基础电信企业木马和僵尸网络监测与处置系统运行效能测试规范

2023 年 5 月

目　　录

前　　言

本文件依据《基础电信企业木马和僵尸网络监测与处置系统企业侧平台建设指南》和《基础电信企业木马和僵尸网络监测与处置管理平台接口规范》要求，针对各省公司独立建设的木马和僵尸网络监测与处置系统，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

基础电信企业木马和僵尸网络监测与处置系统运行效能测试规范

1 目的和范围

木马和僵尸网络监测与处置系统主要分为两部分：一是基础电信企业侧平台（下文简称“企业侧”）；二是木马和僵尸网络监测与处置系统部侧平台（下文简称“部侧平台”）。其目的在于实现省网流量的实时采集、协议识别、威胁监测、研判、处置和集中管理等能力，达到推进网络空间安全治理的目标。本文件旨在评估系统运行效能（系统能力、数据质量等），以规范木马和僵尸网络监测与处置系统技术手段的建设。

本文件依据《基础电信企业木马和僵尸网络监测与处置系统企业侧平台建设指南》和《基础电信企业木马和僵尸网络监测与处置管理平台接口规范》及相关规范，针对木马和僵尸网络的监测处置能力提出具体的考核要求和检测评估方法。

本文件适用于对基础电信企业木马和僵尸网络监测与处置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《基础电信企业木马和僵尸网络监测与处置系统企业侧平台建设指南》

工网安函〔2022〕303号文附件《基础电信企业木马和僵尸网络监测与处置管理平台接口规范》

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 僵尸网络

僵尸网络是指采用一种或多种传播手段，将大量主机感染僵尸程序病毒，从而在控制者和被感染主机之间所形成的一个可一对多控制的网络。

3.3 木马程序

木马程序通常称为木马，恶意代码等，是指潜伏在设备中，可受外部用户控制以窃取本机信息或者控制权的程序。

3.4 蠕虫病毒

蠕虫病毒是一种常见的病毒，它通过网络和电子邮件进行复制和传播。

3.5 网络资源

网络资源指的是互联网上有分析价值的IP地址、域名、URL链接、电子信息，包括网站资源、木马和僵尸网络控制端、文件下载链接、攻击地址、电子邮件、即时通讯等。

3.6 流量报文

流量报文指的是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。

3.7 恶意样本

恶意样本又称恶意软件、恶意程序或恶意代码等，指被用于实施网络攻击的恶意文件，包括木马、病毒、蠕虫、僵尸程序和移动恶意程序等多种类型的恶意文件。

4 基础电信企业木马和僵尸网络监测与处置系统运行效能评估体系

基础电信企业木马和僵尸网络监测与处置系统运行效能评估体系包括系统能力和数据质量两个部分，考核评价采用扣分制，对不符合相关测试标准的部分扣除相应分数。

4.1 系统能力

4.1.1 监测带宽指标

监测带宽指标体现出基础电信企业木马和僵尸网络监测处置能力的链路覆盖情况，具体指标项如表1所示。

表1 木马和僵尸网络监测与处置系统监测带宽指标

指标名称	指标项	指标描述	评分规则
监测带宽指标	覆盖率和部署位置评估	木马和僵尸网络监测与处置系统在省网出入口的覆盖率	木马和僵尸网络监测与处置系统全量覆盖受测企业自用互联网出入口流量，总体覆盖率满足要求，优先覆盖专线流量，可实现对特定用户的流量覆盖，省出入口、直辖市出入口带宽覆盖率应不低于9%。

4.1.2 功能完备指标

功能完备指标主要评估基础电信企业木马和僵尸网络监测与处置系统的采集能力、监测能力、处置能力、研判能力、集中管理等能力情况。

4.1.2.1 采集能力

表2 木马和僵尸网络监测与处置系统采集能力指标

指标名称	指标项	指标描述	评分规则
采集能力指标	协议识别的事件报送能力评估	是否具备协议识别的相关能力	1、应具备3至7层协议的识别解析能力，包括IP、ICMP等网络层协议，TCP、UDP等传输层协议及HTTP、SMTP、POP3、IMAP、FTP、SMB、SMB2、NFS、DNS等通用网络应用层协议； 2、应具备工业互联网协议的识别解析能力，包括OPC、UA、Siemens S7、Modbus、OMRONFINS、IEC 60870-5-1-4、DNP3等； 3、应具备车联网协议的识别解析能力，包括GB/T32960、JT/T808、JT/T905等； 4、应具备虚拟货币协议的识别解析能力，包括GetWork（GWK）、Stratum（STM）、json-rpc等； 5、应具备特定网络协议的识别解析能力，包括Scramblesuit、Obfs3、Obfs4等；（增强要求）

