专项数据报送技术要求和测试方法

2023年5月

目　　录

前　言

本文件依据《部侧安全中台统一接入数据集标准》及相关接口规范要求，针对网络安全告警日志、行为日志、NetFlow、DNS 解析日志、基础资源等专项数据上报相关的覆盖范围、报送质量等提出具体的技术要求和测试方法。

本文件用于指导基础电信企业省级公司通过集团公司向部侧平台上报专项数据的能力建设和数据上报质量评测。

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

专项数据报送技术要求和测试方法

1 范围

本文件规定了网络安全告警日志、行为日志、NetFlow、DNS 解析日志、基础资源等专项数据上报相关的覆盖范围、报送质量等方面的技术要求和测试方法。

本文件适用于基础电信企业省级公司通过集团公司向部侧平台上报专项数据的能力评测。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，标注日期的引用文件，仅该日期对应的版本适用于本文件。不标注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

工网安函〔2022〕303 号文《信息通信行业网络安全威胁分类分级指南》

工网安函〔2022〕303 号文《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》

工网安函〔2022〕303 号文《基础电信企业移动互联网恶意程序监测与处置管理平台接口规范》

工网安函〔2022〕303 号文《基础电信企业网络安全态势感知平台接口规范》

《部侧安全中台统一接入数据集标准》

3 术语

下列术语用于本文件。

3.1

部侧平台

部侧平台包括部侧 DDoS 攻击事件监测与处置平台、部侧 APT 事件监测与处置平台、部侧跨网溯源平台以及部侧安全中台。

3.2

常态化监测类数据

基础电信企业主动监测到安全事件并上报到部侧平台的相关数据。例如，木马和僵尸网络受控事件报送等。

3.3

指令监测类数据

基础电信企业根据部侧平台下发的监测指令要求，监测相关安全事件，并反馈到部侧平台的监测结果数据和关联文件。

