ICS 35.040
L 80

CIIA

中 国 信 息 协 会 团 体 标 准

T/CIIA xxx—xxxx

政务网络安全监测平台总体技术要求

Technical Requirements of The Security Monitoring Platform for The national E-Government Netork

（征求意见稿）

xxxx-xx-xx 发布　　xxxx-xx-xx 实施

中国信息协会 发布

目　　次

前　言

本标准按照 GB/T 1.1-2009 的规则起草。

本标准由中国信息协会提出并归口。

本标准起草单位：

本标准主要起草人：

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

政务网络安全监测平台总体技术要求

1 范围

本标准规定了政务网络安全监测平台的基本要求，提出了政务网络安全监测平台技术框架和相应的技术要求。

本标准适用于非涉密政务网络，规范各级政务网络安全监测平台（或监测系统）的规划、设计、建设和运行管理，相关网络安全监测平台产品的研发和安全测评工作。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 5271.8-2001 信息技术 词汇 第8部分：安全

GB/T 25069-2010 信息安全技术 术语

GB/T 36635-2018 信息安全技术 网络安全监测基本要求与实施指南

GB/T 36643-2018 信息安全技术 网络安全威胁信息格式规范

GW 0203-2014 国家电子政务外网安全监测体系技术规范与实施指南

GW 0204-2014 国家电子政务外网安全管理系统技术要求与接口规范

3 术语和定义

GB/T 25069-2010 和 GB/T 5271.8-2001 界定的以及下列术语和定义适用于本文件。

3.1

安全监测 Security Monitoring

以信息安全事件为核心，通过对网络和安全设备日志、系统运行数据等信息的实时采集，以关联分析等方式，实现对监测对象进行风险识别、威胁发现、安全事件实时报警及可视化展现。

[GW 0203-2014，定义 3.1]

3.2

安全态势分析 Security Situation Analysis

态势分析是指在一定的时空条件下，对网络环境因素进行获取、理解以及对其未来安全状态进行预测。

3.3

信息安全事件 Information Security Incident

由单个或一系列意外或有害的信息安全时态所组成的，极有可能危害业务运行和威胁信息安全。

[GB/T 25069-2010，定义 2.1.53]

3.4

安全威胁 Security Threat

某个人、物、事件或概念对某一资源的保密性、完整性、可用性、真实性或可控性造成的危害。
[GW 0203-2014，定义 3.5]

3.5

威胁情报 Threat Intelligence

威胁情报主要是指收集、评估和应用关于安全威胁、威胁分子、攻击利用、恶意软件、漏洞和漏洞指标的数据集合。

3.6

安全策略 Security Policy

用于治理组织及系统在安全上如何管理、保护和分发资产（包括敏感信息）的一组规则、知道和事件，特别是哪些对系统安全及相关元素具有影响的资产。
[GB/T 25069-2010，定义 2.3.30]

3.7

脆弱性 Vulnerability

资产中能被威胁利用的弱点。
[GB/T 25069-2010，定义 2.3.30]

3.8

告警 Alarm

针对收集到的各种安全事件进行综合关联分析后形成的报警事件。
[GW 0204-2014，定义 3.7]

3.9

Web service

基于网络的、分布式的模块化组件，它执行特定的任务，遵守具体的技术规范，其他应用通过使用相应的规范，可以与它进行互操作。
[GW 0204-2014，定义 3.9]

3.10

政务云 Government Cloud

用于承载各级政务部门开展公共服务、社会管理的业务信息系统和数据,并满足跨部门业务协同、

数据共享与交换等的需要，提供 IaaS、PaaS 和 SaaS 服务的云计算服务。

4 缩略语

下列缩略语适用于本文件。

DNS：域名系统（Domain Name System）

FTP：文件传送协议（File Transfer Protocol）

HTTP：超文本传输协议(Hyper Text Transport Protocol)

JDBC：Java数据库连接（Java Database Connectivity）

SFTP：安全文件传送协议（Secure File Transfer Protocol）

SNMP：简单网络管理协议(Simple Network Management Protocol)

