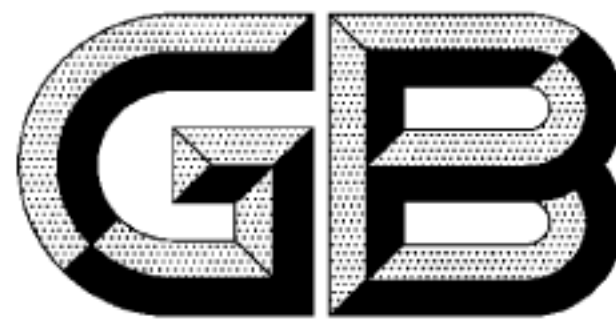


ICS 35.040
L 80



中华人民共和国国家标准

GB/T 36958—2018

信息安全技术 网络信息安全等级保护

安全管理中心技术要求

Information security technology—Technical requirements of security

management center for classified protection of cyber security

2018-12-28 发布

2019-07-01 实施

国家市场监督管理总局

中国国家标准化管理委员会

| | |
|--|----|
| 前言 | I |
| 引言 | II |
| 1 范围 | 1 |
| 2 规范性引用文件 | 1 |
| 3 术语和定义 | 1 |
| 4 缩略语 | 1 |
| 5 安全管理中心概述 | 2 |
| 5.1 总体说明 | 2 |
| 5.2 功能描述 | 3 |
| 6 第二级安全管理中心技术要求 | 3 |
| 6.1 功能要求 | 3 |
| 6.2 接口要求 | 7 |
| 6.3 自身安全要求 | 7 |
| 7 第三级安全管理中心技术要求 | 8 |
| 7.1 功能要求 | 8 |
| 7.2 接口要求 | 13 |
| 7.3 自身安全要求 | 19 |
| 8 第四级安全管理中心技术要求 | 15 |
| 8.1 功能要求 | 15 |
| 8.2 接口要求 | 21 |
| 8.3 自身安全要求 | 21 |
| 9 第五级安全管理中心技术要求 | 22 |
| 10 跨定级系统安全管理中心技术要求 | 23 |
| 附录 A (规范性附录) 安全管理中心与网络安全等级保护对象等级对应关系 | 24 |
| 附录 B (规范性附录) 安全管理中心技术要求分级表 | 25 |
| 附录 C (资料性附录) 四化安全事件属性 | 27 |

信息安全技术 网络安全等级保护 安全管理中心技术要求

1 范围

本标准规定了网络安全等级保护安全管理中心的技术要求。

本标准适用于指导安全厂商和运营使用单位依据本标准要求设计、建设和运营安全管理中心。

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 信息技术 词汇 第8部分:安全

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 25069 信息安全技术 术语

GB/T 25070—2010 信息安全技术 信息系统等级保护安全通用技术要求

3 术语和定义

GB 17859—1999、GB/T 5271.8、GB/T 25069 和 GB/T 25070 界定的以及下列术语和定义适用于本文件。

3.1

数据采集接口 data acquisition interface

库系统、网络设备、安全设备等各监测对象上的安全事件、脆弱

采集网络环境中的主机操作系统、数据脆弱性以及相关配置及其状态信息的接口。

3.2

采集器 collector

设备上收集网络安全源数据和事件信息的组件。

从网络安全等级保护对象或其所在区域

3.3

安全管理中心 security management center

境、安全区域边界和安全通信网络的安全机制实施统一管理

对定级系统的安全策略及安全计算环境

的平台或区域

注:修改 GB/T 25070—2010 定义 3.6。

注:修改 GB/T 25070—2010 定义 3.6。

4 缩略语

下列缩略语适用于本文件。

CPU 中央处理器(Central Processing Unit)

CVE 通用脆弱性及披露(CVE - Vulnerability and Disclosure Equivalency)

DDoS 分布式拒绝服务(Distributed Denial of Service)

| | |
|------|--|
| IP | 互联网协议(Internet Protocol) |
| IPv6 | 互联网协议第六版(Internet Protocol version 6) |
| SNMP | 简单网络管理协议(Simple Network Management Protocol) |

5 安全管理中心概述

5.1 总体说明

其中,功能要求从系统管理、安全管理和审计管理三个方面提出具体要求;接口要求对安全管理中心涉及到的接口协议和接口安全提出具体要求;自身安全要求对安全管理中心自身安全功能提出具体要求。