			6、应具备对多种操作系统文件的识别能力，应支持的操作系统类型见《基础电信企业网络安全系列平台接口规范通用数据代码表（v1.0）》操作系统枚举表。
	文件捕获的能力评估	是否具备流量还原和文件捕获的能力	应具备将实时流量经数据包重组还原为文件的能力，且还原生成的样本文件满足准确性和完整性要求，从用户完成样本下载到部侧平台收到企业报送样本的时间间隔不得超过24小时；应支持还原的文件格式见《基础电信企业木马和僵尸网络监测与处置系统企业侧平台建设指南》附录A。
	流捕获的能力评估	是否具备流捕获的能力	应具备抓取pcap包且保证其无损不丢包的能力，且采集的原始流量满足准确性和完整性要求。应具备针对评估检测流量的捕获结果应在测试完成90分钟内完成上报。

4.1.2.2 监测能力

表3 木马和僵尸网络监测与处置系统监测能力指标

指标名称	指标项	指标描述	评分规则
监测能力指标	木马和僵尸网络受控事件监测能力	是否具备发现用户受控的网络通联记录数据和控制端信息的能力	1、应具备利用自有监测规则和部侧平台下发的监测规则，对木马和僵尸网络受控事件、传播事件，网络安全威胁事件，专题任务相关事件进行监测，并上报监测结果数据的能力，企业侧平台应在部侧指令下发60分钟内部署生效，从发现监测事件到部侧平台收到报送的时间间隔不超过90分钟； 2、应具备监测IP、ICMP等网络层协议，TCP、UDP等传输层等协议，以及HTTP、
	木马和僵尸网络传播事件监测能力	是否具备采集还原样本、获取传播记录的能力	
	网络安全威胁事件监测能力	是否具备监测和识别攻击行为，并提取攻击端信息及通联记录数据的能力	
	专题任务相关事件监测能力	是否具备监测和识别工业互联网安全等特定网络行为，提取留存相关通联日志记录数据，并	

		根据部侧平台指令需求上报的能力	SMTP、POP3、IMAP、FTP、SMB、NFS、DNS 和专题任务涉及的常见应用层协议的能力，包括工业互联网协议如OPC、UA、Siemens S7、Modbus等，车联网协议如GB/T32960 、 JT/T808 、 JT/T905等，虚拟货币协议如GetWork（GWK）、Stratum（STM）、json-rpc等； 3、木马和僵尸网络受控事件、木马和僵尸网络传播事件、网络安全威胁事件、专题任务事件的特定监测规则应满足规范要求，且监测结果应满足接口规范要求。

4.1.2.3 处置能力

表4 木马和僵尸网络监测与处置系统处置能力指标

指标名称	指标项	指标描述	评分规则
处置能力指标	阻断处置能力评估	是否具备阻断处置的相关能力	1、应具备根据部侧平台下发的处置指令，通过阻断和重定向等相应措施，对URL链接、IP地址、域名等进行处置的能力； 2、收到部侧平台下发的处置指令后，在受测企业指定的链路中，阻断或重定向处置措施应在60分钟内部署生效，在部侧平台下发处置规则生效90分钟内完成处置并上报结果，且处置成功率应不低于80%。
	重定向处置能力评估	是否具备重定向处置的相关能力	

