融讯光通
RONG XUN GUANG TONG

网络安全系列产品彩页

网络安全分析仪

产品概述

网络安全分析仪提供及时攻击威胁信息探测能力，以便立即采取网络安全应急保障纠正措施。网络安全分析仪通过旁路镜像的方式检测安全风险

- 通过采集网络数据流量结合最新安全情报库去检测最新的安全威胁。
- 也可以通过输入外部 PCAP 文件的方式去检测文件或者日志中是否有安全威胁。

产品特性

- 智能探测最新的安全情报威胁：网络安全分析仪能够智能探测您网络中最新的安全情报威胁.。它支持快速探测威胁风险以降低网络安全风险。

-勒索病毒检测

-木马通信检测

- 暗网通信检测
- 恶意下载检测
- 僵尸网络检测
- 网络钓鱼攻击检测
- 比特币挖矿检测

- 网络可视化：网络安全分析仪提供快速，易用的可视化安全分析界面，让您对网络安全威胁一目了然，为您下一步网络安全应急保障提供数据支撑。
  - 威胁事件列表
  - 威胁事件过滤和检索
  - 威胁 IP，域名，攻击信息分类
  - 一目了然连接安全事件状态

- 网络安全取证：网络安全分析仪通过采集网络数据包或者可疑通信协议数据来识别安全事件，用于网络安全取证，以防将来再次发生类似事件。
  - HTTP,HTTPS：请求 / 响应
  - DNS：域名查询
  - SMB：文件操作
  - SMTP：邮件地址

产品参数

产品线配置	
类型	（10G 指标）
产品图片	
CPU	Intel® Xeon® E-2278G
内存	64GB
监测接口	2 x1/10GbE
数据存储	2TB
RAID	5
电源	400
工作环境	10-35℃/50-95℉/8%-85%
重量（kg）	10.0
尺寸 H×W×D(cm)	30.5×40×18.5

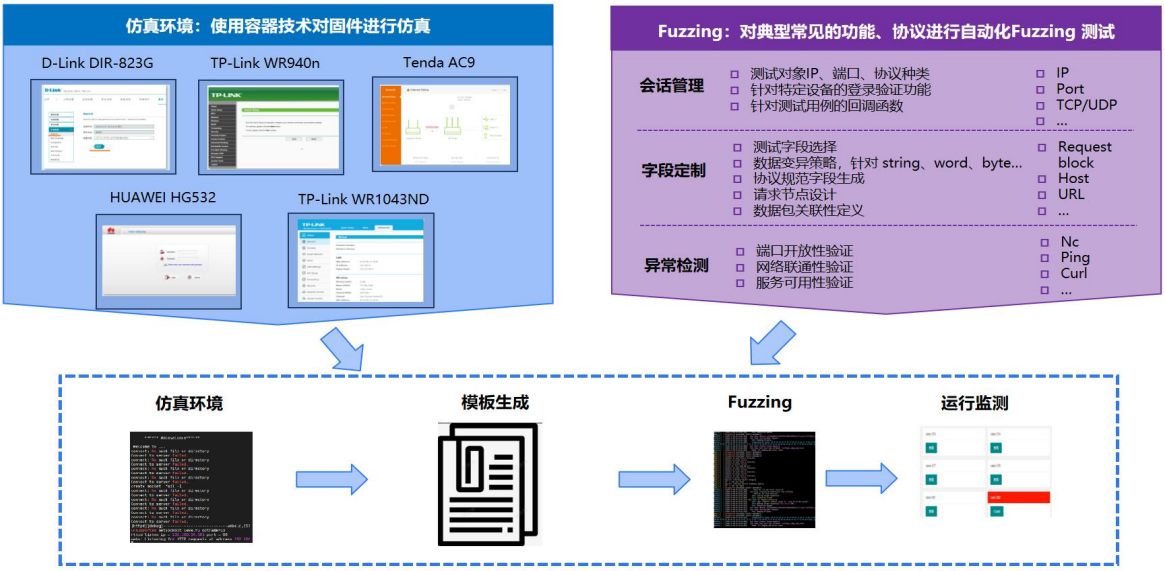
攻击威胁列表（部分）
1、CnC 暗网通信网络攻击者用来向恶意软件发出恶意命令并窃取敏感信息的服务器 2、感染僵尸网络受感染的僵尸机器接收来自外部网络攻击者的各种恶意命令并执行它们 3、垃圾邮件源大量发送垃圾邮件的来源 4、被盗网站窃取企业机密信息和日志的服务器 5、恶意间谍软件通信监视计算机中的个人信息和用户行为，并在不知情的情况下向外发送信息 6、在线游戏网站通过网络赌博、游戏等方式监控个人信息和用户行为，并在不知情的情况下向外发送信息 7、恶意代码滥用各种有害代码的网站 8、聊天服务器被滥用为恶意软件命令和控制服务器的聊天服务器 9、TOR 暗网通信用于隐藏通信路由信息的服务器 10、信息泄露被入侵、被漏洞的利用攻击以及被信息泄漏的服务器 11、P2P 在客户端之间交换文件而不通过服务器的节点