3.4

指令查询类数据

基础电信企业根据部侧平台下发的查询指令要求反馈的查询结果数据和关联文件。

4　专项数据报送网络架构

4.1　网络架构图

专项数据报送网络架构示意如图1所示：

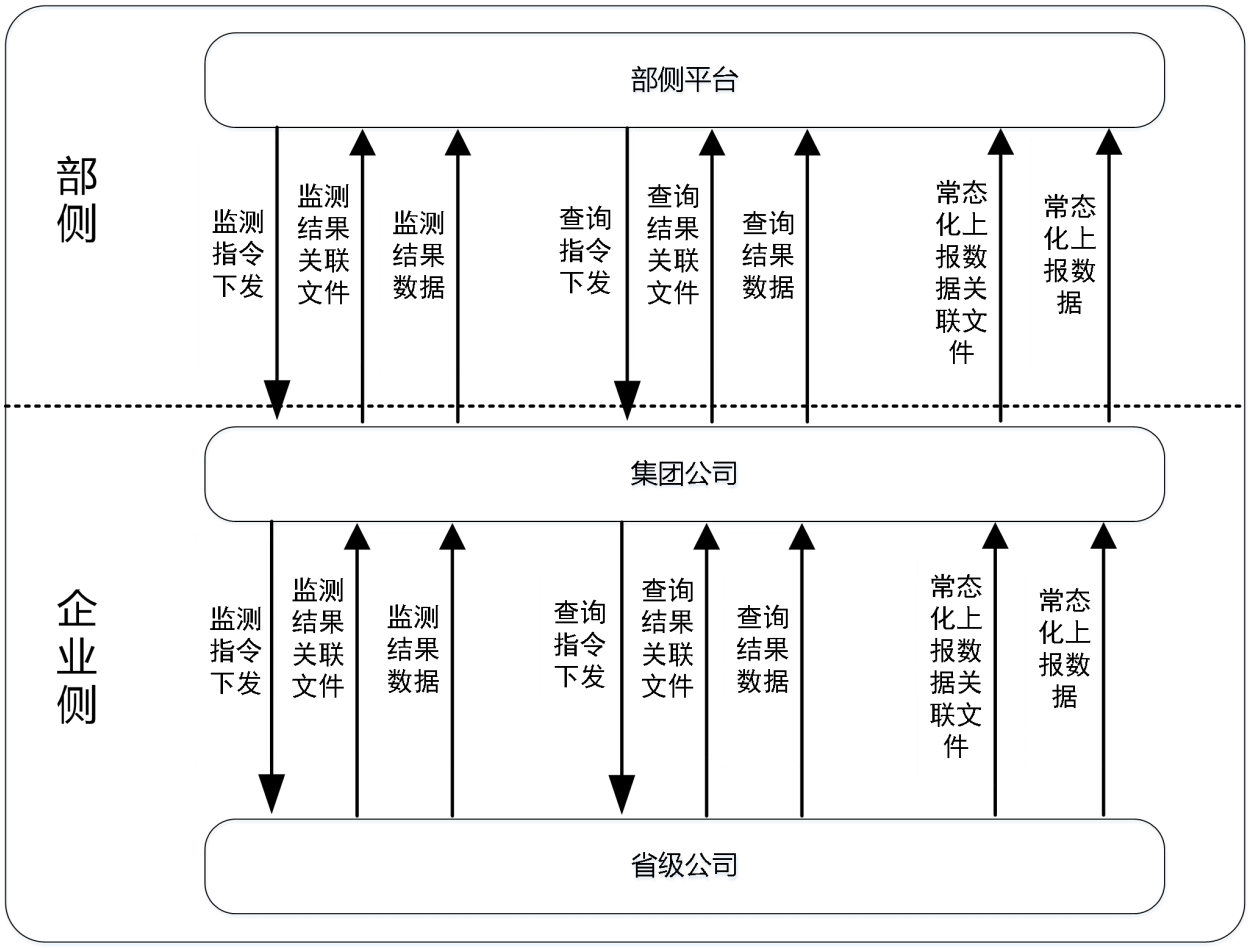

图 1 专项数据报送网络架构示意图

基础电信企业省级公司通过集团公司向部侧平台上报的专项数据主要包括，IDC 网络安全事件、僵木蠕安全事件、移动恶意程序安全事件、企业办公网态势感知网络安全事件、DNS 解析日志、NetFlow 日志、移动上网日志、IDC 访问日志以及 APT 探针巡检数据 9 类。这 9 类专项数据根据其报送特征可分为常态化监测类数据、指令监测类数据和指令查询类数据。其中常态化监测类数据主要包括常态化上报数据和常态化上报关联文件；指令监测类数据主要包括监测结果数据和监测结果关联文件；指令查询类数据主要包括查询结果数据和查询结果关联文件。专项数据报送共包含 30 个数据项，具体如下：

1)　常态化监测类数据（12项）

常态化监测类数据包含：IDC网络威胁监测记录、木马和僵尸网络受控事件、木马和僵尸网络安全威胁事件、木马和僵尸网络传播事件、木马和僵尸网络专题任务事件、移动恶意受控事件、移动恶意网络安全威胁事件、移动恶意传播事件、移动恶意特定类型应用事件、态势感知安全事件、态势感知邮件安全事件、DDoS保障对象NetFlow日志消息。

2)　指令监测类数据（11项）

指令监测类数据包含： IDC恶意报文监测记录、IDC恶意文件监测记录、木马和僵尸网络资源监测记录、木马和僵尸网络流量报文监测记录、木马和僵尸网络恶意样本监测记录、移动恶意网络资源监测记录、移动恶意流量报文监测记录、移动恶意样本监测记录、态势感知网络资源监测结果、态势感知流量报文监测结果、态势感知恶意样本监测结果。

3) 指令查询类数据（7项）

指令查询类数据包含：木马和僵尸网络历史恶意样本查询结果、移动恶意历史恶意样本查询结果、态势感知历史恶意样本查询结果、DNS日志通用查询反馈、NetFlow日志通用查询反馈、移动上网日志通用查询反馈、IDC访问日志通用查询反馈。