SYSLOG：系统日志（System Log）

WMI：Windows 管理规范（Windows Management Instrumentation）

WSDL：网络服务描述语言（Web Services Description Language）

XML：可扩展标记语言（Extensible Markup Language）

5 政务网络一般性说明

政务网络功能区划分图如图1所示。

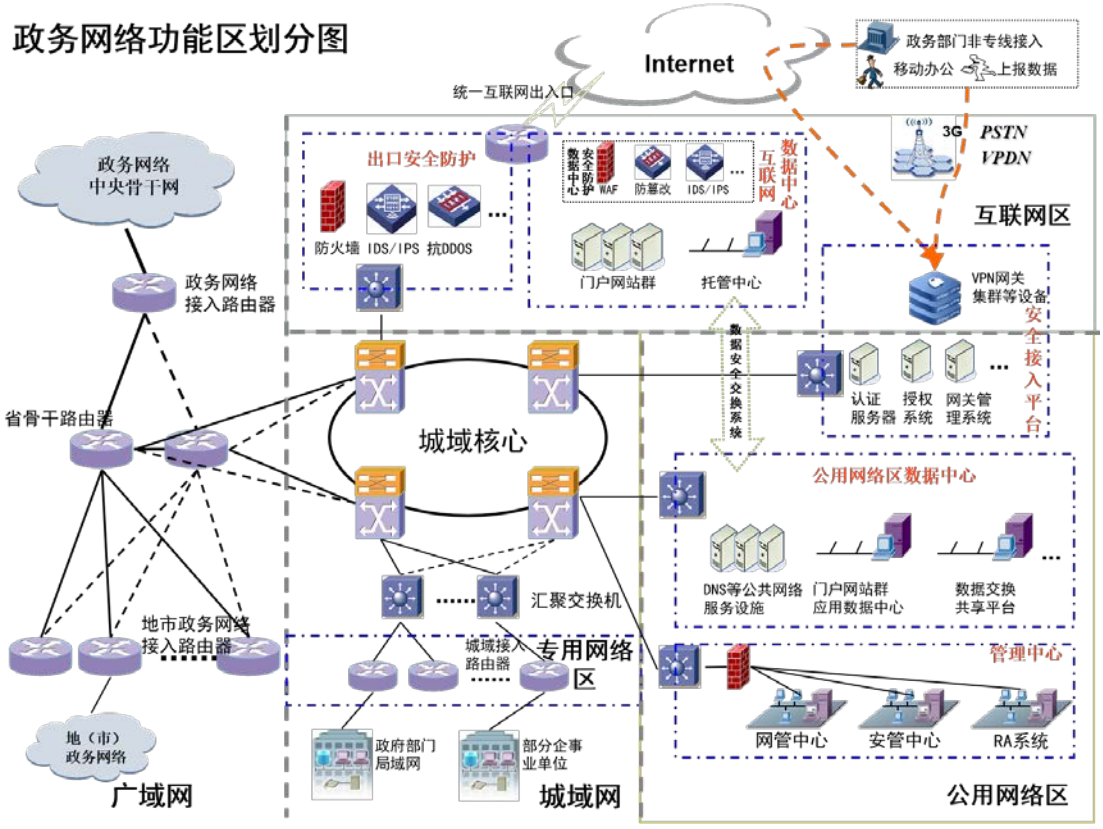

图 1 政务网络功能区划分图

根据所承载电子政务业务的需要，政务网络按其功能和作用可划分为：

a) 互联网接入区：是政务部门通过逻辑隔离安全接入互联网的网络区域，满足政务部门利用互联网开展公共服务、社会管理、经济调节和市场监管的电子政务业务需要；

b) 公用网络区：是各部门、各地区互联互通的网络区域，为政务部门公共服务及开展跨部门、跨地区的业务应用、协同和数据共享提供支撑平台；

c) 专用网络区：是为有特定安全需求的部门或业务设置的网络区域，实现本部门内的全国性业务在政务网络上开展，保证与不同部门业务应用系统的相互隔离，非本部门用户和互联网用户不能直接访问这个区域的数据和信息系统。专用网络区不在政务网络安全监测平台的监测范围之内；

