1. 元数据威胁感知设备

基于威胁情报库与复杂DPI规则，对元数据与采集原始数据进行深度检测，标记输出。

需求：输入是元数据或者pcap文件，输出是告警信息

* 1. 运行模式

设备分为两个处理模块，元数据威胁标注+基于复杂规则的数据包检测：



两个模块

需求：两个模块在一个设备上，同时具备对pcap文件和元数据的威胁检测能力。

* 1. 功能性能要求
     1. **功能指标**

1. **IO要求**
2. 具备转换后的自定义元数据接收能力，支持SOCKET/KAFKA等数据传输方式；

需求：优先支持socket（zmq）方式，最终需要支持kafka方式

1. 具备通过指定全局文件系统接口或者FTP方式读取采集文件的能力；

需求：

* 流量接收：探针接收的原始流量数据是pcap包，pacp包是探针的规则前置模块对原始流量过滤后生成

pcap:探针取，通过ftp到全局文件系统中获取

* 功能调试：web界面提供流量文件导入，用于研发、交付期间的调试，文件分两种，原始流量文件和原数据方式封装的文件

1. 具备检测数据按需封装输出的能力，日志数据支持SOCKET/KAFKA等数据传输方式，文件数据按指定全局文件系统接口进行存储；

需求：

1. 传感器：传感器外发日志格式、字段定义，既双方确定外发日志格式标准，发送给大数据平台（客户的业务系统，目前无相关产品）
2. 沙箱：涉及沙箱外发日志格式（检测结果）标准，同样发送给大数据平台
3. **元数据威胁检测与标注能力**
4. 具备基于输入的协议元数据，利用威胁情报资源进行元数据威胁标注与输出的能力；

需求：支持

1. 具备基于输入的文件MD5信息，利用威胁情报资源进行文件信誉度匹配、标注与输出的能力；

需求：计划探针通过第三方的md5信誉度调用接口，获取文件信誉度。（目前没有第三方信誉度查询库）

1. 具备白名单过滤能力，是否输出可配置；

需求：支持，需定制如下

1. 界面需支持批量白名单导入
2. 奇安信提供白名单，包括IP库、爬虫IP、dns服务器-
3. 提供元数据输入接口，支持多方数据输入，并根据数据来源进行区分；

需求：通过字段支持，既支持线路号、任务号ID

1. 支持自定义检测威胁情报加载，例如针对SSL加密算法的检测，用户上载SSL检测规则，设备引擎自动适配

需求：即ssl黑证书识别规则

1. **基于复杂规则的数据包检测能力**
2. 具备基于复杂规则进行恶意行为检测的能力；

需求：支持

1. 支持单向数据流输入；

需求：不做文件还原，只做数据规则匹配

1. 具备检测日志与会话pcap文件同步输出的能力，通过全局唯一ID保证可匹配查询；

需求：pcap检测的情况下，告警输出中包含对应pcap的id

1. 支持将复杂规则简化输出（按甲方转换要求进行转换），不能自动简化的需要支持手动转换，简化规则原则上不允许形成数据传感器数据泛洪；

需求：前置规则过滤

1. 支持复杂检测规则的定期离线升级或者从威胁情报中心定期升级；

需求：提供规则离线升级包

1. **受控管理能力（必选定制化能力）**
2. 设备应按照工程规范，向管控设备（运控系统）定期上报运行状态，包括输入输出数据量、输入错误日志（留存错误数据样本）、各个协议命中比例、规则命中比例等统计信息；

需求：定期向管控设备上报运行数据

1. 设备应提供web管理界面或者telnet命令行管理界面，支持设备服务启停、实时状态查询，并支持部分关键功能的在线调试。

需求：易于调试和分析观测的辅助信息

1. **威胁情报库支撑能力**
2. 设备本地留存威胁情报库，并定期支持从威胁情报中心获取更新情报，保证本机设备的威胁情报的新鲜度；
3. 支持本机威胁情报库的离线升级；
4. 支持本机自定义威胁情报信息的添加。

需求：提供规则离线升级包

* + 1. **性能指标**

1. 元数据威胁检测的输入能力不低于20WPPS。（可以提升，根据包长，数据类型）

需求：要求不低于80Wpps

1. 元数据威胁检测支持的协议类型包括但不仅限于（供应商确认）

需求：已经定义，在另外的元数据接口文档描述

1. 基于元数据的威胁情报告警类型不低于9种（列出具体的），其中APT组织的识别不低于20个（列出具体的），总的攻击行为不低于1000个（列出具体的）；（供应商确认）

