ICS 点击此处添加 ICS 号

团 体 标 准

T/COSOCC XXXX—XXXX

信息安全技术 关键信息基础设施安全监测预警产品技术要求

Information security technology--Technical requirements for critical information infrastructure security monitoring and warning products

（征求意见稿）

（完成时间：2023-11-24）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国基本建设优化研究会　　发 布

目　　次

前　　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布结构不承担识别专利的责任。

本文件由中国基本建设优化研究会提出并归口。

本文件起草单位：

本文件主要起草人：

引　　言

为落实《中华人民共和国网络安全法》、《关键信息基础设施安全保护条例》关于保护关键信息基础设施运行安全的要求，在国家网络安全等级保护制度以及关键信息基础设施安全保护要求的基础上，借鉴我国相关部门以及网络安全企业在开展安全监测预警工作的成熟经验，并吸纳国内外在关键信息基础设施监测、保护和预警方面的举措，结合我国实际情况，满足关键信息基础设施的安全诉求，提升关键信息基础设施的安全保护能力，提出关键信息基础设施安全监测预警产品技术要求，采取必要措施保护我国关键信息基础设施业务的正常运行和不受破坏。

本文件符合我国现行《中华人民共和国标准化法》和《中华人民共和国质量法》等法律法规要求，与现行法律法规无冲突和违背情况。本标准产品的技术要求没有知识产权问题。

信息安全技术 关键信息基础设施安全监测预警产品技术要求

1 范围

本文件规定了关键信息基础设施安全监测预警产品的功能要求、安全要求和保障要求。

本文件适用于关键信息基础设施产品提供者进行产品的设计和研发，以及指导第三方测评机构对产品进行测评，也可用于产品使用者参考使用。

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，注日期的引用文件，仅该日期对应的版本适用于本文件；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 7408—2005 数据元和交换格式 信息交换 日期和时间表示法

GB/T 20986—2023 信息安全技术 网络安全事件分类分级指南

GB/T 25069 信息安全技术 术语

GB/T 31509—2015 信息安全技术 信息安全风险评估实施指南

3 术语和定义

GB/T 20986、GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

关键信息基础设施 critical information infrastructure

公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

[来源：GB/T 39204—2022，3.1]

3.2

网络安全监测 network security monitoring

通过对关键信息基础设施网络和安全设备日志、系统运行数据、网络流量等信息的采集，采用伴随分析、关联分析等方式，对监测对象进行风险识别、威胁发现、安全事件告警及可视化展示等。

[来源：GB/T 36635—2018，3.1，有修改]

3.3

网络安全预警 network security warning

基于建模预测分析、告警阈值设置等手段，对关键信息基础设施即将或正在发生的网络安全事件、风险事件或威胁，提前或实时发出的告警信息。

[来源：GB/T 25069—2022，3.739，有修改]

3.4

网络安全事件 network security incident

由于人为原因、网络遭受攻击、网络存在漏洞隐患、软硬件缺陷或故障、不可抗力因素，对关键信息基础设施的网络和信息系统的数据和业务应用造成危害，对国家、社会、经济造成负面影响的事件。

[来源：GB/T 20986—2023，3.4，有修改]

3.5

威胁信息 threat information

基于证据的知识，用于描述现有或可能出现的威胁，从而实现对威胁的响应和预防。

注：威胁信息包括上下文、攻击机制、攻击指标、可能影响等信息。
[来源：GB/T 42453—2023，3.2]