d) 城域网：是同级政务部门实现互联互通的网络，各政务部门通过单位的接入设备接入城域网链路，实现互联互通；

e) 广域网：是各级政务部门实现上下互联互通的网络，各级政务网络通过接入设备接入广域骨干网链路，实现上下级政务网络的互联互通。

6 政务网络安全监测体系及技术框架

6.1 监测平台技术框架

政务网络安全监测平台技术框架如图2所示。

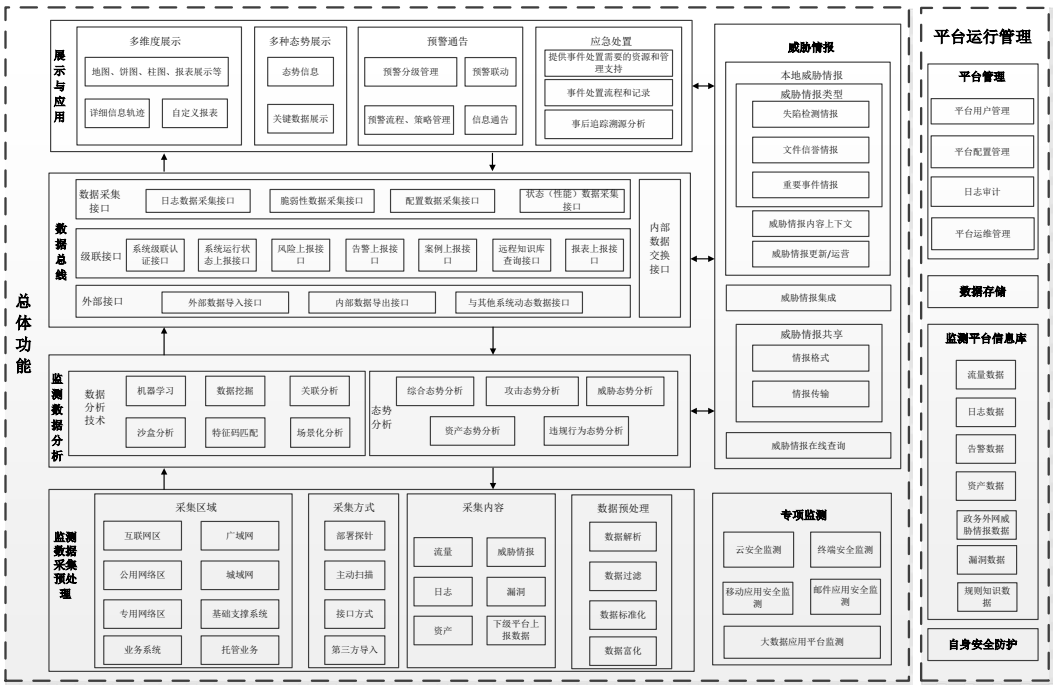

图2 政务网络安全监测平台技术架构

政务网络安全监测平台技术框架分为总体功能和平台运行管理两部分，由七大模块组成，包括：

a) 监测数据采集预处理：确定政务网络监测平台的采集区域、采集方式、采集的数据内容以及预处理方式，数据经过采集预处理后进一步进行数据分析；

b) 监测数据分析：通过机器学习、数据挖掘、关联分析等数据分析技术对政务网络的综合态势、攻击态势、威胁态势、资产态势、违规行为态势等进行分析，分析数据通过数据总线汇总至展示与应用模块；
c) 数据总线：利用内部数据交换接口、数据采集接口、系统级联接口、外部接口等实现监测数据分析后的集中采集和转发，为展示和应用提供数据；
d) 展示与应用：根据决策者、管理人员和运维人员不同的需求和关注重点，进行多种态势的多维度展示，并且支持预警通告和应急处置；
e) 专项监测：根据各政务网络业务需求，针对终端应用、移动应用、邮件应用等专项业务应用开展监测；
f) 威胁情报：有效提升监测平台的能力，其主要能力包括：及时发现关键威胁、为事件响应提供决策需要的上下文、了解攻击者的攻击背景情报信息、提供情报运营能力以及威胁情报数据共享交换等；
g) 平台运行管理：包括平台的管理、存储、自身安全防护以及监测平台信息库，为平台的总体功能实现提供支撑。

6.2 监测平台部署架构

政务网络安全监测平台的部署架构如图 3 所示。

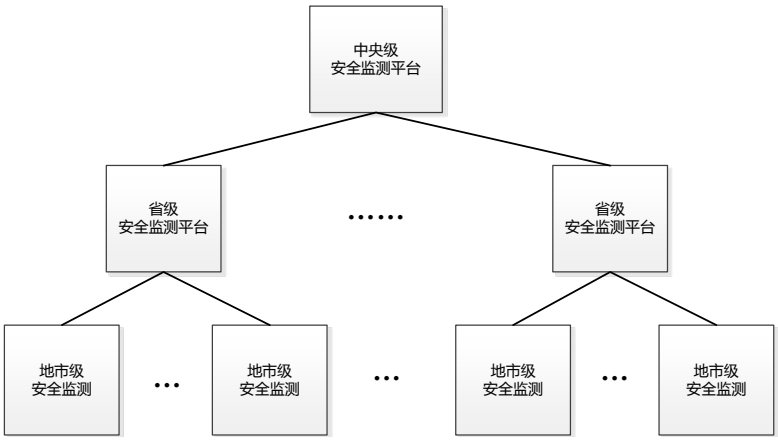

图 3 政务网络安全监测平台部署架构图

政务网络安全监测平台采用中央、省二级架构，每级单位单独建设安全监测平台，具备完整的数据采集预处理、数据分析、数据总线、展示与应用、平台运行管理等功能，各级平台可按照本级安全监测需求建设专项监测。地市级不单独建设监测分析平台，重点部署监测探针或者监测系统。上级平台向下级平台推送或提供远程知识库、威胁情报库、漏洞库、通知通告的查询接口。下级平台向上级平台上报级联认证数据、系统运行状态数据、风险上报数据、告警上报数据、案例上报数据、报表上报数据等。

6.2.1 中央级平台部署

中央级政务网络安全监测平台应部署在带外管理网中，主要对省级广域网接入、中央部门城域网接入、互联网接入区、公用网络区等区域进行流量、日志等维度信息的数据采集处理。

6.2.2 省级平台部署

省级政务网络安全监测平台应部署在带外管理网中，主要对地市级广域网接入、省级部门城域网接入、互联网接入区、公用网络区等区域进行流量、日志等维度信息的数据采集处理，地市级可按需部署平台或者在关键网络边界部署探针，将数据发送至省级平台进行分析。