5 专项数据报送技术要求

5.1 IDC 网络安全事件

数据种类	数据类型	数据项定义	考核指标	考核指标说明
IDC 网络安全事件	常态化监测类数据	见“附录 A 专项数据定义”的如下章节： 附录 A.1.1 IDC 网络威胁监测记录上报	覆盖范围	应覆盖各基础电信企业的全国 IDC 节点。
			及时性	从安全事件发生到受测企业报出该事件的时间间隔应不超过 2.5 小时；从用户完成恶意样本下载到受测企业报出该事件的时间间隔应不超过 2 小时。
			完整性	受测企业上报的数据字段应与“数据项定义”中对应数据字段保持一致；如有恶意文件，恶意文件命名规则应符合“数据项定义”中相关命名要求，且文件完整并未被篡改。
			准确性	受测企业上报的数据格式应符合“数据项定义”中对应数据的字段类型、长度、取值范围等要求。
	指令监测类数据	见“附录 A 专项数据定义”的如下章节： 附录 A.1.2 IDC 恶意报文监测记录上报结果 附录 A.1.3 IDC 恶意文件监测记录上报结果	覆盖范围	应覆盖各基础电信企业的全国 IDC 节点。
			及时性	从监测到指令触发的安全事件到完成日志上报之间的时间间隔不超过 20 分钟。
			完整性	受测企业反馈的监测结果数据字段应与“数据项定义”中对应数据字段保持一致；如有关联文件，关联文件命名规则应符合“数据项定义”中相关命名要求，且文件完整并未被篡改。
			准确性	受测企业反馈的监测结果数据格式应符合本表“数据项定义”中对应数据的字段类型、长度、取值范围等要求。

5.2 僵木蠕安全事件

数据种类	数据类型	数据项定义	考核指标	考核指标说明
僵木蠕安全事件	常态化监测类数据	见“附录 A 专项数据定义”的如下章节： 附录 A.2.1 木马和僵尸网络受控事件报送消息 附录 A.2.2 木马和僵尸网络安全威胁事件报送消息 附录 A.2.3 木马和僵尸网络传播事件报送消息 附录 A.2.4 木马和僵尸网络专题任务事件报送消息	覆盖范围	应覆盖各基础电信企业省网 9%带宽。
			及时性	从事件发生到部侧平台发现该事件记录的时间间隔应不超过 4 小时；从用户完成样本下载到部侧平台收到该样本上报，时间间隔应不超过 24 小时。
			完整性	受测企业上报的数据字段应与“数据项定义”中对应数据字段保持一致；如有恶意文件，恶意文件命名规则应符合“数据项定义”中相关命名要求，且文件完整并未被篡改。
			准确性	受测企业上报的数据格式应符合“数据项定义”中对应数据的字段类型、长度、取值范围等要求。
	指令监测类数据	见“附录 A 专项数据定义”的如下章节： 附录 A.2.5 木马和僵尸网络资源监测记录上报内容 附录 A.2.6 木马和僵尸网络流量报文监测记录上报内容 附录 A.2.7 木马和僵尸网络恶意样本监测记录上报内容	覆盖范围	应覆盖各基础电信企业省网 9%带宽。
			及时性	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数据的时间间隔应不超过 90 分钟。
			完整性	受测企业反馈的监测结果数据字段应与“数据项定义”中对应数据字段保持一致；如有关联文件，关联文件命名规则应符合“数据项定义”中相关命名要求，且文件完整并未被篡改。
			准确性	受测企业反馈的监测结果数据格式应符合“数据项定义”中对应数据的字段类型、长度、取值范围等要求。
	指令查询类数据	见“附录 A 专项数据定义”的如下章节： 附录 A.2.8 木马和僵尸网络历史恶意样本查询结果上报内容	覆盖范围	应覆盖各基础电信企业省网 9%带宽。
			及时性	从部侧平台下发查询指令，到部侧平台查询结果的时间间隔应不超过 60 分钟。
			完整性	受测企业反馈的查询结果数据字段应与“数据项定义”中对应数据字段保持一致；如有恶意文件，恶意文件命名规则应符合“数据项定义”中相关命名要求，且文件完整并未被篡改。
			准确性	受测企业反馈的查询结果数据应可正