4.1.2.4 研判能力

表5 木马和僵尸网络监测与处置系统研判能力指标

指标名称	指标项	指标描述	评分规则
研判能力指标	行为特征库指标建立和更新能力评估	是否具备建立行为特征库、并根据相关流量和样本的分析结果进行更新的能力	应建立木马、僵尸网络、蠕虫病毒、网络安全威胁及专题任务有关行为特征库、恶意样本主控URL库、恶意样本下载URL库和恶意样本MD5特征库等，并具备根据分析研判结果更新相关特征库的能力。
	恶意样本研判能力评估	是否具备恶意样本识别和研判的能力	具备分析研判疑似恶意样本的能力，且研判结果应包含恶意程序名称、恶意程序类型、控制端地址、下载地址等。

4.1.2.5 集中管理能力

表6 木马和僵尸网络监测与处置系统集中管理能力指标

指标名称	指标项	指标描述	评分规则
集中管理能力指标	存储能力评估	是否具备日志、事件、样本等数据的存储能力	样本文件、流量报文文件、事件和其它相关数据的留存时间应满足建设指南要求。

4.1.3 协同联动指标

协同联动指标主要评估基础电信企业木马和僵尸网络监测与处置系统与部侧平台的联动能力，包括数据常态化上报、指令接收、数据回传等，具体如表7所示。

表7 木马和僵尸网络监测与处置系统协同联动指标

指标名称	指标项	指标描述	评分规则

协同联动指标	指令交互能力评估	是否具备接受部侧平台下发的监测、处置、查询等类型指令，解析、执行指令内容，并反馈结果数据的能力	1、应具备对部侧平台下发的指令进行识别、解析，并按内容要求执行的能力，并可以提取指令中相关监测、处置等行为规则，扩充企业侧平台规则库； 2、应具备向部侧平台反馈指令执行结果数据的能力，且上报数据内容和时间符合第6.1.3章节测试规范的要求。

4.2 数据质量

数据上报质量主要评估基础电信企业木马和僵尸网络监测与处置系统常态化上报及指令反馈数据在及时性、准确性、完整性、可用性指标上的达成情况。

4.2.1 及时性

数据上报及时性考核指标如表8所示。

表8 木马和僵尸网络监测与处置系统数据上报及时性指标

指标名称	指标项	指标描述	评分规则
及时性指标	安全事件上报	各类上报数据是否满足及时性要求	常态化数据及指令反馈数据及时性要求应符合检测要点要求。
	样本文件上报		
	统计数据上报		
	工控设备数据上报		
	平台基础信息数据上报		
	设备状态信息上报		
	监测指令反馈数据		
	处置指令反馈数据		
	历史查询指令反馈数据		
	库存同步指令反馈数据		

4.2.2 准确性

数据上报准确性考核指标如表9所示。

表9 木马和僵尸网络监测与处置系统数据上报准确性指标

指标	指标项	指标描述	评分规则

名称			
准确性指标	安全事件上报	各类上报数据是否满足准确要求	准确性要求如下： 1） 数据类型准确：上报数据应按规范要求，准确上报到相应的类别； 2） 字段填报准确：各字段的类型、长度和内容填写应符合接口规范要求和数据业务逻辑要求。
	样本文件上报		
	统计数据上报		
	工控设备数据上报		
	平台基础信息数据上报		
	设备状态信息上报		
	监测指令反馈数据		
	处置指令反馈数据		
	历史查询指令反馈数据		
	库存同步指令反馈数据		

4.2.3 完整性

数据上报完整性考核指标如表10所示。

表10 木马和僵尸网络监测与处置系统数据上报完整性指标

指标名称	指标项	指标描述	评分规则
完整性指标	安全事件上报	各类上报数据是否满足完整要求	完整性要求如下： 1） 上报数据类型完整：按照要求上报安全事件（木马和僵尸网络受控事件、木马和僵尸网络传播事件、网络安全威胁事件、专题任务事件）、样本文件、统计数据、工控设备数据、平台基础信息、设备状态信息等； 2） 字段填写完整：各字段应按照接口规范要求完整填报。
	样本文件上报		
	统计数据上报		
	工控设备数据上报		
	平台基础信息数据上报		
	设备状态信息上报		
	监测指令反馈数据		
	处置指令反馈数据		
	历史查询指令反馈数据		
	库存同步指令反馈数据		