依据 GB/T 25070 的定义,第二级及第二级以上的定级系统安全保护环境需要设置安全管理中心,

三级、第四级的差异。



图 1 安全管理中心技术要求框架图

安全管理自身区域的网络边界访问控制设备,与被管理的网络设备区域、服务器区域进行安全配置数据交互,完成整个系统环境安全策略和安全运维的统一管理。

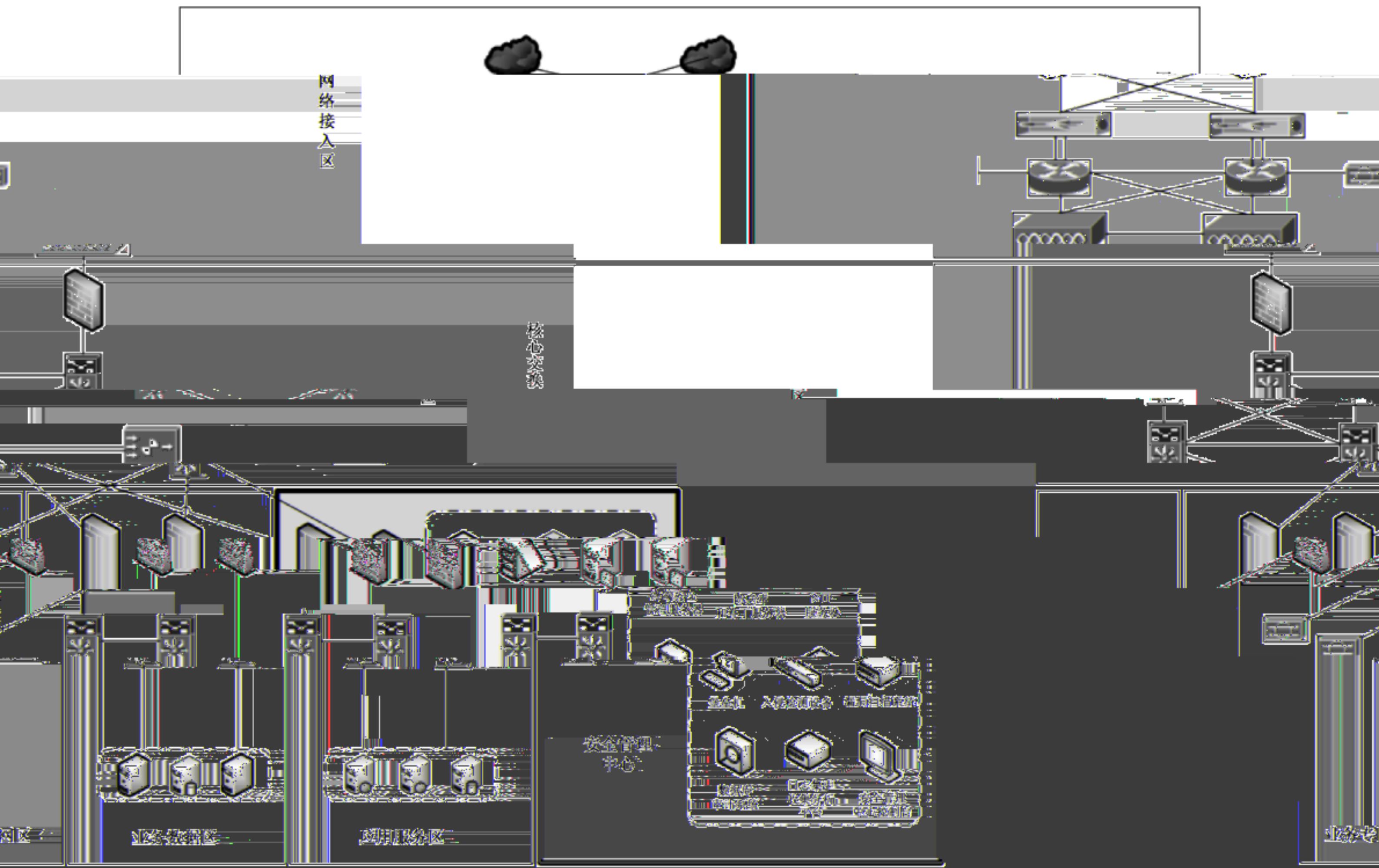


图 2 安全管理中心模型图

描述

5.2 功能

安全管理中心应能实现对网络设备和系统的安全策略和配置的统一控制和管理,并能根据

策略和配置的变化,自动下发配置到网络设备和系统,并能根据策略和配置的变化,自动

对网络设备和系统进行安全策略和配置的统一管理,并能根据策略和配置的变化,自动

安全策略,并确保标记、授权和安全策略的数据完整性。

审计管理主要通过安全审计员对分布在系统各个组成部分的安全审计机制进行集中管理,包括根据安全审计策略对审计记录进行分类,提供按时间段开启和关闭相应类型的安全审计机制,对各类审计记录进行存储、管理和查询等。安全审计员对审计记录进行分析,并根据分析结果进行及时处理。

6 第二级安全管理中心技术要求

6.1 功能要求

6.1.1 用户身份管理

6.1.1.1 用户身份管理

6.1.1.1.1 用户身份管理

用户身份管理应满足以下要求。

安全风险通告,通告中应包括通告内容、描述信息、

- b) 能够提供安全通告功能,可以创建或导入 CVE 编号、影响的操作系统等;

系统,提供受影响的被保护资产列表

- c) 能够根据通告提示的安全风险影响的操作

6.1.1.3.4 统计分析报表

统计分析报表应满足以下要求:

- a) 能够按照时间、事件类型等条件对安全事件进行查询;
- b) 能够提供统计分析和报表生成功能。

6.1.1.4 风险管理

6.1.1.4.1 资产管理

资产管理应满足以下要求:

- a) 实现对被管理对象资产的管理,提供资产的添加、修改、删除、查询与统计功能;
- b) 资产管理信息应包含资产名称、资产 IP 地址、资产类型、资产责任人、资产的机密性、完整性、可用性赋值等资产属性;
- c) 支持资产属性的自定义;
- d) 支持手工录入资产记录或基于指定模板的批量资产导入。

6.1.1.4.2 威胁管理

威胁管理应满足以下要求:

- a) 具备预定义的安全威胁分类;
- b) 支持自定义安全威胁分类,如将已发生的安全事件对应的威胁设置为资产面

6.1.1.4.3 脆弱性管理

脆弱性管理应允许创建并维护资产脆弱性列表,支持脆弱性列表的合并及更新。

6.1.1.4.4 风险分析

风险分析应满足以下要求:

- a) 安全风险的计算周期和计算公式能够根据部署环境的实际需要,通过修改配置的方式进行相应调整;
- b) 安全风险的计算周期和计算公式能够根据部署环境的实际需要,通过修改配置的方式进行相应调整;

6.1.1.5 资源监控

6.1.1.5.1 可用性监测

可用性监测应满足以下要求:

操作系统、数据库、中间件、应用系统等重要性能指标,

- a) 支持通过监测网络设备、安全设备、主机探

用率、硬盘使用率、进程占用资源、交换分区、网络流

- b) 支持对关键指标(如:CPU 使用率、内存使

量等方面)设置阈值,触发阈值时产生告警

6.2 接口要求

6.2.1 第三方插件/代理接口协议要求

ice 等常规接口和自定义接口以及第三方的插
数据交换

安全管理中心应支持 SNMP Trap、Syslog、Web Serv
件或者代理的接口实现各组件之间、与第三方平台之间的

6.2.2 接口安全要求

接口安全要求应满足以下要求:

- a) 采用安全的接口协议,保证接口之间交互数据的完整性;
- b) 采用加密技术实现接口之间交互数据的保密性。

6.3 自身安全要求

6.3.1 身份鉴别

安全管理中心控制台的管理员身份鉴别应满足以下要求:

- a) 提供专用的登录控制模块对管理员进行身份标识和鉴别;
- b) 提供管理员用户身份标识唯一和鉴别信息复杂度检查功能,但不存在重复用户身份标识、身

6.3.2 访问控制

安全管理中心控制台的访问控制应满足以

- a) 提供访问控制功能,依据安全管理

6.3.3 安全审计

安全审计

6.3.4 软件容错

安全管理

输入的数据格式

6.3.5 资源控制

安全管理中心控制台的资源控制应满足以下要求:

