ICS 35. 040
L 80
备案号：

天 津 市 商 用 密 码 团 体 标 准

T/TCCIA 0007-2024

信息安全技术 网络安全运维审计产品技术规范

Information security technology -Technical specification for network security operation and maintenance audit products

天津市商用密码行业协会 发布

目　　次

前　言

本文件根据 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。本文件的发布机构不承担识别专利的责任。

本文件由天津市商用密码行业协会归口。

本文件起草单位：天津光电安辰信息技术股份有限公司、天津光电通信技术有限公司、天津大学、天津光电通电子科技有限公司、天津云安科技发展有限公司、宝牧科技（天津）有限公司、河北承高智慧交通有限公司、聚能信安（天津）科技有限公司、轩辕（天津）智能科技有限公司。

本文件主要起草人：胡双喜、钟明旸、许光全、申烨、焦庆玲、曹晓冬、贾玉凤、姚嘉、苏明、方浩、宋津津、孟祥文、肖海涛、刁文钦、吴超、徐文大、李长宇、张璐琳、张文涛、徐洋。

引　　言

为了配合《中华人民共和国网络安全法》、《中华人民共和国网络密码法》和《中华人民共和国数据安全法》的实施，立足网络安全运维审计工作实际，着力解决运维审计安全领域突出问题，保障运维审计通路和日志数据安全，促进网络运维审计安全技术发展，需要从技术上针对网络安全运维审计产品提出相关要求。本标准从自身安全、安全运维审计功能、安全保障、测评评价四个方面规定了网络安全运维审计产品基本级和增强级的安全技术要求，为网络安全运维审计产品设计、开发和测试提供指导。

信息安全技术 网络安全运维审计产品技术规范

1 范围

本文件规定了网络安全运维审计产品的自身安全功能要求、安全运维审计功能要求和安全保障要求。

本文件适用于网络安全运维审计产品设计、开发和测试，本文件所规定的网络安全运维审计产品主要部署于信息系统的机房，用于对服务器、网络设备、安全设备、数据库、应用系统等信息系统重要资产进行运维管理。

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 25069-2010 信息安全技术术语

GB/T 18336.3-2015 信息技术 安全技术 信息技术安全评估准则第3部分：安全保障组件

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 25070-2019 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

GA/T 1394-2017 信息安全技术 运维安全管理产品安全技术要求

3 术语和定义

3.1 账户管理 Account manage

不同身份人员登录系统的身份验证的管理。

3.2 认证管理 Authentication manage

对访问不同资产需要的认证方式管理。

3.3 授权管理 Authorization manage

按用户身份及其所归属的某项定义组来授权用户对某些信息项的访问管理。

3.4 审计管理 Audit manage

对运维用户行为的监督和审核管理。

3.5 运维用户 operation and maintenance user

对服务器、网络设备和数据库等信息系统的重要资产进行运行维护的人员。

3.6 网络安全运维审计产品 Network security operation and maintenance aduit product

对信息系统重要资产的维护过程实现单点登录、集中授权、集中管理和审计的产品。

3.7 运维对象 operation and maintenance object

受运维安全管理产品保护的资产。

4 缩略语

下列缩略语适用于本文件。
SSH：安全外壳协议（Secure Shell）
RDP：远程桌面协议（RemoteDesktopProtocol）
VNC：虚拟网络控制台（Virtual Network Console）
FTP：文件传输协议（File Transfer Protocol）
SFTP：SSH文件传输协议（SSH File Transfer Protocol）
Telnet：远程终端协议
HTTPS：安全超文本传输协议(Hyper Text Transfer Protocol over Secure Socket Layer)
WEB：万维网（World Wide WEB）
SYSLOG：系统日志（System Log）

5 概述

网络安全运维审计产品为运维用户提供统一的身份认证接口、多种远程运维管理方式，对资产及其账号 等进行集中管理和授权，监控和审计运维操作过程，并对违规操作行为进行报警、阻断。该类产品保护 的对象是服务器、网络设备、安全产品、数据库、应用系统等信息系统重要资产。

网络运维安全审计产品通常以旁路方式部署。网络运维安全审计产品的典型运行环境见图1。

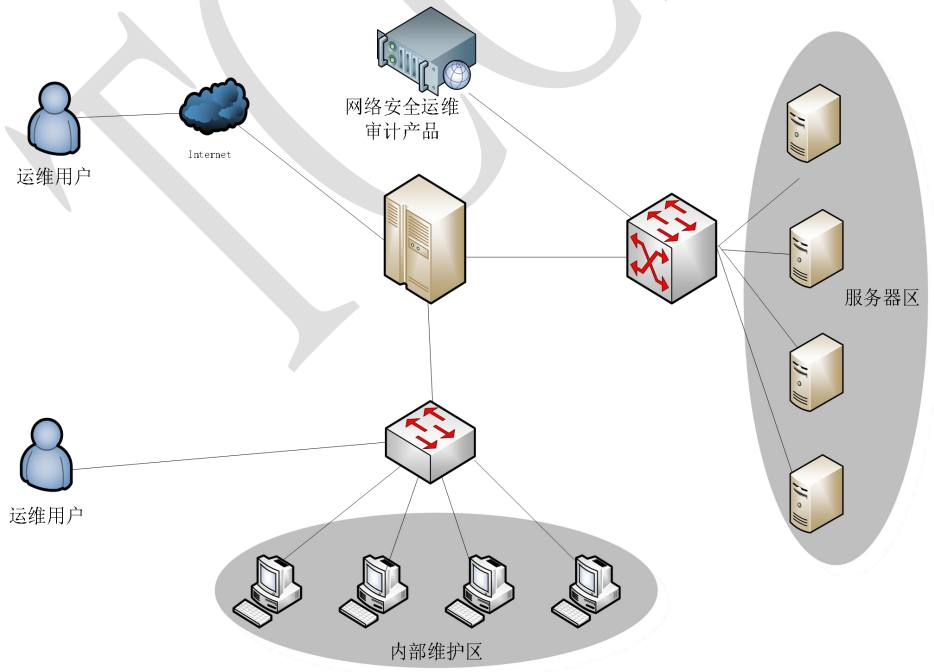

图1 网络运维安全审计产品的典型运行环境

在功能点上包括但不限于：身份鉴别、访问控制、运维通道安全、安全审计、安全管理、分析预警、违规操作阻断、审计数据留存、集中监控、运维策略配置、高可用性、数据完整性和机密性保护以及开发测试安全等一系列网络安全运维审计技术措施，且涉及网络等级保护以及密码应用安全性评估等重点要求内容。此外，运维安全管理产品本身及其内部的重要数据也是受保护的对象。

