基础电信企业物联网专网网络安全监测系统运行效能测试规范

2023 年 5 月

目　　录

前　　言

本文件依据《基础电信企业物联网专网网络安全监测技术能力要求》和《基础电信企业物联网专网网络安全监测接口规范》要求，针对各专业公司独立建设的物联网专网网络安全监测系统，在系统能力达标情况和数据质量两方面提出具体的评估指标项及评分规则，同时也提出了相应的检测评估方法和要点。

本文件指导单位：工业和信息化部网络安全管理局

本文件编制单位：中国信息通信研究院、中国电信集团有限公司、中国移动通信集团有限公司、中国联合网络通信集团有限公司

基础电信企业物联网专网网络安全监测系统运行效能测试规范

1 目的和范围

物联网专网网络安全监测技术体系主要分为两部分：一是基础电信企业侧平台（下文简称“企业侧”）；二是物联网专网网络安全监测部侧平台（下文简称“部侧平台”）。其目的在于实现物联网专网网络流量的实时采集、流量协议识别、网络威胁监测、威胁研判和集中管理等能力，为推进网络空间安全治理提供重要技术支持。本文件旨在评估系统运行效能（系统能力、数据质量等），以规范物联网专网网络安全监测技术手段的建设。

本文件依据《工网安函〔2022〕303号》中要求，针对物联网安全监测技术提出具体的建设要求和评分标准，同时也提出了相应的检测评估方法。

本文件适用于对基础电信企业物联网专网监测系统建设情况的评测评估。

2 参考文件

工网安函〔2022〕303号文附件《基础电信企业物联网专网网络安全监测技术能力要求》

工网安函〔2022〕303号文附件《基础电信企业物联网专网网络安全监测接口规范》

3 术语和定义

下列术语和定义适用于本文件。

3.1 有害程序

有害程序指的是在用户不知情或未授权的情况下，在系统中安装、运行以达到不正当目的，或具有违反国家相关法律法规行为的可执行文件、代码模块或代码片段。

3.2 网络攻击

网络安全事件，是指网络系统中的软件、硬件及信息资源，受到偶然或恶意的破坏、控制、篡改、攻击、劫持和泄露的事件，分为Web攻击事件、系统漏洞利用事件、拒绝服务事件等。

3.3 主机受控

主机受控事件是指因主机（物联网终端）通过漏洞或受到僵尸、木马等恶意程序远程控制而导致的网络安全事件。

3.4 恶意资源

恶意资源指的是被用于实施网络攻击的恶意IP地址、恶意域名、恶意URL、恶意电子信息，包括木马和僵尸网络控制端，钓鱼网站，钓鱼电子邮件、短信/彩信、即时通信等。

3.5 恶意报文

恶意报文指的是疑似被用于实施网络攻击、传输恶意程序而在互联网上传输的网络数据包，包括基本协议包头、源目的IP、源目的端口、数据长度、通信载荷等。

3.6 恶意文件

恶意文件指的是被用于实施网络攻击的恶意程序，包括木马、病毒、僵尸程序、移动恶意程序等的样本文件。

4 基础电信企业物联网专网网络安全监测系统运行效能评估体系

基础电信企业物联网专网网络安全监测系统运行效能评估体系分为系统能力和数据质量评估。物联网专网网络安全监测系统运行效能评估体系采用扣分制，如果有评分指标不满足，则扣除相应分数。

4.1 系统能力

基础电信企业物联网专网网络安全监测系统能力主要包括流量实时采集、流量协议识别、网络威胁监测、威胁研判、集中管理等能力，具体指标项如下。

4.1.1 监测带宽覆盖

监测带宽覆盖指标体现出基础电信企业物联网专网网络流量覆盖情况，具体指标项如表1所示。

表1 物联网专网网络安全监测带宽覆盖指标

指标名称	指标项	指标描述	评分规则
监测带宽覆盖指标	物联网专网覆盖范围	物联网专网网络安全监测系统在物联网基地的覆盖部署情况，评估覆盖率。	覆盖本企业物联网基地2/3/4G和NB-IoT通信网络制式，覆盖率100%。

