www.topsec.com.cn

天融信高级威胁检测系统TopATD

产品概述

天融信高级威胁检测系统（Topsec Advanced Threat Detection System，以下简称TopATD产品）是天融信自主研发的全能沙箱类产品，系统主要检测文件行为的安全威胁，使用动静结合的鉴定方式和先进的机器学习引擎，可深度分析文档类、可执行类、压缩类、脚本类等文件的安全威胁。通过系统软件模块化设计，基于沙箱的恶意代码检测技术、机器学习检测技术、反逃逸行为检测技术等多种高级检测技术，精准检测文件的病毒、木马、蠕虫、勒索等已知和未知威胁。可通过内容详实的分析报告呈现威胁鉴定结果，并提高客户对高级可持续性威胁的防御能力。

产品特点

全能沙箱

TopATD产品为天融信自主研发的全能沙箱产品，系统集成Windows、Uninx、Linux、Android所有主流操作系统环境，能够深度检测可执行文件、文档文件、压缩文件、脚本文件、图片、音频、视频等百余种文件类型，检测已知和未知恶意程序。

APT挖掘

TopATD产品利用TAI-2智慧鉴定器和动态行为分析方法，并结合DGA域名检测，发现高价值恶意程序样本，通过深度挖掘技术最终获得APT线索。

七大鉴定器

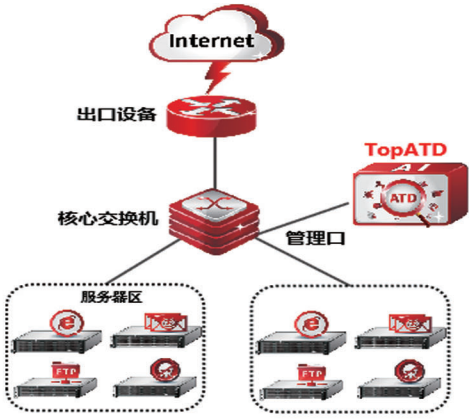
TopATD产品内置七大鉴定器，包含黑白名单鉴定器、NSRL索引鉴定器、证书信誉鉴定器、病毒引擎鉴定器、TAI-2智慧鉴定器、YARA规则鉴定器、动态行为鉴定器，采用动静结合的技术手段进行多维分析，从而准确地鉴定已知和未知恶意程序。

多维分析报告

TopATD产品可对鉴定的结果进行详细的报告分析，包含9大类三十多种内容。可对子文件深度分析、释放文件、静态分析、执行信息、风险行为、进程、EXIF信息、样本分析结果、来源信息等多个维度分析报告，确保报告的完整性和细致性。

典型应用

TopIDP产品通常以串联方式部署于网络边界区域，用于检测和实时阻断从外网到内网的网络入侵行为。为应对复杂的环境需求，可提供多种部署方式，无需改动客户的网络结构，支持透明、路由、旁路、混合等多种模式。



产品规格

型号	TI-61158-ATD
固定接口	4GE&4SFP
USB接口	4个
产品形态	硬件
尺寸(宽深高)	2U
冗余电源	是
电压	输入100~240V
频率	47-63Hz
电流	4.5-2A
功率	300W MAX
运行温度	0℃—40℃
存储温度	-20℃~70℃
相对湿度	20%—90%，非冷凝

功能列表

设备管理	必须为软硬一体的2U设备，支持B/S管理模式，无需安装独立的控制台软件署；
	支持对设备登陆WEB页面配置管理，可直接从web中实现命令行方式管理，支持图形验证码登录验证，防止暴力破解；
	支持开通Restful API接口联动检测，系统通过标准的“API服务”与多种第三方设备联动，与第三方设备联动时设备通过网络传输的样本文件（自动检测样本），减少配置的复杂性和工作量，提升部署效率；
多文件检测类型	支持百余种文件检测类型，包含但不限于可执行文件、文档文件、压缩文件、移动端文件、图片文件、脚本文件、其他文件等文件类型，且支持自定义文件类型；
多样本上传模式	支持三种样本上传方式，可根据不同的需求选择不同的检测模式，检测模式包含：Web手动提交、SMB/FTP自动获取、联动检测；
多工作模式	支持多种工作模式，包含极速模式、智能模式、深度模式，可根据用户的不同需求进行调整，选择方式多灵活性高；
多鉴定器	支持系统内置多鉴定器，用于分析和挖掘样本信息，包含：黑白名单鉴定器、NSRL索引鉴定器、证书信誉鉴定器、病毒引擎鉴定器、TAI-2智慧鉴定器、YARA规则鉴定器、动态行为鉴定器七大鉴定器；
多虚拟机	至少支持Windows、Linux、Android三种操作系统的检测环境，对各操作系统广泛兼容，支持系统根据样本类型自动选取匹配的虚拟机分析环境，也支持用户自定义配置单个或多个虚拟机分析环境分析样本；

产品资质

证书名称	认证机构
计算机软件著作权登记证书	国家版权局