KUAIYE

快页信息技术有限公司

“NextTF”全流量溯源取证系统

产品概述

全流量溯源取证系统基于网络全流量分析技术，将采集到的流量以元数据和 PCAP 的形式存储。通过特征检测、威胁情报检测、网络异常行为检测和 AI 检测引擎，对原始流量进行交叉检测、验证，结合高效便捷的数据检索能力，对流量中存在的网络威胁进行有效的溯源取证。

产品功能

全面的流量统计分析

NextTF 可分析出网络流量中各协议的占比情况、各主机在流量中的占比情况、接收/发送数据包的情况等。解析后的字段，可协助用户排查网络中是否存在网络扫描、DDOS 等网络威胁。。

基于会话的流量数据展示

NextTF 可以基于会话流量数据，使原始的网络流量具备更高的可读性，对网络流量根据会话进行关键字段的提取和展示。

基于内容快速取证

支持基于内容进行取证，对于未解析为元数据的内容支持对原始流量进行取证，支持根据关键字、正则表达式进行检索，可通过元数据检索缩小内容取证范围，提高检索效率。

基于多级索引的智能检索

支持 TCP、UDP、ICMP 等传输层协议解析，支持 20 多种主流的应用层协议解析，140 多种网络元数据解析。支持灵活的检索条件及组合，可根据会话精准定位原始数据包并提供下载。

海量数据的原始流量超快检索

能够做到在 PB 级别的原始流量或者百亿级的会话量级中，快速检索到会话级原始流量，并提供下载。

丰富直观的图表展示

TFS 提供给了强大的图表自定义功能，为用户提供丰富的图形化流量实时监控视图，可以自定义选择关注的内容以及各种阈值

详细的通联关系分析

利用图标的形式更好的展示节点间的通联关系，其中的源/目的节点可配置为各种不同的对象字段，线可配置为不同的连接阈值，可根据需求查看对象的通联关系，例如图中的源/目的 IP 的通联关系，还可以查看文件与主机间的通联关系，邮件收发的通联关系等。

产品特点

高性能全流量留存

高可靠、高性能的数据包捕获及记录，高磁盘数据存储压缩比。支持抓包策略灵活配置，基于五元组、域名、BPF 规则和应用等策略的流量过滤。

秒内超快检索

秒内检索到 PB 级数据（百亿会话）中的指定会话及 PCAP 文件。

完善的溯源取证能力

可对任意解析后的数据字段进行快速过滤检索及对留存的 PCAP 包原始内容检索，基于图和智能算法进行事件追溯。

高效的网络协议分析及异常行为检测能力

具备基于特征、威胁情报和 AI 智能检测的威胁检测分析能力，从源头快速发现网络恶意行为，有效发现高级威胁。

强大的处理性能

提供强大的溯源取证能力，单台流量处理能力最高可达 20Gbps，并可按需扩展处理能力和存储周期，适用于用户对业务网络高度、实时化监控保障的要求。

客户价值

帮助用户实时了解安全运行态势，发现潜在的恶意行为

实现完整的攻击溯源和取证分析

基于图和智能算法对攻击过程全链条追溯

帮助用户建立完备的网络安全检测分析架构。