- a) 对管理员登录地址范围进行限制;
- b) 当管理员在一段时间内未作任何动作,应能够自动结束会话;
- c) 能够对最大并发会话连接数进行限制;

提供对信息运行状态的监测,应能对服务器资源使用情况进行实时监测,并能

6.3.6 入侵防范

安全管理中心控制台的入侵防范应满足以下要求：

- a) 能够检测到对各服务器、网络设备和安全设备进行入侵的行为；
- b) 能够通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；
- c) 服务器操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持各组件的补丁及时得到更新；
- d) 应关闭不需要的各组件系统服务和高危端口。

6.3.7 数据安全

安全管理中心控制台的数据安全应满足以下要求：

- a) 能够检测到管理数据和鉴别信息在传输和存储过程中完整性受到破坏；
- b) 采用密码技术或其他保护措施实现管理数据和鉴别信息的数据传输和存储保密性。

7 第三级安全管理中心技术要求

7.1 功能要求

7.1.1 系统管理要求

7.1.1.1 用户身份管理

用户身份管理应满足以下要求：

- b) 能够采用两种或两种以上组合的鉴别技术对用户进行身份鉴别；
- c) 能够对被管理对象的系统管理员进行身份鉴别，并对身份标识及鉴别信息进行复杂度检查；
- d) 在物联网系统中，应通过被管理对象的系统管理员对感知设备、感知层网关等进行统一身份标识。

7.1.1.2 数据保护

7.1.1.2.1 数据保密性

数据保密性应满足以下要求：

- b) 应使用密码技术对安全管理中心与被管理对象之间传输或暂存的敏感信息进行保密保护。

7.1.1.2.2 数据完整性

要求：

对象鉴别信息、配置管理数据在传输过程中完整性受到破坏，并在检测到完
要的恢复措施；

对象鉴别信息、配置管理数据在存储过程中完整性受到破坏，并在检测到完
要的恢复措施。

数据完整性应满足以下

- a) 能够检测到被管理
完整性错误时采取必
- b) 能够检测到被管理
完整性错误时采取必

7.1.1.2.3 数据备份与恢复

数据备份与恢复应满足以下要求：

- a) 提供数据本地备份与恢复功能,完全数据备份至少每天一次,备份介质场外存放;
- b) 备份数据应至少包含安全管理中心采集的原始数据、主/客身份标识数据、主/客体安全标记数据、主/客体配置管理数据、安全管理中心自身审计数据等;
- c) 在云计算平台中,应提供查询云服务客户数据及备份存储位置的方式,云计算平台的运维应在中华人民共和国境内,禁止从境外对境内云计算平台的运维。

7.1.1.2.4 剩余信息保护

剩余信息保护应保证主体和客体的鉴别信息所有的高管密钥被解密或不会交给其他主体鉴别信息。

7.1.1.3 安全事件管理

7.1.1.3.1 安全事件采集

安全事件采集应满足以下要求：

- a) 支持安全事件监测采集功能,及时发现和采集发生的安全事件;
- b) 能够对安全事件进行归一化处理,将不同来源、不同格式、不同内容组成的原始事件转换成标准的事件格式;
- c) 安全事件的内容应包括日期、时间、主体标识、客体标识、类型、结果、IP 地址、端口等信息;
- d) 安全事件采集的范围应涵盖主机设备、网络设备、数据库、安全设备、各类中间件、机房环境控制系统等;
- e) 能够对采集的安全事件原始数据的集中存储。

注：安全事件的属性可参考附录 C。

7.1.1.3.2 安全事件告警

安全事件告警应满足以下要求：

- a) 具备告警功能,在发现异常时可根据预先设定的阈值产生告警;
- b) 在产生告警时,应能够触发预先设定的事件分析规则,执行预定义的告警响应动作,如:控制台对话框告警、控制台告警音、电子邮件告警、手机短信告警、创建工单、通过 Syslog 或 SNMP Trap 发布告警事件等;
- c) 具有对高频度发生的相同安全事件进行合并告警,避免出现告警风暴的能力。

7.1.1.3.3 安全事件响应

安全事件响应应满足以下要求：

- a) 能够提供工单管理的功能,支持基于告警响应动作创建工单的流转流程;
- b) 能够提供安全通告功能,可以创建或导入安全风险通告,通告中应包括通告内容、描述信息、CVE 编号、影响的操作系统等;
- c) 能够根据通告提示的安全风险影响的操作系统,提供受影响的被保护资产列表。

7.1.1.3.4 事件关联分析

事件关联分析应满足以下要求：

7.1.1.3.5 统计分析报表

统计分析报表应满足以下要求：

- a) 能够按照时间、事件类型等条件
- b) 能够提供统计分析和报表生成功

7.1.1.4 风险管理

7.1.1.4.1 资产管理

资产管理应满足以下要求：

- a) 实现对被管理对象资产的管理，
- b) 次立管理待自右右合次立力物

提供资产的添加、修改、删除、查询与统计功能；

资产IP地址、资产类型、资产责任人、资产名称、价值以及资产

资产IP地址、资产类型、资产责任人、资产名称、价值以及资产

资产IP地址、资产类型、资产责任人、资产名称、价值以及资产

资产IP地址、资产类型、资产责任人、资产名称、价值以及资产

7.1.1.4.2 资产业务价值评估

7.1.1

资产业务价值评估应支持自定义资产业务价值评估模型，能够依据资产类型、资产重要性、损坏后造成的影响、涉及的范围等参数形成资产业务价值等级。

造成

7.1.1.4.3 威胁管理

7.1.1

威胁管理应满足以下要求：

威胁管理应满足以下要求：

威胁管理应满足以下要求：

威胁管理应满足以下要求：

7.1.1.4.4 脆弱性管理

7.1.1.4.4 脆弱性管理

脆弱性管理应满足以下要求：

脆弱性管理应满足以下要求：

7.1.1.4.5 风险分析

风险分析应满足以下要求：

- a) 能够根据资产的业务价值、资产当前的脆弱性及安全风险；
- b) 安全风险的计算周期和计算公式能够根据部署环境进行调整；
- c) 安全管理系统能够以图形化的方式展现当前资产