6 安全技术要求

6.1 基本级安全技术要求

6.1.1 自身安全要求

6.1.1.1 用户身份鉴别

产品的身份标识与鉴别安全要求包括但不限于：

a)对用户身份进行标识和鉴别，身份标识具有唯一性；

b)应采用密码技术对用户身份鉴别信息进行安全保护，保障用户鉴别信息在传输过程中的机密性；

c)具有登录失败处理功能，如限制连续的非法登录尝试次数等相关措施；

d)具有登录超时处理功能，当登录连接超时自动退出；

e)鉴别机制应具有抗重放的能力，授权管理员及其他用户不能复制使用上一次通过的鉴别信息再次鉴别成功；

f)在采用基于口令的身份鉴别时，要求对用户设置的口令进行复杂度检查，确保用户口令满足一定的复杂度要求；

g)当产品中存在默认口令时，提示用户对默认口令进行修改，以减少用户身份被冒用的风险。

6.1.1.2 用户访问控制

用户访问控制安全要求包括但不限于：

a）应支持用户权限管理功能，包括但不限于对用户功能权限和数据权限的创建/查看/修改/删除等 功能；

b）应定期对多余或已过期的用户自动进行清除；

c）应确保默认账户的安全，禁止默认账户出现重命名或被删除等异常情况；

d）新建用户时，应提示修改默认口令；

e）管理用户应根据角色类型进行明确划分，且不同类型的角色权限要求分离，用户权限要求与预置访问控制策略是否一致，并满足最小权限原则。

f）应能根据运维用户、源地址、运维对象及其账户、管理方式、操作命令、操作时间等对运维用户实施访问控制。

6.1.1.3 系统安全审计

产品的管理审计安全要求包括但不限于：

a)对用户账户的登录和注销、系统启动、重要配置变更、增加/删除/修改管理员、保存/删除审计日志等操作行为进行日志记录；

b)对产品及其组件的异常状态进行告警，并记录日志；

c)日志记录中包括如下内容：事件发生的日期和时间，事件的类型，事件主体，事件操作结果；

d)日志存储周期设定不小于六个月；

6.1.1.4 安全管理

6.1.1.4.1 安全管理能力

产品的管理能力安全要求包括但不限于：

a)向授权管理员提供设置和修改安全管理相关的数据参数的功能；

b)向授权管理员提供设置、查询和修改各种安全策略的功能；

c)向授权管理员提供管理审计日志的功能；

d)支持更新自身系统的能力，包括对软件系统的升级以及各种特征库的升级；

e)支持具有至少两种不同权限的管理员角色，例如系统管理员、安全管理员和审计管理员等；

f)支持与外部时间服务器进行时间同步。

g)应采用密码技术，在运维终端和网络安全运维审计产品之间，建立安全的运维管理通道；

h)应采用密码技术，在网络安全运维审计产品和应用服务器、数据库服务器等核心资产之间，建立安全的运维管理通道。

6.1.1.4.2 安全管理方式

产品的管理方式安全要求包括：

a)支持本地管理，如console口；

b)连接不同安全域的内外网分开管理；

c)支持通过网络接口进行远程管理，并能限定进行远程管理的IP、MAC地址；

d)远程管理过程中，管理端与产品之间的所有通信数据应采用非明文传输，应采用密码技术，实现对相关通信数据在传输过程中的机密性和完整性保护。

6.1.1.5 用户数据完整性

应采用校验技术保证用户重要数据在传输过程中的完整性。

6.1.1.6 用户数据保密性保护

本项要求包括：

a）应采用采用密码技术保证用户重要数据在传输过程中的保密性；

b）应禁止未授权访问和非法使用用户数据。

6.1.2 安全运维审计功能要求

6.1.2.1 单点登录

产品应提供统一的身份鉴别功能，实现运维用户的单点登录，运维用户仅需经过产品的身份鉴别 后，即可访问授权范围内的资产。

6.1.2.2 授权控制

本项要求包括：

a）应支持对资产进行授权；

b）应支持对授权资产的文件上传、下载以及连接动作的控制；支持复制/黏贴(windows资产)；

c）应支持对授权资产使用时间段的限制 ；

d）应支持命令的黑白名单及对用户所执行的命令进行控制 。

6.1.2.3 设备管理

本项要求包括：

a）应支持常用的运维协议：SSH、TELNET、VNC、RDP、SFTP；

b）应支持对设备进行按设备类型分组、按部门分组，支持设备批量导入/导出；

c）应支持对主流数据库Mysql、Redis数据库作为资产进行管理；

d）应支持通过本地客户端直接连接资产，建立 RDP、VNC、数据库等协议的图形会话。

e）应具备高并发会话处理能力，字符型操作会话并发超过500，图形会话并发超过300

6.1.2.4 运维方式

本项要求包括：

a）应支持提供无插件化的浏览器访问方式，支持登陆Linux和Windows资产；