4.1.2 功能完备情况

4.1.2.1 流量实时采集能力

表2 物联网专网网络安全监测流量实时采集能力指标

指标名称	指标项	指标描述	评分规则
功能完备指标	流量实时采集能力	具备对本企业全部物联网基地进行双向原始流量实时获取、数据包重组和文件还原等操作的能力。	1. 应具备按照指令规则（如APN、IMEI号、IP五元组等）筛选流量，向部侧预处理模块发送原始流量； 2. 依据规则将实时流量还原为文件，文件格式包括apk、ipa、jar、dex、hap、zip、elf、so等，文件格式见《基础电信企业物联网专网网络安全监测技术能力要求》附录A 表A.1；还原率不得低于90%； 3. 增强级：具备按照涉车终端IMEI号、APN、Host、SNI等规则筛选车联网原始流量并输出至部侧预处理模块。

4.1.2.2 流量协议识别能力

表3 物联网专网网络安全监测流量协议识别能力指标

指标名称	指标项	指标描述	评分规则
功能完备指标	流量协议识别能力	具备物联网（含车联网）流量协议解析能力。	1. 流量协议解析应包括但不限于MQTT、XMPP、COAP、ONVIF、RTSP、GB/T32960、JT/T808、JT/T809、UPNP等主流的物联网（含车联网）协议，共不少于15种，协议类型见《基础电

			信企业物联网专网网络安全监测技术能力要求》附录A 表A.2； 2. 增强级：支持物联网终端、涉车终端、车联网APP、物联网平台、车联网平台相关的通联日志。
		具备物联网（含车联网）设备识别能力。	基于流量识别主流物联网/涉车终端不少于100种，并记录包括终端类型、行业类型、IMEI号码等信息。

4.1.2.3 网络威胁监测能力

表4 物联网专网网络威胁监测能力指标

指标名称	指标项	指标描述	评分规则
功能完备指标	网络威胁检测能力	具备物联网安全事件监测能力。	1. 安全事件特指网络攻击事件、主机受控事件、有害程序传播事件； 2. 从安全事件发生，到部侧平台接收网络安全事件监测记录的时间不超过2小时； 3. 安全事件监测准确率达到90%。注：监测准确率是指在实际测试中，系统按特定规则监测到的事件数量与测试中实际投放符合该规则事件总数的比值。
		具备物联网恶意程序的监测能力。	1. 能根据自带的恶意程序特征及部侧平台下发的特征，识别恶意程序，捕获其中的恶意样本和疑似恶意样本文件； 2. 恶意样本信息至少包括样本文件的原始文件名、样本文件MD5值、样本文件的文件大小、恶意程序属性分类、恶意样本描述，恶意程序病毒名称等日志信息； 3. 已知恶意样本捕获率不得低于85%，注：样本捕获率是指在实际测试中，系统捕获恶意样本数量与测试中投放恶意样本总数的比值； 4. 增强级：具备在物联网专网中识别对车、车联网平台造成隐私泄露、系统破坏、窃听等

			涉车恶意APP的能力，包括涉车恶意APP传播事件和涉车恶意APP样本信息提取。

4.1.2.4 威胁研判能力

表5 物联网专网网络安全监测威胁研判能力指标

指标名称	指标项	指标描述	评分规则
功能完备指标	威胁研判能力	具备恶意程序应用样本的研判能力。	1. 对疑似样本和恶意网络行为进行分析和判定，并依据结果报送黑样本至部侧平台； 2. 支持APP应用的基础数据提取，包括APP的下载链接、开发者、API调用信息、家族等信息； 3. 恶意程序研判结果包括但不限于：样本MD5、研判评分、恶意程序名称、恶意程序类型、主控地址、下载地址（若有）、控制端邮箱（若有）、控制端号码（若有）等； 4. 支持针对有重大社会影响，严重影响网络运行的新型恶意代码，在3天内研判出恶意代码特征、下载URL、主控URL等信息，并上报部侧平台。
		基础信息的管理能力。	具备对专网覆盖物联网平台、车联网平台、物联网终端、涉车终端等基础信息数据进行管理的能力，终端信息库应包括但不限于物联网终端、涉车终端的终端名称、终端型号、行业类型、厂商、终端软件版本等信息；平台信息库应包括但不限于物联网平台、车联网平台的平台名称、平台IP地址、平台域名地址（若有）等信息。
		涉车恶意APP（包括车联网手机APP和车载APP）的研判能	增强级：支持研判涉车恶意APP相关信息，包括但不限于版本号、开发者、主控URL地址、恶意样本MD5、恶意行为类型等信息。