省级政务安全监测平台应按照要求和中央级政务安全监测平台进行数据的级联对接。

6.2.3 地市级监测系统

地市级政务网络可不单独建设监测分析平台，部署相应的监测系统或监测探针。监测系统或监测探针主要针对地市级广域网接入、地市级城域网接入、互联网接入区、公用网络区等区域进行流量、日志等维度信息的数据采集预处理。

地市级网络安全监测系统或监测探针应按要求和省级安全监测平台进行所需数据的级联对接。

7 平台总体功能技术要求

7.1 数据采集预处理

7.1.1 采集区域

采集区域应覆盖：互联网接入区、公用网络区、专用网络区、城域网、广域网等网络区域，以及基础支撑系统、业务系统、托管业务等应用。

7.1.2 采集内容

7.1.2.1 网络流量

a) 采集内容应包含常用的网络协议流量，类型包括但不限于HTTP、FTP、POP3、SMTP、DNS、SNMP、ARP等；
b) 应对网络流量进行还原解析生成流量日志并进行采集，在发生信息安全事件时可基于流量日志进行事件回溯分析。

7.1.2.2 日志

应对IT设施的设备日志进行采集，包括但不限于网络设备、安全设备、操作系统、数据库、中间件、应用系统等日志类型。

7.1.2.3 资产信息

应支持对主机设备、网络设备、安全设备、应用系统设备等资产信息进行采集。

7.1.2.4 威胁情报

采集内容应包含多种类型的威胁情报，威胁情报包含失陷检测、文件信誉、安全预警通告等。

7.1.2.5 漏洞

应支持对主机设备、网络设备、安全设备、应用系统设备等的漏洞信息进行采集。

7.1.2.6 下级平台上报数据

下级单位上报给上级单位的数据应包括但不限于系统运行状态、风险状况、告警、案例、重大安全事件、报表等信息。

7.1.3 采集方式

应支持部署流量探针，通过流量镜像的方式获取被检测的流量。

应支持Syslog、WMI、JDBC、SNMP Trap、Netflow、FTP、SFTP等方式被动采集设备日志，支持插件代理主动采集日志。

应支持本地手动导入资产信息、网络流量发现资产、主动探测资产。

应支持自定义威胁情报、代理服务器进行升级、第三方导入等方式进行情报采集。

应支持本地离线导入或通过代理服务器获取漏洞库。

应支持API接口方式采集上报数据。

7.1.4 数据预处理

应通过配置相关解析规则、过滤规则、富化规则、日志类型，来达到归一化、过滤、丰富、分类日志信息的目的。

应支持自定义预处理解析规则文件，可根据应用场景，通过配置选择插件、正则表达式、分隔符、Key-Value、JSON 等方法定义解析规则。

7.2 监测数据分析

7.2.1 分析技术

7.2.1.1 机器学习

机器学习算法应能够涵盖有监督与无监督学习模型，方法包括但不限于聚类分析和分类分析。

7.2.1.2 数据挖掘

支持从大量的数据中通过统计、在线分析处理、情报检索和模式识别等诸多方法，搜索隐藏于其中的信息。

7.2.1.3 关联分析

关联分析模块应支持在分布式部署情况下提供不同大量复杂事件的关联分析。提供至少一百条预定义和自定义的关联规则，包括但不限于网络异常、暴力破解、账号异常等多种场景的规则，并支持预定义规则的更改。

7.2.1.4 沙箱分析

从分析文件类型，静态、动态方式描述，输出报告/检测结果。

应支持接收来自联动安全产品的可疑威胁对象，自动执行针对可疑文件及URL的分析检测。

7.2.1.5 特征码匹配

应支持将待检测内容与恶意流量特征、恶意文件特征、恶意代码特征等特征值进行匹配，然后根据匹配结果判断待检测的内容是否被感染。

7.2.1.6 场景化分析

应支持基于关联分析技术提供丰富的场景化分析，包括但不限于：业务资产主动外连、异地账号登录、违规上传下载等等。

7.2.2 态势分析

7.2.2.1 综合态势分析

应支持对网络的整体安全态势进行分析。

7.2.2.2 攻击态势分析

应支持对来自网络外部的攻击行为进行分析。包括但不限于DDos攻击、后门攻击、漏洞攻击、网络扫描窃听、网络钓鱼、SQL注入、信息篡改、信息泄露、信息窃取等。

7.2.2.3 威胁态势分析

应支持基于威胁情报进行威胁分析，包含对脆弱性分析。包括但不限于病毒、漏洞、蠕虫、木马程序、僵尸网络、恶意代码等。

7.2.2.4 资产态势分析

应支持针对资产的漏洞和配置弱点进行分析，自动计算出相关的风险指数。

7.2.2.5 违规行为分析

应支持基于场景化分析等手段分析内部违规行为，包括但不限于访问频次超限、访问流量超限、文件外发、非法外联、非法访问、非法文件下载等。

7.3 数据总线

平台数据总线应按照国家标准和国家电子政务外网对接口规范的要求进行建设和管理。

7.3.1 数据总线组成

数据总线主要有四部分组成：内部数据交换接口、数据采集接口、系统级联接口和外部接口。

a) 内部数据交换接口：是安全监测平台为平台内部数据格式不同的设备或模块之间数据的规范化交换而提供的标准接口；
b) 数据采集接口：是安全监测平台从各种监测对象中采集日志数据、脆弱性数据、配置数据和状态数据的接口；
c) 级联接口：是处于不同管理层次上的上下级之间进行管理信息和安全运行数据交互的接口。建立级联关系的安全监测平台之间，应采用基于可靠的身份认证手段实现可靠的访问控制；
d) 外部接口：安全监测平台通过各种外部接口与其他应用系统（例如运维管理系统、日志审计系统等）之间实现集成和数据交互。