4.2.4 可用性

数据上报可用性考核指标如表11所示。

表11 木马和僵尸网络监测与处置系统数据上报可用性指标

指标名称	指标项	指标描述	评分规则

可用性指标	安全事件上报	系统是否满足可用性要求	可用性要求如下： 近1个月内上报数据中断时间累计不超过24小时

5 基础电信企业木马和僵尸网络监测处置能力评估方法

5.1 评估方法

对企业侧互联网木马和僵尸网络监测与处置平台的检测评估方式如下：

检测评估人员通过在实网中部署使用相关技术工具，对企业侧平台的采集能力、监测能力、处置能力、指令协同能力等进行测试，评估其是否满足考核要求。

5.2 评估环境要求

木马和僵尸网络监测与处置系统技术测试验证工具部署环境如下图所示，其中测试工具部署在受测企业网络内。

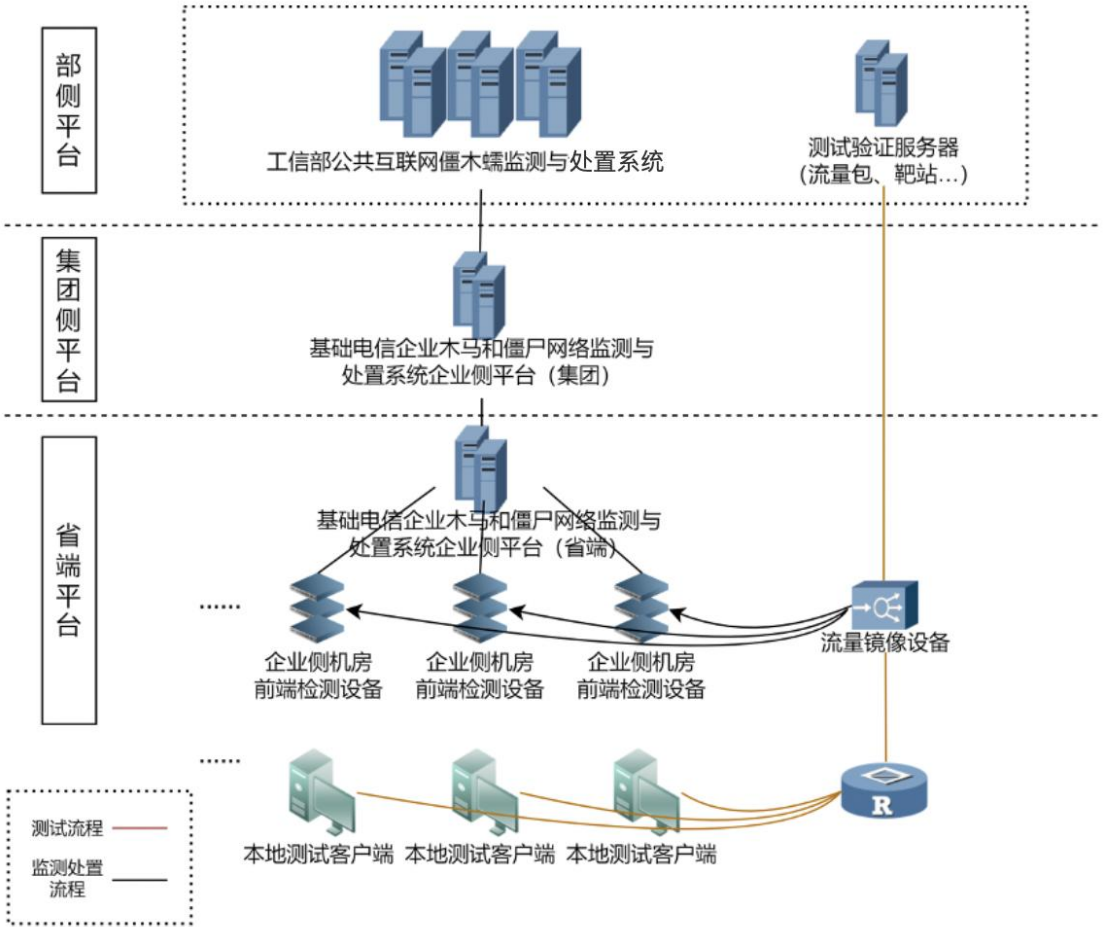

图1 木马和僵尸网络监测与处置系统测试验证环境

部侧测试验证服务器提供测试所需的样本数据、流量数据和靶站服务，并汇总受测企业的测试执行记录，同步至部侧平台用于考核评测。

受测企业在木马和僵尸网络监测与处置系统流量采集设备所部署的机房，提前准备本地测试客户端（不低于4物理核CPU、16GB内存、80GB硬盘），并按要求安装测试工具，确保本地测试客户端收发的网络流量可被木马和僵尸网络检测设备所覆盖，并为本地测试客户端配置相应的网络访问权限，确保可与部侧测试验证服务器所处的公共互联网网络通联。