		力。	

4.1.2.5 集中管理能力

表6 物联网专网网络安全监测集中管理指标

指标名称	指标项	指标描述	评分规则
功能完备指标	集中管理能力	具备对网络威胁监测结果数据、基础信息数据、通联数据等的集中管理、存储能力。	数据存储应满足以下列具体要求：疑似及恶意样本文件及相关文件信息（MD5、样本类型等）的留存时间不少于60天；报文文件（例如原始流量PCAP文件）及相关信息的留存时间不少于7天；事件的监测日志留存时间不少于6个月；事件的监测统计数据留存时间不少于6个月；维护管理产生的审计记录数据留存时间不少于6个月；基础信息数据记录留存时间不少于6个月；增强级：通联日志记录留存时间不少于6个月。

4.1.3 协同联动能力

协同联动指标主要评估企业侧系统与部侧平台指令协同能力，即指令接收、数据回传、日志存储等，具体指标如表7所示。

表7 物联网专网网络安全监测系统协同联动指标

指标名称	指标项	指标描述	评分规则
协同联动指标	指令协同能力评估	具备与部侧平台指令交互的能力。	1. 接收部侧平台下发的监测（恶意报文、恶意文件）指令，解析并执行指令内容，向部侧平台反馈指令执行结果数据； 2. 接收部侧平台下发的流量筛选指令，解析并执行指令内容，向部侧平台反馈PCAP包或向部侧流量预处理输出原始流量； 3. 增强级：接收部侧平台下发的通联日志查询指令，解析并执行指令内容，向部侧平台反馈符合规则的通联日志信息。

4.2 数据质量

基础电信企业物联网专网网络安全监测系统数据质量指标分为常态化数据上报和指令协同数据上报，具体指标项如下。

4.2.1 及时性

常态化上报及反馈数据的及时性指标如表8所示。

表8 物联网专网网络安全监测数据及时性指标

指标名称	指标项	指标描述	评分规则
及时性指标	物联网（含车联网）终端信息上报	按照《基础电信企业物联网专网网络安全监测接口规范》验证企业侧上报的物联网（含车联网）终端信息、网络安全事件、恶意程序文件、原始流量文件、状态信息上报和指令反馈数据的及时性。	及时性要求如下： 1. 上报数据及时性：比较验证数据上报时间和数据生成时间是否满足要求； 2. 恶意文件研判及时性：针对有重大社会影响，严重影响网络运行的新型恶意代码，在3天内上报部侧平台。
	网络安全事件上报		
	恶意程序文件上报		
	原始流量、PCAP包上报		
	状态信息上报		
	指令反馈数据上报		

4.2.2 准确性

常态化上报及反馈数据的准确性指标如表9所示。

表9 物联网专网网络安全监测数据准确性指标

指标名称	指标项	指标描述	评分规则
准确性指标	物联网（含车联网）终端信息上报	按照《基础电信企业物联网专网网络安全监测接口规范》验证企业侧上报的物联	准确性要求如下： 1. 字段字符格式准确性：验证所填字段的字符格式是否符合规范要求，包括但不限于是否包含非法字符、是否超出最大长度限制、是否缺
	网络安全事件上报		
	恶意程序文件上报		
	原始流量、PCAP包上报		

	状态信息上报	网（含车联网）终端信息、网络安全事件、恶意程序文件、原始流量文件、状态信息上报和指令反馈数据的准确性。	少必要的字符、是否符合字段特征（如IP、域名等）等； 2. 验证所填字段的枚举值是否符合规范要求，即是否在枚举列表中存在； 3. 异常值准确性：检查上报数据中是否存在异常数据，如重复数据等； 4. 数据类型准确性：依据数据类型判断数据准确率，如非其他安全事件按照其他安全事件类型报送； 5. 数据业务逻辑准确性：依据业务逻辑判断数据准确性要求，如根据事件类型判定攻击方向、攻击阶段、危害等级、攻击载荷等关键字段是否匹配。
	指令反馈数据上报		

