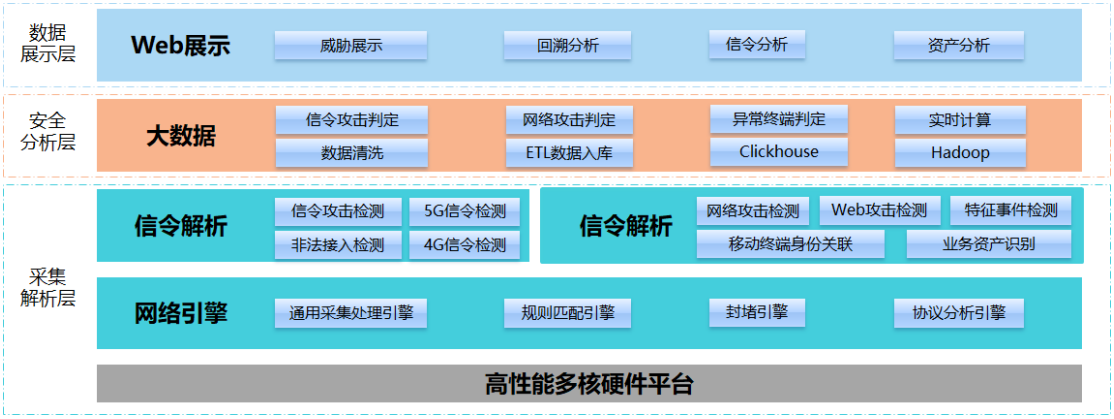
5GC 全流量分析系统

1、产品简介

5GC全流量分析系统是对5G核心网全流量安全检测分析，异常终端接入检测、信令攻击检测、漏洞和威胁利用行为检测、业务渗透入侵检测，资产识别、流量回溯取证等。检测5GC核心网面临新的安全风险，包括信令安全、用户访问安全及5GC云部署环境的安全问题。

2、产品架构



3、核心功能

- **采集解析：**

支持常用协议和5G协议的解析和还原，包括但不限于NGAP、PFCP、GTPv2、HTTP2协议，支持5G核心网信令面各接口的信令协议解析和还原，支持工作在非默认端口下的常见服务的协议识别与协议分析能力。支持5G核心网管理面流量的解析和还原，包括但不限于SFTP、SNMP、REST、SOAP、FTPS协议。

支持导入HTTPS证书，对流量进行解密和还原。

支持自定义规则抓取和留存原始流量，自定义规则内容应包括：源IP/源端口、目的IP/目的端口、匹配类型（二进制、字符串、正则表达式）、匹配特征、会话数量等。支持数据包Pcap文件存储功能，支持对采集的全部流量进行存储、检索和下载，检索条件包括源IP、目的IP、源端口、目的端口、起止时间。

支持但不限于HTTP协议、DNS协议、邮件协议、FTP协议、TELNET、数据库操作、SSL/TLS协商记录、登录记录、认证记录、ICMP协议、TCP会话、UDP会话等元数据提取。

- **威胁检测**

5G 信令安全检测：支持对 5GC 信令存在的安全风险进行识别，包括但不限于非法接入、

信令风暴、信令攻击、切片安全、伪基站监测。

终端非法接入检测：支持对影响 5GC 正常运行的问题终端进行检测识别，包括但不限于对来历不明信令、异常行为（如频繁上下线）进行检测。

自定义特征事件检测：支持基于异常时间、异常 IP、多 IP 登录、高频访问、绕行登录等异常行为的特征事件检测。

- **回溯分析**

支持对存储的流量日志进行回溯查询，包括 TCP/UDP 会话日志、DNS 解析日志、Web 访问日志、文件传输日志、SSL/TLS 协商日志、数据库操作日志、登录日志、认证日志、ICMP 日志，回溯时间可以自定义。

支持对历史流量进行回溯分析，支持自定义时间范围、攻击类型、攻击阶段、严重程度等。支持以源/目标 IP、源/目标端口、协议、时间范围、关联的流量日志进行 Pcap 包取证，支持对取证到的 Pcap 包进行下载。

- **资产监控**

支持暴露面资产和未知资产发现：具备自动发现并上报网络资产的 IP 地址、MAC 地址以及是否为暴露面资产信息的能力，支持提取网络资产的指纹信息（包括但不限于 IP 地址、MAC 地址、设备类型、设备厂商、服务端口等）。

失陷资产监控：支持基于资产名称、资产类别、资产 IP、失陷时间、攻击类型等进行失陷资产监控，支持失陷资产统计图、失陷攻击类型分布图、失陷资产列表等多个维度的统计，支持失陷资产的查询和处理，支持对失陷资产的处理状态进行标记。

4、 产品优势

- **移动信令全解析：**支持 5G、4G、3G、2G 全制式信令采集和解析，解析高效，数据准确；支持 4/5G 无线侧 Uu、X2、Xn 等接口解析；支持 5G 消息和短信解析；
- **5GC 全方位保障：**采用自研的信令攻击算法，准确高效识别异常行为终端和信令攻击，能够及时检测核心网漏洞、威胁和网络攻击，保障重要通信设备网络安全；
- **全流量溯源：**对安全事件进行回溯和调查，抓包取证提供完整攻击证据，并绘制出完整的攻击链条；