本地测试客户端通过部侧测试验证服务器更新本地测试工具，下载测试所需的流量包和样本文件，以支持相关测试工作。

6 基础电信企业木马和僵尸网络监测处置能力检测要点

基础电信企业木马和僵尸网络监测与处置系统运行效能体系以评分体系和评估方法为基础，对木马和僵尸网络监测与处置系统企业侧平台的系统能力、数据质量情况进行检测评估。

6.1 系统能力检测要点

6.1.1 监测带宽检测要点

测试编号：01
测试项目： 检查木马和僵尸网络监测与处置系统的覆盖范围、部署情况，并评估覆盖率和部署位置。评估采集点为省网出口、城域网出口的双向原始流量。
测试步骤： （1） 确认评测环境； （2） 部侧根据受测企业通过接口上报的设备监测带宽等相关信息，统计受测企业已覆盖带宽总量，测算受测企业已部署检测设备带宽覆盖率；
预期结果： （1） 在步骤（2）中，受测企业带宽覆盖率应不低于9%；
判定原则： 应符合预期结果要求，否则为不合格

6.1.2 功能完备情况检测要点

功能完备指标主要评估基础电信企业木马和僵尸网络监测与处置系统的采集能力、监测能力、处置能力、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 采集能力检测要点

6.1.2.1.1 协议和文件识别解析能力检测

测试编号：02
测试项目： 测试木马和僵尸网络监监测与处置系统的协议识别解析能力，包括对监测位置双向原始流量进行实时获取、协议解析、数据包重组等操作的能力。
测试目的：验证3至7层协议识别解析能力
测试环境：测试环境
测试步骤： （1） 确认评测环境； （2） 使用测试工具向受测网络环境中模拟发起基于IP、ICMP等网络层协议，TCP、UDP等传输层协议及HTTP、SMTP、POP3、IMAP、FTP、SMB、SMB2、NFS、DNS等通用网络应用层协议中指定类型的协议封装的网络安全威胁事件； （3） 受测企业实时监测发现对应协议下的网络安全威胁事件，并上报至部侧平台； （4） 在部侧平台中，查看受测企业侧平台上报的网络安全威胁事件的数据。
预期结果： （1） 在步骤（2）中，受测企业侧前端检测设备需要能监测识别到测试流量数据包中指定类型3至7层协议相关的网络安全威胁事件； （2） 在步骤（4）中，部侧平台在测试验证结束90分钟内能查询到企业侧平台上报的网络安全威胁事件，至少包含：事件分类、源IP地址、源端口、目的IP地址、目的端口、传输层协议类型、应用层协议类型等字段。
判定原则： 应符合预期结果要求，否则为不合格

测试编号：03
测试项目： 测试木马和僵尸网络监测与处置系统的应用层协议识别解析能力，包括对工业互联网协议、车联网协议、虚拟货币协议，以及Scramblesuit等特定协议进行识别解析、数据包重组等操作的能力。
测试目的：验证工业互联网协议、车联网协议、虚拟货币协议，以及Scramblesuit等特

定协议的识别解析能力
测试环境：测试环境
测试步骤： （1） 确认评测环境； （2） 使用测试工具向受测网络环境中模拟发起基于工业互联网协议、车联网协议、虚拟货币协议，以及Scramblesuit等特定协议中指定类型协议封装的网络安全威胁事件； （3） 受测企业实时监测发现对应协议下的网络安全威胁事件，并上报至部侧平台； （4） 部侧平台在测试验证结束90分钟内能查看受测企业侧平台上报的网络安全威胁事件的数据。
预期结果： （1） 在步骤（2）中，受测企业侧前端检测设备需要能监测识别到测试流量数据包中指定类型工业互联网协议相关的网络安全威胁事件； （2） 在步骤（4）中，在部侧平台，能查询到企业侧平台上报的网络安全威胁事件，至少包含：事件分类、源IP地址、源端口、目的IP地址、目的端口、传输层协议类型、应用层协议类型等字段。
判定原则： 应符合预期结果要求，否则为不合格