4.2.3 完整性

常态化上报及反馈数据的完整性指标如表10所示。

表10 物联网专网网络安全监测数据完整性指标

指标名称	指标项	指标描述	评分规则
完整性指标	物联网（含车联网）终端信息上报	按照《基础电信企业物联网专网网络安全监测接口规范》验证企业侧上报的物联网（含车联网）终端信息、网络安全事件、恶意程序文	完整性要求如下： 1. 上报数据类型完整性：按照要求上报终端信息、安全事件（主机受控事件、网络攻击事件、有害程序传播事件含恶意文件、监测指令反馈记录、通联日志查询结果等数据； 2. 必填字段上报：根据接口规范要求，验证必填字段是否
	网络安全事件上报		
	恶意程序文件上报		
	原始流量、PCAP包上报		
	状态信息上报		
	指令反馈数据上报		

		件、原始流量文件、状态信息上报和指令反馈数据的完整性。	符合规范； 3. 选填字段上报：验证选填字段（如攻击载荷、终端类型、终端所属行业、受影响单位网络方向等字段）是否完整填报。

4.2.4 可用性

常态化上报及反馈数据的可用性指标如表11所示。

表11 物联网专网网络安全监测数据及时性指标

指标名称	指标项	指标描述	评分规则
可用性指标	网络安全事件上报	按照《基础电信企业物联网专网网络安全监测接口规范》验证企业侧上报网络安全事件的可用性。	可用性要求如下： 近1个月内累计故障时间累计不超过24小时。

5 基础电信企业物联网专网网络安全监测系统运行效能评估方法

5.1 概述

对于物联网专网网络安全监测系统运行效能的检测评估方法如下：

评估人员使用相关技术工具部署和测试，以检测基础电信企业的物联网专网网络安全监测系统的运行效能，并评估其是否满足考核要求，包括系统能力和数据质量。部署环境如下图所示：

