# 宁夏烟草溯源分析平台测试报告

# 1.测试目标

本次测试数据资产监测与溯源分析平台（DAST）的测试目标如下：

* 验证DAST的数据发现和分类、分级能力，即，能够发现宁夏烟草网络中流动的数据，并根据预先定义好的关键字对数据内容进行分类和分级（敏感程度）；
* 验证DAST对用户的发现能力，全息平台通过从网络流量中提取用户账户，包括：政务微信账户、电子邮件账户；
* 验证DAST系统的“数据，用户，应用”三个维度的画像和关联分析能力，特别是验证从“敏感数据”维度追溯到用户和应用；以及从应用维度追溯到数据和用户；
* 验证DAST的数据监控和追溯能力，支持实时查看、以及历史数据追溯，即，哪些用户，以何种方式（通过什么应用）访问了什么数据，并追踪数据传送的位置（内网、外网、互联网等）等，及时发现内部数据外传等行为。
* 验证DAST对宁夏烟草业务场景的社会热点事件的回溯能力，支持手机号、身份证号、关键字等敏感信息回溯，从而提供关联附加信息的线索，帮助宁夏烟草提高工作效率。

## 2.测试环境

### **2.1****数据资产监测与溯源分析平台DAST概述**

数据资产监测与溯源分析平台（DAST）通过对网络流量的长期持续采集，从网络原始数据（Meta Data）中，按照时间序列提取“用户，设备，应用，数据”四个维度的信息，实现对业务系统的刻画：

* 数据维度：DAST系统可以还原采集器获取的网络流量中的文档文件（如：Word，Excel，PPT，PDF，源代码等），例如：邮件附件，HTTP，FTP，SMB上传/下载的文件，对文件内容进行扫描，并根据预定义的敏感信息规则判断文件的类别及敏感级别，为不同敏感级别的文件打标签。以此构建客户业务系统数据维度的信息；
* 用户维度：DAST默认采用IP地址标识用户，如果能够抓取该IP地址的登录账号信息（包括：邮件账号，HTTP登录账号以及RADIUS登录账号，KERBEROS登录账号，LDAP协议，RDP协议），则使用用户账号作为用户标识。DAST也可以和企业LDAP集成获取用户账号信息，或者采用人工导入方式，导入“IP地址——用户名”对应关系，以此建立业务系统“用户”维度的信息；
* 设备维度：DAST数据采集器（MetaFlow）可以采用多种方式获取用户使用的设备的MAC地址（例如：DHCP Snooping方式，SNMP或者ARP查询方式等），采用MAC地址作为用户使用的终端设备的标识。
* 应用维度：DAST通过对协议解码，获取网络会话所使用的应用层协议，根据内置的应用服务数据库，标识用户所访问的应用。如：Web网站，邮件收发，云盘，音视频，IM等。

DAST对上述4个维度进行画像，并将相关的4个维度信息关联，感知“什么人，什么设备（Who），在什么时间（When），什么地点（Where），通过什么应用（How），访问或操作了哪些数据资产（What）”，构建以用户和设备为基点的业务系统画像，形成对用户的全息立体刻画，刻画网络中抽象的IP所对应用户和设备，并刻画用户和实体（设备）通过网络访问应用的行为，以及传输文件的行为。

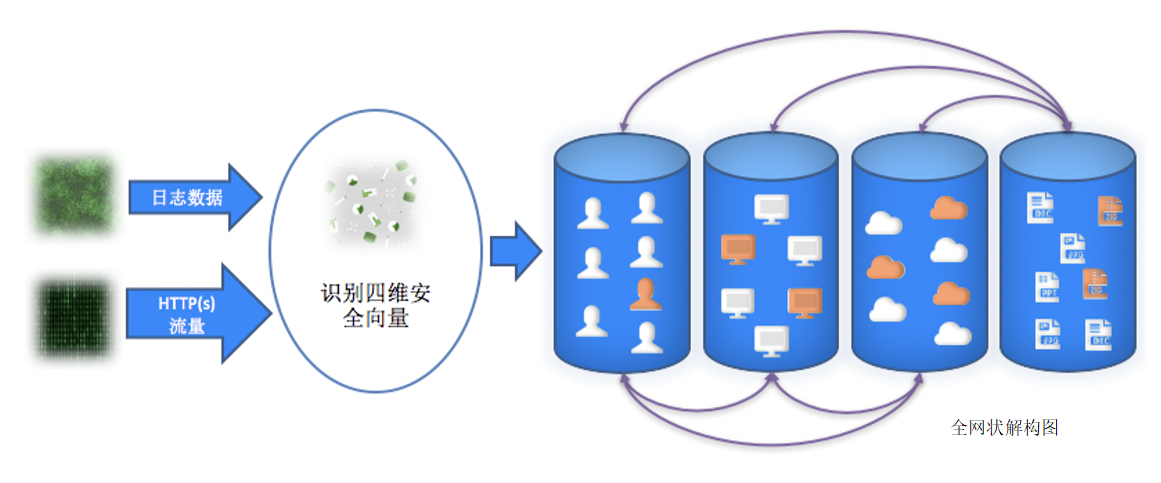
DAST的全息立体刻画，可以支持用户从任意维度的数据挖掘和追溯，如：从可疑应用维度追溯用户维度、设备维度、文件维度的行为；从敏感文件追溯用户维度、设备维度、应用维度等；或者从可疑用户维度追溯文件维度、应用维度。这种对业务系统的刻画和关联分析是发现用户和设备异常行为的基础，不论是自动的机器学习方式，还是人工分析方式，都是抵御企业内部威胁，未知行为和高级安全威胁（APT攻击，“0”Day攻击，勒索病毒等）导致的安全风险的基础。

在“刻画”的基础上，UEBA（User and Entity Behavior Analystic，用户和实体行为分析）就是针对不同场景的用户和设备行为特征，通过机器学习的方式“捕获”异常的用户和设备，从而定位威胁，即，通过对用户和实体的行为的刻画，以时间轴为基准，采用机器学习技术，对用户和设备行为建立基线，实现多个场景的异常行为发现和告警（DAST系统默认需要2-3周的时间进行机器学习，建立用户、设备行为基线）。

### **2.2DAST系统测试平台部署**

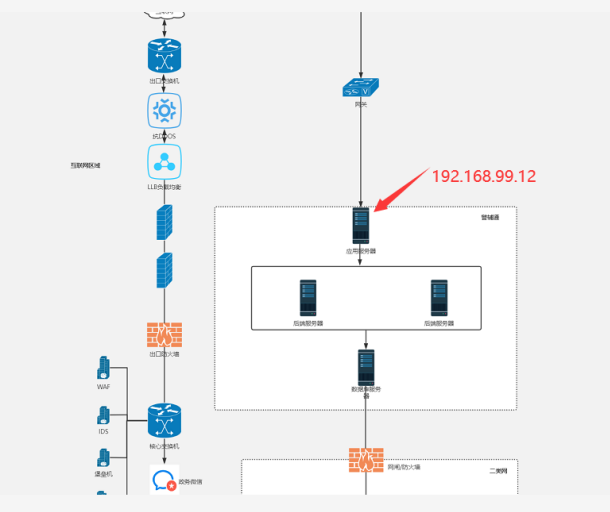
DAST系统主要分为2个核心组件：

* 数据采集器（MetaFlow）：数据采集器（Meta-Flow）可以采用旁路模式和代理模式，代理模式下有两种具体部署方式，分别为透明模式和路由模式。从网络流量中提取四个维度（用户、设备、应用、文件等）的数据特征，并支持从流量中还原出来的文件进行深度内容检测（Deep Content Inspection），根据预制或自定义的敏感规则为每个文件打上相对应标签。也可以根据设计需求，配置为留存网络中传输的敏感文件。采集器采用专用硬件，支持100M/1G/10G接口。
* 元溯分析平台（MetaVison）：元溯分析系统（MetaVision）是企业级大数据采集、存储、分析计算、查询和洞察数据安全风险感知和可视化的统一平台，支持海量结构化与非结构化数据的存储与分布式计算能力，能够满足大数据批处理、微批处理、 实时处理等业务需求。全息分析平台通过接收数据采集器 (MetaFlow)经过预处理后的网络流量日志（含有“用户，设备，应用，文件”四个维度的信息），采用独特的网络全息图专利技术，发现并重构文件、用户、设备和应用这四个关键安全元素之间的关联关系，实现用户业务系统刻画，并采用UEBA发现异常，定位威胁，实现威胁预警、告警，以及事后的追溯和取证。分析平台为软件包，可以部署在物理服务器或虚拟机上。