b）应支持支持数据库资源运维时语法高亮、SQl格式化、SQL历史查询等；

c）应支持数据库资源全生命周期的运维。不限于表、库的增删改查，virew视图等；

d）应支持vnc、ssh、telnet、rdp等协议。支持多种协议的历史会话回放

6.1.2.5 操作审计

本项要求包括：

a）应对运维用户的操作进行审计，生成审计记录,应至少包括：操作时间、运维用户、源地址、运维对象、管理方式、操作内容和操作结果等其他信息

b）应支持管理员设置可使用命令与高危命令的审计 ；

c）应支持运维用户对资产进行操作的录像审计。

d）应提供对审计记录数据进行统计、分析及生成审计报表的功能

e）应仅允许授权管理员查阅审计记录，支持条件查询并以通用格式导出，查询条件包括：操作时间、运维用户、源地址、运维对象和操作命令等。

6.1.2.6 会话监视与回放

本项要求包括：

a）应提供对访问运维对象会话过程的图形化实时监视功能；

b）应支持字符型、图形化界面画面监控回放；

c）按操作命令或时间进行定位回放；

d）应支持vi、smit、setup等字符菜单操作同步显示；

e）应支持管理员对运维用户操作会话的实时监视。

6.1.2.7 分析告警

本项要求包括：

a)应依据告警策略对运维用户的违规操作进行告警，告警信息应至少包括：操作时间、运维用户、源地址、运维对象、管理方式、事件描述和触发的策略等。

b)应支持多种告警方式：WEB界面告警、短信告警、邮件告警等

6.1.2.8 违规操作阻断

本项要求包括：

a） 应能阻断未经授权用户访问主机；

b） 应能阻断从异常客户端、异常时间段发起的访问行为；

c） 应能阻断指令黑名单的操作行为；

d） 应能阻断方式支持：断开会话、忽略指令等

6.1.2.9 高可用性

当产品发生故障时，通过冗余或bypass等方式保证产品的高可用性。

6.1.2.10 审计日志

6.1.2.10.1 审计日志生成

产品应对下列事件生成审计日志，审计日志的内容至少应包括事件发生的日期、时间、主体标识、事件描述和结果：

a）管理员/运维用户的鉴别成功和失败；

b）对安全策略进行更改的操作；

c）对角色进行增加、删除和属性修改的操作；

d）对审计日志的备份；
e）管理员的其他操作。

6.1.2.10.2 审计日志存储

产品应提供以下功能对审计日志进行存储：
a）存储于掉电非易失性存储介质中；
b）当存储空间达到阈值时,能通知授权管理员；
c）当存储空间将要耗尽时，采取相应的防止审计日志丢失的技术措施。

6.1.2.10.3 审计日志管理

产品应提供下列审计日志管理功能：
a）只允许授权管理员访问审计日志；
b）对审计日志的条件查询功能；
c）对审计日志的备份功能。

6.1.2.11 业务数据留存

本项要求包括：
a）应只允许授权管理员能够对留存数据进行核查和删除操作，留存数据原则上不允许导出；
b）应支持数据副本留存时间至少6个月；
c）支持存储空间不足时自动归档并删除最早数据；
d）支持通过FTP、SFTP自动上传归档文件。

6.1.2.12 业务数据完整性

本项要求包括：
a）应保障运维审计过程中业务数据的完整性。
b）应保障审计日志数据的完整性；

6.1.2.13 业务数据保密性

本项要求包括：
a）不应明文留存业务数据；
b）仅应向符合控制策略的合法目标提供业务数据，不应向其他任何方提供业务数据；
c）应保障审计日志的保密性。

6.1.3 安全保障要求

6.1.3.1 开发安全

6.1.3.1.1 开发文档

开发者应提供开发安全文档。开发安全文档应描述在产品的开发环境中，为保护产品设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

6.1.3.1.2 生命周期定义

开发者应建立一个生命周期模型对产品的开发和维护进行的必要控制.并提供生命周期定义文档描述用于开发和维护产品的模型。

6.1.3.1.3 配置管理

6.1.3.1.3.1 配置管理能力

开发者的配置管理能力应满足以下要求：

a）为产品的不同版本提供唯一的标识；

b）使用配置管理系统对组成产品的所有配置项进行维护并进行唯一标识；

c）提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法；

d）配置管理系统提供自动方式来支持产品的生成通过自动化措施确保配置项仅接受授权变更；

e）配置管理文档包括一个配置管理计划。描述用来接受修改过的或新建的作为产品组成部分的配置项的程序。配置管理计划应描述如何使用配置管理系统开发产品．开发者实施的配置管理应与配置管理计划相一致。

