迪普科技网络安全威胁感知大数据平台

杭州迪普科技股份有限公司

产品概述

网络安全已成为人类信息时代重要的主题，网络安全问题的日益突出主要体现在：计算机系统受病毒感染和破坏的情况相当严重；地下黑产组织已形成重要威胁；企业信息系统在预测、响应、防护和恢复能力方面存在许多薄弱环节；网络政治颠覆活动频繁...面对复杂且不断变化的网络环境，大多数用户缺乏综合性的安全管理解决方案。

在现实网络中，企业通过部署安全设备来防护入侵行为及病毒威胁，从网络攻击的发展历程来看，早期攻击的方式具备着目标单点、手段单一的特点，但现阶段的网络攻击却存在着隐蔽性强、攻击周期长、手段多样化等特点，例如：APT、Miral（DDoS）、SQL 注入、DNS 劫持等，可以发现网络攻击的自动化程度越来越高，黑客所使用的工具也越来越复杂。因此，我们需要一个全面、智能的安全威胁分析平台，来补充和完善企业级用户的安全防护体系，帮助企业用户从容的面对当前各种安全威胁。

迪普科技通过态势感知技术解决上述难题，态势感知技术是指：在一定规模化的系统环境中，对能够引起系统状态发生变化的安全要素进行获取、理解、显示以及预测未来安全威胁的发展趋势。因此，迪普科技推出了网络安全威胁感知大数据平台，帮助用户发现 APT 攻击、失陷主机、僵木蠕传播等安全威胁，实现精准溯源及应急处置。 平台以安全大数据+AI 智能分析技术为核心，结合主/被动检测、威胁情报、 UEBA、攻击行为建模、失陷主机检测等技术，实现安全事件可视化、全网威胁可视化、 全网流量可视化、资产及脆弱性可视化等，帮助客户评估安全状态并决策处置。同时平台设计遵循 GBT-20984-2007 及等保 2.0 等相关要求，全面满足合规性需求。

产品特点

- **安全可视化**

基于先进的安全可视化技术，平台通过安全总览、威胁分析等不同分析维度为用户实时呈现网络安全状况，帮助用户快速识别网络异常入侵行为，及时把握网络安全事件发展趋势，为用户营造全新安全管理体验。

- **安全威胁态势感知**

平台系统提供全面的网络威胁入侵检测能力，同时具备丰富的安全特性：支持信息资产的识别，可对资产进行长期监控；支持对僵尸、木马、蠕虫等系统类攻击，SQL 注入、网络爬虫等 Web 类攻击，HTTP Flood、ACK Flood 等 DDoS 类攻击进行态势感知。平台从全网整体安全监测入手，再细化到信息资产以及安全数据的监测，实现全方位安全的态势感知。

- **大数据引擎技术**

该引擎技术作为态势感知的“大脑”，能够对海量数据日志进行存储、特征提取以及挖掘分析。其通过机器学习的特征积累方式来不断优化平台的处理精度，以及通过对历史日志信息进行关联、回溯等手段，帮助用户发现潜在的安全威胁，进而实现对未来安全威胁趋势的科学预测。

- **资产感知**

通过流量学习、主动探测机制结合海量资产指纹库精准识别 IT 资产，包括各类业务系统、物联网终端、行业化装置等。

■ **威胁发现**

通过多种攻击检测引擎、病毒检测引擎结合威胁情报有效识别高危攻击、病毒木马等已知威胁；通过 AI 检测引擎、沙箱检测引擎发现恶意代码变种、APT 攻击、网络异常行为等未知威胁。

■ **风险判定**

关联分析攻击日志、资产漏洞、网络流量变化、威胁情报、第三方安全日志等数据源进行安全事件有效判定，发现失陷主机，提升告警准确性，减少误报；针对威胁事件进行原始数据全包追溯，实现精确溯源举证。

■ **响应处置**

根据客户决策联动安全防护设备，实现安全风险闭环处置。

■ **高性能**

平台处理能力可达 20G 以上。

功能价值

技术优势	功能价值
安全事件监控	支持对僵木蠕传播、漏洞利用、C&C 通道、APT、敏感信息泄漏等各类安全事件的聚合和管理，可基于告警制定进一步的处置策略，并生成黑客档案信息
安全威胁分析	支持多维度多场景建模，可从内部威胁、外部威胁、外联威胁等多个维度展开分析，具备攻击溯源能力，以关系图呈现并包含攻击链信息
威胁情报关联	支持海量威胁情报的获取，探针上报数据可与威胁情报实时关联，增强对高级威胁线索的发现能力
漏洞探测及验证	支持对资产漏洞的全面检测，并可基于模拟人工渗透技术进行漏洞验证，对漏洞的修复结果进行跟踪闭环
异常流量分析	支持对网络流量的常态监测能力，基于流量自学习和用户自定义模型，智能发现网络中异常流量
全网资产监控	支持主动扫描、流量镜像结合的方式进行资产识别，并支持自定义标签及权重设置，对在线资产进行精细化管理
安全态势呈现	支持全方位安全态势呈现能力，将用户业务及行业场景进行深度耦合，在网络安全宏观监管层面和微观运维层面实现双赢
联动处置	展示未处置威胁地址列表，可对威胁地址进行封禁、解封、忽略等处置动作
平台架构	分布式处理框架，支持平滑扩展；支持分布式部署，支持集中式管理，支持灵活组网
专用软硬件平台**	采用飞腾 CPU、盛科交换芯片的专用硬件平台，软件平台拥有麒麟内核使用授权

**此特性仅在特定款型支持

杭州迪普科技股份有限公司
地址：浙江省杭州市滨江区通和路68号中财大厦6楼
邮编：310051
官方网站：www.dptechnology.net
服务热线：400-6100-598