资产面临的安全威胁，计算目标资产的安全

环境的实际需要通过修改配置的方式进行相应

的风险级别、当前风险的排名统计等。

7.1.1.5 资源监控

7.1.1.5.1 可用性监测

可用性监测应满足以下要求：

支持通过监测网络设备、安全设备、主机操作系统、数据库、中间件、应用系统等重要性能指标，实时了解其可用性状态；

a) 支持

支持对关键指标(如:CPU 使用率、内存使用率、磁盘使用率、进程占用资源、交换分区、网络流量等方面)设置阈值,触发阈值时产生告警;

b) 支持

在物联网系统平台,应通过系统管理员对感知设备状态(电力供应情况、是否在线、位置等)进

c) 在

在工作控制系统中应能够对工作控制系统设备的可用性和安全性进行实时监控,可以对监控指标设置告警阈值,触发告警并记录。

7.1.1.5.2 网络拓扑监测

网络拓扑监测应满足以下要求:

监测节点或链路;

a) 支持对网络拓扑图进行在线编辑,允许手工添加或删除

安全设备、服务器主机等)和链路的运行状

b) 能够展现当前网络环境中关键设备(包括网络设备、安
态,如网络流量、网络协议统计分析等指标;

并产生告警;

c) 在网络运行出现异常时,能够展现在当前网络拓扑图中

用户直接及间接用户(如设备商)的识别输入。

d) 能够发现并阻断非授权设备的连接及接入。

2 安全管理要求

7.1.

2.1 安全标记

7.1.

安全标记应满足以下要求:

安全标记应满足以下要求:

进程、终端等;设备策略

a) 能够对不同主体的安全标记统一管理,主体标记范围包括用户、设备、网络设备等;

全属性,且应具有防止篡改

b) 安全标记应具备唯一性,能够准确反映主机/终端在系统级系统中的安
和删除的能力;

行高低判断,安全范围应可

c) 标记属性应包括安全级别、安全范围等信息,安全级别应可排序进
进行是否包含判断;

解关系。

d) 能够实现对不同安全级别的系统中安全标记与安全属性的单一映射

7.1.2.2 授权管理

授权管理应满足以下要求:

网络访问权限管理、应用访问

a) 实现对每一个标记所能访问范围的统一管理;
b) 实现主体对客体访问权限的统一管理,包括主机访问权限管理、网
权限管理;

控制主体对客体的访问

c) 实现根据主体标记和客体标记安全级别的不同,制定访问控制策略

7.1.2.3 设备策略管理

7.1.2.3.1 安全配置策略

库系统、网络设备、安全设备的安全配置策略的统一查询。

设备管理应实现对主机操作系统、数据

7.1.2.3.2 入侵防御

入侵防御应满足以下要求:

御和主机入侵防御的事件采集、接收和指令下发;

a) 提供统一接口,实现对网络入侵防

- b) 提供安全域内统一的操作系统、服务组件补丁更新服务；
- c) 在云计算平台,云计算安全管理应具有对攻击行为回溯分析以及对网络安全事件进行预测和预警的能力;应具有对网络安全态势进行感知、预测和预判的能力。

7.1.2.3.3 恶意代码防范

恶意代码防范应满足以下要求:

- a) 对恶意代码防范产品统一升级进行监控和管理;
- b) 对恶意代码防范情况的数据采集与上报。

7.1.2.4 密码保障

密码保障应为被管理对象的密码技术、产品、服务的正确性、合规性、有效性提供保障。在物联网系

7.1.3 审计管理要求

7.1.3.1 审计策略集中管理

审计策略集中管理应能够查看主机操作系统、数据库系统、网络设备、安全设备、安全设备的审计策略配置情

7.1.3.2 审计数据集中管理

7.1.3.2.1 审计数据采集

审计数据采集应满足以下要求:

- a) 能够实现审计数据的归一化处理,内容应涵盖日期、时间、主体标识、地址、端口等信息;
- b) 支持设定查询条件进行审计数据查询;
- c) 严格限制审计数据的访问控制权限,限制管理用户对审计数据的访问,实现管理用户和审计用
- d) 支持对数据集中管理
- e) 支持对数据集中管理

7.1.3.2.2 审计数据采集对象

审计数据采集对象应满足以下要求:

- a) 支持对网络设备(如交换机、路由器、流量管理、负载均衡等网络设备)的审计数据采集;
- b) 支持对主机设备(如服务器操作系统等)和终端设备(如笔记本电脑、台式计算机、移动终端等)的审计数据采集;
- c) 支持对数据库的审计数据采集;
- d) 支持对安全设备(如防火墙、入侵监测系统、抗拒绝服务攻击设备、防病毒系统、应用安全审计系统、访问控制系统等)与信息安全系统安全相关的各种系统和设备

计,应通过运维审计系统对管理员的运维行为进行安全审计;应通过租户隔离机制,确保审计数据隔离的有效性;

d) 在工业控制系统中,应对工业控制现场控制设备、网络安全设备、网络设备、服务器、工作站等

7.1.3.2.3 审计数据采集方式

审计数据采集方式应满足以下要求:

- a) 支持通过如 Syslog、SNMP 等协议采集各种系统
- b) 通过统一接口,接收被管理对象的安全审计数据

7.1.3.2.4 审计数据关联分析

7.2 接口要求

7.2.1 第三方插件/代理接口协议要求

接口协议要求应满足以下要求:

- a) 安全管理中心应实现对 IPv4 及 IPv6 双协议环境的支持(包括 IPv4 环境、IPv6 环境及 IPv4/IPv6 混合环境);

7.2.2 接口安全要求

接口安全要求应满足以下要求:

- a) 采用安全的接口协议,保证接口之间交互数据的完整性;
- b) 采用加密技术实现接口之间交互数据的保密性。

7.3 自身安全要求

7.3.1 身份鉴别

安全管理中心控制台的管理人员身份鉴别应满足以下要求:

- a) 安全管理中心控制台应支持至少一种强身份鉴别技术,如口令鉴别、数字证书鉴别、生物特征鉴别、动态口令鉴别、多因素鉴别等;

安全管理中心控制台应支持至少一种强身份鉴别技术,如口令鉴别、数字证书鉴别、生物特征鉴别、动态口令鉴别、多因素鉴别等;

结束会话、限制非法登录次数和自动退出等措施。

- c) 提供登录失败处理功能,可采取

7.3.2 访问控制

安全管理中心控制台的访问控制应满足以下要求:

全策略控制管理员对各功能的访问;话所有管理员、功能及它们之间的操作;