由于DAST系统是数据驱动的分析系统，如果仅仅通过构造数据（样本系统，样本数据）很难体现系统的刻画功能，因此，宁夏烟草的POC测试是将DAST系统部署到了宁夏烟草现网环境中完成的，具体部署情况如下：

1.测试拓扑



宁夏烟草采用旁路模式，通过TAP设备获取网络流量，进而分析、呈现。

2.部署位置

在宁夏烟草部署了1套独立的DAST系统进行系统测试：

* MF采集器采集2路流量，分别是：互联网出口流量，办公网、分支机构到数据中心的流量；
* 元溯分析平台与MF部署一体机模式，运维人员可以在终端PC上，通过Web浏览器访问元溯平台Web页面，查看数据分析结果。

### **2.3软硬件需求**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 位置 | 采集器 | 分析平台 | 运维终端 |
| 1 | 宁夏烟草 | 硬件  型号DAST-500  MF版本：V1.28.5.4 | 软件  OS：CentOS7.9  元溯版本：v2.01 | Windows IE或  Chrome浏览器 |

## 3.测试内容

### **3.1文件识别**

上传下载或通过邮件发送各种类型的文件，采集器可抓取相关类型的文件。

|  |  |
| --- | --- |
| 测试项目 | 文件识别 |
| 测试目的 | 验证产品对不同格式文件的识别能力 |
| 测试环境 | 参考测试拓扑 |
| 测试步骤 | 1. 上传下载doc、pdf、ppt、excel、txt等格式的文档 2. 上传下载png、jng格式图片 3. 上传下载源代码格式文件 4. 上传下载压缩包 5. 上传下载音频格式文件 6. 上传下载加密文件 |
| 预期结果 | 系统成功抓取不同格式的文件 |
| 实际结果 | 通过 |

### **3.2敏感数据监测**

#### **3.2.1敏感数据识别**

识别策略是指不当使用或未经授权被人接触或修改会不利于国家利益计划的实行或不利于个人依法享有的个人隐私权的所有信息。在本平台上，敏感信息是指数据元素定义出来的信息。

根据业务数据类型和级别，定义各种敏感规则发现网络中流动的敏感文件。

识别策略：

* 内置规则，如：身份证，手机号，银行卡号等通用规则
* 自定义企业网络中的涉密、敏感信息，包括：
  + 费率表
  + 投标书
  + 项目开发
  + 合作协议（银行合作协议、中介合作协议、年度合作协议、产品补充协议）
  + 绩效考核（评分表、核定表、反馈面谈表）
  + 人员信息（人员花名册）
  + 员工收入（工资明细表、劳务费明细、绩效奖金）
  + 重要会议记录（季度销售工作会议纪要、季度经营分析会议纪要）
  + 重要合同（房产买卖合同、委外管理人委托投资协议）
  + 审计报告（专项审计报告、内部审计报告）
  + 财务预决算报告（年度决算报告、财务预算报告）
  + 客户资料（手机号、身份证号、家庭住址）

支持的方式：关键字，正则表达式，文件名，文件类型（word、excel、ppt、pdf、源代码），文件哈希值。

##### **3.2.1.1 关键字**

关键字又称保留字（keyword）是指在搜索引擎行业中，希望访问者了解的产品、服务或者公司等内容名称的用语。

本测试项将定义关键字为元素，并通过识别策略将关键字信息下发至采集器进行预处理，并将关键字相关的信息在平台进行展示。

自定义识别策略中的敏感元素包含关键字，上传下载文件数据时，可根据关键字将数据识别为敏感数据。

|  |  |
| --- | --- |
| 测试项目 | 关键字测试 |
| 测试目的 | 验证产品对关键字信息的识别能力 |
| 测试环境 | 参考测试拓扑 |
| 测试步骤 | 1. 添加敏感元素为关键字的识别策略 2. 上传下载带有该关键字的文件 3. 发送/接收带有该关键字的邮件 |
| 预期结果 | 文件被识别为敏感文件  邮件被识别为敏感邮件 |
| 实际结果 | 通过 |

##### **3.2.1.2 正则表达式**

正则表达式，又称规则表达式,（Regular Expression，在代码中常简写为regex、regexp或RE），是一种文本模式，包括普通字符（例如，a 到 z 之间的字母）和特殊字符（称为"元字符"），是计算机科学的一个概念。

本测试项将定义正则表达式为元素，并通过识别策略将正则表达式信息下发至采集器进行预处理，并将正则表达式相关的信息在平台进行展示，比如：身份证号、手机号、银行卡号等。

自定义识别策略中的敏感元素包含正则表达式，如身份证正则表达式，上传下载文件数据时，数据中匹配该正则表达式，则该数据会被识别为敏感数据。

|  |  |
| --- | --- |
| 测试项目 | 正则表达式测试 |
| 测试目的 | 验证产品对正则表达式的识别能力 |
| 测试环境 | 参考测试拓扑 |
| 测试步骤 | 1. 添加敏感元素为正则表达式的识别策略 2. 上传下载匹配该正则表达式的文件 3. 发送/接收带有匹配该正则表达式的邮件 |
| 预期结果 | 文件被识别为敏感文件  邮件被识别为敏感邮件 |
| 实际结果 | 通过 |

##### **3.2.1.3 特殊hash**

哈希值一般指哈希函数，哈希函数指将哈希表中元素的关键键值映射为元素存储位置的函数。任意一个文件都可以通过哈希函数的算法而计算出一串数值，从而保证此文件的内容统一性，一旦文件内容进行修改，则哈希值变更。

本测试项主要依据固定哈希值，从而识别其特定的文件等。比如：某个机密文件的固定哈希值。

识别策略中配置特定hash值的文件，文件hash值和配置中的内容一致时，会被识别成敏感文件。

|  |  |
| --- | --- |
| 测试项目 | 特殊hash值测试 |
| 测试目的 | 验证产品对特定hash值文件的识别能力 |
| 测试环境 | 参考测试拓扑 |
| 测试步骤 | 1. 添加敏感元素为特殊hash的识别策略 2. 上传下载匹配该hash的文件 |
| 预期结果 | 文件被识别为敏感文件 |
| 实际结果 | 通过 |

##### **3.2.1.4 特定文件类型**

系统可以针对文档的特定类型进行识别。

识别策略中配置特定文件类型，上传下载该文件类型时，同类型的文件会被识别成敏感文件。

|  |  |
| --- | --- |
| 测试项目 | 特定文件类型测试 |
| 测试目的 | 验证产品对特定文件类型的识别能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 添加敏感元素为某文件类型的识别策略 2. 上传下载该类型的文件 |
| 实际结果 | 通过 |

##### **3.2.1.5 特定文件名**

系统可以针对某个特殊文档的特定名称进行识别。

识别策略中配置特定文件名，上传下载文件时有，文件名同配置中的文件名一样的文件会被识别成敏感文件。

|  |  |
| --- | --- |
| 测试项目 | 特定文件名测试 |
| 测试目的 | 验证产品对特定文件名的识别能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 添加敏感元素为某文件名的识别策略 2. 上传下载该类型的文件名的文件 |
| 预期结果 | 文件被识别为敏感文件 |
| 实际结果 | 通过 |

##### **3.2.1.6 数据类别&数据级别**

数据分类就是把具有某种共同属性或特征的数据归并在一起，通过其类别的属性或特征来对数据进行区别。为了实现数据共享和提高处理效率，必须遵循约定的分类原则和方法，按照信息的内涵、性质及管理的要求，将系统内所有信息按一定的结构体系分为不同的集合，从而使得每个信息在相应的分类体系中都有一个对应位置。