需求：满足需求

1. 文件信誉度匹配能力不低于1亿个/天/台；（供应商确认）

需求：暂时没有信誉库，没有数据

1. 基于复杂规则的恶意行为检测类型不低于9种（列出具体的），有效规则数量不少于2万个；（供应商确认）

需求：满足需求

1. 采集文件的恶意性检测能力不低于15TB/天/台；

需求：用TB而非bps的原因是从“恶意流量初筛与过滤”模块取的原始流量文件，后续实现阶段具体评估性能

* 1. 数据输入输出规范

1. 文件系统访问、FTP访问等规范由甲方提供；
2. 供应商应提供其具体检测设备的输入接口、输出接口

需求：支持，已经联调

* 1. 形态要求

1. 建议单台4U专用设备；
2. 按照保密要求，机箱标志、包装标志应符合甲方要求，产品界面或者包装不允许出现甲方或者供应商标签。

需求：

* 探针功能合并为一台探针
* 设备需白牌机，无任何公司logo，客户粘贴自己的logo
  1. 保障性要求

1. 联调期间，驻场7\*24小时支持；
2. 3年的免费维护。

需求：提供第三方环境适用性文档，包括高低温、MTBF测试

* 1. 其他要求

暂无。

1. 恶意文件检测设备

恶意文件检测设备利用静态检测和动态分析相结合的检测方法，实现在文件中的攻击样本发现。设备具备文件静态检测、动态检测、文件漏洞分析能力，利用静态扫描引擎提取文件基础静态信息，发现已知威胁和文件异常，利用动态分析全面捕获文件动态行为，发现其中可疑、恶意行为，利用漏洞检测功能实现对已知漏洞发现、未知漏洞检测能力。

定位：工具类设备，作为一类重型组件嵌入安全监测流程中。

* 1. 运行模式



* 1. 功能性能要求
     1. **功能要求**

1. **文件静态检测能力**
   1. 具备文件病毒检测功能，内置病毒检测引擎，能够输出明确恶意代码名；
   2. 具备压缩文件检测功能， 支持对压缩文件进行多层解压，并对解压后文件进行检测；
   3. 具备文件签名检测和判定功能，支持签名厂商和签名MDS识别；
   4. 具备不依赖于 后缀名自动识别样本文件的类型能力；
2. **文件动态检测能力**
   1. 支持的虚拟机操作系统包括Windows XP.Windows 7、Windows 10、 Windows Server、Linux等32位、64位系统；

需求：目前不支持Window10，Linux32,64位操作系统

* 1. 支持exe、dll、 sys、doc、docx、 ppt、 pptx、xIs、 xlsx、rtf、 wps、 pdf、html、jpg、jar、bat、 chm、swf等各种格式样本文件分析；
  2. 支持zip、rar、 7z、 gz、ace、arj、 z、 bz、tar、tgz、cab、iso、 eml、msg等数十种压缩包格式样本文件分；
  3. 虚拟机分析环境可定制，并预置多种常见的虚拟机分析环境，包括:办公软件Microsoft Office 2003、Microsoft Office 2007、Microsoft Office 2010、WPS 2010、WPS 2012、WPS 2013，文档阅读器Adobe Acrobat Reader v7-v11、浏览器IntermnetExplorer v6-v11,以及Flash Player、Visual C++ Runtime、Java、 .NET Framework等运行环境；
  4. 具备记录文件运行期间的注册表行为、文件行为、网络行为等所有行为能力；
  5. 支持敏感操作识别，可识别动态释放文件、动态启动进程、远程线程注入、文件自删除等操作，并能提取和还原相应参数;
  6. 支持采集样本运行过程中产生和释放的中间文件；
  7. 支持采集样本运行过程中产生的网络流量数据，保存为标准的pcap 格式；
  8. 具备检测策略动态配置功能，可对相关检测参数和模式进行动态配置；
  9. 具备文件缓冲池机制，对于周期性重复验证时能够快速匹配已有结果；

1. **文件漏洞检测能力**
   1. 具备对已知漏洞利用特征进行识别和检测功能；
   2. 可提取软件漏洞利用等攻击过程导致的异常执行代码片段；
2. **数据IO**
   1. 支持手动导入检测文件进行批量检测的方式；
   2. 支持对指定FTP目录下的文件（文件信息用同名的xml描述）进行循环扫描检测方式，*xml组织方式参考工程 规范，本协议不做描述；*（--定制化指标）
   3. 支持以实时任务方式，对指定位置的文件进行检测的能力，*任务参数与传输方式参考工程规范要求，本协议不做描述*；（定制化指标）