6.1.3.1.3.2 配置管理范围

开发者应提供产品配置项列表，并说明配置项的开发者。配置项列表应包含以下内容：产品、安全保障要求的评估证据和产品的组成部分；

6.1.3.1.4 安全架构

开发者应提供产品安全功能的安全架构描述，安全架构描述应满足以下要求：

a）与产品设计文档中对安全功能的描述范围相一致；

b）充分描述产品采取的自我保护、不可旁路的安全机制。

6.1.3.1.5 功能规范

开发者应提供完备的功能规范，功能规范应满足以下要求：

a）完整描述 6.1.1、6.1.2 中定义的功能；

b）标识和描述产品所有安全功能接口的目的、使用方法及相关参数；

6.1.3.1.6 产品设计

开发者应提供产品设计文档，产品设计文档应满足以下要求；

a）通过子系统描述产品结构，标识和描述产品安全功能的所有子系统，并描述子系统间的相互作用；

b）提供子系统和安全功能接口间的对应关系；

6.1.3.1.7 测试

6.1.3.1.7.1 测试覆盖

开发者应提供测试覆盖文档，测试覆盖描述应满足以下要求：

a）表明测试文档中所标识的测试项与功能规范中所描述的产品安全功能的对应性；

6.1.3.1.7.2 功能测试

开发者应测试产品安全功能，并提供测试文档。测试文档应包括以下内容：

a）测试计划，标识要执行的测试，并描述执行每个测试的方案，这些方案包活对于其他测评结果的任何顺序依赖性；

b）预期的测评结果，表明测试成功后的预期输出；

c）实际测评结果和预期的测评结果的对比。

6.1.3.1.7.3 独立测试

开发者应提供一组与其自测安全功能时使用的同等资源，以用于安全功能的抽样测试。

6.1.3.2 指导性文档

6.1.3.2.1 用户操作指南

开发者应提供明确和合理的操作用户指南，对每一种用户角色的描述应满足以下要求：

a）描述用户能够访问的功能和特权，包含适当的警示信息；

b）描述产品安全功能及接口的用户操作方法．包括配置参数的安全值等；

c）标识和描述产品运行的所有可能状态，包括操作导致的失败或者操作性错误；

d）描述实现产品安全目的必需执行的安全策略。

6.1.3.2.2 准备程序

开发者应提供产品及其准备程序，准备程序描述应满足以下要求：

a）描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；

b）描述安全安装产品及其运行环境必需的所有步骤。

6.1.3.2.3 系统交付

开发者应使用规定的交付程序交付产品，并将交付过程文档化。在给用户方交付各版本产品时，交付文档应描述为维护安全所必需的所有程序。

6.1.4 测试评价

6.1.4.1 测试环境与工具

测试评价方法包括针对基本级产品和增强级产品的安全功能要求测试和安全保障要求评估，其测试的典型网络拓扑图如下图2所示。

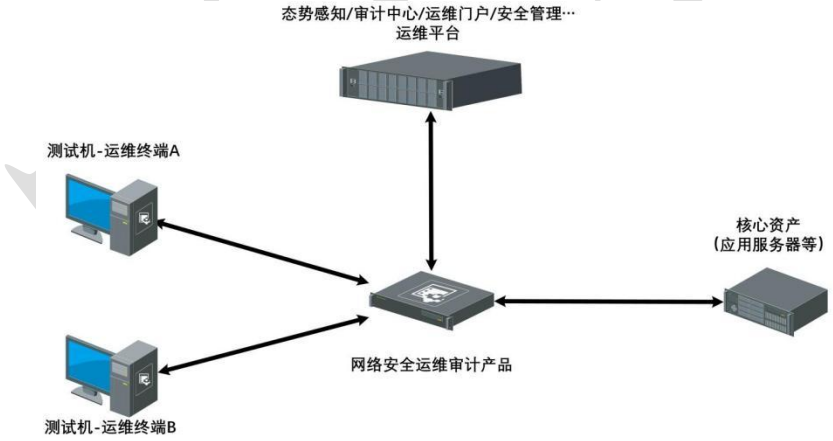

图2 网络安全运维审计产品测试典型网络拓扑图

测试设备包括但不限于测试所需的交换机、网络安全运维审计产品、产品控制终端等其他设备。

测试机包括但不限于2台及以上测试终端、性能测试仪、测试工具集、测试数据集等。

6.1.4.2 自身安全功能测试

6.1.4.2.1 用户身份鉴别

测试评价方法如下：

a）测试方法

1)登录用户管理模块，查看已有用户列表，并尝试创建同名用户；

2)尝试使用合法和非法用户分别登录，验证期身份鉴别是否有效；

3)尝试修改用户默认口令，验证是否可正常修改口令；

4)通过创建新用户或修改用户口令，验证是否对口令的复杂度进行了校验；

5)尝试使用错误鉴别信息登录，验证鉴别失败处理是否有效；

6)配置会话超时时间，验证超时后是否正常断开链接；

7)检查产品对于用户鉴别信息的存储和传输过程中，采取何种措施对其保密性和完整性进行保护。

b）预期结果

1）无法创建同名用户，身份标识可保证唯一性；

2）合法用户可以正常登录，非法用户无法登录；

3）可修改用户默认口令；

4）创建用户及修改用户口令时，均对口令复杂度进行了校验，并在校验失败时无法完成用户创建或口令修改；

5）当非法身份验证超过一定次数后，终止已建立的连接并限制用户操作；

6）当连接超时后，自动断开连接并清除登录信息；

7）支持非明文的鉴别信息存储和传输且明文存储、传输方式关闭。

c）结果判定

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.1.4.2.2 用户访问控制

测试评价方法如下：

a）测试方法

1） 登录权限管理模块，查看是否可以创建/修改/删除用户的功能权限、数据权限；

2） 登录用户管理模块，查看是否存在多余、过期用户；

3） 登录用户管理模块，查看是否已重命名默认账户或默认账户已删除；

4） 登陆新建用户，查看是否提示修改默认口令；

5） 检查管理用户是否进行角色划分、权限是否已进行分离，用户权限是否与预置访问控制策略是否一致，并满足最小权限原则。

b）预期结果

1） 可正常创建/修改/删除用户的功能权限、数据权限；

2） 用户列表不存在多余、过期用户；

3） 用户列表不存在默认账户名称；

4） 用户默认口令未修改时，提示修改默认口令；

5） 已按角色划分用户，用户与权限分离，与预置访问控制策略一致，并满足最小权限原则。

c）结果判定

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.1.4.2.3 系统安全审计

测试评价方法如下：

a）测试方法

1） 分别执行用户登陆、注销、创建、删除、口令修改及产品使用操作，查看是否由审计记录；

2） 查看审计日志是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

3） 尝试采用非法授权用户访问、选择性删除记录等方式，验证审计记录是否具有保护、备份措施防止非预期的删除、修改和覆盖等。

b）预期结果

1） 执行用户登陆、注销、创建、删除、口令修改及产品使用操作均记录其行为，并在审计日志中可查看相关信息；

2） 审计日志包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

3） 具备审计日志保护措施，可避免未预期的删除、修改或覆盖。

c）结果判定

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.1.4.2.4 安全管理

测试评价方法如下：

a）测试方法

1） 检查是否划分了管理员级别，并依据不同级别分配了不同管理范围和权限；

2） 尝试登陆管理员用户，检查是否具有身份鉴别、权限控制、参数配置及审计记录的管理功能。

3） 通过嗅探等方式抓取相关运维通道中的数据包，确认是否采用密码技术建立了安全运维管理通道。

