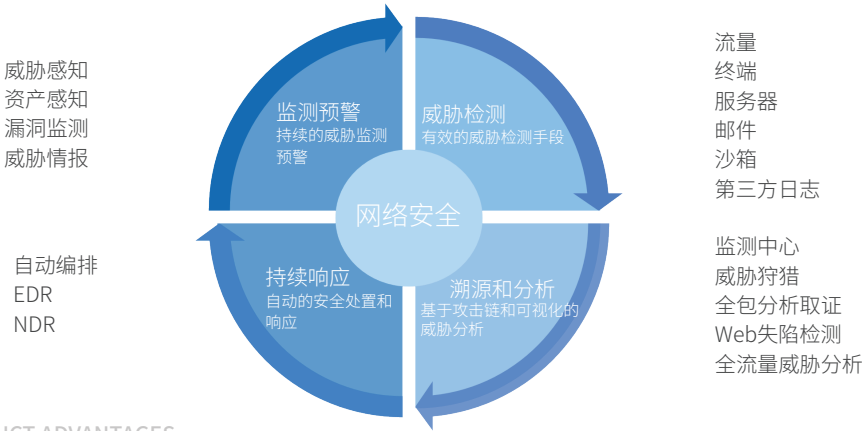
告警响应处置

天眼系统为企业用户提供攻击告警的列表、统计、查询、调查等功能, 且提供基于ATT&CK标签分析告警的能力, 并支持终端EDR联动、防火墙NDR联动与自动化编排处置, 帮助安全运营人员快速研判和处置告警事件。



攻击回溯分析

天眼系统支持全包取证分析，并提供线索可视化图谱拓线分析能力（威胁狩猎）能为企业用户呈现一次攻击的完成过程，帮助用户对网络攻击进行回溯和深度分析。



产品优势 PRODUCT ADVANTAGES

领先APT检测和追踪能力

奇安信具有专业安全专家团队分析和追踪APT攻击，奇安信威胁情报中心监测到的针对中国境内政府机构、科研教育、大型企业等组织单位发动 APT 攻击的境内外黑客组织累计达 40 个，最早可追溯到2007年。

基于多维度、覆盖全球的数据收集能力，利用云端大数据技术自动化处理配合顶尖安全研究团队的人工运营，为用户提供精准的威胁情报。基于上下文关联的情报，帮助用户对告警进行快速分析、研判和处置。

国内领先的威胁情报能力

强大的协同联动能力

通过终端EDR联动、防火墙NDR联动与自动化编排处置，帮助用户快速定位感染主机和恶意软件，并及时的阻断威胁，提升网络攻击的响应和处置能力。

天眼创新的采用搜索引擎技术作为本地数据存储和检索核心技术，这样可极大提高检索性能，为企业提供TB级的数据快速搜索能力，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。

海量数据的运算和检索能力

丰富的行业案例

天眼系统的客户超过1000家，遍及全国各省份，在公检法、金融、政府部委、运营商、石油石化、电力、教育、医疗等行业都具有成功案例，帮助客户发现和处置超过百起APT攻击事件。在十九大重保、一带一路、两会等重要时期以及攻防演习期间，现场的安全专家通过天眼系统累计监测攻击行为30余万次，发现漏洞利用行为上千起，根据攻击信息有效的协助用户对上百台服务器进行加固防护，收到用户的感谢信百余封。