天融信APT安全监测系统TopAPT

www.topsec.com.cn

产品概述

天融信APT安全监测系统（以下简称TopAPT产品）是一款聚焦于检测、研判、处置的一体化安全监测设备。系统集成了九大检测引擎和九大研判引擎，并结合AI检测、动态沙箱等技术，实现对已知和未知威胁的快速精确识别。TopAPT支持作为探针与态势感知产品协同，满足行业监管需求，同时也可作为APT设备，满足企业自我监管需求，全面提升网络安全防护能力。

产品特点

全检测

TopAPT产品内置九合一检测引擎，具备网络攻击检测、僵尸主机检测、WEB攻击检测、DDoS攻击检测、威胁情报检测、恶意文件检测、加密流量检测、高级威胁检测、未知威胁检测九大检测功能。实现对扫描探测、拒绝服务攻击、跨站攻击、注入攻击、暴力猜解、弱口令、溢出攻击、木马、蠕虫、挖矿、勒索、隐蔽隧道、DGA恶意域名、爬虫、钓鱼邮件、敏感信息泄露、恶意加密流量、APT活动等威胁的全面检测，对网络节点中的流量可检尽检、应检尽检。

全留存

TopAPT产品可对业务流量、加密流量、攻击流量、恶意程序传播流量、异常流量实现7×24小时实时无遗漏的留存，确保网络活动的每一个细节都被精准记录与检测。通过完整流量留存为攻击溯源提供关键证据链，支持快速回溯攻击路径、精准定位威胁源头，大幅提高安全事件定位效率，提升应急响应速度，满足从日常运维到高级威胁应对的全场景溯源需求。

全场景

TopAPT产品依托深度协议解析引擎，可以在固网、移动网、工业互联网、物联网、车联网及云环境等所有场景中使用，全面监测各场景通信交互与数据传输，深度解析各场景流量的应用协议，实时预警潜在威胁，为能源、运营商、交通、金融、企业等全行业用户提供安全监测保障。

全闭环

TopAPT产品是集检测、研判、处置为一体的一体化安全监测设备。当产品监测到攻击事件、恶意程序传输、异常流量或数据泄露等情况时，会实时触发告警，并自动从事件、攻击者、受害者等视角分析研判，在海量告警中发现高价值威胁事件，可直接或联动其它产品进行处置。形成从预警到处置的高效全闭环流程，有效提高用户网络安全运营效率。