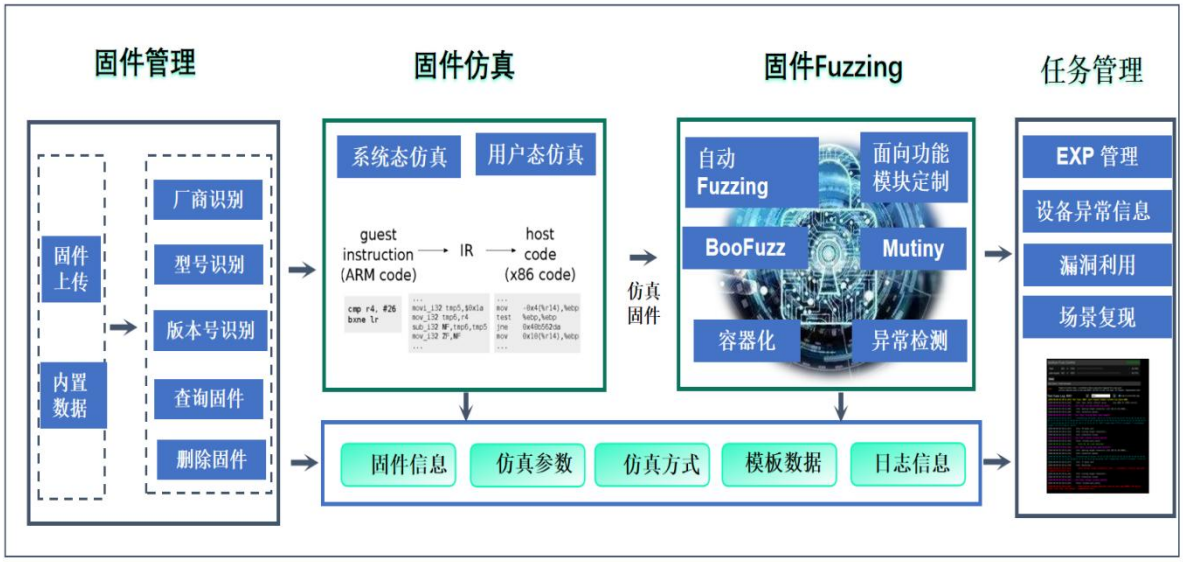
		12、僵尸代理主机感染的僵尸网络的代理主机 13、僵尸网络 IP 疏通被恶意软件利用 IP 和 GEO 检查服务 14、已知威胁工具被恶意使用的互联网工具和服务 15、DDoS 攻击目标洪水式网络攻击，通过向网站和服务器发送过多的访问和数据来干扰正常的运营服务 16、主机扫描一种攻击准备行为，例如扫描服务器上运行的服务、检查开放端口和尝试弱密码 17、字典攻击尝试所有可能的字符组合来识别密码的攻击 18、假冒反病毒非法销售或分发假冒防病毒和假冒反间谍软件产品的网站 19、动态 DNS 服务与动态 DNS 服务相关的滥用 IP 地址和域名 20、未定义威胁不是非法网站，而是提供黑客论坛、漏洞社区等信息的网站 21、挖矿威胁与比特币挖矿相关的服务器 22、DDoS 发起攻击 DDoS 发起攻击的源