数据分级，按照数据的价值、内容的敏感程度、影响和分发范围不同对数据进行敏感级别划分。

添加识别策略时需选择数据类别，数据类别绑定数据级别，数据触发识别策略后可被识别成敏感数据，可在溯源中查看该数据的数据级别和类别。

|  |  |
| --- | --- |
| 测试项目 | 数据类数据别级别识别测试 |
| 测试目的 | 验证产品对敏感文件的数据类别以及级别的识别测试 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 添加类别，选择某个级别 2. 添加识别策略选择该类别 3. 上传匹配该策略的文件和邮件 |
| 预期结果 | 文件被识别为敏感文件，该文件对应类别和级别问策略中的类别和级别  邮件被识别为敏感邮件，该邮件对应类别和级别问策略中的类别和级别 |
| 实际结果 | 通过 |

#### **3.2.2 敏感数据下载**

发现用户下载各种敏感文件的行为。企业组织内部用户有数据导出操作，对于用户数据导出行为，通过溯源平台可以实时监控、追溯、审计用户从内网服务器上下载敏感数据，通过监控这种行为可以发现恶意用户在内网搜索、收集敏感数据的行为，并可以配置具体应用数据下载异常的场景。

识别策略中勾选保存原始文件，文件触发敏感规则后，可在画像页面下载该文件，查看该文件所有内容。

|  |  |
| --- | --- |
| 测试项目 | 敏感数据下载测试 |
| 测试目的 | 验证敏感数据下载功能 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 添加识别策略，勾选保存原始文件 2. 上传下载匹配该策略的文件 3. 发送接收匹配该策略的邮件 |
| 预期结果 | 文件和邮件画像页面可点击下载下载敏感文件和敏感邮件 |
| 实际结果 | 通过 |

#### **3.2.3 敏感数据态势**

记录所有敏感文件信息，文件被识别为敏感文件时，可在该列表下查看，包括文件追踪

|  |  |
| --- | --- |
| 测试项目 | 敏感数据态势测试 |
| 测试目的 | 验证敏感数据态势下敏感文件展示的能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 上传下载敏感文件 |
| 预期结果 | 敏感数据态势-敏感文件列表可查看该文件，点击追踪按钮可查看文件溯源  敏感数据态势-敏感文件地图下可查看该文件 |
| 实际结果 | 通过 |

#### **3.2.4 出网数据**

一般来说，外网，即互联网，局域网通过一台服务器或是一个路由器对外连接的网络，这个IP地址是唯一的。也就是说内网里所有的计算机都是连接到这一个外网IP上，通过这一个外网IP对外进行交换数据的。

在本测试项中，网的定义可以由客户侧人员，自主定义，默认情况下即包含：10.0.0.0-10.255.255.255,172.16.0.0-172.31.255.255,192.168.0.0-192.168.255.255。

在配置中配置好内网网段，数据上传外网或从外网向内网下载数据，则会被识别成出网数据。

|  |  |
| --- | --- |
| 测试项目 | 出网数据测试 |
| 测试目的 | 验证产品对出网数据识别的能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 网段配置自定义内网网段 2. 该网段下发送数据 3. 从该网段下载数据至外网 |
| 预期结果 | 该数据被识别为出网数据，数据监控-出网数据下可查看 |
| 实际结果 | 通过 |

#### **3.2.5 出境数据**

依照《评估办法》的规定，“数据出境”是指网络运营者将在中华人民共和国境内运营中收集和产生的个人信息和重要数据，提供给位于境外的机构、组织、个人。根据以上定义，数据出境的情形包括：第一，境内网络运营者将数据通过网络直接传输给境外主体；第二，境外主体通过网络主动访问并读取境内的数据；第三，境内网络运营者将数据通过网络传输以外的方式（如物理携带）提供给境外主体。

本测试项目将通过IP归属地进行查询，并将出境的数据展示出来。

向国外网站上传数据时，或国外向国内下载数据，则该数据会被识别成出境数据，如本地上传文件至github仓库，则该文件会被识别成出境数据。

|  |  |
| --- | --- |
| 测试项目 | 出境数据测试 |
| 测试目的 | 验证产品对出境数据识别的能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 向境外网段发送数据 2. 境外网段向国内网站下载数据 |
| 预期结果 | 该数据被识别为出境数据，数据监控-出境数据下可查看 |
| 实际结果 | 通过 |

#### **3.2.6 出域数据**

域是由一组具有相同需求并互相信任的系统组成的逻辑区域。比如网络安全域是指同一系统内有相同的安全保护需求，相互信任，并具有相同的安全访问控制和边界控制策略的子网或网络，且相同的网络安全域共享一样的安全策略。

在本测试项中，域的定义可以由客户侧人员，自主定义。

数据上传下载的源ip目的ip满足自主定义的出域配置，则会被识别成出域数据。

|  |  |
| --- | --- |
| 测试项目 | 出域数据测试 |
| 测试目的 | 验证产品对出域数据识别的能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 网段配置下配置出域规则 2. 上传下载数据的ip在该出域规则内 |
| 预期结果 | 该数据被识别为出域数据，数据监控-出域数据下可查看 |
| 实际结果 | 通过 |

### **3.3 数据溯源**

溯源平台实时发现网络中的数据资产、对数据的流转路径进行监测、持续不断的对数据行为进行全面刻画，构建数据全息关联图，提供多维度实时关联分析；呈现敏感数据安全态势，发现出境数据、数据泄露、数据滥用等风险行为；提供强大的数据溯源能力，为事件调查取证提供全面的证据链。

该页面展示文件和邮件所有收发信息，点击文件邮件可查看溯源信息，上传下载具体时间信息，业务数据只展示触发识别策略的业务数据。

|  |  |
| --- | --- |
| 测试项目 | 数据溯源-文件测试 |
| 测试目的 | 验证产品对文件的抓取能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 上传下载文件 |
| 预期结果 | 数据溯源-文件列表下可查看该文件信息，该文件匹配数据类别级别，活动次数，用户、设备、应用信息，点击文件可跳转至该文件溯源详情列表 |
| 实际结果 | 通过 |

|  |  |
| --- | --- |
| 测试项目 | 数据溯源-邮件测试 |
| 测试目的 | 验证产品对邮件抓取能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 发送接收邮件 |
| 预期结果 | 数据溯源-邮件列表下可查看该邮件信息，该邮件匹配数据类别级别，活动次数，用户、设备、应用信息，点击文件可跳转至该邮件溯源详情列表 |
| 实际结果 | 通过 |

|  |  |
| --- | --- |
| 测试项目 | 数据溯源-业务数据测试 |
| 测试目的 | 验证产品对敏感业务数据的识别能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 下载业务数据 |
| 预期结果 | 数据溯源-业务列表下可查看该邮件信息，该业务数据匹配数据类别级别，活动次数，用户、设备、应用信息，点击文件可跳转至该业务数据溯源详情列表 |
| 实际结果 | 通过 |

溯源条件查询将以多种条件包含“与”和“或”的逻辑进行查询。

包含的查询条件有：

* 文件名称
* 文件类型
* API业务数据
* 邮件主题
* 匹配正文
* 数据级别
* 数据类别
* 识别策略
* 源IP
* 源端口
* 目的IP
* 目的端口
* 源MAC
* 应用
* 应用协议
* HASH
* 主机

|  |  |
| --- | --- |
| 测试项目 | 溯源条件查询识别 |
| 测试目的 | 验证产品对溯源条件查询的识别展示能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 通过“文件名称”的查询方式查询相关数据的溯源情况 2. 通过“文件类型”的查询方式查询相关数据的溯源情况 3. 通过“API业务数据”的查询方式查询相关数据的溯源情况 4. 通过“邮件主题”的查询方式查询相关数据的溯源情况 5. 通过“匹配正文”的查询方式查询相关数据的溯源情况 6. 通过“数据级别”的查询方式查询相关数据的溯源情况 7. 通过“数据类别”的查询方式查询相关数据的溯源情况 8. 通过“识别策略”的查询方式查询相关数据的溯源情况 9. 通过“源IP”的查询方式查询相关数据的溯源情况 10. 通过“源端口”的查询方式查询相关数据的溯源情况 11. 通过“目的IP”的查询方式查询相关数据的溯源情况 12. 通过“目的端口”的查询方式查询相关数据的溯源情况 13. 通过“源MAC”的查询方式查询相关数据的溯源情况 14. 通过“应用”的查询方式查询相关数据的溯源情况 15. 通过“应用协议”的查询方式查询相关数据的溯源情况 16. 通过“HASH”的查询方式查询相关数据的溯源情况 17. 通过“主机”的查询方式查询相关数据的溯源情况 |
| 预期结果 | 成功展示查询结果 |
| 实际结果 | 通过 |