7.3.2 内部数据交换接口

内部数据交换接口应实现平台内部数据格式不同的设备或模块之间数据的规范化交换，应包括数据采集预处理、监测数据分析、展示与应用、专项监测、威胁情报、平台运维管理、数据存储、监测平台信息库等模块之间的数据规范化交换。

7.3.3 数据采集接口

数据采集接口应实现安全监测平台从监测对象采集日志数据、脆弱性数据、配置数据和状态数据信息。

7.3.3.1 数据采集方式要求

应支持（但不限于）通过下述手段实现数据的主动或被动采集。

a) SNMP Trap
应启动SNMP Service服务，使用统一的团体串在默认或自定义端口上监听，以获取安全设备发来的SNMP Trap信息。

b) SYSLOG
应启动SYSLOG服务，使用默认或自定义端口监听，以获取安全设备发来的SYSLOG信息。
c) 文件
应具备网络文件、本地文件的定期或触发提取功能，获取其中的日志信息。
d) 数据库
应具备网络数据库、本地数据库的定期或触发提取功能，获取其中的日志信息。
e) 代理
对于特殊的、缺乏共性的信息存储方式，应支持通过编写代理程序方式获取其中的日志信息，代理程序应支持与目标数据部署在一起，也支持远程部署。

7.3.3.2 数据采集内容要求

a) 日志数据采集
应采集政务网络中的网络设备、安全设备、服务器设备所产生的所有日志信息。
b) 脆弱性数据采集
应采集政务网络中的网络设备、安全设备、操作系统、应用系统的脆弱性、补丁信息。安全监测平台可直接采集脆弱性数据，也可支持将其他相关设备的脆弱性数据导入到安全监测平台。
c) 配置数据采集
应采集政务网络中的网络设备、安全设备、服务器设备的账号安全策略、口令安全策略、授权安全策略和日志安全策略信息。安全监测平台可直接采集配置数据，也可支持第三方的配置数据导入。
d) 状态（性能）数据采集
应采集政务网络中的网络设备、安全设备、服务器设备的运行状态、性能相关数据。

7.3.4 系统级联接口

7.3.4.1 接口协议

系统级联接口按Web Service标准对外提供服务，通讯过程中请求和响应的数据采用标准XML格式来封装。对于开放的接口函数，厂商需发布相应的WSDL文档，用于描述Web Service的接口信息。

系统级联接口函数分为两类。一类是同步调用函数，即函数的返回值就是结果；另一类是异步调用函数，返回结果通过回调函数发送至调用方。异步类函数的返回值只表示“是/否接受命令”，调用方应提供满足标准的回调函数。

7.3.4.2 接口格式定义

接口格式定义包括函数名称、参数列表及返回值类型，参与交互数据的编码应符合GB/T 18030-2005标准。参数与返回值的具体XML格式由接口提供者根据具体业务的实际情况制定，应层次简单、结构清晰，接口提供者需提供相应的WSDL文档及接口的详细说明文档。

函数基本格式如下：

```
public String methodName(String xml);
```

说明：

a) methodName为函数名，由接口提供者根据具体业务确定；
b) XML为调用参数，应采用XML标准描述；
c) 返回结果为XML标准格式数据。

7.3.4.3 系统级联认证接口

为保证各级安全监测平台之间的通讯安全，系统之间在进行通讯前应进行有效的认证与授权。

系统级联认证接口主要包括系统级联注册接口和系统级联注销接口。系统级联注册接口完成下级系统至上级系统的注册功能，保证上下级系统之间通信的安全性。系统级联注销接口用于上下级系统之间的认证注销，当上下级系统出现变更或废止时，由上级系统进行系统间级联的注销。