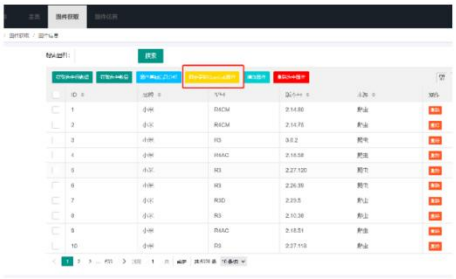
物理网固件安全分析平台

产品功能

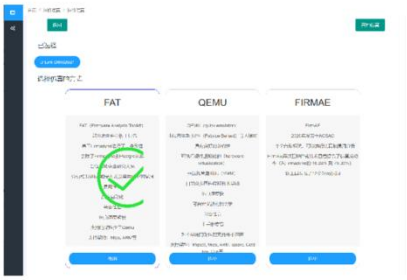
- 能够并行调度多个模糊测试器对不同可仿真嵌入式设备固件进行模糊测试以支持大规模自动化漏洞挖掘。
- 持不同来源模糊测试器数量≥10 个，支持新增模糊测试器，支持网络协议型模糊测试器。可仿真固件及其配套全自动化仿真环境数量≥100 个，模糊测试种子数量≥4500 个，支持新增可仿真固件配套环境。



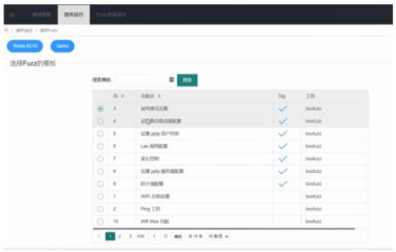




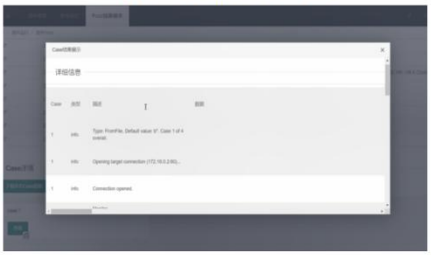
平台内置包含 30000 余款路由器固件



多种固件仿真方式



定制模糊测试策略模板



实时查看模糊测试日志

融讯光通
RONG XUN GUANG TONG

供应链安全分析平台

产品概述

- 分析结果呈现和管理：对结果进行和可视化、面向专业人员提供专业结论和依据。
- 算法层：由若干专门开发的软件分析算法构成，底层采用算子管理和任务调度平台进行灵活管理。
- 特征抽取层：将分析目标和样本进行软件统一化表示。部分软件特征需要在运行时才能提取，系统自动构造软件执行环境，并加载执行，抽取动态执行特征。
- 样本库：包括了样板自动采集、样本手工上传以及自动对采集的样本进行预处理和特征抽取等功能。
- 分析目标和任务管理：对分析目标和分析任务进行管理、进行结果记录和查询。

产品特性

应用场景

关键信息基础设施自主可控分析

- 软件是关键信息基础设施中的自主可控的薄弱部分，具有复杂多样、分析与监管困难，更新变化迅速等特点。本系统可快速批量验证软件自主可控和可靠性。是解决关键信息基础设施中软件薄弱环节的利器。

重要核心领域软件可靠性测评

- 在国防、通讯、交通、电力、电子政务等核心领域，相关软件的可靠性是关系网络安全、数据安全的重要问题。需要采用总体国家安全观的思维考虑其安全性。本系统是进行核心领域软件可靠性测评的利器。

软件知识产权保护

- 本软件可以证明软件的原创性和非原创性，并能够溯源非原创成分的最终来源，是保护软件知识产权的利器。

漏洞与威胁情报软件安全风险分析

- 在软件开发时不小心引入含有漏洞的组件和代码片段是当前网络安全的主要威胁之一。基于威胁情报和漏洞信息建立公共漏洞识别模型，识别软件漏洞及第三方组件漏洞，识别供应链安全风险。