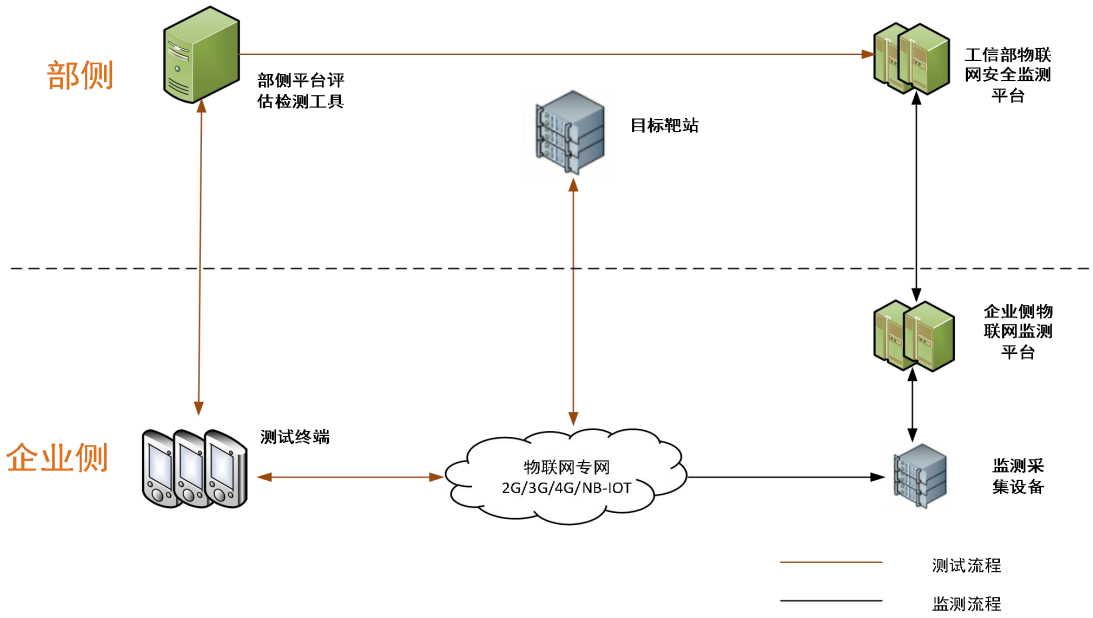

图1 物联网专网网络安全监测效能评估环境

部署部侧平台测试评估工具，连接到公网的固定IP地址。测试评估工具包括控制界面和测试靶站，用于指令下发、测试结果展示等功能。

在各物联网基地的测试终端上安装客户端程序（APK），通过物联网卡连接到公网。测试终端接收并执行测试任务，并将结果数据上报给部侧平台。

5.2 评估环境要求

受测企业在各个物联网基地注册不同类型的物联网卡，包括4G、NB-IOT等网络类型，此外需安装客户端程序（APK）来激活测试终端，并确保移动网流量充足。

测试终端需满足以下要求：①Android运行环境②配置不低于8GB运行内存和256GB存储内存。

6 基础电信企业物联网专网网络安全监测系统运行效能评估检测要点

基础电信企业物联网专网网络安全监测系统运行效能的检测标准是以评分体系和评估方法为基础，对物联网专网网络安全监测技术能力系统能力和数据质量进行检测评估。

6.1 系统能力检测要点

6.1.1 监测带宽覆盖检测要点

测试编号： 01
测试项目：核验物联网监测带宽覆盖范围
测试目的：评估企业侧物联网专网覆盖范围能力
测试环境：无要求
测试步骤： 1）确认测试环境； 2）部侧平台下发恶意URL监测指令； 3）使用测试终端模拟访问被测网络环境中恶意URL地址，受测企业上报监测记录； 4）部侧平台查看上报事件结果。
预期结果： 1）步骤3受测企业能够发现监测事件； 2）步骤4部侧平台查看上报事件结果，上报结果与测试验证结果一致。
判定原则： 应符合预期结果要求，否则为不合格。

6.1.2 功能完备检测要点

功能完备指标主要评估基础电信企业物联网专网网络安全监测系统的流量采集能力、流量协议识别能力、网络威胁监测能力、威胁研判能力、集中管理等能力情况。上述任一能力不满足则功能完备指标项不通过。

6.1.2.1 流量采集能力检测要点

6.1.2.1.1 物联网（含车联网）流量筛选能力检测要点

测试编号： 02
测试项目：物联网（含车联网）流量筛选能力验证
测试目的：评估企业侧物联网（含车联网）流量筛选能力
测试环境：现网环境
测试步骤： 1）确认评测环境； 2）通过部侧平台依次按照IP五元组规则、掩码五元组规则、CS规则、全包固定位置特征码规则、窗口范围浮动特征码规则、全包浮动位置特征码规则、掩码五元组+固定位置特征码规则、掩码五元组+窗口范围浮动特征码规则、IMEI号规则、APN规则、Host规则、SNI规则下发特定的物联网流量筛选指令到受测企业基地； 3）受测企业按照指令规则进行流量筛选，并上报至部侧流量预处理模块；

4）检测部侧预处理模块输出通联日志与上述指令规则的一致性。
预期结果： 1）在步骤3中，部侧预处理模块能接收筛选后的二进制流量和全量信令面流量； 2）在步骤4中，部侧预处理模块输出通联日志数据符合指令IP五元组规则、掩码五元组规则、CS规则等指令筛选规则。
判定原则： 应符合预期结果要求，否则为不合格。

6.1.2.1.2 文件捕获还原能力检测要点

测试编号： 03
测试项目：文件捕获还原能力验证
测试目的：评估企业侧文件捕获还原能力
测试环境：现网环境
测试步骤： 1）确认评测环境； 2）使用测试终端模拟在被测网络环境中访问测试靶站中测试样本（测试样本包括apk、jar、zip、elf、so样本类型等），记录产生的传播次数和测试样本信息； 3）受测企业在测试结束后60分钟内提供测试期间内发现到的有害程序传播事件信息和恶意样本文件； 4）在部侧平台登录并核实有害程序传播事件中恶意样本MD5、文件类型等信息是否与测试样本一致。
预期结果： 1）在步骤3中，受测企业在测试结束后60分钟内上报有害程序传播事件信息和恶意样本文件，文件类型包括apk、ipa、jar、dex、hap、zip、elf、so等； 2）在步骤4中，有害程序事件中的恶意样本MD5、文件类型与测试样本保持一致。
判定原则： 应符合预期结果要求，否则为不合格。