- a) 提供自主访问控制功能,依据安
- b) 自主访问控制的覆盖范围应包

最小权限,并在它们之

- c) 实现特权用户的权限分离,应授予不同用户为完成各自承担任务所需
- 间形成相互制约的关系。

7.3.3 安全审计

安全管理中心控制台的安全审计应满足以下要求：

- a) 提供覆盖到每个管理员的安全审计功能，记录
- b) 保证无法单独中断审计进程，无法删除、修改
- c) 审计记录的内容至少应包括事件的日期、时间
- d) 提供对审计记录数据进行统计、查询、分析及
- e) 根据统一安全策略，提供集中审计接口。

7.3.4 剩余信息保护

安全管理中心控制台的剩余信息保护应保证管理员的

其他管理要素即点即消，不留任何痕迹，无论这些信息是否被

7.3.5 软件容错

安全管理中

a) 提供数

续按定

b) 提供自动

7.3.6 资源控制

安全管理中心

a) 对管理员登录地址范围进行限制；

b) 当管理员在一段时间内未作任何动作，应能

c) 能够对最大并发会话连接数进行限制；

d) 能够动态管理管理终端的登录策略，除登录

e) 提供对自身运行状态实时监控，应能够发现

7.3.7 入侵防范

安全管理中心控制台的入侵防范应满足以下

a) 能够检测到对各服务器、网络设备和安全

报警；

b) 能够通过设定终端接入方式或网络地址范围对访问网络进行管理

c) 服务器操作系统漏洞扫描和入侵检测，使安全策略能及时发现

并采取相应安全措施；

d) 应关闭不需要的各组件系统服

7.3.8 数据安全

安全管理中心控制台的数据安全

a) 能够检测到管理数据和鉴别

误时采取必要的恢复措施；

8 第四级安全管理中心技术要求

8.1 功能要求

8.1.1 系统管理要求

8.1.1.1 用户身份管理

用户身份管理应满足以下要求：

- 能够对被管理对象环境中的主体进行标识；
- 能够采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，并且身份鉴别信息至少有一种是不可伪造的并采用密码技术来实现；
- 能够对被管理对象的系统管理员进行身份鉴别，并对身份标识及鉴别信息进行复杂度检查；
- 在物联网系统中，应通过被管理对象的系统管理员对感知设备、感知层网关等进行统一身份标识管理。

8.1.1.2 数据保护

8.1.1.2.1 数据保密性

数据保密性应满足以下要求：

- 在安全管理中心与被管理对象之间建立连接之前，应利用密码技术进行会话初始化验证；
- 使用密码技术对安全管理中心与被管理对象之间通信过程中的整个报文或会话过程进行机密性保护；
- 采用加密或其他保护措施实现被管理对象的鉴别信息、配置管理数据的存储保密性；
- 应使用经国家密码管理主管部门批准的硬件密码设备进行密码运算和密钥管理；
- 对重要通信提供专用通信协议或安全通信协议服务，避免来自基于通用协议的攻击破坏数据保密性。

8.1.1.2.2 数据完整性

数据完整性应满足以下要求：

- 能够检测到被管理对象的鉴别信息、配置管理数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；
- 能够检测到被管理对象的鉴别信息、配置管理数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；
- 对重要通信提供专用通信协议或安全通信协议服务，避免来自基于通用通信协议的攻击破坏数据完整性。

8.1.1.2.3 数据备份与恢复

数据备份与恢复应满足以下要求：

- 提供数据本地备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放；

b) 备份数据至少包含安全管理中心采集的原始数据、主/客身份标识数据、主/客体安全标识数

据、主/客体配置管理数据、安全管理中心自身运

行数据等；

c) 提供异地实时备份功能，利用通信网络将数据实

时备份至灾难备份中心；

d) 在云计算平台型，应提供查询云服务客户数据及

备份存储位置的方式；云计算平台的运维应在

中华人民共和国境内,禁止从境外对境内云计算平台的运维。

8.1.1.2.4 可信路径

可信路径应满足以下要求:

- a) 在对主体进行身份鉴别时,应能够建立一条安全的信息传输路径;
- b) 在主体对客体进行访问时,应保证在被访问的客体与主体之间应能够建立一条安全的信息传输路径。

8.1.1.2.5 剩余信息保护

剩余信息保护应保证主体和客体的鉴别信息所在的存储空间被释放或再分配给其他主体前得到完全清除,无论这些信息是存放在硬盘上还是在内存中。

8.1.1.3 安全事件管理

8.1.1.3.1 安全事件采集

安全事件采集应满足以下要求:

- a) 支持安全事件监测采集功能,及时发现和采集发生的安全事件;
- b) 能够提供与第三方系统的数据采集接口,发送或接收安全事件;
- c) 能够对安全事件进行归一化处理,将不同来源、不同格式、不同内容组成的原始事件转换成标准的事件格式;
- d) 安全事件的内容应包括日期、时间、主体标识、客体标识、类型、结果、IP地址、端口等信息;
- e) 安全事件采集的范围应涵盖主机设备、网络设备、数据库、安全设备、各类中间件、机房环境控制系统等;
- f) 能够对采集的安全事件原始数据的集中存储。

注:安全事件的属性可参考附录C。

8.1.1.3.2 安全事件告警

安全事件告警应满足以下要求:

- a) 具备告警功能,在发现异常时可根据预先设定的阈值产生告警;
- b) 在产生告警时,应能够触发预先设定的事件分析规则,执行预定义的告警响应动作,如:控制台对话框告警、控制台告警音、电子邮件告警、手机短信告警、创建工单、通过 Syslog 或 SNMP 向第三方系统转发告警信息等;
- c) 具备对高频度发生的相同安全事件进行合并告警,避免出现告警风暴的能力。

8.1.1.3.3 安全事件响应

安全事件响应应满足以下要求:

- a) 能够提供工单管理的功能,支持基于告警响应动作创建工单的流转流程;
- b) 能够提供安全通告功能,可以创建或导入安全风险通告,通告中应包括通告内容、描述信息、受影响的数据和资产列表、安全预警、综合风险、资产信息、安全通告等数据;
- c) 能够根据通告提示的安全风险影响的相关系统,提供
- d) 支持向第三方系统发送和接收工单信息、安全告警