融讯光通
RONG XUN GUANG TONG

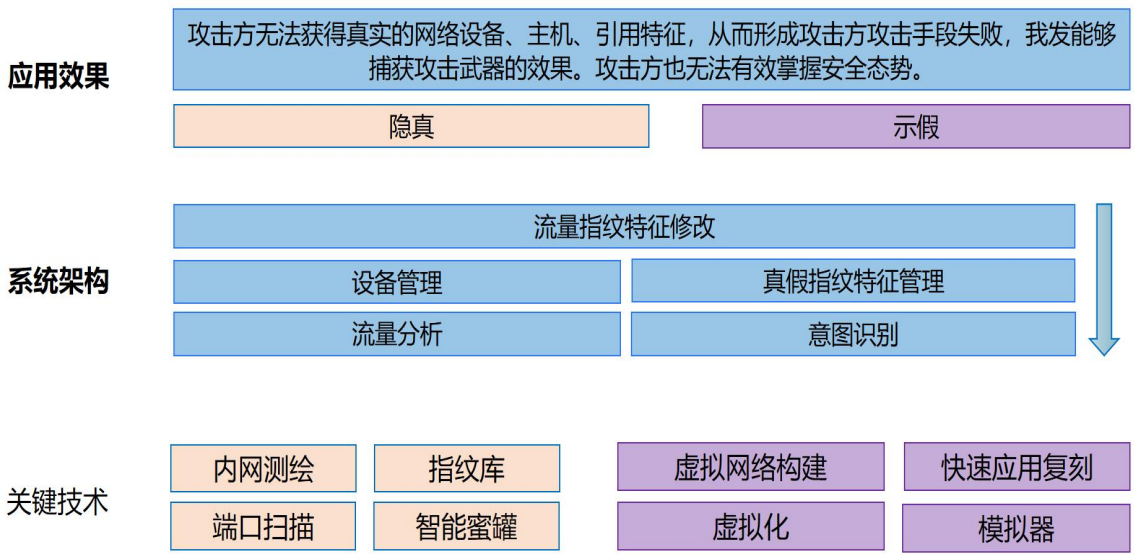
网络空间反测绘系统

产品概述

- 基于杀伤链模型的逐阶段对抗模型

针对杀伤链模型，在侦查跟踪阶段，主要的欺骗方式有指纹隐藏、虚假端口、虚假网络应用、主机指纹伪装、主机屏蔽、探测识别等。在武器构建和载荷投递阶段，主要的欺骗方式有仿真漏洞环境、虚假网络地址、虚假人员和账号等，还可结合攻击方对虚假目标误用检测，来实现攻击行为判定。在漏洞利用和安装植入阶段，主要的欺骗手段有利用模拟、动态合成欺骗数据、伪装响应、构建沙箱等，配合仿真环境动态生成等决策控制功能。在命令控制阶段，欺骗防御手段有节点仿真、伪装响应、内网拓扑欺骗、虚假系统信息，此外为了进行诱捕，还配合了流量捕获与分析。在目标达成阶段，主要欺骗方式有诱饵主机、诱饵文件、诱饵流量、合成数据等，同时进行隔离和取证溯源等后续工作。