### **3.4 数据资产检测**

#### **3.4.1 资产统计**

显示所有上传下载的文件，流动资产为系统抓取中的文件，静态资产为在静态资产列表上传的文件，总资产是流动文件和静态资产总和。

|  |  |
| --- | --- |
| 测试项目 | 资产列表统计 |
| 测试目的 | 验证产品对抓取到文件的展示能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 上传下载文件 |
| 预期结果 | 资产列表可查看该文件信息，匹配数据类别、数据级别、识别策略、hash值、属性、文件类型、大小、最近活动时间信息  点击文件可跳转至文件全息图 |
| 实际结果 | 通过 |

#### **3.4.2 文件画像**

显示该文件特有信息，比如文件曾用名、敏感级别、哈希值、用户、设备、应用等信息。

|  |  |
| --- | --- |
| 测试项目 | 文件画像 |
| 测试目的 | 验证产品对文件画像识别的展示能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 资产列表点击某个文件，切换至该文件画像页面 2. 该文件触发识别策略 |
| 预期结果 | 文件画像展示该文件最近三个月的统计信息，包括文件曾用名、敏感级别、哈希值、用户、设备、应用、时间、活动等该文件的具体信息。可以进行文件的用户追踪和位置追踪。  用户画像中该文件可点击下载按钮下载文件 |
| 实际结果 | 通过 |

#### **3.4.3 文件全息图**

文件全息图从文件角度去展现与用户、设备和应用之间的关系，该文件被哪些用户访问，通过哪些设备和哪些应用接触了该文件。

|  |  |
| --- | --- |
| 测试项目 | 文件全息图 |
| 测试目的 | 验证产品对文件全息维度的展示能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 资产列表点击某个文件，切换至该文件全息图页面 |
| 预期结果 | 全息图展现这个文件的全息关联。展示该文件关联的用户、设备、应用。 |
| 实际结果 | 通过 |

#### **3.4.4 文件溯源**

敏感文件在网络中活动路径的追溯，提供对敏感文件轨迹的追踪、还原，包括详细的敏感文件访问的详细记录信息。特别如果发现了特定数据被泄漏后，可以以该数据为线索，进一步追溯访问该数据的用户，以及该数据的流动路径和传送方式（通过何种应用被外泄）。

|  |  |
| --- | --- |
| 测试项目 | 文件溯源 |
| 测试目的 | 验证产品对文件溯源的展示能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 资产列表点击某个文件，切换至该文件溯源页面 |
| 预期结果 | 展示该文件在当前时间段内溯源信息，包含基础信息和敏感信息 |
| 实际结果 | 通过 |

#### **3.4.5 文件关联信息**

显示文件关联用户，设备，应用的详细信息。

|  |  |
| --- | --- |
| 测试项目 | 文件-用户 |
| 测试目的 | 验证产品对文件关联用户的能力展示 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 资产列表点击某个文件，切换至该文件用户页面 |
| 预期结果 | 展示该文件所关联用户的账号，设备ip，设备类型，操作系统，上传下载次数，最近活动时间 |
| 实际结果 | 通过 |

|  |  |
| --- | --- |
| 测试项目 | 文件-设备 |
| 测试目的 | 验证产品对文件关联设备的能力展示 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 资产列表点击某个文件，切换至该文件设备页面 |
| 预期结果 | 展示该文件所关联设备的mac，用户账号，设备ip，设备类型，操作系统 |
| 实际结果 | 通过 |

|  |  |
| --- | --- |
| 测试项目 | 文件-应用 |
| 测试目的 | 验证产品对文件关联应用的能力展示 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 资产列表点击某个文件，切换至该文件应用页面 |
| 预期结果 | 展示该文件所关联设备的应用名，应用ip，上传下载次数，最近活动时间 |
| 实际结果 | 通过 |

|  |  |
| --- | --- |
| 测试项目 | 文件-活动 |
| 测试目的 | 验证产品对文件活动的识别能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 资产列表点击某个文件，切换至该文件活动页面 |
| 预期结果 | 展示该文件追踪图，时间，活动类型，hash值，文件大小，文件名，关联应用，用户，设备，源地址，目的地址信息 |
| 实际结果 | 通过 |

### **3.5 用户资产检测**

#### **3.5.1 用户统计**

发现和记录用户的各种账号使用情况，无遗漏的记录和跟踪每一个账号的使用情况，作为后续预警、调查取证和溯源的基础。发现宁夏烟草内部用户使用的账号，例如： 用户的企业账户，用户的互联网账户（互联网邮箱，网盘账号等），并记录用户的各种账号使用情况，无遗漏的记录和跟踪每一个账号的使用情况，作为后续预警、调查取证和溯源的基础。

|  |  |
| --- | --- |
| 测试项目 | 用户列表统计 |
| 测试目的 | 验证产品对用户信息的识别能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 用户登录各种应用 |
| 预期结果 | 成功抓取用户信息，列表可查看用户名称，关联文件、应用、设备数量，流量，下载上传文件数量，位置，时间 |
| 实际结果 | 不通过，用户名抓取失败，抓取失败的用户名带有特殊字符 |

#### **3.5.2 用户全息图**

用户全息图从用户角度去展现与文件、设备和应用之间的关系，显示该用户访问了那些文件和应用，那些设备归属该用户

|  |  |
| --- | --- |
| 测试项目 | 用户全息图 |
| 测试目的 | 验证产品对用户全息维度的展示能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 点击列表的的某个用户，切换至用户全息图 |
| 预期结果 | 全息图展现该用户所关联设备，文件，应用 |
| 实际结果 | 通过 |

#### **3.5.3 用户画像**

显示用户特有信息，如所属部门，登录名，设备统计，应用统计，日均流量，30天邮件收发分布图，邮箱及邮件服务器列表，内部邮件收发设备网段拓扑图。

|  |  |
| --- | --- |
| 测试项目 | 用户画像 |
| 测试目的 | 验证产品对用户画像的识别能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 用户列表点击某个用户，切换至该用户画像页面 |
| 预期结果 | 用户画像页面展示该用户最近三个月的统计信息，包括该用户的所属部门，登录名，设备统计，应用统计，日均流量，总流量，首次活动时间，最近活动时间，位置信息。  列表显示该设备的设备mac，最近ip，位置，首次活动时间，最近活动时间  画像页面展示用户近30天邮件收发分布图，邮箱及邮件服务器列表，内部邮件收发设备网段拓扑图 |
| 实际结果 | 通过 |

#### **3.5.4 用户关联信息**

显示用户关联文件详细信息。

|  |  |
| --- | --- |
| 测试项目 | 用户-文件 |
| 测试目的 | 验证产品对用户关联文件的能力展示 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 用户列表点击某个用户，切换至该用户文件页面 |
| 预期结果 | 展示该用户关联的文件相关信息，包括文件名，敏感类型，文件类型，文件大小，上传下载次数，应用数，最近活动时间 |
| 实际结果 | 通过 |

### **3.6 应用资产检测**

#### **3.6.1 应用统计**

应用资产的统计对于业务人员和IT人员来说重要性不言而喻，实时统计网络中的各种应用系统，从IP地址、端口、服务器等多个维度进行统计。

|  |  |
| --- | --- |
| 测试项目 | 应用列表统计 |
| 测试目的 | 验证产品对应用信息的识别能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 应用登录或上传下载文件 |
| 预期结果 | 成功抓取应用信息，应用列表可查看应用名称，协议，类别，域名，ip，活动类型，设备文件用户数，时间信息 |
| 实际结果 | 通过 |

#### **3.6.2 应用全息图**

应用全息图从应用角度去展现与文件、设备和用户之间的关系，显示该应用被那些用户设备和文件相关联。

|  |  |
| --- | --- |
| 测试项目 | 应用全息图 |
| 测试目的 | 验证产品对应用全息维度的展示能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 应用列表点击某个应用，切换至该应用全息图 |
| 预期结果 | 展示该应用关联的文件，用户，设备相关信息 |
| 实际结果 | 通过 |