8.1.1.3.4 事件关联分析

事件关联分析应满足以下要求：

- a) 支持将来自不同事件源的事件在一个分析规则中进行分析，从而能从海量事件中过滤出有逻辑关系的事件序列，并能统计相关的告警。

支持对事件序列，按逻辑是相关的告警。

支持对事件序列，按逻辑是相关的告警。

支持对事件序列，按逻辑是相关的告警。

- b) 提供多事件源事件关联、时序关联、统计关联以及对长周期事件的关联分析功能，并能够提供告警。

提供对告警关联规则编辑功能。

8.1.1.3.5 统计分析报表

统计分析报表应满足以下要求：

- a) 能够按照时间、事件类型等条件对安全事件进行查询；

提供统计分析报表生成功能。

提供统计分析报表生成功能。

风险管理

8.1.1.4 风险管理

资产管理

8.1.1.4.1 资产管理

管理应满足以下要求：

资产管理

现对被管理对象资产的管理，以安全域等方式组织资产，提供资产的添加、修改、删除、查询

a) 实时

统计功能；

与

资产管理信息应包含资产名称、资产 IP 地址、资产类型、资产责任人、资产业务价值以及资产

b) 资产

IP 地址、资产名称、资产 IP 地址、资产类型、资产责任人、资产业务价值以及资产

- c) 支持资产属性的自定义扩展。

- d) 支持手动录入资产记录或基于模板的批量资产导入。

- e) 支持对资产的自动发现，并能够将其自动添加到资产库中。

8.1.1.4.2 资产业务价值评估

支持对资产的业务价值进行评估，并能根据资产的业务价值等级，对资产进行分级管理。

8.1.1.4.3 威胁管理

威胁管理应满足以下要求：

- a) 具备预定义的安全威胁分类；

8.1.1.4.4 脆弱性管理

脆弱性管理应满足以下要求：

- a) 允许创建并维护资产脆弱性列表，支持脆弱性列表的合并及更新；
- b) 支持导入特定代理程序或扫描器获取的相关设备或系统的脆弱性信息；
- c) 能够根据脆弱性信息，自动生成所涉及的信息资产清单。

8.1.1.4.5 风险分析

风险分析应满足以下要求：

- a) 能够根据资产的业务价值、资产当前的脆弱性及资产面临的安全威胁，计算目标资产的安全风险和资产所在整个安全域的安全风险；

8.1.1.5 资源监控

8.1.1.5.1 可用性监测

可用性监测应满足以下要求：

- a) 支持通过监测网络设备、安全设备、主机操作系统、数据库、中间件、应用系统等重要性能指标，实时了解其可用状态；

- b) 支持对关键指标(如，CPU 使用率、内存使用率、磁盘使用率、进程占用资源、交换分区、量等方面)设置阈值，触发阈值时产生告警，执行预定义的响应动作；

- c) 在物联网系统平台，应通过系统管理员对感知设备状态(电力供应情况、是否在线、位置)行统一监测和处理；

- d) 在工业控制系统中，应能够对工业控制系统设备的可用性和安全性进行实时监控，可以指标设置告警阈值，触发告警并记录。

8.1.1.5.2 网络拓扑监测

网络拓扑监测应满足以下要求：

- a) 支持对网络拓扑图进行在线编辑，允许手工添加或删除监测节点或链路；
- b) 能够展现当前网络环境中关键设备(包括网络设备、安全设备、服务器主机等)和链路的状态，如网络流量、网络协议统计分析等指标；
- c) 在网络运行出现异常时，能够展现在当前网络拓扑图中并产生告警；
- d) 能够发现并阻断非授权设备的外联及接入；
- e) 支持在指定网络范围内进行拓扑发现并自动生成网络拓扑图。

8.1.2 安全管理要求

8.1.2.1 安全标记

安全标记应满足以下要求：

- a) 能够对主/客体的安全标记统一管理，主体标记范围包括用户、代理进程、终端等，客体

- b) 安全标记应具有唯一性，能够新增、删除和删除的能力；

- c) 标记属性应包括安全级别、安全范围等信息，并能进行是否保密判断；

- d) 能够处理对不同安全级别的系统的安全标记

8.1.2.2 授权管理

8.1.2.2.1 授权策略管理

授权管理应满足以下要求：

- a) 实现对每一个标记所能访问范围的统一管理；
- b) 实现主体对客体访问权限的统一管理,包括主机访问权限管理、网络访问权限管理；
- c) 实现根据主体标记和客体标记安全级别的不同,制定访问控制策略,控制主

8.1.2.3 设备策略管理

8.1.2.3.1 安全配置策略

设备管理应满足以下要求：

- a) 实现对主机操作系统、数据库系统、网络设备、安全设备的安全配置策略
- b) 实现对主机操作系统、数据库系统、网络设备、安全设备等安全配置策略

8.1.2.3.2 入侵防御

入侵防御应满足以下要求：

- a) 实现对工业控制系统的入侵防御
- b) 实现对工业控制系统的入侵防御
- c) 实现对工业控制系统的入侵防御
- d) 在云计算平台、云计算安全管
- e) 在工业控制系统中,安全管理

8.1.2.3.3 恶意代码防范

恶意代码防范应满足以下要求：

- a) 对恶意代码防范
- b) 对恶意代码防范

8.1.2.4 密码保障

密码保障应为被管理对象的密码保障,应通过安全管理员对系统中所使用的密钥进行统一管理,包括密钥的生成、分发、更新、存储、备份、销毁等,并采取必要措施保证密

8.1.3 审计管理要求

8.1.3.1 审计策略集中管理

审计策略集中管理应满足以下要求：

- a) 能够查看主机操作系统、数据库系统、网络设备、安全设备的审计策略配置情况,包括策略是否开启、参数设施是否符合安全策略等；
- b) 能够实现对主机操作系统、数据库系统、网络设备、安全设备的审计策略的统一配置管理。

8.1.3.2 审计数据集中管理

8.1.3.2.1 审计数据采集

审计数据采集应满足以下要求：

- a) 能够实现审计数据的归一化处理，内容应涵盖日期、时间、主体标识、客体标识、类型、结果、IP地址、端口等信息；

b) 支持通过本设备外进行审计数据查询；

c) 应严格控制审计数据的访问权限，限制非授权用户对审计数据的访问，实现用户的权限分离，避免非授权的删除、修改或覆盖；

d) 支持对各种审计数据按规则进行过滤处理；

e) 支持对数据采集信息按照特定规则进行合并；

2 审计数据采集对象

8.1.3.2.2

审计数据采集对象应满足以下要求：

审

支持对网络设备(如交换机、路由器、流量管理、负载均衡等网络基础设备)的审计数据采集；

a)