产品架构

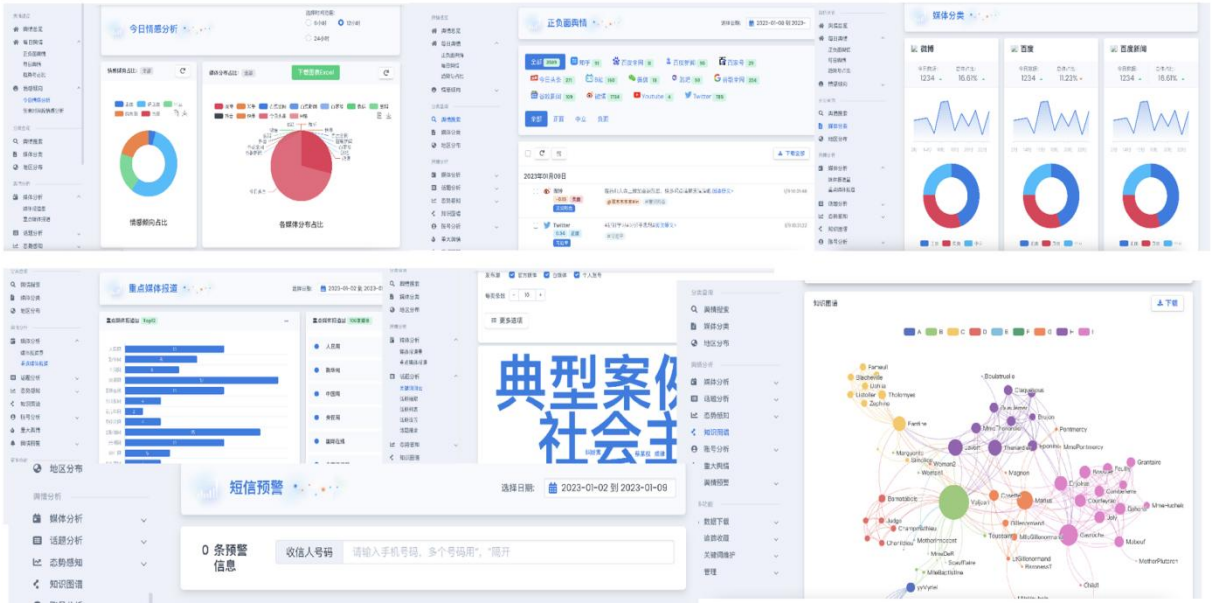


融讯光通
RONG XUN GUANG TONG

舆情检测预警

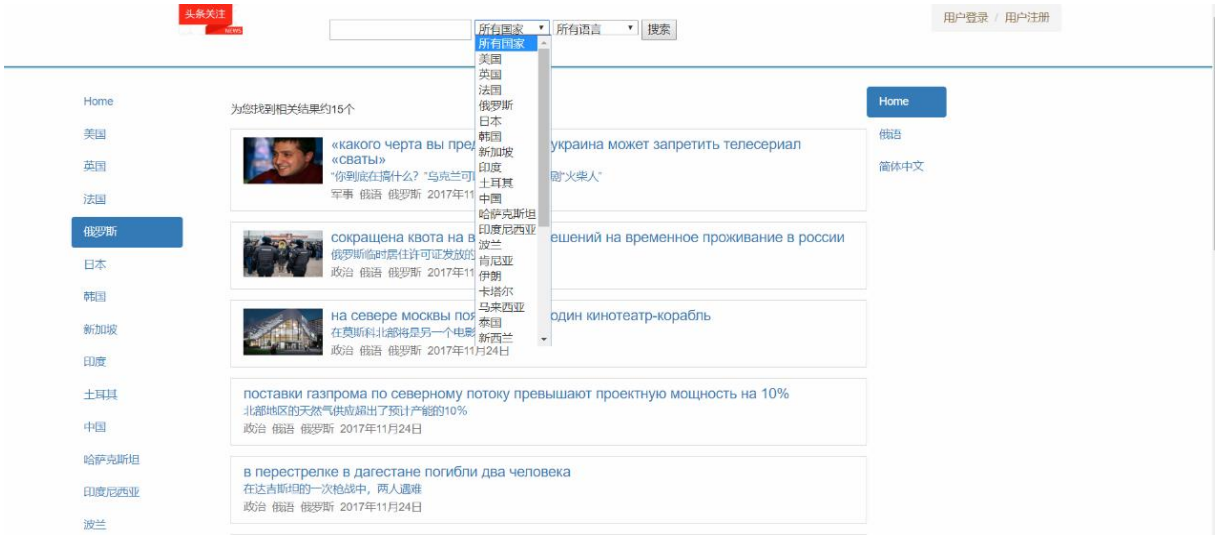
产品功能

网络信息分析平台



多语种网络新闻监测分析

- 多语种新闻平台旨在**实现网络空间舆情实时展现**，通过新闻主题分类、用户评价等为网络空间的舆情评价指标体系的建构及验证提供有力持续的**数据支撑。**
- 目前已构建多语种全球媒体报道数据库，包括 **40 多个国家，28 个语种，近千家多家境外媒体**，截至目前，**总监测量为达到近亿篇。**语种全面性和数据库国际新闻数国内最权威构建。



融讯光通
RONG XUN GUANG TONG

舆情可视平台 - 领域分析

舆情可视平台 - 事件分析