				常解析，其数据范围应符合查询指令的“起始时间”等查询条件，数据格式应符合“数据项定义”中对应数据的字段类型、长度、取值范围等要求。

5.3 移动恶意程序事件

数据种类	数据类型	数据项定义	考核指标	考核指标说明
移动恶意程序安全事件	常态化监测类数据	见“附录 A 专项数据定义”的如下章节： 附录 A.3.1 移动恶意受控事件报送消息 附录 A.3.2 移动恶意网络安全威胁事件报送消息 附录 A.3.3 移动恶意传播事件报送消息 附录 A.3.4 移动恶意特定类型应用事件报送消息	覆盖范围	应覆盖各基础电信企业 3G/4G/5G 网络。
			及时性	从事件发生到部侧平台发现该事件记录的时间间隔应不超过 4 小时；从用户完成样本下载到部侧平台收到该样本上报，时间间隔应不超过 24 小时。
			完整性	受测企业上报的数据字段应与“数据项定义”中对应数据字段保持一致；如有恶意文件，恶意文件命名规则应符合“数据项定义”中相关命名要求，且文件完整并未被篡改。
			准确性	受测企业上报的数据格式应符合“数据项定义”中对应数据的字段类型、长度、取值范围等要求。
	指令监测类数据	见“附录 A 专项数据定义”的如下章节： 附录 A.3.5 移动恶意网络资源监测记录上报内容 附录 A.3.6 移动恶意流量报文监测记录上报内容 附录 A.3.7 移动恶意样本监测记录上报内容	覆盖范围	应覆盖各基础电信企业 3G/4G/5G 网络。
			及时性	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数据的时间间隔应不超过 90 分钟。
			完整性	受测企业反馈的监测结果数据字段应与“数据项定义”中对应数据字段保持一致；如有关联文件，关联文件命名规则应符合“数据项定义”中相关命名要求，且文件完整并未被篡改。
			准确性	受测企业反馈的监测结果数据格式应符合“数据项定义”中对应数据的字段类型、长度、取值范围等要求。
	指令查询类数据	见“附录 A 专项数据定义”的如下章节： 附录 A.3.8 移动恶意历史恶意样本	覆盖范围	应覆盖各基础电信企业 3G/4G/5G 网络。
			及时性	从部侧平台下发查询指令，到部侧平台查询结果的时间间隔应不超过 60 分钟。

		查询结果反馈	完整性	受测企业反馈的查询结果数据字段应与“数据项定义”中对应数据字段保持一致；如有恶意文件，恶意文件命名规则应符合“数据项定义”中相关命名要求，且文件完整并未被篡改。
			准确性	受测企业反馈的查询结果数据应可正常解析，其数据范围应符合查询指令的“起始时间”等查询条件，数据格式应符合“数据项定义”中对应数据的字段类型、长度、取值范围等要求。

5.4 企业办公网态势感知网络安全事件

数据种类	数据类型	数据项定义	考核指标	考核指标说明
企业办公网态势感知网络安全事件	常态化监测类数据	见“附录 A 专项数据定义”的如下章节： 附录 A.4.1 态势感知安全事件信息上报 附录 A.4.2 态势感知邮件安全事件信息上报	覆盖范围	应覆盖各基础电信企业办公网的互联网出口。
			及时性	从事件发生到部侧平台发现该事件记录的时间间隔应不超过 4 小时；从用户完成样本下载到部侧平台收到该样本上报，时间间隔应不超过 24 小时。
			完整性	受测企业上报的数据字段应与“数据项定义”中对应数据字段保持一致。
			准确性	受测企业上报的数据格式应符合“数据项定义”中对应数据的字段类型、长度、取值范围等要求。
	指令监测类数据	见“附录 A 专项数据定义”的如下章节： 附录 A.4.3 态势感知网络资源监测结果上报 附录 A.4.4 态势感知流量报文监测结果上报 附录 A.4.5 态势感知恶意样本监测结果上报	覆盖范围	应覆盖各基础电信企业办公网。
			及时性	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数据的时间间隔应不超过 90 分钟。
			完整性	受测企业反馈的监测结果数据字段应与“数据项定义”中对应数据字段保持一致；如有关联文件，关联文件命名规则应符合“数据项定义”中相关命名要求，且文件完整并未被篡改。
			准确性	受测企业反馈的监测结果数据格式应符合“数据项定义”中对应数据的字段类型、长度、取值范围等要求。
	指令查询类数据	见“附录 A 专项数据定义”的如下章节： 附录 A.4.6 态势感	覆盖范围	应覆盖各基础电信企业办公网。
			及时性	从部侧平台下发查询指令，到部侧平台查询结果的时间间隔应不超过 60 分钟。