#### **3.6.3 应用画像**

应用特性的展示，显示该应用特有信息，如包括类别，url，用户统计数，设备统计数，文件统计数，日均流量，总流量。

|  |  |
| --- | --- |
| 测试项目 | 应用画像 |
| 测试目的 | 验证产品对应用画像的识别能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 应用列表点击某个应用，切换至该应用画像 |
| 预期结果 | 展示该应用近三个月统计信息，包括类别，url，用户统计数，设备统计数，文件统计数，日均流量，总流量，首次出现时间，最近出现时间，位置，描述，ip地址 |
| 实际结果 | 通过 |

#### **3.6.4 业务数据**

业务数据主要包含格式为json，xml以及表单数据。

JSON（JavaScript Object Notation）是一种轻量级的数据交换格式。易于人阅读和编写，可以在多种语言之间进行数据交换。XML，可扩展标记语言 (Extensible Markup Language, XML) ，标准通用标记语言的子集，可以用来标记数据、定义数据类型，是一种允许用户对自己的标记语言进行定义的源语言。表单在网页中主要负责数据采集功能。

本测试项主要关注API接口中，交互数据内容的载体信息进行识别呈现。

|  |  |
| --- | --- |
| 测试项目 | 业务数据列表 |
| 测试目的 | 验证产品对敏感业务数据的识别能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 业务数据触发识别策略 |
| 预期结果 | 显示所有触发策略的业务数据，包括接口数，数据类别，数据级别，识别策略，用户数，设备数，最近活动时间  点击+号展开，显示api名称，hash值，数据类别，数据级别，识别策略，用户数设备数，最近活动时间 |
| 实际结果 | 通过 |

#### **3.6.5业务数据全息图**

业务数据全息图从业务数据角度角度去展现与应用、设备和用户之间的关系，显示该业务数据被那些用户设备应用件相关联。

|  |  |
| --- | --- |
| 测试项目 | 业务数据全息图 |
| 测试目的 | 验证产品对业务数据全息维度的展示能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 业务数据下点击某api的hash值，切换至全息图 |
| 预期结果 | 展示该业务数据所关联的用户，设备，应用信息 |
| 实际结果 | 通过 |

#### **3.6.6业务数据画像**

显示业务数据的特有信息，如务数据名称，匹配数据级别，hash值统计数，相关设备mac，用户名，应用，所有ip。

|  |  |
| --- | --- |
| 测试项目 | 业务数据画像 |
| 测试目的 | 验证产品对业务数据画像的识别能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 业务数据下点击某api的hash值，切换至画像 |
| 预期结果 | 展示近三个月该api的统计信息，包括业务数据名称，匹配数据级别，hash值统计数，相关设备mac，用户名，应用，所有ip，首次出现时间，最近出现时间  业务数据详细信息下可点击下载，下载业务数据信息，展示所有业务数据触发的数据级别，策略名称和匹配次数  显示所有hash值，用户数，设备数，应用数，活动次数，详情可点击查看详情 |
| 实际结果 | 通过 |

#### **3.6.7 业务数据溯源**

业务数据在网络中活动路径的追溯，提供对敏感业务数据轨迹的追踪、还原，包括详细的敏感数据访问的详细记录信息。特别如果发现了特定数据被泄漏后，可以以该数据为线索，进一步追溯访问该数据的用户，以及该数据的流动路径和传送方式（通过何种应用被外泄）。

|  |  |
| --- | --- |
| 测试项目 | 业务数据溯源 |
| 测试目的 | 验证产品对业务数据的溯源能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 业务数据下点击某api的hash值，切换至溯源 |
| 预期结果 | 展示该业务数据在当前时间段内溯源信息，详情显示该业务数据的基础信息和敏感信息 |
| 实际结果 | 通过 |

#### **3.6.8 业务数据分布图**

显示业务数据在地图上的分布图以及列表信息。

|  |  |
| --- | --- |
| 测试项目 | 业务数据分布图 |
| 测试目的 | 验证产品对业务数据分布的识别能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 业务数据下点击某api的hash值，切换分布图 |
| 预期结果 | 展示该业务数据在地图上的分布  列表显示该业务数据出现时间，业务数据名称，数据级别，数据类别，用户，应用，活动，大小信息 |
| 实际结果 | 通过 |

#### **3.6.9业务数据报表概览**

溯源平台实时发现网络中的数据资产、对数据的流转路径进行监测、持续不断的对数据行为进行全面刻画，构建数据全息关联图，提供多维度实时关联分析；呈现敏感数据安全态势，发现出境数据、数据泄露、数据滥用等风险行为；提供强大的数据溯源能力，为事件调查取证提供全面的证据链。溯源报表将通过固定模板生成对应的数据溯源能力展示。

本测试项测试溯源报表的生成功能。

|  |  |
| --- | --- |
| 测试项目 | 业务数据报表概览 |
| 测试目的 | 验证产品对业务数据生成报表的能力展现 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 业务数据下点击某api的hash值，切换报表概览，点击生成报表 |
| 预期结果 | 可查看报表详情，可生成pdf，日志报表-报表管理-溯源报表可查看该报表信息 |
| 实际结果 | 通过 |

### **3.7配置管理**

#### **3.7.1 基础信息**

网络层关系，计算机网络中，网络层的功能是包括寻址和路由选择、连接的建立、保持和终止等。它提供的服务使传输层不需要了解网络中的数据传输和交换技术。如果您想用尽量少的词来记住网络层，那就是"路径选择、路由及逻辑寻址"。网络层的目的是实现两个端系统之间的数据透明传送。

当路由器没有给设备mac分配对应的ip时，在网络层关系中配置好，可将mac与对应ip相关联起来。

|  |  |
| --- | --- |
| 测试项目 | 网络层关系 |
| 测试目的 | 验证产品对mac与ip的关联能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 添加ip与mac对应关系，路由器没有给该ip分配mac |
| 预期结果 | 系统将自动把配置中的ip和mac关联起来 |
| 实际结果 | 通过 |

邮件服务器是用来测试邮件服务器能够正常发送邮件的配置。

|  |  |
| --- | --- |
| 测试项目 | 邮件服务器 |
| 测试目的 | 验证邮件服务器发送邮件能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 配置邮件服务器 |
| 预期结果 | 可发送邮件，检测邮件服务器正常使用 |
| 实际结果 | 通过 |

syslog是UNIX系统中提供的一种日志记录方法(RFC3164)，syslog本身是一个服务器，程序中凡是使用syslog记录的信息都会发送到该服务器，服务器根据配置决定此信息是否记录，是记录到磁盘文件还是其他地方，这样使系统内所有应用程序都能以统一的方式记录日志，为系统日志的统一审计提供了方便。

|  |  |
| --- | --- |
| 测试项目 | SYSLOG |
| 测试目的 | 验证syslog日志输入输出的能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 日志输入 2. 日志输出 |
| 预期结果 | 对接深信服上网管理系统信息，获取用户登录信息  输出系统所有日志，存储到Syslog文件中 |
| 实际结果 | 通过 |

网段配置可配置内网，出域，代理服务器。

一般来说，外网，即互联网，局域网通过一台服务器或是一个路由器对外连接的网络，这个IP地址是唯一的。也就是说内网里所有的计算机都是连接到这一个外网IP上，通过这一个外网IP对外进行交换数据的。

在本测试项中，网的定义可以由客户侧人员，自主定义，默认情况下即包含：10.0.0.0-10.255.255.255,172.16.0.0-172.31.255.255,192.168.0.0-192.168.255.255。

域是由一组具有相同需求并互相信任的系统组成的逻辑区域。比如网络安全域是指同一系统内有相同的安全保护需求，相互信任，并具有相同的安全访问控制和边界控制策略的子网或网络，且相同的网络安全域共享一样的安全策略。

在本测试项中，域的定义可以由客户侧人员，自主定义。

员工有意识或无意识的在内网私自搭建代理服务器情况，给内网安全带来隐患，需要快速发现乱建代理服务器的行为。

|  |  |
| --- | --- |
| 测试项目 | 网段配置 |
| 测试目的 | 验证产品对网段配置的能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 内网网段配置 2. 代理服务器配置 3. 域定义配置，出域规则 |
| 预期结果 | 目的地址不为内网网段的数据为出网数据  配置后可在应用列表下查看服务器名称为proxy+ip  匹配出域规则的数据为出域数据 |
| 实际结果 | 通过 |

