产品简介

360态势感知与安全运营平台是面向政府、金融、能源等大中型企事业单位的综合安全事件分析与全局安全态势感知系统。本系统基于360云端威胁情报和企业本地安全大数据，通过对海量数据进行多维度快速、自动化的关联分析发现本地的威胁和异常行为，并及时与终端管理系统和下一代防火墙进行联动，对威胁和异常行为进行处置。同时，系统可通过图形化、可视化技术将这些威胁和异常的总体安全态势用最直观的方式展现给用户，有利于业务管理者迅速做出判断和决策。

产品功能

全量日志采集

可对本地全量安全日志进行采集，包括：网络原始流量日志、主机防御日志、网络设备日志、安全设备和软件日志、软件和中间件日志等。

多维关联分析

可对本地全量历史数据、互联网威胁情报数据、互联网基础数据，按照多个维度进行关联分析。安全分析人员可以通过攻击者留下的任意线索进行多维拓展，绘制出完整的攻击链条并形成分析报告。

告警响应中心

可对多维度日志设置关联规则，从海量日志中发现可疑的行为并生成告警。同时可将告警详情、处置建议及时通告给主机防御和下一代防火墙等安全管控设备，由安全管控设备进行处置。

态势感知大屏

可提供多种全局安全态势大屏界面，如：全局风险态势、高风险外联行为监控、安全告警监控、资产风险监控、DDoS攻击态势、僵木蠕毒安全态势、Web网站群安全态势 。业务管理和决策者能通过大屏总览当下全局威胁态势 。

资产管理

系统可自动识别本地资产，安全管理员可对资产赋予不同的安全属性，如安全权重、安全域、资产管理员信息等，并通过可视化技术将资产用不同的拓扑类型进行展示。在进行威胁分析的时候安全分析人员可以通过资产分组来进行安全数据统计和分析，大大提高了安全分析人员的工作效率。

产品介绍

特色价值

全面灵活的功能模块帮助客户实现安全业务闭环

可视化技术帮助客户掌握内外网安全态势

自动化关联技术提升客户发现威胁的能力

威胁情报为客户建立专属安全智库

本地大数据存储为客户建立安全大脑

快速搜索技术提升客户分析威胁的效率

使用场景

分析平台、规则引擎、流量传感器、日志采集器，支撑所有应用;流量传感器、日志采集器与分析平台支持多对一模式，可支持多级部署;多软件模块灵活组合，为客户提供专属的定制化态势展示;分析平台预置私有云存储模式，可轻松实现水平扩展;旁路部署，实施简单，对客户网络环境无影响

产品介绍

产品介绍