6.1.2.2 流量协议识别能力检测要点

6.1.2.2.1 物联网（含车联网）流量协议识别能力检测要点

测试编号： 04
测试项目：物联网（含车联网）流量协议识别能力验证

测试目的：评估企业侧物联网（含车联网）流量协议识别能力
测试环境：现网环境
测试步骤： 1）确认评测环境； 2）使用测试终端模拟在被测网络环境中访问测试靶站，依次进行MQTT、XMPP、COAP、ONVIF、RTSP、JT/T808、JT/T809、GB/T32960等协议（详细参考技术能力要求附录A.2应用层协议类型）通信，记录产生的通联日志信息； 3）受测企业在测试结束后60分钟内提供测试期间内的通联日志信息； 4）在部侧平台登录并核实通联日志中通信时间、应用层协议字段与测试信息是否一致。
预期结果： 1）在步骤3中，受测企业按照接口规范要求上报通联日志； 2）在步骤4中，通联日志结果中应用协议字段与测试信息一致。
判定原则： 应符合预期结果要求，否则为不合格。

6.1.2.2.2 物联网（含车联网）终端识别能力检测要点

测试编号： 05
测试项目：物联网（含车联网）终端识别能力验证
测试目的：评估企业侧物联网（含车联网）终端识别能力
测试环境：现网环境
测试步骤： 1）确认评测环境； 2）按照多种已知物联网终端类型的IMEI规则在部侧下发通联日志查询指令到受测企业； 3）受测企业提供测试期间内上述物联网终端实时通联日志记录，并上报至部侧平台； 4）在部侧平台登录并检查通联日志中IMEI对应的终端类型与步骤2中终端类型一致性。
预期结果： 1）在步骤2中，物联网终端类型数量不少于100种； 2）在步骤3中，部侧平台接收到通联日志记录，字段包括源IP、源端口、目的IP、目的端口、终端类型、行业类型、IMEI号等（详细字段参照《基础电信企业物联网专网网络安全监测接口规范》）；

3）在步骤4中，通联日志中终端类型、IMEI号与步骤2中一致。
判定原则： 应符合预期结果要求，否则为不合格。

6.1.2.3 网络威胁监测能力检测要点

6.1.2.3.1 网络攻击事件监测能力检测要点

测试编号： 06
测试项目：网络攻击事件检测能力验证
测试目的：评估企业侧网络攻击事件监测能力
测试环境：现网环境
测试步骤： 1）确认评测环境； 2）使用部侧面平台评估检测工具模拟被测网络环境中通信数据包，通过测试终端回放数据包来触发协议欺骗、系统漏洞利用和Web攻击等网络攻击事件； 3）受测企业在测试结束后60分钟内提供测试期间内上述网络攻击事件至部侧平台； 4）在部侧平台登录并检查网络安全事件特征规则是否符合实际投放样本规则。
预期结果： 1）在步骤3中，部侧平台在60分钟内接收到网络攻击事件，事件内容至少包括：源IP、源端口、目的IP、目的端口、发现时间、事件一级分类、事件二级分类、终端类型等（字段详细参照《基础电信企业物联网专网网络安全监测接口规范》）； 2）在步骤4中，网络安全事件特征规则符合实际投放样本规则。
判定原则： 应符合预期结果要求，否则为不合格。

6.1.2.3.2 有害程序传播监测能力检测要点

测试编号： 07
测试项目：有害程序传播监测能力检测能力验证
测试目的：评估企业侧有害程序传播监测能力
测试环境：现网环境
测试步骤： 1）确认评测环境；

2）使用部侧面平台评估检测工具模拟被测网络环境中通信数据包，通过测试终端回放数据包来触发网络蠕虫、僵尸网络和挖矿病毒等有害程序传播事件，记录产生的传播次数和测试样本信息； 3）受测企业在测试结束后60分钟内提供测试期间内发现到的有害程序传播事件信息和恶意样本文件； 4）在部侧平台登录并检查有害程序传播事件、恶意样本文件信息与测试样本信息一致。
预期结果： 1）在步骤3中，部侧平台在60分钟内接收到有害程序传播事件和恶意样本信息，其中有害程序传播事件至少包括：源IP、源端口、目的IP、目的端口、发现时间、事件一级分类、事件二级分类、有害程序类型、恶意样本的MD5等（详细字段参照《基础电信企业物联网专网网络安全监测接口规范》）； 2）在步骤4中，有害程序传播事件、恶意样本文件信息与测试样本信息一致。
判定原则： 应符合预期结果要求，否则为不合格。