网络时间协议，英文名称：Network Time Protocol（NTP）是用来使计算机时间同步化的一种协议，它可以使计算机对其服务器或时钟源（如石英钟，GPS等等)做同步化，它可以提供高精准度的时间校正（LAN上与标准间差小于1毫秒，WAN上几十毫秒），且可介由加密确认的方式来防止恶毒的协议攻击。NTP的目的是在无序的Internet环境中提供精确和健壮的时间服务。

|  |  |
| --- | --- |
| 测试项目 | Ntp设置 |
| 测试目的 | 验证产品对ntp配置的能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 添加ntp服务器 |
| 预期结果 | 可成功校准时间 |
| 实际结果 | 通过 |

#### **3.7.2 数据管理配置**

配置数据级别和类别，数据类别可绑定级别，识别策略需选择数据数据类别，数据触发识别策略后，可查看该数据匹配的数据级别和类别。

|  |  |
| --- | --- |
| 测试项目 | 数据级别 |
| 测试目的 | 验证产品对敏感数据的数据级别的识别能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 添加数据级别，文件触发识别策略 |
| 预期结果 | 资产列表可查看该文件数据级别 |
| 实际结果 | 通过 |

|  |  |
| --- | --- |
| 测试项目 | 数据类别 |
| 测试目的 | 验证产品对敏感数据的数据类别的识别能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 添加数据类别，文件触发识别策略 |
| 预期结果 | 资产列表可查看该文件数据类别 |
| 实际结果 | 通过 |

#### **3.7.3 分级分类**

配置数据元素，识别策略和脱敏策略，。数据元素可设置关键字和正则表达式，新增识别策略时可选择数据元素，匹配到该元素里面内容的数据为敏感数据，识别策略也可选择特定的hash，文件名，文件类型作为敏感文件选项；脱敏规则配置后可在账户列表被用户选择，对应的脱敏规则可限制用户查看页面信息，对应的信息会被加密。

|  |  |
| --- | --- |
| 测试项目 | 数据元素&识别策略 |
| 测试目的 | 验证产品对正则表达式识别策略的识别能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 添加数据元素身份证，元素内容为身份证正则表达式，添加识别策略包含数据元素身份证并下发 2. 上传下载内容包含身份证的文件 3. 数据元素导入政务通用数据模板，添加元素至56个 4. 识别策略添加导入至51条识别策略 |
| 预期结果 | 文件被识别为敏感文件，资产列表可查看该文件触发的识别策略，文件画像可查看匹配的敏感规则  数据元素模板导入成功，添加元素成功  识别策略添加导入成功 |
| 实际结果 | 通过 |

|  |  |
| --- | --- |
| 测试项目 | 脱敏策略 |
| 测试目的 | 验证产品对脱敏策略的识别能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 添加脱敏策略，添加账户时给人员添加策略 |
| 预期结果 | 该人员查看系统时对应对象被脱敏加密 |
| 实际结果 | 通过 |

#### **3.7.4 用户管理**

可导入组织结构，可根据账户名匹配用户名称。

AD LDAP 目录是基于条目的网络资源数据库，一个条目就是一个信息合集，是 LDAP 中一个基本的存储单元。在 LDAP 中，目录的条目是按树状的层次结构组织的。Ad ldap服务器可拉取用户信息，前提是在服务器上配置好相关的组合用户，连接成功后可拉取相关的组和用户至组织结构中。

|  |  |
| --- | --- |
| 测试项目 | 组织结构 |
| 测试目的 | 验证产品对组织架构导入的识别能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 导入组织结构 |
| 预期结果 | 成功导入，可在用户资产下查看 |
| 实际结果 | 通过 |

|  |  |
| --- | --- |
| 测试项目 | AD LDAP服务器 |
| 测试目的 | 验证产品对拉取ad ldap服务器用户信息的能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 配置AD LDAP服务器连接成功 |
| 预期结果 | 获取AD LDAP服务器用户信息 |
| 实际结果 | 未测试 |

#### **3.7.5 应用管理**

对应用进行配置，可添加或导入企业应用。

|  |  |
| --- | --- |
| 测试项目 | 应用配置 |
| 测试目的 | 验证产品添加导入应用的能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 添加或导入应用 |
| 预期结果 | 添加导入成功，应用资产可查看 |
| 实际结果 | 通过 |

#### **3.7.7 采集模块**

采集器即平台自研的流量采集探针，用来监测企业组织中的网络流量信息，它包括旁路镜像模式、代理模式和混合模式，分别用在不同的场景。

本测试项将测试采集器的基础信息展示情况。

|  |  |
| --- | --- |
| 测试项目 | 基础配置 |
| 测试目的 | 验证采集模块基础配置功能 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 配置采集器信息，包括采集策略，版本升级，采集器调试，采集器删除 2. Bypass异常触发条件配置 3. 采集模块升级包导入 |
| 预期结果 | 成功 |
| 实际结果 | 通过 |

配置白名单后可过滤对应ip的流量。

|  |  |
| --- | --- |
| 测试项目 | 白名单 |
| 测试目的 | 验证产品对白名单的过滤功能 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 域名白名单设置监控域名和不监控域名 2. 添加源ip白名单 3. 添加目的ip白名单 4. 添加特殊账号白名单 |
| 预期结果 | 解析监控域名的流量，不解析域名流量不抓取  不解析源ip为白名单中的ip流量  不解析ip为白名单中的ip流量  不解析账号为白名单中的账号流量（目前只针对于深信服ac系统，盈高wifi准入系统） |
| 实际结果 | 通过 |

在测试场景中，当采集器部署在Proxy模式，则需要导入证书。如果客户环境不具有证书体系，无法提供证书，则系统可以提供自签名证书用于测试，需要提供电脑版证书和移动端证书。勾选证书后可解密加密的流量信息。

本次测试环境为Tap模式，无法测试该功能。

|  |  |
| --- | --- |
| 测试内容 | 证书加密设置 |
| 测试目的 | 验证产品对加密流量解析功能 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1.勾选证书加密选项 |
| 预期结果 | 1.可抓取加密流量 |
| 实际结果 | 本次未测试，部署环境为旁路tap模式，不支持抓取加密流量 |

应用特征，即自定义账号特征，在客户侧通常会有非标准的业务系统及账号的使用，通过TAC人员介入，可以对私有化应用的账户名进行二次开发配置，以达到自动识别并展示账号的目的。

本测试项主要针对特殊用途的业务应用的账户名进行提取。

|  |  |
| --- | --- |
| 测试项目 | 应用特征 |
| 测试目的 | 验证应用特征规则对登录名的识别功能 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 添加客户平台登录行为规则 2. 添加中烟新商盟订货商务平台登录行为规则 |
| 预期结果 | 成功抓取登录账号信息  成功抓取登录账号信息 |
| 实际结果 | 通过 |

|  |  |
| --- | --- |
| 测试项目 | SSL解密 |
| 测试目的 | 验证私钥对加密流量解析功能 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1.导入私钥，添加ip端口 |
| 预期结果 | 解密ip端口加密的流量 |
| 实际结果 | 通过 |

#### **3.7.8 许可证**

显示许可证过期时间，过期后系统将不允许访问，可重新导入未过期的许可证信息。

|  |  |
| --- | --- |
| 测试项目 | 许可证测试 |
| 测试目的 | 验证产品对许可证的识别能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 导入许可证，修改授权过期时间 |
| 预期结果 | 导入成功，过期时间修改成功 |
| 实际结果 | 通过 |

#### **3.7.9 账户管理**

管理账户信息，配置账户的角色以及脱敏规则。

|  |  |
| --- | --- |
| 测试项目 | 账户管理 |
| 测试目的 | 验证产品对账户的管理能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 账户管理设置，包括账户的新增，编辑，修改，删除，给账户配置角色，选择脱敏策略 |
| 预期结果 | 测试成功 |
| 实际结果 | 通过 |

#### **3.7.10 告警通知**

配置告警通知，规则告警或智能告警触发或系统告警，发送邮件给告警中的人员。

|  |  |
| --- | --- |
| 测试项目 | 告警通知组 |
| 测试目的 | 验证产品对告警通知组的识别能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 添加告警通知，规则告警或智能告警触发或系统告警，发送邮件给告警中的人员 |
| 预期结果 | 成功发送邮件，告警通知中的人员成功收到邮件 |
| 实际结果 | 通过 |