		知历史恶意样本查询结果上报	完整性	受测企业反馈的查询结果数据字段应与“数据项定义”中对应数据字段保持一致；如有恶意文件，恶意文件命名规则应符合“数据项定义”中相关命名要求，且文件完整并未被篡改。
			准确性	受测企业反馈的查询结果数据应可正常解析，其数据范围应符合查询指令的“起始时间”等查询条件，数据格式应符合“数据项定义”中对应数据的字段类型、长度、取值范围等要求。

5.5 DNS 日志

数据种类	数据类型	数据项定义	考核指标	考核指标说明
DNS 日志	指令查询类数据	见“附录 A 专项数据定义”的如下章节： 附录 A.5.1 DNS 日志通用查询反馈	覆盖范围	应覆盖各基础电信企业公共互联网。
			及时性	部侧平台下发查询指令后，查询时间间隔 ≤ 1 个小时（1 天可累计查 24 次），并发 500 个以内 IP 任务，受测企业应在 1 个小时内返回查询结果（无并发查询任务时）。 注：查询时间间隔指查询指令中“起始时间”到“结束时间”的时间跨度。
			完整性	受测企业反馈的 DNS 日志数据字段应与“数据项定义”中对应数据字段保持一致。
			准确性	受测企业反馈的 DNS 日志数据应可正常解析，其数据范围应符合查询指令的“起始时间”等查询条件，数据格式应符合“数据项定义”中对应数据的字段类型、长度、取值范围等要求。

5.6 NetFlow 日志

数据种类	数据类型	数据项定义	考核指标	考核指标说明
NetFlow 日志	常态化监测类数据	见“附录 A 专项数据定义”的如下章节： 附录 A.6.1 DDoS 保障对象 NetFlow 日志消息	覆盖范围	应覆盖各基础电信企业 20 个城域网。
			及时性	部侧平台监测到安全事件后，受测企业应在 24 小时内向部侧平台报出相关 NetFlow 日志数据。
			完整性	受测企业上报的 NetFlow 日志数据字段应与“数据项定义”中对应数据字段保持一致。
			准确性	受测企业上报的 NetFlow 日志数据的

				数据格式应符合“数据项定义”中对应数据的字段类型、长度、取值范围等要求。
	指令查询类数据	见“附录 A 专项数据定义”的如下章节： 附录 A.6.2 NetFlow 日志通用查询反馈	覆盖范围	应覆盖各基础电信企业 20 个城域网。
			及时性	部侧平台下发查询指令后，查询 7 日内数据时，查询时间间隔 ≤ 1 个自然日，并发 50 个以内 IP 任务，受测企业应在 2 个小时内返回查询结果； 查询 7 日前数据时，查询时间间隔 ≤ 1 个自然日，并发 50 个以内 IP 任务，受测企业应在 6 个小时内返回查询结果。 注：查询时间间隔指查询指令中“起始时间”到“结束时间”的时间跨度；针对任一查询条件，当返回的记录条数大于 5000 条时，查询结果返回时间按照 30 秒/5000 条等比递增。
			完整性	受测企业反馈的 NetFlow 日志数据字段应与“数据项定义”中对应数据字段保持一致。
			准确性	受测企业反馈的 NetFlow 日志数据应可正常解析，其数据范围应符合查询指令的“起始时间”等查询条件，数据格式应符合“数据项定义”中对应数据的字段类型、长度、取值范围等要求。