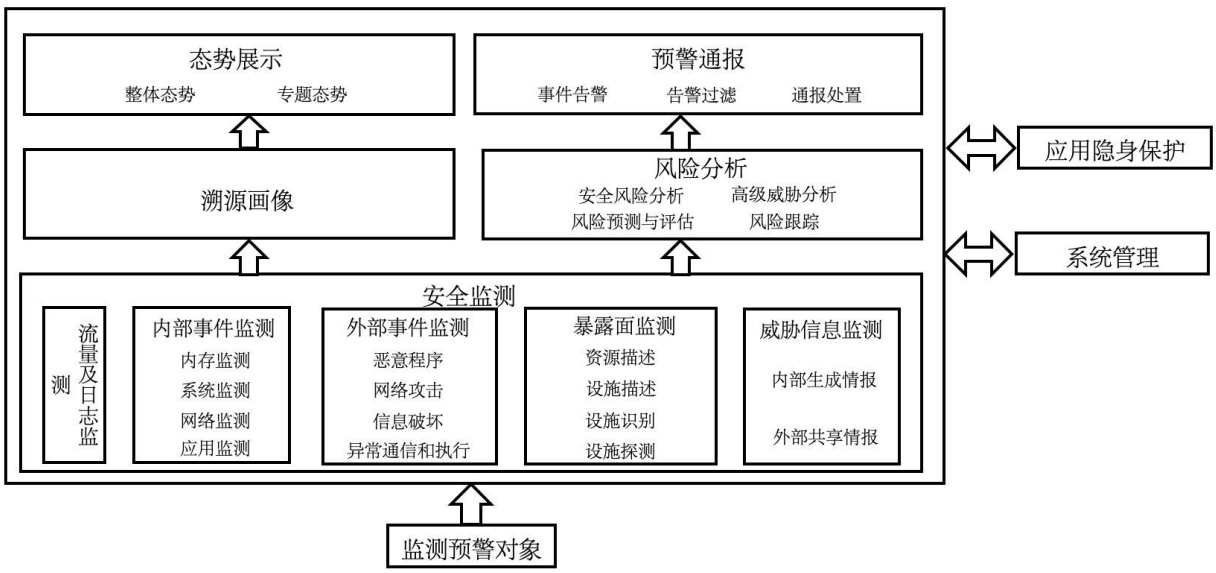
4 缩略语

下列缩略语适用于本文件。
FTP：文件传输协议（File Transfer Protocol）
IP：网际互连协议（Internet Protocol）
IPS：入侵防御系统（Intrusion Prevention System）
SYSLOG：系统日志（System Log）
SOAR：安全编排自动化与响应（Security Orchestration Automation and Response）
WAF：Web应用防火墙（Web Application Firewall）

5 概述

关键信息基础设施安全监测预警技术架构见图1。关键信息基础设施安全监测预警平台主要由安全监测、溯源画像、风险分析、态势展示、预警通报等部分组成。通过对关键信息基础设施网络或系统等监测预警对象进行信息监测，基于风险分析关联识别以及和溯源画像技术对获取到的监测数据(数据字段格式见附录C)进行解析与研判等处理，发现和评估安全事件（网络安全事件编号编码规则见附录A、B）和安全风险，及时准确预警通报，进行态势展示，最后通过预警通报关联处置安全威胁，保障关键信息基础设施的安全运行。

图1 关键信息基础设施安全监测预警技术架构



6 功能要求

6.1 网络部署

网络部署功能应满足以下要求：
a） 支持串联与旁路部署方式，支持 channel、trunk 等接口模式，并支持 802.1Q 等网络环境；
b） 支持管理口、镜像口、阻断口及业务口分离部署。

6.2 安全监测

6.2.1 流量监测

流量监测功能支持串联与旁路部署情况下，对流量进行实时监测，应符合以下要求：

a) 支持监测关键信息基础设施的流量报文，支持流量元数据、过程特性分析软件包（pcap）、网络监测功能（netflow）等方式的采集、存储和转发；
b) 支持监测、解析和还原指定的 IP 地址；
c) 支持监测、解析和还原指定的网络协议，包括超文本传输协议（HTTP）、简单邮件传输协议（SMTP）、邮局协议第三版（POP3）、文件传输协议（FTP）、交互邮件访问协议（IMAP）等网络协议。

6.2.2 日志监测

日志监测功能应符合以下要求：

a) 支持监测关键信息基础设施的设备和系统日志，支持 SYSLOG、镜像等日志采集方式，实时采集设备及系统日志；
b) 支持监测系统、安全、审计、应用程序等日志文件。