支持对主机设备(如服务器操作系统等应用支撑平台和桌面电脑、笔记本电脑、手持终端等终端用户访问信息系统所使用的设备)的审计数据采集；

b)

支持对数据库的审计数据采集；

c)

支持对安全设备(如防火墙、入侵监测系统、抗拒绝服务攻击设备、防病毒系统、应用安全审计系统、访问控制系统等与信息系统安全防护相关的各种系统和设备)的审计数据采集；

d)

支持对各类中间件的审计数据采集；

e)

支持对机房环境控制系统(如空调、温度、湿度控制、消防设备、门禁系统等)的审计数据采集；

f)

支持对其他应用系统或中间平台的审计数据采集；

g) 支持对工业控制系统(如工业控制现场控制设备、网络安全设备、网络设备、服务器、操作系统、数据库、应用系统等)的审计数据采集；

h) 在工业控制系统中，应对工业控制现场控制设备、网络安全设备、网络设备、服务器、操作系统、数据库、应用系统等设备的网络安全监控和报警、网络安全隐患信息进行集中管理。

8.1.3.2.3 审计数据采集方式

审计数据采集方式应满足以下要求：

- a) 支持通过如 Syslog、SNMP 等协议采集各种系统或设备上的审计数据；

b) 支持通过软件代理的方式采集特定系统或设备上的审计数据。

采集组件要求

8.1.3.2.4 数据

采集组件应支持本地缓存和断点续传，在网络通信发生故障时，能够在数据采集组件对数据进

数据采集组

行本地缓存，当网络连通恢复以后，信息采集组件重新恢复向安全管理中心上报断网期间采集的数据。

行本地缓存，当

8.1.3.2.5 审计数据关联分析

下要求：

审计数据关联分析应满足以

- a) 应支持将来自不同采集对象的审计数据在一个分析规则中进行分析；
- b) 应提供审计关联规则自定义功能；
- c) 在工业控制系统中,系统通过各设备安全日志信息的关联分析提取出少量的

8.2 接口要求

8.2.1 第三方插件/代理接口协议要求

接口协议要求应满足以下要求:

- a) 安全管理中心应实现对 IPv4 及 IPv6 双协议环境的支持(包括 IPv4 环境、IPv6 环境及 IPv4/IPv6 混合环境);

8.2.2 接口安全要求

接口安全要求应满足以下要求:

- a) 采用安全的接口协议,保证接口之间交互数据的完整性;
- b) 采用加密技术实现接口之间交互数据的保密性;

8.3 自身安全要求

8.3.1 身份鉴别

安全管理中心控制台的管理员身份鉴别应满足以下要求:

- a) 提供专用的登录控制模块对管理员进行身份标识和鉴别,以上组合的鉴别技术实现用户身份鉴别,其中至少有一种实现;
- b) 提供管理员用户身份标识唯一和鉴别信息复杂度检查;

8.3.2 访问控制

安全管理中心控制台的访问控制应满足

8.3.3 可信路径

安全管理中心控制台可信路径应满足以下要求:

- a) 在安全管理中心控制台对管理员进行身份鉴别时,应能够建立一条安全的信息传输路径;
- b) 在管理员通过安全管理中心控制台对资源进行访问时,安全管理中心控制台应保证在被访问的资源与管理员之间能够建立一条安全的信息传输路径。

8.3.4 安全审计

安全管理中心控制台的安全审计应满足以下要求:

- a) 应能够对安全事件进行记录,记录内容应包含事件发生日期、时间、发起者信息、类型、描述和结果等;
- b) 应能够对记录数据进行统计、查询、分析及生成审计报告的功能;
- c) 应提供集中审计接口。

8.3.5 剩余信息保护

安全管理中心控制台的安全审计记录应满足以下要求:

8.3.6 软件容错

软件容错应满足以下要求:

功能,保证通过人机接口输入或通过接口输入的数据格式或长度符合系

当故障发生时自动保护当前所有状态;

当故障发生时能够恢复工作状态。

安全管理中心控制台的软

a) 提供数据有效性检验

统设定要求;

b) 提供自动保护功能;

c) 提供自动恢复功能;

8.3.7 资源控制

资源控制应满足以下要求:

范围进行限制;

c) 能够对最大并发会话连接数进行限制;

d) 能够对单个管理员账户的多重并发会话进行限制;

e) 提供对自身运行状态的监测,应能够对服务水平降低到预先规定的最小值进行检测和报警。

安全管理中心控制台的资

a) 对管理员登录地址范

入侵防范

8.3.8

安全管理中心控制台的入侵防范应满足以下要求:

a) 能够检测到对各服务器、网络设备和安全设备进行入侵的行为,并在发生严重入侵事件时提供报警;

b) 能够通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制;

c) 应能够对入侵行为进行溯源,并能对入侵行为进行溯源,并能对入侵行为进行溯源,并能对入侵行为进行溯源。

8.3.9 数据安全

数据安全应满足以下要求:

鉴别信息在传输和存储过程中完整性受到破坏,并在检测到完整性错

安全管理中心控制台的数据

a) 能够检测到管理数据和

必要时采取必要的恢复措施。

或安全通信服务，避免来自基于语音通信劫听的攻击威胁。

④ 对重要通信提供专用通信或数据完整性和保密性。

自批准的硬件密码设备进行密码运算和密钥管理。

⑤ 应使用经国家密码管理主管部门

认证的加密设备。

中心技术要求另行制定。

第五级安全管理中心

管理中心技术要求

10 跨定级系统安全管理

管理中心应满足以下要求：

跨定级系统安全管理

一的安全互联策略，通过与各定级系统安全管理中心相连，保证跨定级系统中用户

a) 能够实施统一

本标记、访问控制策略等安全要素的一致性；

身份、主/客体

级系统之间的数据传输交换进行保密性与完整性保护；

b) 能够对跨定级

安全互联部件，对各定级系统中与安全互联相关的系统资源和运行进行配置和管理。

c) 能够通过安全

安全互联部件，对各定级系统中与安全互联相关的系统资源进行标识、授权、审计。

d) 能够对跨定级

主/客体在定级系统中的安全属性，对主体进行授权，配置统一的安全策略。

能够准确度

安全策略实施、审计、日志记录、报警、应急处置。

③ 应按照国家密码管理主管部门

认证的加密设备。

在国境范围内及跨境网络中提供安全通信服务。

对通信内容采取必要的保护措施，防止泄密、篡改、丢失、损毁、伪造、假冒、欺骗、窃取、破坏等安全风险。

信息安全管理和技术要求。

附 录 A

(规范性附录)

