www.topsec.com.cn

天融信昆仑系列僵尸网络木马和蠕虫监测与处置系统TopTVD

产品概述

天融信昆仑系列僵尸网络木马和蠕虫监测与处置系统（以下简称TopTVD）是基于国产化硬件平台和国产操作系统自主设计开发的网络安全产品，该产品集合了攻击检测、僵木蠕检测、DDoS检测、恶意程序检测、APT检测、WEB安全检测、虚拟沙箱、元数据提取、流量分析九大功能，即九合一全流量检测探针。该产品通过深度解析网络流量，结合特征匹配、异常行为分析、机器学习、虚拟沙箱等技术，实现迅速、精准识别网络中各种已知和未知网络威胁。

产品特点

九合一检测探针

TopTVD产品是集攻击检测、僵木蠕检测、DDoS检测、恶意程序检测、APT检测、WEB安全检测、虚拟沙箱、元数据提取、流量分析九大功能于一体，实现对网络威胁全面检测的效果。在多需求的探针应用场景，无需部署其他设备，TopTVD单款设备即可做到多种检测效果，即节省安全建设成本，又减少运维管理工作量。

未知恶意程序检测

TopTVD产品首创应用TAI-1智慧引擎，结合虚拟沙箱的检测技术，在不依赖任何规则库情况下，达到高效、精准的恶意程序检测能力。TAI-1智慧引擎通过海量样本训练的机器学习模型识别恶意程序。虚拟沙箱检测采用仿真技术，模拟操作系统环境，构建执行引擎，动态化分析发现恶意程序。TAI-1智慧引擎+虚拟沙箱的方式，打破了传统特征匹配技术的束缚，既能检测已知恶意程序，更能够检测未知恶意程序，是发现未知威胁特别是APT攻击的有力工具。

嵌入式威胁情报

TopTVD产品的威胁情报库是由天融信安全云服务产品线分析生产的，具备恶意IP、恶意URL、恶意域名、恶意文件等多种情报类型，包含800W+高可靠的威胁情报数据。嵌入式威胁情报库情报来源可靠精准、情报种类丰富、更新速度快、独立性强。

多维知识库支撑

TopTVD产品拥有攻击检测规则库、应用识别库、地理信息库、僵尸主机规则库、威胁情报库、URL分类库六大知识库。多维、丰富的知识库，使产品在威胁检测、攻击定位、上网行为分析等方面更加精确、迅速。

全流量元数据挖掘

TopTVD能够对攻击事件信息、僵尸主机行为信息、恶意软件信息、恶意域名\URL访问信息、DDoS攻击等多种安全事件信息记录，对安全事件进行攻击报文、恶意样本文件取证，并且能够详细记录多种网络通信的元数据信息。

典型应用

旁路部署

对于规模较小、结构简单的网络环境，TopTVD通常是在网络出口处或核心网络节点处旁路部署。对于规模较大、结构复杂的网络环境，TopTVD可在客户下级单位、分支机构等多个网络出口处部署。TopTVD旁路部署在不影响网络的前提下，做到对客户网络环境中多种威胁事件监测。