b）预期结果

1） 已按级别对管理员角色进行划分，并依据不同级别的管理员角色分配不同管理范围和权限；

2） 具备身份鉴别、权限控制、参数配置及审计记录的管理功能。

3） 采用密码技术建立了安全运维管理通道。

c）结果判定

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.1.4.2.5 用户数据完整性

测试评价方法如下：

a）测试方法

1） 检查重要数据在传输和存储过程中是否采用了密码技术保证完整性；

b）预期结果

1） 采用密码技术保证了传输过程中的用户数据完整性；

2） 具备传输过程结束后的数据完整性检测措施，并能够恢复传输的重要数据；

c）结果判定

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.1.4.2.6 用户数据机密性保护

测试评价方法如下：

a）测试方法

1） 通过嗅探等方式抓取传输过程中的数据包，鉴别用户数据是否进行了加密处理；

2） 尝试使用未授权用户访问或使用用户数据。

b）预期结果

1） 用户数据传输过程中的数据包已被加密，无法还原原始数据；

2） 未授权用户不可访问和使用用户数据。

c）结果判定

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.1.4.3 安全保障评估

6.1.4.3.1 开发安全评估

6.1.4.3.1.1 安全架构

测试评价方法如下：

a）测试方法

检查开发者提供的安全架构证据，并检查开发者提供的信息是否满足证据的内容和形式的所有要求：

1） 与产品设计文档中对安全功能的描述范围是否相一致；

2） 是否充分描述产品采取的自我保护、不可旁路的安全机制。

b）预期结果

开发者提供的信息应满足 6.1.3 要求。

c）结果判定

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.1.4.3.1.2 功能规范

测试评价方法如下：

a）测试方法：

检查开发者提供的功能规范证据，并检查开发者提供的信息是否满足证据的内容和形式的所有要求：

1） 是否清晰描 6.1.1 中定义的产品安全功能；

2） 是否描述产品所有安全功能接口的目的、使用方法及相关参数；

3） 描述安全功能实施过程中，是否描述与安全功能接口相关的所有行为；

4） 是否描述可能由安全功能接口的调用而引起的所有直接错误消息。

b）预期结果

开发者提供的信息应满足 6.1.3 要求。

c）结果判定

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.1.4.3.1.3 产品设计

测试评价方法如下：

a）测试方法：

检查开发者提供的产品设计证据，并检查开发者提供的信息是否满足证据的内容和形式的所有要求：

1） 是否根据子系统描述产品结构，是否标识和描述产品安全功能的所有子系统，是否描述安全功能所有子系统间的相互作用；

2） 提供的对应关系是否能证实设计中描述的所有行为映射到调用的安全功能接口；

3） 是否根据实现模块描述安全功能，是否描述所有实现模块的安全功能要求相关接口、接口的返回值、与其他模块间的相互作用及调用的接口；

4） 是否提供实现模块和子系统间的对应关系。

b）预期结果

开发者提供的信息应满足 6.1.3 要求。

c）结果判定

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.1.4.3.2 指导性文档评估

6.1.4.3.2.1 用户操作指南

测试评价方法如下：

a）测试方法：

检查开发者提供的操作用户指南证据，并检查开发者提供的信息是否满足证据的内容和形式的所有要求：

1） 是否描述用户能访问的功能和特权（包含适当的警示信息）；

2） 是否描述如何以安全的方式使用产品提供的可用接口，是否描述产品安全功能及接口的用户操作方法（包括配置参数的安全值）；

3） 是否标识和描述产品运行的所有可能状态，包括操作导致的失败或者操作性错误；

4） 是否描述实现产品安全目的必需执行的安全策略。

b）预期结果

开发者提供的信息应满足 6.1.3 要求。

c）结果判定

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.1.4.3.2.2 系统交付

测试评价方法如下：

a）测试方法：

检查开发者提供的准备程序证据，并检查开发者提供的信息是否满足证据的内容和形式的所有要求：

1） 是否描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；

2） 是否描述安全安装产品及其运行环境必需的所有步骤。预期结果

开发者提供的信息应满足 6.1.3 要求。

b）结果判定

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.2 增强级安全技术要求

6.2.1 密码技术应用通用要求

下述相关密码技术、密码服务的应用应符合以下通用要求：

a）所使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求；

b）所使用的密码技术应遵循密码相关国家标准和行业标准；

c）所使用的密码产品、密码服务应符合法律法规的相关要求。

6.2.2 自身安全要求

6.2.2.1 用户身份鉴别

用户的身份标识与鉴别安全要求包括但不限于：

a)应采用密码技术，对用户身份进行标识和鉴别，身份标识具有唯一性；

b)应采用密码技术，对用户身份鉴别信息进行安全保护，保障用户鉴别信息传输过程中的机密性和完整性；

c)具有登录失败处理功能，如限制连续的非法登录尝试次数等相关措施；

d)具有登录超时处理功能，当登录连接超时自动退出；

e)鉴别机制应具有抗重放的能力，授权管理员及其他用户不能复制使用上一次通过的鉴别信息再次鉴别成功；

f)应选择两种或两种以上组合的鉴别技术，如密码设备的硬件PIN码和国密数字证书相结合的方式，进行身份鉴别。

6.2.2.2 用户访问控制

用户访问控制安全要求包括但不限于：

a）应支持用户权限管理功能，包括但不限于对用户功能权限和数据权限的创建/查看/修改/删除等 功能；

b）应定期对多余或已过期的用户自动进行清除；

c）应确保默认账户的安全，禁止默认账户出现重命名或被删除等异常情况；

d）新建用户时，应提示修改默认口令；

e）管理用户应根据角色类型进行明确划分，且不同类型的角色权限要求分离，用户权限要求与预置访问控制策略是否一致，并满足最小权限原则。

f）应能根据运维用户、源地址、运维对象及其账户、管理方式、操作命令、操作时间等对运维用户实施访问控制:

g）应采用商用密码技术对访问控制权限列表进行完整性保护。

6.2.2.3 设备身份鉴别

设备身份鉴别安全要求包括但不限于：

应采用密码技术，对网络安全运维审计产品设备自身身份进行标识和鉴别，身份标识应具有唯一性。

6.2.2.4 设备访问控制信息完整性

设备访问控制安全要求包括但不限于：

应采用密码技术，实现对网络安全运维审计产品设备自身访问控制信息的完整性保护。

6.2.2.5 系统安全审计

产品的管理审计安全要求包括但不限于：

a)对用户账户的登录和注销、系统启动、重要配置变更、增加/删除/修改管理员、保存/删除审计日志等操作行为进行日志记录；

b)对产品及其组件的异常状态进行告警，并记录日志；

c)日志记录中包括如下内容：事件发生的日期和时间，事件的类型，事件主体，事件操作结果；

d)日志存储周期设定不小于六个月；

e)仅允许授权管理员访问日志；

6.2.2.6 安全管理

6.2.2.6.1 安全管理能力

产品的管理能力安全要求包括但不限于：

a)向授权管理员提供设置和修改安全管理相关的数据参数的功能；

b)向授权管理员提供设置、查询和修改各种安全策略的功能；

c)向授权管理员提供管理审计日志的功能；

d)支持更新自身系统的能力，包括对软件系统的升级以及各种特征库的升级；

e)支持通过SYSLOG协议向日志服务器同步日志等信息；

f)产品应支持与外部时间服务器进行时间同步；

g)应区分管理员角色，能划分为系统管理员、安全管理员和审计管理员，三类管理员角色权限能相互制约；

h)应采用密码技术，在运维终端和网络安全运维审计产品之间，采用国密SSL协议或国密IPSec协议，建立安全的运维管理通道；

i)应采用密码技术，在网络安全运维审计产品和应用服务器、数据库服务器等核心资产之间，采用国密SSL协议或国密IPSec协议，建立安全的运维管理通道；

j)应采用密码技术，在网络安全运维审计产品和态势感知/审计中心/运维门户/安全管理等运维平台之间，采用国密SSL协议或国密IPSec协议，建立安全的运维管理通道。

6.2.2.6.2 安全管理方式

产品的管理方式安全要求包括：

a)支持本地管理，如console口；

b)连接不同安全域的内外网分开管理；

c)支持通过网络接口进行远程管理，并能限定进行远程管理的IP、MAC地址；

d)远程管理过程中，管理端与产品之间的所有通信数据应采用非明文传输，应采用密码技术，实现对相关通信数据在传输过程中的机密性和完整性保护；

e)管理接口与业务接口分离。

6.2.2.7 用户数据完整性

网络隔离产品安全功能应保护存储于设备中的鉴别数据和信息传输策略不受未授权查阅、修改和破坏。

a）应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；

b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、配置重要数据、重要视频数据和重要个人信息等。

6.2.2.8 用户数据保密性保护

本项要求包括

a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；

b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；

c）应确保用户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定。

d）应确保传输过程中重要数据的完整性，并在检测到完整性收到破坏时采取必要的恢复措施。

6.2.2.9 可信验证

可基于可行根对边界设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后报警，并将验证结果形成审计记录送至安全管理中心。

6.2.2.10 配置可信检查

可配置基于可行根对边界设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后报警，并将验证结果形成审计记录送至安全管理中心。