5.7 移动上网日志

数据种类	数据类型	数据项定义	考核指标	考核内容说明
移动上网日志	指令查询类数据	见“附录 A 专项数据定义”的如下章节： 附录 A.7.1 移动上网日志通用查询反馈	覆盖范围	应覆盖各基础电信企业 3G/4G/5G 网络。
			及时性	部侧平台下发查询指令后，查询 7 日内数据时，查询时间间隔 ≤ 1 个自然日，并发 50 个以内 IP 任务，受测企业应在 2 个小时内返回查询结果； 查询 7 日前数据时，查询时间间隔 ≤ 1 个自然日，并发 50 个以内 IP 任务，受测企业应在 6 小时内返回。 注：查询时间间隔指查询指令中“起始时间”到“结束时间”的时间跨度；针对任一查询条件，当返回的记录条数大于 5000 条时，查询结果返回时间按照 30 秒/5000 条等比递增。

			完整性	受测企业反馈的移动上网日志数据字段应与“数据项定义”中对应数据字段保持一致。
			准确性	受测企业反馈的移动上网日志应可正常解析，其数据范围应符合查询指令的“起始时间”等查询条件，数据格式应符合“数据项定义”中对应数据的字段类型、长度、取值范围等要求。

5.8 IDC 访问日志

数据种类	数据类型	数据项定义	考核指标	考核内容说明
IDC 访问日志	指令查询类数据	见“附录 A 专项数据定义”的如下章节： 附录 A.8.1 IDC 访问日志通用查询反馈	覆盖范围	应覆盖各基础电信企业的全国 IDC 节点。
			及时性	部侧平台下发查询指令后，查询 7 日内数据时，查询时间间隔 ≤ 1 个自然日，并发 50 个以内 IP 任务，受测企业应在 2 个小时内返回查询结果； 查询 7 日前数据时，查询时间间隔 ≤ 1 个自然日，并发 50 个以内 IP 任务，受测企业应在 6 小时内返回。 注：查询时间间隔指查询指令中“起始时间”到“结束时间”的时间跨度；针对任一查询条件，当返回的记录条数大于 5000 条时，查询结果返回时间按照 30 秒/5000 条等比递增。
			完整性	受测企业反馈的 IDC 访问日志数据字段应与“数据项定义”中对应数据字段保持一致。
			准确性	受测企业反馈的 IDC 访问日志数据应可正常解析，其数据范围应符合查询指令的“起始时间”等查询条件，数据格式应符合“数据项定义”中对应数据的字段类型、长度、取值范围等要求。

5.9 APT 探针巡检数据

数据种类	数据类型	数据项定义	考核指标	考核指标说明
APT 探针巡检数据	常态化监测类数据	暂无	监测数据	确保设备获取到的网络流量数据真实完整，无重复、无效或无关数据，且流量数据内容未被篡改、遗漏或截断。
			网络带宽	确保与部侧平台连通网络带宽不小于

				50Mbps。
			网络性能	确保与部侧平台连通网络网速时延不大于 150ms。
			部署位置	确保监测设备部署在事发网络单元内，或离其最近的流量关口。

6 专项数据报送测试方法

6.1 IDC 网络安全事件

测试编号：6.1
测试项目：IDC 网络安全事件检测
测试目的：验证 IDC 网络安全事件满足专项数据考核要求
测试环境：现网环境
测试步骤： 1.技术测试 *常态化监测类测试：* （1）触发网络攻击相关安全事件。 （2）受测企业上报 IDC 网络安全事件告警日志数据和恶意文件（如有恶意文件）到部侧 APT 监测平台。 （3）登录部侧 APT 监测平台，核验上报的 IDC 网络安全事件告警日志数据和恶意文件（如有恶意文件）。 *指令监测类测试：* （1）部侧 APT 监测平台下发监测指令。 （2）下发监测指令 90 分钟后，触发网络攻击相关安全事件。 （3）受测企业上报监测结果数据和关联文件（如有关联文件）到部侧 APT 监测平台。 （4）登录部侧 APT 监测平台，核验上报的监测结果数据和关联文件（如有关联文件）。 2.文档核验 核验相关文档，如：技术方案、验收报告等，证明 IDC 网络安全事件覆盖范围。
预期结果： 1.技术测试 *常态化监测类测试：* （1）覆盖范围要求：在指标要求的覆盖范围内，受测企业在将 IDC 网络安全事件告警日志数据上报到部侧平台；如有恶意文件，受测企业将恶意文件也上报到部侧平台。 （2）及时性要求：从安全事件发生到受测企业报出该事件的时间间隔应不超过 2.5 小时；从用户完成恶意样本下载到受测企业报出该事件的时间间隔应不超过 2 小时。 （3）完整性要求：IDC 网络安全事件告警日志数据与“附录 A 专项数据定义”中对应数据字段保持一致；如有恶意文件，恶意文件命名规则符合“附录 A 专