7.3.4.4 系统运行状态上报接口

上级安全监测平台需要对下级系统的上报接口实施周期检测，及时发现接口异常，减少上报数据的丢失。

下级安全监测平台周期性上报自己状态的心跳消息，上级系统根据是否能周期收到下级状态的心跳消息，来判断下级系统上报是否正常。

上报接口状态分为：

1——正常：上级系统收到下级系统的上报消息后，将下级的上报接口判断为正常；

0——离线：当上级系统在一个上报周期内未收到上报信息，则判断下级系统的上报接口离线，同时产生该下级安全监测平台上报接口离线告警。

上报频率为10分钟一次。

7.3.4.5 风险上报接口

下级安全监测平台需要向上级系统上报本级系统的安全域的风险值和风险等级。上报频率至少为10分钟一次。

风险的上报由上级安全监测平台进行请求。下级安全监测平台按照请求的内容进行风险的实时上报。

风险上报的内容包括：系统所属行政区编码，安全域名称，风险值，风险等级。

7.3.4.6 告警上报接口

下级安全监测平台将本系统发现的告警信息通过告警上报接口向上级安全监测平台进行上报。

告警的上报由上级安全监测平台进行订阅，订阅信息中包含是否上报、上报的时间范围和级别信息。下级安全监测平台按照请求的内容进行告警的实时上报或停止上报。

本级安全监测平台将本级发生的告警进行实时上报，传输采用面向连接的方式。相同的告警信息仅发送一次。若本级安全监测平台的告警清除，则向上级发送该告警消除的消息，上级安全监测平台进行相应的处置。

告警上报的内容应包括：告警的ID、系统所属行政区编码、告警名称、告警内容描述、告警的级别、告警发生的时间、告警涉及的IP地址、告警清除标志和预留字段信息。

7.3.4.7 案例上报接口

下级安全监测平台应将本系统发生的典型案例进行上报，以便上级系统对各种典型案例进行汇总。

下级安全监测平台从本系统数据库中将本系统发生的典型案例取出，调用案例上报接口，将本系统发生的案例上报给上级系统，上级系统获取到案例后可根据知识库的类别（规则库、案例库、预案库、策略库、漏洞库）对案例进行分类汇总并存储在数据库中，以便下级系统查询并为处置类似事件提供技术支撑。

案例上报接口仅为下级系统使用，接口要求的相关字段需按照字段类型、是否必填信息传递给上级系统，接口参数为XML格式。

接口返回值为XML格式，应说明调用该接口返回成功或失败的状态，返回值为失败时应给出失败原因提示。

7.3.4.8 远程知识库查询接口

下级安全监测平台可查询上级系统的知识库共享内容。

下级系统调用知识库查询接口，根据传递的接口参数获取相应的知识库案例内容，如该案例存在附件，则附件文档可供下载导出。

知识库查询接口为下级系统使用，下级系统可调用本接口，以触发查询功能；根据接口的参数，获取知识库内容，本接口为触发调用。

本接口的参数可为空，如为空则表明要查询所有知识库内容，知识库标题为模糊匹配，开始时间、结束时间可按时间段查询，结束时间需大于开始时间。

7.3.4.9 报表上报接口

下级安全监测平台应按要求向上级系统汇报本系统的月报报表汇总信息。

下级安全监测平台将本系统产生的月报定期自动上报给上级安全监测平台，报表以文件方式传送，文件类型包括DOC、DOCX、XLS、XLSX、PDF、HTML、CSV等。文件名称遵循一定格式要求，报表文件上传方式采用SFTP加密传输方式。

报表上报内容应包括系统所属行政区编码、报表名称、内容。

7.3.5 外部接口

安全监测平台应建立开放式的架构，能够通过必要的定制或使用内置的接口服务实现与IT运维管理平台等第三方平台的信息交换和管理协同。

7.3.5.1 安全监测平台外部接口要求

安全监测平台的外部接口内容：

a) 安全监测平台向第三方系统提供的信息（包括但不限于）：告警信息；
b) 安全监测平台从第三方系统接收的信息（包括但不限于）：资产信息、告警信息。

安全监测平台的外部接口方式：

a) 数据文档导入/导出：提供数据的导出功能，提供格式化文档的数据导入处理；
b) 使用通用协议进行数据动态交换：通过SYSLOG、SNMP trap实现安全监测平台与其他平台的信息交换；
c) 提供Socket或Web Service接口实现不同系统之间的同步或异步的数据交互。

7.3.5.2 外部数据导入接口

导入数据包括但不限于：资产信息、告警信息。

接口方式：

a) 安全监测平台可通过文件方式，获取并导入资产信息；
b) 安全监测平台可通过Syslog或SNMP Trap的接口方式从第三方系统获取其告警信息；
c) 安全监测平台可通过FTP或HTTP方式获取数据文件，并提供导入解析接口。

7.3.5.3 内部数据导出接口

安全监测平台提供安全告警信息内容的导出功能，可导出为XLS、TXT、RTF、PDF、HTML等标准格式。具体内容的组织和文档格式根据业务需要确定，本标准不作进一步的限定。

7.3.5.4 与其他系统动态数据接口

安全监测平台可根据需要与其他系统建立接口，将告警和事件信息传送给其他系统，如事件处理系统，集中告警管理系统，实现相关安全信息的动态交换。并可将工单和运维信息传送给第三方运维管理

