天融信网络安全态势感知系统 TopSA-EE

www.topsec.com.cn

产品概述

天融信网络安全态势感知系统（以下简称TopSA-EE产品）企业版，是企业和组织对自有通用型办公内网进行态势感知的系统，按照一体化、标准化、智能化、可视化要求建设“安全数据集中存储、态势感知场景丰富、动态建模分析及可视化综合展示”的高价值安全信息存储及分析展示系统。本系统可实现对网络安全的态势觉察、跟踪和预警，全面、实时掌握网络安全态势，及时掌握网络安全威胁、风险和隐患，监测漏洞、病毒木马、网络攻击情况，发现网络安全事件线索，预警通报重大网络安全威胁，处置安全事件，有效防范和打击网络攻击等恶意行为，进而提升整理网络安全态势感知能力。

产品特点

丰富的多维安全态势

TopSA-EE产品立足客户视角分别从全网、威胁、安全底图、安全处置、资产、脆弱性、攻击、僵木蠕、网站监测九个视角进行安全数据采集、监测、分析、研判和展示，满足不同行业的实时态势感知、准确安全监测、及时应急处置等目标 、提升风险识别效率和快速处置能力 。

多厂家多探针接入

TopSA-EE产品采用syslog、snmp等采集方式，支持不同厂商不同类型多源异构数据的接入，接入设备类型包括但不限于系统漏洞扫描、Web漏洞扫描、僵木蠕检测、入侵检测、Web攻击检测、DDoS检测、蜜罐、应用行为审计、数据库行为审计、日志审计。客户可根据实际网络、预算情况灵活选择所需探针进行部署，选择不同类型的探针进行组合不影响系统运行 。

联动式设备管理

TopSA-EE产品支持一键式联动漏洞扫描设备、驱动漏洞扫描设备、导入第三方报告等多方式的脆弱性监测管理，并根据监测信息关联相应资产进而实现资产漏洞监控展示。支持防火墙、IDP等安全设备的策略集中收集、下发等集中式管理 ，可以动态实现一对多的策略分发拦截和封堵等功能 。

可视化分析场景管理

TopSA-EE产品支持基于流量特征进行网络安全状态关联分析，支持驱动场景引擎进行情报匹配分析，支持安全事件基于特征检测的攻击分析，支持基于内置+自定义场景关联规则，包括失陷、暴力破解、账号异常等多种场景的网络共性异常监测规则，方便客户使用。同时支持根据目标网络特性环境可灵活自定义增加、删除、修改定义场景规则。

典型应用

TopSA-EE产品适用于规模大、分支机构分散的企业组织、构建了多厂家多类型安全设备信息网络、安全管理工作繁杂的应用场景，可为客户提供全网安全态势展示、多维调查分析、一体化网站监测、联动式脆弱性监测、集中设备管控、全生命资产管理等安全功能，提升整体网络安全监测预警和应急处置能力。TopSA-EE可应用于需要提升安全管理和安全监管能力的全行业，包括政务、企业、公安、网信、军队、交通、能源、教育、卫生等需要提升安全管理和安全监管的全行业。