6.2.3 内部事件监测

内部事件监测功能应符合以下要求：

a) 支持监测系统访问行为，包括但不限于文件的读、写、重命名、删除等行为；
b) 支持监测系统入侵行为，包括环境变量劫持等篡改劫持行为；非法外联、暴力破解、隐藏进程等风险行为；异常登录、端口复用等远程控制行为；
c) 支持监测网络攻击行为，包括命令控制（C&C）通讯和数据库可用性组（DGA）域名检测，发现隐蔽通道和窃取数据行为；
d) 支持监测应用入侵行为，包括结构化查询语言数据库（sql）注入攻击、内存马注入攻击、跨站脚本攻击（XSS）、请求伪造、信息窃取等事件；
e) 支持监测应用服务异常行为，包括进程异常关闭、应用服务端口异常等问题。

6.2.4 外部事件监测

系统外部事件监测功能应符合以下要求：

a) 能够满足识别和发现攻击行为，包括但不限于以下方式：
   1) 支持监测恶意程序事件，包括但不限于计算机病毒、蠕虫、木马等；
   2) 支持监测网络攻击事件，包括但不限于拒绝服务攻击、后门攻击、漏洞利用攻击、网络钓鱼等；
   3) 支持监测信息破坏事件，包括但不限于信息篡改、信息假冒、信息泄露、信息窃取等；
b) 能够满足识别和发现异常通信和执行行为，包括不限于挖矿程序、外联程序、DNS 隧道等。

6.2.5 暴露面监测

暴露面监测功能应符合以下要求：

a) 支持监测关键信息基础设施的设备、系统、服务、应用等指纹信息；
b) 支持监测关键信息基础设施的网络资源等信息，包括 IP、端口、协议、应用等；
c) 支持监测关键信息基础设施设备、系统、应用的安全漏洞，及时通报，闭环处置；
d) 支持监测关键信息基础设施资产的合规性，包括重要 IP 资源离线监测、禁用软件监测、禁用端口监测、禁用服务监测等。

6.2.6 威胁信息监测

威胁信息监测功能应符合以下要求：

a) 具备监测威胁信息的能力：
   1) 支持威胁信息的内部生成，支持基于 WAF、IPS、语义检测、上下文分析等引擎至少四类，实时监测生成威胁信息数据；

2） 支持威胁信息的外部共享，支持接入第三方威胁信息源和自定义威胁信息源的能力；
3） 支持监测多源威胁信息，包括但不限于正向攻击威胁信息源、受控外联威胁信息源、IP 画像威胁信息源以及自定义威胁信息源等类型，应支持 ipv6 格式的威胁信息数据；

b） 具备威胁信息联防联控的能力，包括旁路阻断能力、与 WAF 引擎、IPS 引擎等至少两类引擎的联动防控能力、事件与告警的共享能力。

6.2.7 阻断

阻断应符合以下要求：

a） 支持自动阻断异常访问行为和人工研判攻击阻断方式；
b） 支持阻断策略配置，支持阻断范围配置，至少包含 IP、网段等。

6.3 应用隐身保护

应用隐身保护应符合以下要求：

a） 支持通过授权可信终端对应用进行隐身保护；
b） 具备对重要数据采取国密等算法加密和校验机制保障数据的机密性和完整性功能。

6.4 溯源画像

支持对网络安全事件的自动回溯画像，应符合以下要求：

a） 支持基础属性画像，至少包括归属地、经纬度等属性
b） 支持资产属性画像，至少包含资产标签、组件标签、开放端口等属性；
c） 提供对安全事件进行跟踪管理，支持攻击轨迹溯源，能够对安全事件进行反追踪。

6.5 风险分析

6.5.1 安全风险分析

应具备安全风险分析能力，包括网络安全事件分析、威胁分析、暴露面分析、运行状态分析、策略与配置分析等。按照GB/T 31509—2015中的5.2.3.3.1要求分析威胁发生的可能性和影响程度，按照GB/T 31509—2015中的5.3.2和5.3.3要求计算信息安全风险值。