系统，通过工单流程化处理，实现告警和事件的应急响应。也可将资产信息传送给资源管理系统或网络管理系统，实现资产信息交互。

接口方式可采用Web Service或Socket协议。具体的数据格式根据业务需要确定，本标准不作进一步的限定。

7.4 展示与应用

7.4.1 态势展示应用

7.4.1.1 多维度展示

7.4.1.1.1 地图/饼图/柱图等

在态势展示页面应能够利用各种表达方式，通过图形化的方式呈现各安全态势专题的情况。如柱状图、折线图、饼图、散点图、气泡图、雷达图、热力图、力导向图等。

应支持上级平台的GIS地图页面调用。

7.4.1.1.2 详细信息轨迹

应支持在态势展示页面通过信息钻取查看安全事件的详情，可以多层钻取。

7.4.1.1.3 自定义报表

应具备灵活的规则编辑器，可以基于预先定义的模板，实现各类报告数据的统计和展示，并支持报表的结果输出。

7.4.1.2 多种态势展示

可视化态势展示内容包括综合安全态势、攻击态势、威胁态势、资产态势等。

应支持B/S结构，分析结果以地图、饼图、柱图、报表等方式呈现。

7.4.2 预警通告联动

7.4.2.1 预警分级管理

应提供预警分级，将接收到的预警信息按照重要程度、影响范围等进行分级，支持进一步的预警处理。

7.4.2.2 预警流程、策略管理

应支持预警流程自定义，发生预警事件时，支持依照设定的流程发布信息通告。

应提供策略管理维护页面，协助安全分析人员进行规则和策略的开发和维护。

7.4.2.3 预警联动

应支持预警信息和应急处置实现联动。

7.4.2.4 信息通告

通告内容包括但不限于：告警名称、告警时间、告警类型、告警级别、告警对象、所属部门、告警描述等。

通告方式应支持平台告警、邮件告警、短信告警等方式。

7.4.3 应急处置

支持将各类安全告警信息基于其安全告警等级、分级分类结果结合相应的处置策略形成处置任务，通报相关机构的责任人进行后续操作和处理，并进行记录和归档。

7.5 专项监测

根据各政务网络业务需求，可建设各种专项业务应用监测。包括云平台安全监测、移动应用安全监测、终端安全监测、邮件应用安全监测、大数据应用平台监测等。

7.5.1 云平台安全监测

应检测基于政务网络云的攻击，如DDoS攻击、恶意内部攻击、共享内存攻击、欺诈攻击、恶意文件、云审计等。

7.5.2 移动应用安全监测

应检测基于移动应用的攻击，如漏洞利用、恶意软件等。

7.5.3 终端安全监测

应检测基于终端的攻击，如终端病毒信息、漏洞信息、违规外联信息、终端资产信息、高级威胁行为、漏洞攻击、弱口令等。

7.5.4 邮件应用安全监测

应检测基于邮件应用安全的攻击，如垃圾邮件、钓鱼邮件、广告邮件、邮件系统攻击等。

7.5.5 大数据应用平台监测

应检测基于大数据应用平台的攻击，如DDoS攻击、注入漏洞攻击、APT攻击等。

7.6 威胁情报

各级监测平台可根据实际情况建设威胁情报或通过接口调用等方式使用上级平台的威胁情报。

7.6.1 本地威胁情报

7.6.1.1 威胁情报类型

安全监测平台本地威胁情报应包含失陷检测情报、文件信誉情报、安全预警通告情报等类型。

失陷检测情报应该支持发现内部被攻击失陷的主机，监测威胁类型要覆盖APT攻击、勒索软件、网络蠕虫、远控木马、窃密木马、黑市工具等,中央级与省级威胁情报至少要包含百万级的失陷检测情报，地市级至少要包含30万条的失陷检测情报，并确保情报判断的准确性。

文件信誉情报应支持判别文件黑白，并提供具体恶意类型及家族等上下文，要求能覆盖僵尸网络、勒索软件、远控木马、窃密木马、黑市工具、恶意病毒等威胁，文件信誉情报数量要在5亿以上。省级和地市级不对文件信誉情报能力做要求，可视本地情况酌情建设或与中央级平台共享此部分情报内容。

安全预警通告情报应支持针对重要威胁事件、漏洞信息的预警通告，可以据此做针对性的预防、监控。信息需要汇集全球范围安全厂商、机构的相关数据，帮助提前预防可能出现的攻击活动。省级和地市级不对安全预警通告情报能力做要求，可视本地情况酌情建设或与中央级平台共享此部分情报内容。

7.6.1.2 威胁情报内容上下文

失陷检测情报应支持基于IP、域名等维度进行查询。上下文字段需要包含：风险IOC、风险等级、情报标签、置信度、威胁类型、恶意家族或者攻击团伙信息、是否是定向攻击、影响平台、威胁详细描

述等基础信息；威胁情报要能够记录域名解析、会话连接、文件传输、恶意样本投递、恶意样本运行等威胁主要活动信息。

文件信誉情报应支持基于文件的MD5、SHA1进行查询。上下文字段需要包含：文件类型、恶意类型、恶意家族/攻击事件、是否定向攻击、相关网络活动的IOC（如果存在）等。