6.2.2.11 入侵检测和恶意代码防范

本项要求包括：

a）应安装入侵检测软件或配置具有相应功能的软件，能将入侵检测结果推送至管理员，并定义进行升级和更新；

b）应遵循最小安装的原则，仅安装需要的组件和应用程序；

c）应关闭不需要的系统服务、默认共享和高危端口；

d）应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库；

e)应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；

f）应提供数据有效性检验功能，保证输入的内容符合系统设定要求；

g）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。

6.2.3 安全运维审计功能要求

6.2.3.1 单点登录

本项要求包括：

a）应提供统一的身份鉴别功能，实现运维用户的单点登录，运维用户仅需经过产品的身份鉴别后，即可访问授权范围内的资产。

b）应支持当失败的用户身份登录次数达到规定的数值时，能够中止用户与系统之间的登录过程。

c）应支持动态口令认证软件和硬件令牌（例如：智能密码钥匙）等多因子方式。

d）应支持国密算法的全链路身份鉴别。

6.2.3.2 授权控制

本项要求包括：

a）应支持对资产进行授权 ；

b）应支持对授权资产的文件上传、下载以及连接动作的控制；支持复制/黏贴(windows资产) ；

c）应支持对授权资产使用时间段的限制 ；

d）应支持命令的黑白名单及对用户所执行的命令进行控制 。

e）应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限

f）应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户

g）应支持用户通过堡垒机连接Kubemetes集群；

h）应支持关键访问操作二次授权审批。

6.2.3.3 设备管理

本项要求包括：

a）应支持常用的运维协议：SSH、TELNET、VNC、RDP、SFTP；

b）应支持对设备进行按设备类型分组、按部门分组，支持设备批量导入/导出；

c）应支持对主流数据库作为资产进行管理；

d）应支持通过本地客户端直接连接资产，建立 RDP、VNC、数据库等协议的图形会话。

e）应支持对资产、应用账号进行定时备份

f）宜支持自动发现指定云中的资产，并自动导入。

g）宜具备超高并发会话处理能力，字符型操作会话并发超过1000，图形会话并发超过600

6.2.3.4 运维方式

本项要求包括：

a）应支持提供无插件化的浏览器访问方式，支持登陆Linux和Windows资产；

b）应支持支持数据库资源运维时语法高亮、SQl格式化、SQL历史查询等；

c）应支持数据库资源全生命周期的运维。不限于表、库的增删改查，virew视图等；

d）应支持vnc、ssh、telnet、rdp等协议。支持多种协议的历史会话回放

e）应支持客户端访问方式：支持使用本地的Xshell，putty等客户端工具通过堡垒机访问资产，并具备搜索、资产树、分组能力

f）应支持批量对Linux类系统执行命令操作

6.2.3.5 操作审计

本项要求包括：

a）产品应对运维用户的操作进行审计，生成审计记录,应至少包括：操作时间、运维用户、源地址、运维对象、管理方式、操作内容和操作结果等其他信息；

b）应支持管理员设置可使用命令与高危命令的审计；

c）应支持运维用户对资产进行操作的录像审计；

d）应支持对文件的上传/下载记录进行审计；

e）应支持用户操作行为同步发送到态势感知对比平台进行实时对比；

f）应提供对审计记录数据进行统计、分析及生成审计报表的功能

g）应仅允许授权管理员查阅审计记录，支持条件查询并以通用格式导出，查询条件包括：操作时间、运维用户、源地址、运维对象和操作命令等。

h）应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

6.2.3.6 会话监视与回放

本项要求包括：

a）应提供对访问运维对象会话过程的图形化实时监视功能；

b）应支持字符型、图形化界面画面监控回放；

c）按操作命令或时间进行定位回放；

d）应支持vi、smit、setup等字符菜单操作同步显示；

e）应支持管理员对运维用户操作会话的实时监视。

f）应支持录像和会话的水印信息；

g）应支持离线播放录像，并且离线播放的时候要显示出日期、操作者，录像时长等信息。

6.2.3.7 分析告警

本项要求包括：

a）应依据告警策略对运维用户的违规操作进行告警，告警信息应至少包括：操作时间、运维用户、源地址、运维对象、管理方式、事件描述和触发的策略等；

b)应支持多种告警方式：WEB界面告警、短信告警、邮件告警。

6.2.3.8 违规操作阻断

本项要求包括：

a）应阻断未经授权用户访问主机
b）应阻断从异常客户端、异常时间段发起的访问行为；
c）应阻断指令黑名单的操作行为；
d）应阻断方式支持：断开会话、忽略指令
e）应实时监视违规命令，一旦发现违规操作，立刻阻断，并保存日志，确保信息系统安全运行；
f)应支持发现违规操作，立刻上报管理员，超过违规次数，停止该用户访问权限；

6.2.3.9 高可用性

当产品发生故障时，通过冗余或bypass等方式保证产品的高可用性。

6.2.3.10 审计日志

6.2.3.10.1 审计日志生成

产品应对下列事件生成审计日志，审计日志的内容至少应包括事件发生的日期、时间、主体标识、事件描述和结果:
a）管理员/运维用户的鉴别成功和失败；
b）对安全策略进行更改的操作；
c）对角色进行增加、删除和属性修改的操作；
d）对审计日志的备份；
e）改密日志；
f）文件传输日志
g）管理员的其他操作。

6.2.3.10.2 审计日志存储

产品应提供以下功能对审计日志进行存储：
a）存储于掉电非易失性存储介质中；
b）当存储空间达到阈值时,能通知授权管理员；
c）当存储空间将要耗尽时，采取相应的防止审计日志丢失的技术措施。

6.2.3.10.3 审计日志管理

产品应提供下列审计日志管理功能：
a）只允许授权管理员访问审计日志；
b）对审计日志的条件查询功能；
c）对审计日志的备份功能。

6.2.3.11 业务数据留存

本项要求包括：
a）应采用商用密码技术对需留存的数据副本进行强加密保护；
b）应只允许授权管理员能够对留存数据进行解密、核查和删除操作，留存数据原则上不允许导出；
c）应支持数据副本留存时间至少6个月。
c）支持存储空间不足时自动归档并删除最早数据；
d）周期性自动归档功能
e）支持采用商用密码技术实现自动上传归档文件。

6.2.3.12 业务数据完整性

本项要求包括：

a）应使用商用密码技术保障运维审计过程中业务数据的完整性，
b）应使用商用密码技术保障审计日志数据的完整性。

6.2.3.13 业务数据保密性

本项要求包括：
a）应采用商用密码技术保证留存业务数据的保密性；
b）仅应向符合控制策略的合法目标提供业务数据，不应向其他任何方提供业务数据；
c）应保用商用密码技术障审计日志的保密性。

6.2.4 安全保障要求

同6.1.3安全保障要求。

6.2.5 测试评价

6.2.5.1 测试环境与工具

同6.1.4.1测试环境与工具。

6.2.5.2 自身安全功能测试

6.2.5.2.1 用户身份鉴别

测试评价方法如下：
a）测试方法
1)登录用户管理模块，查看已有用户列表，并尝试创建同名用户；
2)尝试使用合法和非法用户分别登录，验证期身份鉴别是否有效；
3)尝试使用错误鉴别信息登录，验证鉴别失败处理是否有效；
4)配置会话超时时间，验证超时后是否正常断开链接；
5)检查是否采用了两种或两种以上组合的身份鉴别技术。
b）预期结果
1)无法创建同名用户，身份标识可保证唯一性；
2)合法用户可以正常登录，非法用户无法登录；
3)可修改用户默认口令；
4)创建用户及修改用户口令时，均对口令复杂度进行了校验，并在校验失败时无法完成用户创建或口令修改；
当非法身份验证超过一定次数后，终止已建立的连接并限制用户操作；
5)当连接超时后，自动断开连接并清除登录信息；
6)采用了两种及两种以上组合的身份鉴别技术。
c）结果判定
实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.2.5.2.2 用户访问控制

测试评价方法如下：
a）测试方法
1）登录权限管理模块，查看是否可以创建/修改/删除用户的功能权限、数据权限；
2）登录用户管理模块，查看是否存在多余、过期用户；
3）登录用户管理模块，查看是否已重命名默认账户或默认账户已删除；
4）登陆新建用户，查看是否提示修改默认口令；