项数据定义”中相关命名要求，且文件完整并未被篡改。 （4）准确性要求：IDC 网络安全事件告警日志数据符合“附录 A 专项数据定义”中对应数据的字段类型、长度、取值范围等要求，字段内容准确。 *指令监测类测试：* （1）覆盖范围要求：在指标要求的覆盖范围内，受测企业将监测结果数据反馈到部侧平台；如有关联文件，受测企业将关联文件也反馈到部侧平台。 （2）及时性要求：从监测到指令触发的安全事件到完成日志上报不超过 20 分钟。 （3）完整性要求：监测结果数据与“附录 A 专项数据定义”中对应数据字段保持一致；如有关联文件，关联文件命名规则符合“附录 A 专项数据定义”中相关命名要求，且文件完整并未被篡改。 （4）准确性要求：监测结果数据符合“附录 A 专项数据定义”中对应数据的字段类型、长度、取值范围等要求，字段内容准确。 2.受测企业提供的文档明确了 IDC 网络安全事件覆盖范围，且与该数据的覆盖范围考核指标相符。
测试说明： **常态化监测类数据定义见“附录 A 专项数据定义”的如下章节：** 附录 A.1.1 IDC 网络威胁监测记录上报 **指令查询类数据定义见“附录 A 专项数据定义”的如下章节：** 附录 A.1.2 IDC 恶意报文监测记录上报结果 附录 A.1.3 IDC 恶意文件监测记录上报结果

6.2 僵木蠕安全事件

测试编号：6.2
测试项目：僵木蠕安全事件检测
测试目的：验证僵木蠕安全事件满足专项数据考核要求
测试环境：现网环境
测试步骤： 1.技术测试 *常态化监测类测试：* （1）触发网络攻击相关安全事件。 （2）受测企业上报僵木蠕安全事件告警日志数据和恶意文件（如有恶意文件）到部侧 APT 监测平台。 （3）登录部侧 APT 监测平台，核验上报的僵木蠕安全事件告警日志数据和恶意文件（如有恶意文件）。 *指令监测类测试：* （1）部侧 APT 监测平台下发监测指令。 （2）下发监测指令 90 分钟后，触发网络攻击相关安全事件。 （3）受测企业上报监测结果数据和关联文件（如有关联文件）到部侧 APT 监测平台。 （4）登录部侧 APT 监测平台，核验上报的监测结果数据和关联文件（如有关联文件）。 *指令查询类测试：*

（1）部侧 APT 监测平台下发查询指令。
（2）受测企业上报查询结果数据和恶意文件（如有恶意文件）到部侧 APT 监测平台。
（3）登录部侧 APT 监测平台，核验上报的查询结果数据和恶意文件（如有恶意文件）。
2.文档核验
核验相关文档，如：技术方案、验收报告等，证明僵木蠕安全事件覆盖范围。