安全预警通告内容需要包含：发布厂商、通告类型、影响行业、威胁等级、攻击者组织、事件概要、参考链接等。

7.6.1.3 威胁情报更新/运营

日常升级频率应不超过24小时，紧急情况要提供小时级更新。

应支持手动升级威胁情报方式，或者通过代理等安全可控方式在线更新。

应支持根据运营需要，导入自身或者其它相关方提供的威胁情报，导入的威胁情报可以通过统一的API接口查询使用。

应支持对已有的威胁情报增加自定义标记。

应支持自定义增加或删除威胁情报；可以对自定义的威胁情报状态进行管理，包括启用、禁用等。

7.6.2 威胁情报集成

应支持提供开放接口，以标准接口的方式来集成第三方威胁情报平台，接口返回数据应支持JSON格式。

7.6.3 威胁情报共享

应支持通过标准情报格式和传输标准和其它国家级、或者行业内情报平台进行数据情报共享。

7.6.3.1 情报格式

应支持以下一种或者多种标准，对外进行情报共享：

GB/T 36643-2018《信息安全技术网络安全威胁信息格式规范》

最新的国际通用标准STIX 2.0

7.6.3.2 情报传输

应支持基于国际威胁情报传输标准TAXII的共享、传输标准,可以和支持相应协议的设备进行互通。

应支持扩展更多的情报传输标准。

7.6.4 威胁情报比对

应支持通过查询接口、邮件等方式和上级平台的威胁情报进行比对，可以覆盖对僵尸网络、勒索软件、远控木马、窃密木马、黑市工具、恶意病毒等威胁类型情报的信息查询。

8 平台运行管理要求

8.1 平台运维管理要求

8.1.1 平台用户管理

应提供统一集中的用户角色管理，支持被管理角色的创建、编辑、删除等功能的基本功能。

具备权限的用户通过角色管理功能，查看系统中目前已创建的角色。

用户基本信息需要包含角色名称，备注，权限等基本属性。

用户角色查询时，支持通过角色名称来快速进行查询定位。

具备权限的用户对角色信息进行新增、编辑、删除操作时，需触发系统记录日志。

8.1.1.1 分组管理

应提供分组的增加、删除、修改、查询及权限归属分组管理。

8.1.1.2 用户管理

应提供用户管理功能。包括用户整个生命周期的管理，提供对安全监测平台用户的创建、修改、删除和查询等功能。

8.1.2 平台配置管理

监测平台配置管理包括以下内容：

a) 应支持对平台运行状态阈值的配置；
b) 应支持对采集对象地址的配置；
c) 应支持对平台参数的配置；
d) 应支持对数据存储时间的配置；
e) 应支持对账户和密码的配置，包括帐号锁定时间、密码有效周期、密码错误次数、密码最小长度的配置等。

8.1.3 日志审计

用户对模块的使用等操作行为应有完整的日志记录，便于审计跟踪和分析。

系统审计模块记录系统中发生的关键事件，包括：审计内容和审计操作。

审计内容包括：用户操作审计和系统事件审计。

审计操作包括：审计查看、审计内容导出和审计内容统计。

应确保审计日志不可删改。

8.1.4 平台运维管理

应配置专职人员对负责监测平台的运维管理。

应支持对平台进行统一监控，监视整个平台的运行状态，保证平台能够安全可靠地运行。

应支持平台运维人员实时获取服务器运行现状，以便对服务器进行维护。包括不限于服务器名称、服务器IP、CPU使用率、内存使用情况、磁盘容量、系统性能监控过程中产生的异常事件告警。

8.2 数据存储要求

8.2.1 存储要求

支持对结构化数据、半结构化数据和非结构化数据进行存储，支持文本、Key-Value、对象等多种数据类型的存储，支持可伸缩的分布式数据存储架构，满足数据量持续增长需求。

支持数据迁移，支持存储数据的备份及异常恢复。

支持节点扩展，支持负载均衡。

对数据存储时间不少于6个月。

8.2.2 存储方式

对数据文件进行分布式存储，按照使用场景对热数据和冷数据进行不同方式的存储，方便后续高效查询使用。

对数据要进行用高压缩比的算法进行压缩，可采用纠删码存储策略，在保障数据可靠性的前提下，降低数据存储冗余度。

应支持备份机制，部分数据丢失或损坏后可以快速恢复。

8.3 监测平台信息库

平台应建立相应的流量数据、日志数据、告警数据、资产数据、政务网络威胁情报数据、漏洞数据、规则知识数据等数据库。

8.4 自身安全防护

8.4.1 等级保护合规性要求

网络安全监测环境应根据自身安全需求确定等级，实施等级保护。

8.4.2 安全要求

应符合如下要求：

a) 重要数据加密存储；
b) 具备口令强度策略、口令强度自动核查及用户登录超时退出机制，应采用符合国家密码管理局、工业和信息化部要求和相关行业主管部门规定的数字证书登录措施；
c) 监测自身运行状态，应支持状态异常告警；
d) 监测敏感数据操作日志，定期执行日志审计；
e) 备份重要系统信息和数据，支持系统快速恢复；
f) 支持标准时间自动同步，每天至少同步一次；