6.5.2 高级威胁分析

应具备高级威胁分析能力，能够识别、分析不同类别的网络攻击行为，包括但不限于攻击属性、攻击路径、建立攻击画像等高级威胁分析。

6.5.3 风险预测及评估

风险预测及评估应符合以下要求：

a） 支持对关键信息基础设施目前状态后续安全、安全运维等趋势的预测；
b） 支持对关键信息基础设施目前状态的评估。

6.5.4 风险跟踪

支持对系统的安全风险（应用漏洞、系统漏洞、风险端口、恶意代码等）进行安全评估，实时掌握业务系统风险状况，当业务系统变更时，自动重新进行安全评估。

6.6 态势展示

6.6.1 整体态势展示

支持按照时间、类型、应用场景等维度对网络的整体或局部网络安全状况进行评估和展示，应展示网络安全状况变化趋势，应支持采用多种视图进行网络安全态势的展示。

6.6.2 专题态势展示

支持资产态势、流量态势、攻击态势、运行态势、脆弱性态势、安全事件态势和异常行为态势等的展示。

6.7 预警通报

6.7.1 事件告警

事件告警应符合以下要求：

a) 支持时间告警机制，告警方式包括但不限于实时提示、邮件短信通知、声音及闪光告警等；
b) 告警分级应符合 GB/T 20986—2023 中 5.2 的要求。

6.7.2 告警过滤

允许安全人员、运维及管理人员定义安全策略，对关键信息基础设施中的指定事件不予告警，支持对高频度发生的相同或同类安全事件进行合并告警，避免出现告警风暴。

6.7.3 通报处置

允许安全人员、运维及管理人员定义通报处置策略，对关键信息基础设施中的行为和事件定制处置方式，例如人工配置防火墙黑名单，联动SOAR通知防火墙封控拦截等策略。

6.8 系统管理

系统管理应符合以下要求：

a) 提供产品软硬件管理和配置图形化界面，支持系统及配置的备份及回退；
b) 具备独立的控制台，支持系统、补丁、规则库等在线升级，支持产品管理、自检、故障恢复等功能。

7 安全要求

7.1 身份标识与鉴别

身份标识应具有唯一性，产品应具备对用户身份的鉴别功能，用户请求执行任何操作前，对每个授权用户进行唯一的身份鉴别。

7.2 授权与访问控制

授权与访问控制应符合以下要求：

a) 具备对用户访问权限控制功能，保障权限的最小化原则，具备用户登录超时退出、锁定机制；
b) 支持 IP 黑白名单及访问控制策略配置，支持按照时间设定生效周期。

7.3 通信安全

通信安全应符合以下要求：

a) 各系统及子系统、组件应使用符合国家密码管理相关规定的密码算法套件；
b) 具备通信安全能力，保证传输通道的安全性，保障数据的机密性、完整性和可用性。

7.4 系统平台安全

系统平台安全应符合以下要求：

a) 具备时间同步功能，每天应至少同步一次；
b) 具备升级回滚机制；
c) 具备安全策略配置功能，应提供默认的策略，支持策略的编辑、修改和导入、导出；
d) 具备全生命周期的管理能力。

7.5 日志记录与审计

具备日志记录与审计管理功能，具备针对检测、分析、防御等过程中产生的各类日志和数据的日志审计能力，具备对用户行为操作的日志审计能力，日志中包含具体时间、日志类别及描述等信息，用户可将日志导出，以便保存、查阅。

8 保障要求

8.1 设计与开发

制定和实施关键信息基础设施安全监测预警产品开发流程，对设计文档、开发文档等进行配置管理，能够识别产品在设计、开发环节的安全风险，采取安全措施保障产品的设计和开发安全。自行、联合或委托第三方对产品进行安全测试，对已发现的安全缺陷、漏洞进行修复，制定并实施在用户侧进行紧急修复的安全管理流程。提供设计与实现之间的对应关系，并证明其一致性。

8.2 生产和交付

应建立和实施规范的产品生产和服务交付流程，采取完整性保护措施降低产品交付过程中的篡改风险，并将交付过程文档化，为用户提供操作指南等指导性文件，用来说明产品的安装、生成、启动等操作过程，给出风险提示和应急相应措施。

8.3 运行与维护

应建立和执行针对产品在运行和维护阶段的应急响应机制和流程，应提供必要的技术支持，为产品提供持续的安全维护。