测试编号：04
测试项目： 测试木马和僵尸网络监测与处置系统的文件识别解析能力，应支持对多操作系统平台文件的识别。
测试目的：验证多操作系统平台文件和识别解析能力
测试环境：测试环境
测试步骤： （1） 确认评测环境； （2） 使用测试工具向受测网络环境中模拟发起样本传播事件（样本为覆盖Windows系列、IOS、Android、Linux、Solaris等平台的多种格式文件），开展测试，记录测试次数和样本信息； （3） 受测企业实时监测发现对应的样本传播事件，并作为木马和僵尸网络传播事件上报至部侧平台； （4） 在部侧平台中，查看受测企业侧平台上报的木马和僵尸网络传播事件，检查受测企业上报的事件信息是否与测试样本信息一致；

（5） 通过比对受测企业监测结果和测试样本文件列表中对应文件的特征（如MD5值等），计算检测准确率。（检测准确率指受测企业监测到的正确样本在测试总样本中的占比）。
预期结果： （1） 在步骤（2）中，受测企业侧前端检测设备需要能监测识别到测试流量数据包中指定平台和文件类型相关的木马和僵尸网络传播事件； （2） 在步骤（4）中，部侧平台在测试验证结束90分钟内能查询到企业侧平台上报的木马和僵尸网络传播事件，字段至少包含：事件分类、源IP地址、源端口、目的IP地址、目的端口、有害程序名称、恶意样本MD5、操作系统等； （3） 在步骤（5）中，已知恶意样本的综合（平均）检测准确率大于85%，非已知疑似样本综合（平均）检测准确率大于65%。注：综合（平均）检测准确率是指多轮测试检测准确率的算数平均值。
判定原则： 应符合预期结果要求，否则为不合格

6.1.2.1.2 流捕获能力检测

测试编号：05
测试项目： 测试木马和僵尸网络监测与处置系统抓取pcap包且保证其无损不丢包的能力。
测试目的：验证流捕获能力
测试环境：测试环境
测试步骤： （1） 确认评测环境； （2） 登录部侧平台，向受测企业侧平台下发流量报文监测指令（是否带pcap上报：带pcap）； （3） 使用测试工具向受测网络环境中在指定时间内模拟发送指定大小匹配报文监测指令事件的测试流量数据包； （4） 受测企业将捕获到的pcap包上报至部侧平台； （5） 在部侧平台中，核验对应的pcap上报结果。
预期结果： （1） 在步骤（4）中，受测企业侧前端检测设备需要根据指令监测匹配到测试流量数据包，并捕获pcap包； （2） 在步骤（5）中，部侧平台在测试验证结束90分钟内能查询到受测企业侧上报的流量报文监测记录，上报字段满足接口规范要求；且通过SFTP接口同步上报无损的

pcap包。
判定原则： 应符合预期结果要求，否则为不合格

6.1.2.1.3 文件捕获能力检测

测试编号：06
测试项目： 测试木马和僵尸网络监测与处置系统依据规则将实时流量经数据包重组还原为文件的能力。
测试目的：验证文件捕获能力
测试环境：测试环境
测试步骤： （1） 确认评测环境； （2） 使用测试工具向受测网络环境中模拟发起基于HTTP、FTP、SMTP、POP3、IMAP协议中指定协议的样本传播事件，样本为多种常见格式文件（可执行文件类、压缩文件类、系统文件类、文本文档类、邮件类、其他类型），如压缩文件类（rar、zip、7z等），详见建设指南附录A； （3） 受测企业将捕获到的文件上报至部侧平台； （4） 在部侧平台中，查看受测企业侧平台上报的样本数据。
预期结果： （1） 在步骤（2）中，受测企业侧前端检测设备需要能监测识别到测试流量数据包中指定格式的样本传播事件； （2） 在步骤（4）中，部侧平台在测试验证结束90分钟内能查询到企业侧通过木马和僵尸网络传播事件报送消息接口上报的数据，上报字段满足接口规范要求；且通过SFTP接口同步上报相关样本数据，样本格式为指定格式文件。
判定原则： 应符合预期结果要求，否则为不合格