#### **3.7.11 聚类分析**

系统运行14天后会产生数据，根据算法检测某些与大部分用户行为不一致的用户。

|  |  |
| --- | --- |
| 测试项目 | 聚类分析 |
| 测试目的 | 验证产品对用户异常行为的识别能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 系统运行14天产生数据，创建聚类分析 |
| 预期结果 | 聚类分析结果生成 |
| 实际结果 | 未测试 |

#### **3.7.12 系统告警**

系统告警，即平台自身检测机制，当平台各组件模块遇到问题时，系统会产生相应的告警，比如可视化模块、机器学习模块、数据存储服务、数据解析服务、日志队列服务和采集器监控等。

|  |  |
| --- | --- |
| 测试项目 | 系统告警 |
| 测试目的 | 验证产品对系统告警的检测能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 选择告警通知时间间隔，触发系统告警 |
| 预期结果 | 成功发送告警通知，并在间隔时间后重新发送告警通知 |
| 实际结果 | 通过 |

### **3.8 系统状态**

#### **3.8.1 运行状态**

展示系统内各个组件的运行状态。

|  |  |
| --- | --- |
| 测试项目 | 分析系统 |
| 测试目的 | 验证产品对各个组件的检测能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 展示cms，机器学习，数据存储服务，数据解析服务，日志队列服务状态信息以及运行时长 |
| 预期结果 | 所有状态都是up，运行时长显示正确 |
| 实际结果 | 通过 |

显示所有采集器的信息。

|  |  |
| --- | --- |
| 测试项目 | 采集模块 |
| 测试目的 | 验证产品对采集器状态的展示能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 显示所有采集器名称，系统状态，bypass状态，创建时间，位置，采集器id，授权过期时间 |
| 预期结果 | 展示正确 |
| 实际结果 | 通过 |

#### **3.8.2 日志记录**

显示系统所有日志。

|  |  |
| --- | --- |
| 测试项目 | 系统通知 |
| 测试目的 | 验证产品对系统组件的状态展示能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 查看系统通知 |
| 预期结果 | 展示系统模块运行日志，包括设备类型，设备id，设备ip，标题，描述，等级，结果，时间信息 |
| 实际结果 | 通过 |

显示cms系统日志。

|  |  |
| --- | --- |
| 测试项目 | CMS日志 |
| 测试目的 | 验证产品对cms日志的采取能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 查看cms日志 |
| 预期结果 | 展示cms web系统的审计日志，包括账号，时间，动作，状态，ip，位置，以及详情信息 |
| 实际结果 | 通过 |

### **3.9 日志报表**

#### **3.9.1报表管理**

运营报表，即数据溯源平台的动态统计报表，可以为报表的阅读者提供作出合理的决策所需要的有关资料，可用来直观的看到平台的相关功能统计结果。它可以通过限定用户群组、按时间周期来查询异常类及统计类的报表。

本测试项将展示平台运营能力的基础报表。

|  |  |
| --- | --- |
| 测试项目 | 运营报表 |
| 测试目的 | 验证产品对运营报表生成的能力检测 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 添加报表，生成报表 |
| 预期结果 | 生成报表内容包含智能告警，按Top 应用 - 按流量统计，网络活动情况 - 流量统计直方图，Top 活跃用户 - 按访问应用数统计，用户活动情况 - 用户数统计直方图，Top 文件访问 - 按访问文件数统计，敏感文件-外网上传，Top 文件访问 - 按流量统计，敏感文件-内网下载信息 |
| 实际结果 | 通过 |

溯源平台实时发现网络中的数据资产、对数据的流转路径进行监测、持续不断的对数据行为进行全面刻画，构建数据全息关联图，提供多维度实时关联分析；呈现敏感数据安全态势，发现出境数据、数据泄露、数据滥用等风险行为；提供强大的数据溯源能力，为事件调查取证提供全面的证据链。溯源报表将通过固定模板生成对应的数据溯源能力展示。

本测试项测试溯源报表的生成功能。

|  |  |
| --- | --- |
| 测试项目 | 溯源报表 |
| 测试目的 | 验证产品对溯源报表生成的能力检测 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 数据溯源下点击文件，邮件，业务数据，报表概览下生成溯源报表 |
| 预期结果 | 溯源报表生成成功，内容包含数据画像，数据分布图，数据关联图/表，数据时序图信息 |
| 实际结果 | 通过 |

#### **3.9.2 查询工具**

应用层（Application layer）是七层OSI模型的第七层。应用层直接和应用程序接口并提供常见的网络应用服务。平台将对类应用层的日志进行统计展示。

本测试项将对类应用层的业务日志进行统计、归类、展示。

|  |  |
| --- | --- |
| 测试项目 | 应用日志 |
| 测试目的 | 验证产品对应用日志的采集能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 可查询应用日志 |
| 预期结果 | 包含时间，主机，源mac，源ip，目的ip，响应时间，目的端口，活动，应用，详情信息 |
| 实际结果 | 通过 |

网络层的目的是实现两个端系统之间的数据透明传送，具体功能包括寻址和路由选择、连接的建立、保持和终止等。它提供的服务使传输层不需要了解网络中的数据传输和交换技术。平台将对类网络层的日志进行统计展示。

本测试项将对类网络层的业务日志进行统计、归类、展示。

|  |  |
| --- | --- |
| 测试项目 | 网络日志 |
| 测试目的 | 验证产品对网络日志的采集能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 可查询网络日志 |
| 预期结果 | 包含时间，协议，源mac，源ip，目的ip，目的端口，总流量，应用，主机，详情信息 |
| 实际结果 | 通过 |

Proxy模式下产品可抓取网络中加密流量，对于加密流量抓取失败的的情况，产品会通过日志进行统计展示。

|  |  |
| --- | --- |
| 测试项目 | SSl失败日志 |
| 测试目的 | 验证产品对ssl失败日志的采集能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 可查询ssl失败日志 |
| 预期结果 | 包含时间，域名，失败原因，源ip，源端口，目的ip，目的端口，详情信息 |
| 实际结果 | 本次未测试，部署环境为旁路tap模式，不支持抓取加密流量 |

#### **3.9.2 账户日志**

用户在设备上从非企业账号切换至企业账号，或者从企业账号a切换至企业账号b，都会产生账户变更日志，账户日志可查看这些信息。

|  |  |
| --- | --- |
| 测试项目 | 账户日志 |
| 测试目的 | 验证产品对账户日志的采集能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 设备登录后变更企业账号 |
| 预期结果 | 账户日志可查看变更信息，包含现用户id，原用户id，源ip，源mac，类型，配置时间，详情信息 |
| 实际结果 | 通过 |

### **3.10规则告警**

规则告警是平台根据大量用户实践，而设立的一些预定义的告警场景，这其中用户可以根据自身的业务场景，可通过平台定义的功能项而建立自定义场景。

系统会默认内置一定的告警规则，告警场景有数据下载异常，数据邮件发送异常，数据外泄异常，数据流转异常，数据出域，数据出境，数据出网，自定义相关的告警规则，系统触发该告警后可在告警下查看处理这些告警。

|  |  |
| --- | --- |
| 测试项目 | 数据下载异常场景测试 |
| 测试目的 | 验证产品对规则告警触发的识别能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 规则告警下配置告警场景为数据下载异常告警 2. 下载数据触发告警 |
| 预期结果 | 触发告警成功，告警详情页面可查看详细告警信息 |
| 实际结果 | 通过 |

### **3.11 机器学习智能告警**

智能告警，即平台自有算法通过为期14天的后台无感知学习，形成基线模型，对之后监测到的数据进行滚动递归学习、匹配、告警、展示等行为。

本测试项目将对人工智能元素匹配到的风险事件进行告警。它包括：应用文件访问异常、用户访问文件异常、用户下载文件异常、用户上传文件异常。

#### **3.11.1 用户-上传敏感文件异常**

对每个用户每天上传的敏感类型文件总次数进行画像，根据历史值计算未来的预测值和上限阀值。

|  |  |
| --- | --- |
| 测试项目 | 用户-上传敏感文件异常 |
| 测试目的 | 验证产品基于机器学习的异常告警的能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 用户连续上传敏感文件14天（系统会根据14天的访问量计算阈值），14天后该用户上传敏感文件超过阈值 |
| 预期结果 | 触发智能告警，告警-智能告警下可查看告警详情 |
| 实际结果 | 通过 |