安全管理中心与网络安全等级保护对象等级对应关系

安全管理中心与网络安全等级保护对象等级对应关系见表 A.1。

表 A.1 安全管理中心与网络安全等级保护对象等级对应表

| 安全管理中心级别 | 网络安全等级保护对象等级 |
|----------|--------------|
| 第二级 | 第二级 |
| 第三级 | 第三级 |
| 第四级 | 第四级 |
| 第五级 | 第五级 |

附录 B
(规范性附录)

安全管理中心技术要求分级表

安全管理中心技术要求分级表

安全管理中心技术要求分级表见表 B.1。

安全管理中心技术要求分级表

表 B.1 安全管理中心技术要求

| | 第二级 | 第三级 | 第四级 |
|----------|-----------|------------|------------|
| | 6.1.1.1 | 7.1.1.1+ | 8.1.1.1+ |
| 机密性 | 6.1.1.2.1 | 7.1.1.2.1+ | 8.1.1.2.1+ |
| 完整性 | 6.1.1.2.2 | 7.1.1.2.2+ | 8.1.1.2.2+ |
| 备份与恢复 | 6.1.1.2.3 | 7.1.1.2.3+ | 8.1.1.2.3+ |
| 路径 | — | — | 8.1.1.2.4 |
| 信息保护 | — | 7.1.1.2.4 | 8.1.1.2.5 |
| 事件采集 | 6.1.1.3.1 | 7.1.1.3.1 | 8.1.1.3.1+ |
| 事件告警 | 6.1.1.3.2 | 7.1.1.3.2+ | 8.1.1.3.2+ |
| 事件关联分析 | — | — | 8.1.1.3.4 |
| 统计分析报表 | — | — | 8.1.1.3.5 |
| 资产管理 | — | 7.1.1.4.1 | 8.1.1.4.1+ |
| 资产业务价值评估 | — | 7.1.1.4.2 | 8.1.1.4.2+ |
| 威胁管理 | — | 7.1.1.4.3 | 8.1.1.4.3+ |
| | | 脆弱性管理 | 7.1.1.4.4 |
| | | 风险分析 | 7.1.1.4.5 |
| 资源监控 | | 可用性监测 | 7.1.1.5.1+ |
| | | 网络拓扑监测 | 7.1.1.5.2+ |
| 安全标记 | — | — | 7.1.2.1 |
| 授权管理 | — | — | 7.1.2.2 |
| 安全管理 | | 安全配置策略 | 7.1.2.3.1 |
| 要求 | | 入侵防御 | 7.1.2.3.2 |
| | | 恶意代码防范 | 7.1.2.3.3 |

| 技术要求 | |
|--------|----------|
| 用户身份管理 | |
| 数据保护 | 数据保护 |
| | 数据完整性 |
| | 数据备份与恢复 |
| | 可信路径 |
| | 剩余信息保护 |
| | 安全事件采集 |
| | 安全事件告警 |
| | 安全事件关联分析 |
| | 统计分析报表 |
| | 资产管理 |
| | 资产业务价值评估 |
| | 威胁管理 |
| | 脆弱性管理 |
| | 风险分析 |
| | 可用性监测 |
| | 网络拓扑监测 |
| | 安全标记 |
| | 授权管理 |
| | 安全配置策略 |
| | 入侵防御 |
| | 恶意代码防范 |
| | 密码策略 |
| | 审计策略集中管理 |

表 B.1 (续)

| 技术要求 | | 第二级 | 第三级 | 第四级 |
|--------|----------------|-------|--------|--------|
| 接口要求 | 第三方插件/代理接口协议要求 | 6.2.1 | 7.2.1+ | 8.2.1+ |
| | 接口安全要求 | 6.2.2 | 7.2.2 | 8.2.2+ |
| 自身安全要求 | 身份鉴别 | 6.3.1 | 7.3.1+ | 8.3.1+ |
| | 访问控制 | 6.3.2 | 7.3.2+ | 8.3.2 |
| | 可信路径 | — | — | 8.3.3 |
| | 剩余信息保护 | — | — | 8.3.4 |
| | 软件容错 | — | — | 8.3.5+ |
| | 资源控制 | — | — | 8.3.6+ |
| | 入侵防范 | — | — | 8.3.7+ |
| 数据安全 | — | — | 8.3.8+ | |

注：“—”表示不具有该项要求，“+”表示具有更高的要求。

附录 C
(资料性附录)
归一化安全事件属性

归一化安全事件属性见表 C.1。

表 C.1 归一化安全事件属性

| 序号 | 属性 | 描述 |
|----|--------------|------------|
| 1 | 采集器 IP | 事件的采集器地址 |
| 2 | 采集器名称 | 事件的采集器名称 |
| 3 | 设备 IP | 产生该事件的设备地址 |
| 4 | 该设备的设备类型 | 设备类型 |
| 5 | 设备名称 | 设备名称 |
| 6 | 事件采集时间 | 接收事件时间 |
| 7 | 归并事件的次数 | 归并数量 |
| 8 | 事件在安全设备的发生时间 | 事件发生时间 |
| 9 | 事件类别 | 事件类型 |
| 10 | 事件名 | 事件名称 |
| 11 | 事件原始信息 | 事件内容 |
| 12 | 事件相关的协议名 | 应用协议 |
| 13 | 目的 IP | 事件目的地址 |
| 14 | 目的端口 | 事件的目的端口 |
| 15 | 目的主机名 | 事件目的主机名称 |
| 16 | 源 IP | 事件源地址 |
| 17 | 源端口 | 事件的源端口 |
| 18 | 源主机名 | 事件源主机名称 |
| 19 | 事件属性 | 事件属性 |

中华人民共和国
国家标准
信息安全技术 网络安全等级保护
安全管理中心技术要求
GB/T 36958—2018

*

中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)

网址: www.spc.org.cn

服务热线: 400-168-0010

2019年1月第一版

*

书号: 155066·1-61703

版权专有 侵权必究



GB/T 36958—2018