6.1.2.2 威胁监测能力检测要点

6.1.2.2.1 木马和僵尸网络受控事件监测

测试编号：07
测试项目： 检查木马和僵尸网络受控事件监测能力

测试目的：验证木马和僵尸网络受控事件的基础监测能力
测试环境：测试环境
测试步骤： （1） 确认评测环境； （2） 使用测试工具向受测网络环境中模拟发起基于HTTP、FTP、SMTP、POP3、IMAP协议中指定类型协议封装的木马和僵尸网络受控事件； （3） 受测企业将监测到的木马和僵尸网络受控事件上报至部侧平台； （4） 在部侧平台中，查看受测企业侧平台上报的木马和僵尸网络受控事件的数据。
预期结果： （1） 在步骤（2）中，受测企业侧前端检测设备需要能监测识别到测试流量数据包中指定类型协议相关的木马和僵尸网络受控事件； （2） 在步骤（4）中，部侧平台在测试验证结束90分钟内能查询到受测企业侧平台上报的木马和僵尸网络受控事件，至少包含：事件分类、源IP地址、源端口、目的IP地址、目的端口、传输层协议类型、应用层协议类型等。
判定原则： 应符合预期结果要求，否则为不合格

6.1.2.2.2 木马和僵尸网络传播事件监测

测试编号：08
测试项目： 检查木马和僵尸网络传播事件监测能力
测试目的：验证木马和僵尸网络传播事件的基础监测能力
测试环境：测试环境
测试步骤： （1） 确认评测环境； （2） 使用测试工具向受测网络环境中模拟发起基于HTTP、FTP、SMTP、POP3、IMAP协议中指定类型协议封装的木马和僵尸网络传播事件； （3） 受测企业将监测到的木马和僵尸网络传播事件上报至部侧平台； （4） 在部侧平台中，查看受测企业侧平台上报的木马和僵尸网络传播事件的数据。
预期结果： （1） 在步骤（2）中，受测企业侧前端检测设备需要能监测识别到测试流量数据包中指定类型协议相关的木马和僵尸网络传播事件； （2） 在步骤（4）中，部侧平台在测试验证结束90分钟内能查询到受测企业侧平台上报的木马和僵尸网络传播事件，至少包含：事件分类、源IP地址、源端口、目的IP

地址、目的端口、有害程序名称、恶意样本MD5、操作系统等。
判定原则： 应符合预期结果要求，否则为不合格

6.1.2.2.3 网络安全威胁事件监测

测试编号：09
测试项目： 检查网络安全威胁事件监测能力
测试目的：验证系统对Web攻击、木马后门攻击、漏洞利用攻击等网络安全威胁的监测能力
测试环境：测试环境
测试步骤： （1） 确认评测环境； （2） 使用测试工具向受测网络环境中模拟发起包含Web攻击、木马后门攻击、漏洞利用攻击等类型的的网络安全威胁事件； （3） 受测企业将监测到的网络安全威胁事件上报至部侧平台； （4） 在部侧平台中，查看受测企业侧平台上报的网络安全威胁事件的数据。
预期结果： （1） 在步骤（2）中，受测企业侧前端检测设备需要能监测识别到测试流量数据包中的网络安全威胁事件； （2） 在步骤（4）中，部侧平台在测试验证结束90分钟内能查询到受测企业侧平台上报的网络安全威胁事件，至少包含：事件分类、源IP地址、源端口、目的IP地址、目的端口、传输层协议类型、应用层协议类型等。
判定原则： 应符合预期结果要求，否则为不合格

6.1.2.2.4 专题任务相关事件监测

测试编号：10
测试项目： 检查专题任务相关事件监测能力
测试目的：验证系统对专题任务相关事件的监测能力
测试环境：测试环境