**报告编号：V22S000XX**

基于零信任架构的业务安全平台

**检 验 报 告**

**产品名称：亿格云枢SASE零信任系统**

**产品型号：V2.3**

**产品版本：V2.3**

**委托单位：杭州亿格云科技有限公司**

**检验类别：委托检验**

**网络安全卓越验证示范中心**

**中国泰尔实验室**

**中国信息通信研究院**

**注 意 事 项**

1、本检验报告是中国泰尔实验室对上述产品进行科学、客观检验的结果，为被检验样品的能力评定提供第三方独立、客观和公正的依据，也为产品购买的最终用户选择产品提供参考和帮助。

2、未经过中国泰尔实验室书面批准，不得复制报告中的内容除全文复制），以免本报告的使用者对受检验产品做出不全面的评价。

3、在任何情况下，若需引用本检验报告中的结果或数据都应保存其本来的意义，不得擅自增加、修改、伪造或掩盖本报告的原有内容。

4、本检验报告不得复制作为广告材料使用。

5、当受检验产品出现型号、版本号更新或其他改变，本检验报告结果不再适用，涉及到的任何技术、模块或子系统甚至整个产品都必须按照要求进行重新检验。不得将本报告检验结果应用于其他型号、版本号的产品。

6、本报告由中国泰尔实验室根据相关检验标准完成产品或系统的成熟度和能力检验。网络安全卓越示范验证中心完成受检验产品或系统的先进能力评估验证。

7、中国泰尔实验室出具的检验报告是针对颁证日期前产品情况进行披露，使用方应留意在使用中可能发生的风险。当产品的版本迭代升级、标准规范修订或检验方法有较大的变化时，建议重新检验。

8、本检验报告仅供XXXXXX公司使用。

北京市海淀区花园北路52号 中国信息通信研究院 - 地址

100191 - 邮政编码

86-10-62301618 - 电话

[www.caict.ac.cn](http://www.caict.ac.cn) - 网址

**检 验 报 告**

报告编号：V22S000XX

|  |  |  |  |
| --- | --- | --- | --- |
| 产品名称 | 亿格云枢 | 产品数量 | 1 |
| 版本/型号 | V2.3 | 商 标 | / |
| 委托单位 | 杭州亿格云科技有限公司 | | |
| 生产单位 | 杭州亿格云科技有限公司 | | |
| 检验类别 | 网络安全产品类 | 送样基数 | / |
| 送 样 人 | 舒琳 | 送样日期 | 2022年X月22日 |
| 检验项目 | 产品的功能、性能及安全性 | 检验日期 | 2022年X月2XX7日 |
| 检验依据 | FT-S04-024-01《网络安全产品能力评价体系 基于零信任架构的业务安全平台评价方法》 | | |
| 样品序号 | 9XX | | |
| 检验结论 | 经中国泰尔实验室的评测，贵单位研发的安全产品参与了“先进网络安全能力验证评估计划第十一期-基于零信任架构的安全产品能力评测”，完成了九大项功能、三大项性能效率和四大项安全性能力验证。通过了FT-S04-024-01《网络安全产品能力评价体系 基于零信任架构的业务安全平台评价方法》的功能性、性能效率和安全性检验。 | | |
| 签发日期 2022年X月 4日 | | |
| 备注 | 1. 免责声明 2. 经与客户确认，本次部分结果非现网环境产生，可能会影响本报告中检验结果的有效性，对此产生的影响和后果由客户承担。 3. 本报告中样品由客户提供，检验结果仅适用于收到的样品。 4. 本检验报告封面以及该表格中标识为“/”的符号代表此内容在本次检验中不适用。 | | |

批准： 审核： 主检：

**检 验 样 品 描 述**

报告编号：V22S000XXX

XXXXXXX关。

**检 验 样 品 照 片**

|  |  |
| --- | --- |
| 产品名称：不适用 | 样品型号/版本号： 不适用 |
| 拍摄地点：不适用 | 日期：不适用 |
| 图1：外观（正、反面） | |
| 不适用 | |
| 图2：外观（侧面） | |
| 不适用 | |

目录

[1 检验范围 1](#_Toc113365823)

[2 检验环境 1](#_Toc113365824)

[3 检验内容 1](#_Toc113365825)

[3.1 功能性 1](#_Toc113365826)

[3.1.1 终端安全 1](#_Toc113365827)

[3.1.2 链路安全 4](#_Toc113365828)

[3.1.3 身份安全 5](#_Toc113365829)

[3.1.4 数据安全 6](#_Toc113365830)

[3.1.5 资源协议支持 8](#_Toc113365831)

[3.1.6 全域风险感知 10](#_Toc113365832)

[3.1.7 持续信任评估 11](#_Toc113365833)

[3.1.8 动态访问控制 12](#_Toc113365834)

[3.1.9 安全管理平台 15](#_Toc113365835)

[3.2 性能效率 20](#_Toc113365836)

[3.2.1 传输特性 20](#_Toc113365837)

[3.2.2 时间特性 20](#_Toc113365838)

[3.2.3 资源利用性 21](#_Toc113365839)