#### **3.11.2 应用-文件访问异常**

对某个应用上传和下载商业文件总次数进行画像，根据历史值计算未来每天的预测值和上限阀值。

|  |  |
| --- | --- |
| 测试项目 | 用户-上传敏感文件异常 |
| 测试目的 | 验证产品基于机器学习的异常告警的能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 用户连续访问文件14天（系统会根据14天的访问量计算阈值），14天后该用户访问文件超过阈值 |
| 预期结果 | 触发智能告警，告警-智能告警下可查看告警详情 |
| 实际结果 | 通过 |

#### **3.11.3 用户-访问文件异常**

对某个用户上传和下载商业文件总次数进行画像，根据历史值计算未来的预测值和上限阀值。

|  |  |
| --- | --- |
| 测试项目 | 用户-访问文件异常 |
| 测试目的 | 验证产品基于机器学习的异常告警的能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 用户连续访问文件14天（系统会根据14天的访问量计算阈值），14天后该用户访问文件超过阈值 |
| 预期结果 | 触发智能告警，告警-智能告警下可查看告警详情 |
| 实际结果 | 通过 |

#### **3.11.4 用户-下载文件异常**

对某个用户下载敏感文件总次数进行画像，根据历史值计算未来的预测值和上限阀值。

|  |  |
| --- | --- |
| 测试项目 | 用户-下载文件异常 |
| 测试目的 | 验证产品基于机器学习的异常告警的能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 用户连续下载文件14天（系统会根据14天的访问量计算阈值），14天后该用户下载文件超过阈值 |
| 预期结果 | 触发智能告警，告警-智能告警下可查看告警详情 |
| 实际结果 | 通过 |

### **3.12 首页信息**

|  |  |
| --- | --- |
| 测试项目 | 资产统计 |
| 测试目的 | 验证产品对资产统计情况的展示能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 登录后跳转至首页 |
| 预期结果 | 数据资产展示文件数和邮件数  用户资产展示企业用户数和非企业用户数  应用资产展示企业应用和互联网应用 |
| 实际结果 | 通过 |

|  |  |
| --- | --- |
| 测试项目 | 风险告警 |
| 测试目的 | 验证产品对告警的展示能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 首页下拉至风险告警模块 |
| 预期结果 | 展示高风险、中风险、低风险数量规则告警环形图  展示用户维度、应用维度、其他数量智能告警环形图  展示系统告警数量环形图 |
| 实际结果 | 通过 |

|  |  |
| --- | --- |
| 测试项目 | 风险数据 |
| 测试目的 | 验证产品对风险数据的展示能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 首页下拉至风险数据模块 |
| 预期结果 | 展示出境数据线性图以及最近5条数据  展示出网数据线性图以及最近5条数据  展示出域数据线性图以及最近5条数据 |
| 实际结果 | 通过 |

|  |  |
| --- | --- |
| 测试项目 | 业务系统 |
| 测试目的 | 验证产品展示数据级别和网段用户的能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 首页下拉至业务系统模块 |
| 预期结果 | 展示所有数据级别触发次数柱状图  展示所有网段用户比例饼状图 |
| 实际结果 | 通过 |

|  |  |
| --- | --- |
| 测试项目 | 系统状态 |
| 测试目的 | 验证产品展示系统日志和系统运行状态的能力 |
| 测试环境 | 参考拓扑图 |
| 测试步骤 | 1. 首页下拉至系统状态模块 |
| 预期结果 | 系统日志下展示系统日志量线形图以及磁盘占用量柱状图  系统运行情况下展示cpu使用率、内测使用率、磁盘使用率环形图 |
| 实际结果 | 通过 |

## 4.测试总结

### **4.1****测试项目一览表**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 类别 | 项目 | 测试结果 |
| 1 | 文件识别 |  | 通过 |
| 2 | 敏感数据监测 | 关键字 | 通过 |
| 3 | 正则表达式 | 通过 |
| 4 | 特殊hash | 通过 |
| 5 | 特殊文件名 | 通过 |
| 6 | 特殊文件类型 | 通过 |
| 7 | 数据级别&类别 | 通过 |
| 8 | 敏感数据下载 | 通过 |
| 9 | 敏感数据态势 | 通过 |
| 10 | 出网数据 | 通过 |
| 11 | 出境数据 | 通过 |
| 12 | 出域数据 | 通过 |
| 13 | 数据溯源 |  | 通过 |
| 14 | 数据资产检测 | 资产统计 | 通过 |
| 15 | 文件画像 | 通过 |
| 16 | 文件全息图 | 通过 |
| 17 | 文件溯源 | 通过 |
| 18 | 文件关联信息 | 通过 |
| 19 | 用户资产检测 | 用户统计 | 不通过 |
| 20 | 用户全息图 | 通过 |
| 21 | 用户画像 | 通过 |
| 22 | 用户关联信息 | 通过 |
| 23 | 应用资产信息 | 应用统计 | 通过 |
| 24 | 应用全息图 | 通过 |
| 25 | 应用画像 | 通过 |
| 26 | 业务数据 | 通过 |
| 27 | 业务数据全息图 | 通过 |
| 28 | 业务数据画像 | 通过 |
| 29 | 业务数据溯源 | 通过 |
| 30 | 业务数据分布图 | 通过 |
| 31 | 业务数据报表概览 | 通过 |
| 32 | 基础信息 |  | 通过 |
| 33 | 数据管理配置 |  | 通过 |
| 34 | 分级分类 |  | 通过 |
| 35 | 用户管理 |  | Ad ldap服务器拉取用户未测试 |
| 36 | 应用管理 |  | 通过 |
| 37 | 规则告警 | 数据下载异常 | 通过 |
| 38 | 机器学习 | 用户-上传敏感文件异常 | 通过 |
| 39 | 应用-文件访问异常 | 通过 |
| 40 | 用户-访问文件异常 | 通过 |
| 41 | 用户-下载文件异常 | 通过 |
| 42 | 告警通知 |  | 通过 |
| 43 | 聚类分析 |  | 未测试 |
| 44 | 系统告警 |  | 通过 |
| 45 | 采集模块 |  | 证书模块未测试 |
| 46 | 许可证 |  | 通过 |
| 47 | 账户管理 |  | 通过 |
| 48 | 系统状态 | 运行状态 | 通过 |
| 49 | 日志记录 | 通过 |
| 50 | 日志报表 | 报表管理 | 通过 |
| 51 | 查询工具 | Ssl失败日志未测试 |
| 52 | 账户日志 | 通过 |
| 53 | 首页信息 |  | 通过 |

### **4.2****测试概述**

宁夏烟草的测试分为3个阶段：

第一阶段：系统上线。该阶段主要是考察设备运行的可靠性和稳定性，以及是否会对客户现网产生影响。经过观察，设备运行可靠，没有对宁夏烟草现网产生任何影响，完全做到了无感知的自动数据采集、刻画和分析；

第二阶段：系统正式运行测试。DAST开始正式运行测试，工程师定期巡检，查看设备状态，优化敏感规则和告警，为了充分收集数据，全面刻画和分析宁夏烟草业务系统在“用户，设备，应用，文件”等四个维度的全息画像。在正式运行测试阶段前期， 对DAST系统进行了多次故障排除、版本升级和BUG修补；

第三阶段：采集数据，编写测试报告。由于DAST是数据驱动的分析系统，一切功能测试和报告都是以现网的实际数据为基础，因此，根据POC测试方案，进行了测试数据采集作为测试报告的素材，并稍后完成了测试报告。

经过一段时间系统运行，主要功能都已测试完成并通过，未通过功能为用户名抓取失败，未测试功能为ad ldap服务器用户信息拉取（未配置ad ldap服务器），ssl失败日志以及采集模块下的证书未测试（用户部署模式为tap模式不支持该功能），聚类分析（用户样本量太少），未测试功能在本地系统测试都已通过。

总体来说，系统运行稳定，DAST通过了要求的测试项目，经验证完成测试目标，能够对宁夏烟草敏感数据追溯提供了有力的工具，对敏感数据的监控、审计、合规检查提供了高效支持，达到了预期测试目标。