6.1.2.3.3 主机受控事件监测能力检测要点

测试编号：08
测试项目：主机受控事件检测能力验证
测试目的：评估主机受控事件监测能力
测试环境：现网环境
测试步骤： 1）确认评测环境； 2）使用部侧面平台评估检测工具模拟被测网络环境中通信数据包，通过测试终端回放数据包来触发主机受控事件； 3）受测企业在测试结束后60分钟内提供测试期间内发现到的主机受控事件信息； 4）检查受测企业监测到的主机受控事件信息与通信包规则信息一致。
预期结果： 1）在步骤3中，部侧平台在60分钟内接收到主机受控事件，事件信息应符合字段要求，至少包括源IP、源端口、目的IP、目的端口、发现时间、事件一级分类、事件二级分类、恶意程序名称等（详细字段参照《基础电信企业物联网专网网络安全监测接口规范》）； 2）在步骤4中，主机受控事件信息与通信包信息一致。
判定原则：

应符合预期结果要求，否则为不合格。

6.1.2.4 威胁研判能力检测要点

测试编号： 09
测试项目：恶意程序研判能力验证
测试目的：评估企业侧恶意程序研判能力
测试环境：现网环境
测试步骤： 1）确认评测环境； 2）使用测试终端模拟在被测网络环境中访问测试靶站中测试样本（测试样本中已知样本与疑似样本数量比例大于1:1），记录产生的传播次数和测试样本信息； 3）受测企业在测试结束后60分钟内提供测试期间内发现到的有害程序传播事件信息和恶意样本文件； 4）在部侧平台登录并检查有害程序传播事件、恶意样本文件信息与测试样本信息一致。
预期结果： 1）在步骤3中，部侧平台在60分钟内接收到有害程序传播事件，研判结果应符合字段要求，包括研判评分、恶意程序名称、恶意程序类型、主控地址、下载地址、风险级别、控制端邮箱、控制端号码等（字段详细参照《基础电信企业物联网专网网络安全监测接口规范》）； 2）在步骤4中，检查受测企业监测到的有害程序传播事件、恶意样本文件信息与测试样本信息一致。
判定原则： 应符合预期结果要求，否则为不合格。

6.1.2.5 集中管理能力检测要点

6.1.2.5.1 数据存储检测要点

测试编号：10
测试项目：数据存储验证
测试目的：评估企业侧数据存储要求
测试环境：无要求

测试步骤： 1）确认评测环境； 2）按照近6个月时间范围要求下发通联日志查询指令到受测企业； 3）受测企业上报测试期间内的通联日志记录数据至部侧平台； 4）检测企业侧通联日志存储时间符合近6个月要求。
预期结果： 在步骤4中，部侧平台收到的通联日志记录时间范围符合步骤2中规定的通联日志查询条件。
判定原则： 应符合预期结果要求，否则为不合格。

6.1.3 协同联动检测要点

协同联动指标主要评估基础电信企业物联网专网网络安全监测系统与部侧平台的联动能力，协同联动指令类型包括监测质量、通联日志查询指令。上述指令协同测试结果任一不满足要求则本指标项不通过。

6.1.3.1 监测指令检测要点

测试编号：11
测试项目：监测指令协同验证
测试目的：评估企业侧监测指令协同能力
测试环境：现网环境
测试步骤： 1）确认评测环境； 2）部侧平台按照接口规范要求下发监测指令至受测企业，监测指令内容包括指令ID、规则编号、事件分类、生效运营商、监测指令类型、指令优先级、生效时间、过期时间、指令执行结果处理方式、数据上报方式、是否带Pcap上报、威胁方向、Snort规则等（字段详细参照《基础电信企业物联网专网网络安全监测接口规范》）； 3）受测企业执行监测指令并上报监测结果记录、流量文件或恶意样本文件至部侧平台； 4）检测监测指令规则与监测结果是否一致性。
预期结果： 1）在步骤2中，企业侧平台接收监测指令，同时回传接收状态； 2）在步骤3中，企业侧平台在部侧指令下发60分钟内部署生效，企业侧平台执行指令,同时部侧平台在指令生效范围时间内接收监测结果记录，从模拟发起事件到部侧平