[3.3 安全性 21](#_Toc113365840)

[3.3.1 安全身份 21](#_Toc113365841)

[3.3.2 安全管理 22](#_Toc113365842)

[3.3.3 自安全性 24](#_Toc113365843)

[3.3.4 密码要求 25](#_Toc113365844)

基于零信任架构的业务安全平台检验报告

* 1. 检验范围

本次检验对象是面向基于零信任架构的业务安全平台或具有基于零信任架构的业务安全功能的产品，对其开展成熟度和能力检验与评价。

本次检验的参考依据是FT-S04-024-01《网络安全产品能力评价体系 基于零信任架构的业务安全平台评价方法》。

* 1. 检验环境

基于零信任架构的业务安全平台检验部署拓扑图如下图所示：



* 1. 检验内容
     1. 功能性
        1. 终端安全
           1. 终端信息采集

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. Windows、MAC、麒麟、统信、深度等操作系统，至少包括设备名称、操作系统及版本、客户端IP、MAC地址、防火墙状态、文件共享状态、高危开放端口、应用软件等终端信息的采集； 2. Android系统、iOS系统、鸿蒙系统至少包括设备名称、操作系统及版本、客户端IP、网络类型等终端信息的采集； 3. 客户端/管理平台提供可视化的终端信息采集结果查看； 4. 支持终端信息周期性采集上报。 |
| **预置条件**： | 1. 完成业务安全平台的部署，准备各种操作系统的设备各1台。 |
| **验证流程：** | 步骤1：使用Windows系统设备登录系统；  步骤2：登录客户端/管理平台，对比终端真实的信息，查看采集的信息是否准确；  步骤3：登录系统状态下，尝试改变终端信息，如关闭防火墙，一定周期后，查看采集到的终端信息是否变化；  步骤4：使用MAC、麒麟、统信、深度、Android、iOS及鸿蒙操作系统重复步骤1-3。 |
| **预期结果：** | 1. Windows、MAC、麒麟、统信、深度等操作系统支持采集终端信息，包括设备名称、操作系统及版本、客户端IP、MAC地址、防火墙状态、文件共享状态、高危开放端口、软件应用等； 2. Android系统、iOS系统、鸿蒙系统至少包括设备名称、操作系统及版本、客户端IP、网络类型等； 3. 客户端/管理平台支持终端信息采集结果查看； 4. 步骤3中，采集到的终端信息会准实时地随终端环境的变化而变化。 |
| **检验结果：** | 1. windows系统     Mac系统    统信系统，如图：     1. 安卓系统，如图：     IOS系统，如图：     1. 如1）、2）中截图所示，云枢管理平台终端管理中可查看采集的终端信息 2. 如图1，     图2，    图3， |

* + - * 1. 安全基线检测

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 系统支持终端安全基线检测能力，仅允许通过基线检测的终端设备接入系统进行业务访问； 2. 安全基线检测包括操作系统及版本、是否开启防火墙、是否安装杀毒软件、是否开放高危端口、是否开启文件共享、是否接入外设等。 |
| **预置条件**： | 1. 完成业务安全平台的部署，准备基线检测相关的软硬件。 |
| **验证流程：** | 步骤1：使用PC设备，设定符合基线检测标准的操作系统版本、操作系统账号口令复杂度、开启防火墙、安装杀毒软件、关闭高危端口、关闭文件共享、不插入外接设备，进行登录，查看登录效果；  步骤2：依次改变操作系统版本、操作系统账号口令复杂度、关闭防火墙、关闭杀毒软件、开放高危端口、开启文件共享、插入U盘，尝试进行用户登录，查看登录效果。 |
| **预期结果：** | 1. 步骤1中，可以正常登录系统并访问业务； 2. 步骤2中，登录系统失败，提示失败原因并提供修复操作。 |
| **检验结果：** | 1. 云枢支持终端基线检查，如图，     合规检查通过，所有风险、基线符合要求      不符合基线的处置，如图：     1. 如1）中截图，   合规检测基线不满足时，如图    策略配置中有不满足断网，如图    管控平台中有日志，如图 |

* + - * 1. 绑定与解绑

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 支持用户与终端设备建立绑定关系，包括一对一、一对多绑定等； 2. 支持用户与终端设备解除绑定关系，包括客户端侧解绑、管理平台侧解绑。 |
| **预置条件**： | 1. 完成业务安全平台的部署，准备至少两台安装客户端的设备。 |
| **验证流程：** | 步骤1：配置用户与终端设备一对一绑定策略；  步骤2：用户1与设备1进行绑定，登录管理平台查看绑定关系；  步骤3：用户1与设备2尝试进行绑定；  步骤4：配置用户与终端设备一对多绑定策略；  步骤5：用户1与设备2再次尝试进行绑定；  步骤6：客户端侧解除用户1与设备1的绑定关系；  步骤7：管理平台侧解除用户1与设备2的绑定关系；  步骤8：配置用户与终端设备一对多绑定策略并检验是否有效。 |
| **预期结果：** | 1. 步骤2中，用户1与设备1建立了绑定关系； 2. 步骤3中，用户1与设备2绑定失败； 3. 步骤5中，用户1与设备2建立了绑定关系； 4. 步骤6中，客户端侧可解除用户1与设备1的绑定关系； 5. 步骤7中，管理平台侧可解除用户1与设备1的绑定关系； 6. 步骤8中，支持用户与终端设备建立一对多绑定关系。 |
| **检验结果：** | 1. 如图，可以配置用户与设备的绑定策略      1. 如图，绑定数量达到策略临界值      1. 如图，配置一对多绑定策略     终端可以绑定，如图     1. 客户端侧可以接触用户与设备的绑定，如图      1. 管控侧支持设备解绑，如图   FInu0WYLDc |