需求：指定位置是指怎样的方式（网盘，额外的数据存储？），沙箱怎样的方式去获取文件检测，目前不支持，需要明确需求

* 1. 支持对于不同方式的文件输入方式，按照指定数据接口、数据封装方式、数据传输方式以及输出目的进行数据输出的能力，传*输方式参考工程规范要求，本协议不做描述*；（定制化指标）

需求：FTP和手动提交已实现规定数据接口，实时任务目前不是很清楚需求（不支持）

* 1. 支持文件检测优先级管理，例如实时任务驱动的检测优先级一般为最高，手动导入其次，指定FTP目录下的文件第三。

需求：支持手动和FTP优先级，实时任务方式需确定怎样传输方式

1. **受控管理能力（必选定制化能力）**
2. 设备应按照工程规范，向管控设备定期上报运行状态，包括文件检测数量，数据输出情况统计，输入错误日志（留存错误数据样本）等信息；

需求：上报信息到管控设备，管控设备接受数据接口不清楚

1. 设备应提供web管理界面或者telnet命令行管理界面，支持设备服务启停、实时状态查询、队列清空。

需求：队列清空是指清空什么队列（动态检测队列？）

沟通结论：c、d、e、6未实现，需实现

注：c、d、e是demo验收期间产生的需求

沙箱检测数据一般是对接分析平台，目前项目需要发送到大数据平台，但是怎么发送到大数据平台接口未定义

* + 1. **性能要求**

1. 文件静态检测引擎种类≥6类；
2. 文件动态检测行为类型≥6类(恶意文件来源，恶意行为类型，恶意文件进程操作，文件操作，网络操作，注册表操作等)；
3. 动静结合的文件检测能力：非可执行文件大于2万/天/台，可执行文件大于20万/天/台；

沟通结论：“3)”规格写错，需更正

1. 动态文件检测能力大于2万/天/台。
2. 数据输入输出规范。
   1. 形态要求
3. 建议单台2U专用设备；
4. 按照保密要求，机箱标志、包装标志应符合甲方要求，产品界面或者包装不允许出现甲方或者供应商标签。
   1. 保障性要求
5. 联调期间，驻场7\*24小时支持；
6. 3年的免费维护。
   1. 其他要求

暂无。

1. 恶意域名检测设备
   1. 运行模式



* 1. 功能性能要求

1. **IO要求**
2. 具备转换后的自定义DNS元数据接收能力，支持ICE/SOCKET/KAFKA等数据传输方式；
3. 具备非正常DNS原始数据包的接收处理能力；

沟通结论：如dns隧道、协议误用等目前实现效果及后续计划

1. **恶意DNS检测能力**
2. 具备基于域名情报、Sinkhole库、DGA库的静态检测能力；
3. 具备C&C、可疑心跳、可疑环路地址、动态域名、DGA动态特征、隐蔽隧道动态特征、FastFlux、IDN检测能力；
4. 具备白名单过滤能力，支持对alexa访问排名前10000的网站以及自定义的白名单进行过滤；
5. 支持对主流的DNS服务器进行过滤或标注输出，支持自定义；
6. 非正常DNS解析处理与检测能力（供应商提供资料，可以做什么不可以做什么）

沟通结论：如dns隧道、协议误用等目前实现效果及后续计划

1. **性能要求：**单机15WPPS实时处理能力。
   1. 数据输入输出规范
2. 文件系统访问、FTP访问等规范由甲方提供；
3. 供应商应提供其具体检测设备的输入接口、输出接口
   1. 形态要求
4. 建议单台2U专用设备；
5. 按照保密要求，机箱标志、包装标志应符合甲方要求，产品界面或者包装不允许出现甲方或者供应商标签。
   1. 保障性要求
6. 联调期间，驻场7\*24小时支持；
7. 3年的免费维护。
   1. 其他要求

暂无

1. 恶意域名分析软件
2. 跨域威胁情报平台

为本地系统提供统一的威胁情报查询、更新服务，支持跨域数据访问

1. 告警日志清洗与实时计算软件

对告警日志进行实时分析、聚合计算、可信度判别等，为后端统计分析、态势展示提供数据支撑