5）检查管理用户是否进行角色划分、权限是否已进行分离，用户权限是否与预置访问控制策略是否一致，并满足最小权限原则。

b）预期结果

1）可正常创建/修改/删除用户的功能权限、数据权限；

2）用户列表不存在多余、过期用户；

3）用户列表不存在默认账户名称；

4）用户默认口令未修改时，提示修改默认口令；

5）已按角色划分用户，用户与权限分离，与预置访问控制策略一致，并满足最小权限原则。

c）结果判定

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.2.5.2.3 设备身份鉴别

测试评价方法如下：

a）测试方法

1）尝试使用合法和非法用户分别登录，验证设备身份鉴别是否有效；

b）预期结果

1）合法用户可以正常登录，非法用户无法登录

c）结果判定

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.2.5.2.4 系统安全审计

测试评价方法如下：

a）测试方法

1）分别执行用户登陆、注销、创建、删除、口令修改及产品使用操作，查看是否由审计记录；

2）查看审计日志是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

3）尝试采用非法授权用户访问、选择性删除记录等方式，验证审计记录是否具有保护、备份措施防止非预期的删除、修改和覆盖等。

b）预期结果

1）执行用户登陆、注销、创建、删除、口令修改及产品使用操作均记录其行为，并在审计日志中可查看相关信息；

2）审计日志包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

3）具备审计日志保护措施，可避免未预期的删除、修改或覆盖。

c）结果判定

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.2.5.2.5 安全管理

测试评价方法如下：

a）测试方法

1）检查是否划分了管理员级别，并依据不同级别分配了不同管理范围和权限；

2）尝试登陆管理员用户，检查是否具有身份鉴别、权限控制、参数配置及审计记录的管理功能；

3）通过嗅探等方式抓取相关运维通道中的数据包，确认是否采用国密 SSL 协议或国密 IPSec 协议建立了安全运维管理通道。

b）预期结果

1）已按级别对管理员角色进行划分，并依据不同级别的管理员角色分配不同管理范围和权限；

2）具备身份鉴别、权限控制、参数配置及审计记录的管理功能；

3）采用国密 SSL 协议或国密 IPSec 协议建立了安全运维管理通道。

c）结果判定

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.2.5.2.6 对接第三方管理平台

测试评价方法如下：

a）测试方法

1）检查用户是否可以通过网络安全运维审计产品访问态势感知/审计中心/运维门户/安全管理等运维平台；

2）检查网络安全运维审计产品和态势感知/审计中心/运维门户/安全管理等运维平台之间是否可以进行数据交互，包括运维审计数据的上传和权限策略数据的下发。

b）预期结果

1）用户可以通过网络安全运维审计产品访问相关运维平台;

2）网络安全运维审计产品和运维平台之间可以进行数据交互;

c）结果判定

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.2.5.2.7 用户数据完整性

测试评价方法如下：

a）测试方法

1）通过嗅探等方式抓取传输和存储过程中的数据包，检查重要数据在传输和存储过程中是否采用了密码技术保证完整性；

2）数据完整性遭到破坏后，能够恢复传输的重要数据。

b）预期结果

1）采用密码技术保证了传输和存储过程中的用户数据完整性;

2）具备传输过程结束后的数据完整性检测措施，并能够恢复传输的重要数据;

c）结果判定

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.2.5.2.8 用户数据机密性保护

测试评价方法如下：

a）测试方法

1）通过嗅探等方式抓取传输和存储过程中的数据包，鉴别用户数据是否进行了加密处理；

2）尝试使用未授权用户访问或使用用户数据。

b）预期结果

1）用户数据传输和存储过程中的数据包已被加密，无法还原原始数据；

2）未授权用户不可访问和使用用户数据。

c）结果判定

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.2.5.2.9 可信验证

测试评价方法如下：

a）测试方法

1）检查是否能够按安全防护技术要求对系统引导程序、系统程序和其他应用程序等进行可信验证；

2）尝试破坏设备可信性，验证是否具有报警的功能；

3）检查是否能够按相应安全防护技术要求将验证结果形成审计记录送至安全管理中心。

b）预期结果

能够按照安全防护技术要求对系统引导程序、系统程序和其他应用程序等进行可信验证；

1）在设备可信性收到破坏时，能够终止相关连接并提示报警；

2）能够在安全管理中心查询可信验证相关审计记录。

c）结果判定

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.2.5.2.10 配置可信检查

测试评价方法如下：

a）测试方法

1）检查是否能够按安全防护技术要求对系统重要配置参数进行可信验证；

2）尝试进行非法的配置时，验证是否具有报警的功能；

3）检查是否能够按相应安全防护技术要求将配置可信检查结果形成审计记录送至安全管理中心。

b）预期结果

1）能够按照安全防护技术要求对重要配置参数进行可信验证；

2）在执行非法配置操作时，能够终止相关连接并提示报警；

3）能够在安全管理中心查询配置可信检查相关审计记录。

c）结果判定

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.2.5.2.11 入侵监测和恶意代码防范

测试评价方法如下：

a）测试方法

1） 尝试利用入侵技术验证产品是否配置入侵检测措施，并将检测结果推送至管理员；

2） 检查是否定期升级和更新入侵检测软件或具有相应功能的软件；

3） 检查是否遵循最小安装原则，仅安装需要的组件和应用程序；

4） 检查是否开启了与系统服务无关的端口以及默认共享和高危端口；

5） 检查是否安装了防恶意代码软件或配置有具有相应功能软件，并定期升级和更新恶意代码库；

6） 检查是否对产品需要的可执行程序、静态库、动态库配置了白名单安全防护措施。

b）预期结果

1） 能够防范常见入侵行为，并将入侵结果推送至管理员；
2） 具备定期升级和更新入侵检测软件或具有相应功能软件的策略；
3） 仅安装需要的组件和应用程序，具备最小安装原则；
4） 仅开启了系统服务相关端口；
5） 安装了防恶意代码软件或配置有具有相应功能软件，具备定期升级和更新的策略；
6） 配置了产品所需的可执行程序、静态库、动态库的白名单安全防护措施。

c）结果判定

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.2.5.3 安全保障评估

同6.1.4.4安全保障评估。

参 考 文 献

[1] GB/Z 20986-2007 信息安全技术 信息安全事件分类分级指南
[2] GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范
[3] GB/T 18336.3-2015 信息技术 安全技术 信息技术安全评估准则 第3部分：安全保障组件
[4] GB/T 22081-2016 信息技术 安全技术 信息安全控制实践指南
[5] GB/T 32921-2016 信息安全技术 信息技术产品供应方行为安全准则
[6] GB/T 32924-2016 信息安全技术 网络安全预警指南
[7] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
[8] GB/T 22239-2019 信息安全技术 网络安全等级保护基础要求
[9] GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求
[10] GA/T 1394-2017 信息安全技术 运维安全管理产品安全技术要求