预期结果：
1.技术测试
常态化监测类测试：
（1）覆盖范围：在指标要求的覆盖范围内，受测企业在要求的覆盖范围内将僵木蠕网络安全事件告警日志数据上报到部侧平台；如有恶意文件，受测企业将恶意文件上报到部侧平台。
（2）及时性要求：从事件发生到部侧平台发现该事件记录的时间间隔应不超过 4 小时；从用户完成恶意样本下载到部侧平台收到该恶意样本上报，时间间隔应不超过 24 小时。
（3）完整性要求：僵木蠕网络安全事件告警日志数据与“附录 A 专项数据定义”中对应数据字段保持一致；如有恶意文件，恶意文件命名规则符合“附录 A 专项数据定义”中相关命名要求，且文件完整并未被篡改。
（4）准确性要求：僵木蠕网络安全事件告警日志数据符合“附录 A 专项数据定义”中对应数据的字段类型、长度、取值范围等要求，字段内容准确。
指令监测类测试：
（1）覆盖范围要求：在指标要求的覆盖范围内，受测企业将监测结果数据反馈到部侧平台；如有关联文件，受测企业将关联文件反馈到部侧平台。
（2）及时性要求：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数据的时间间隔应不超过 90 分钟。
（3）完整性要求：监测结果数据与“附录 A 专项数据定义”中对应数据字段保持一致。
（4）准确性要求：监测结果数据符合“附录 A 专项数据定义”中对应数据的字段类型、长度、取值范围等要求，字段内容准确。
指令查询类测试：
（1）覆盖范围要求：在指标要求的覆盖范围内，受测企业将查询结果数据反馈到部侧平台；如有恶意文件，受测企业将恶意文件反馈到部侧平台。
（2）及时性要求：从部侧平台下发查询指令，到部侧平台查询结果的时间间隔应不超过 60 分钟。
（3）完整性要求：查询结果数据与“附录 A 专项数据定义”中对应数据字段保持一致；如有恶意文件，恶意文件命名规则符合“附录 A 专项数据定义”中相关命名要求，且文件完整并未被篡改。
（4）准确性要求：查询结果数据可正常解析，其数据范围符合查询指令的“起始时间”等查询条件，数据格式符合“附录 A 专项数据定义”中对应数据的字段类型、长度、取值范围等要求，字段内容准确。
2.文档核验

受测企业提供的文档明确了僵木蠕安全事件覆盖范围，且与该数据的覆盖范围考核指标相符。
测试说明： **常态化监测类数据定义见“附录 A 专项数据定义”的如下章节：** 附录 A.2.1 木马和僵尸网络受控事件报送消息 附录 A.2.2 木马和僵尸网络安全威胁事件报送消息 附录 A.2.3 木马和僵尸网络传播事件报送消息 附录 A.2.4 木马和僵尸网络专题任务事件报送消息 **指令监测类数据定义见“附录 A 专项数据定义”的如下章节：** 附录 A.2.5 木马和僵尸网络资源监测记录上报内容 附录 A.2.6 木马和僵尸网络流量报文监测记录上报内容 附录 A.2.7 木马和僵尸网络恶意样本监测记录上报内容 **指令查询类数据定义见“附录 A 专项数据定义”的如下章节：** 附录 A.2.8 木马和僵尸网络历史恶意样本查询结果上报内容

6.3 移动恶意程序事件

测试编号：6.3
测试项目：移动恶意程序安全事件检测
测试目的：验证移动恶意程序安全事件满足专项数据考核要求
测试环境：现网环境
测试步骤： 1.技术测试 *常态化监测类测试：* （1）触发网络攻击相关安全事件。 （2）受测企业上报移动恶意程序事件告警日志数据和恶意文件（如有恶意文件）到部侧 APT 监测平台。 （3）登录部侧 APT 监测平台，核验上报的移动恶意程序事件告警日志数据和恶意文件（如有恶意文件）。 *指令监测类测试：* （1）部侧 APT 监测平台下发监测指令。 （2）下发监测指令 90 分钟后，触发网络攻击相关安全事件。 （3）受测企业上报监测结果数据和关联文件（如有关联文件）到部侧 APT 监测平台。 （4）登录部侧 APT 监测平台，核验上报的监测结果数据和关联文件（如有关联文件）。 *指令查询类测试：* （1）部侧 APT 监测平台下发查询指令。 （2）受测企业上报查询结果数据和恶意文件（如有恶意文件）到部侧 APT 监测平台。 （3）登录部侧 APT 监测平台，核验上报的查询结果数据和恶意文件（如有恶意文件）。 2.文档核验

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/255031144003011221