* + - 1. 链路安全
         1. 安全传输

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 通过零信任业务安全平台访问业务系统，全链路都进行双向加密传输； 2. 加密传输采用经核准的密码算法和技术； 3. 支持国密算法进行加密传输。 |
| **预置条件**： | 1. 完成业务安全平台的部署； 2. 准备抓包工具，如：wireshark。 |
| **验证流程：** | 步骤1：登录系统，发起业务请求；  步骤2：通过抓包工具抓取链路中传输的数据包；  步骤3：查看请求和响应数据包中的加密情况；  步骤4：确定密码算法和技术是否符合规定；  步骤5：确定密码算法是否为国密。 |
| **预期结果：** | 1. 请求和响应数据包中的数据均是加密数据； 2. 密码算法和技术符合规定； 3. 支持国密算法进行加密传输。 |
| **检验结果：** | 1. 1\*.\*.\*.65为本机IP地址，48.1\*\*.\*\*.11为服务端IP地址（敏感数据已加密处理）   sBTjsYd0Wc   1. 加密算法：TLS\_CHACHA20\_POLY1305\_SHA256 (0x1303)   O13YOb5FfW   1. 暂不支持国密算法 |

* + - * 1. 网络隐身

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 系统不对外暴露任何TCP、UDP端口； 2. 在完成单包认证前，默认拒绝一切TCP连接，在完成单包认证后，才允许主体对资源的访问。 |
| **预置条件**： | 1. 准备端口扫描工具，如：Nmap； 2. 完成业务安全平台的部署，代理相关业务系统。 |
| **验证流程：** | 步骤1：未登录系统时，利用端口扫描工具扫描系统是否开放了TCP、UDP端口，尝试访问被代理的业务系统；  步骤2：登录系统后，利用端口扫描工具扫描系统是否开放了TCP、UDP端口，尝试访问被代理的业务系统。 |
| **预期结果：** | 1. 步骤1中，端口扫描工具无法扫描到任何开放的TCP、UDP端口，无法访问被代理的业务系统； 2. 步骤2中，端口扫描工具无法扫描到任何开放的TCP、UDP端口，可成功访问被代理的业务系统。 |
| **检验结果：** | 1）管控已配置放通1-65535端口访问  11  2）云枢可正常访问已搭建的80、90端口内网应用  22  3）使用Nmap工具进行端口扫描，显示未开启任何端口  33  44 |

* + - 1. 身份安全
         1. 用户身份认证

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 系统自身具备多种认证方式，且支持多因素认证登录，包括账号密码、动态口令、证书认证、人脸、声纹、短信验证码等至少两种认证方式； 2. 支持通过标准协议对接第三方认证源，包括LDAP、Radius、AD等至少一种协议； 3. 管理平台支持认证方式的相关配置。 |
| **预置条件**： | 1. 完成业务安全平台的部署； 2. 准备认证相关的软硬件。 |
| **验证流程：** | 步骤1：登录管理平台，查看所支持的认证方式，分别配置各种认证方式进行认证检验，打开登录页面，进行多因素认证登录；  步骤2：对接第三方认证源，并进行登录验证。 |
| **预期结果：** | 1. 步骤1中，管理平台支持认证方式的相关配置，系统自身具备多种认证方式，包括账号密码、动态口令、证书认证、人脸、声纹、短信验证码等至少两种认证方式，支持多因素认证； 2. 步骤2中，支持通过标准协议对接第三方认证源，包括LDAP、Radius、AD等至少一种协议。 |
| **检验结果：** | 1. 登录时支持OTP、短信、邮箱的二次认证。     客户端登录需要二次认证，如图     1. 云枢平台支持钉钉、企微、飞书、LDAP、WindowsAD以及自定义组织的接入，如图 |

* + - * 1. 终端身份标识

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 支持终端设备唯一标识，如：设备指纹、设备证书及其他唯一标识。 |
| **预置条件：** | 1. 准备多台终端设备； 2. 分别在上述设备上完成相关部署。 |
| **验证流程：** | 步骤1：分别获取各台设备的唯一标识，并进行比较。 |
| **预期结果：** | 1. 各台设备的唯一标识不同。 |
| **检验结果：** | 1. 设备一   VFBjHMMbt2   1. 设备二   2Ocvsges0s |

* + - * 1. 应用身份标识

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 每个业务应用都具备唯一的标识，不因应用信息的更改而变化。 |
| **预置条件**： | 1. 完成业务安全平台的部署，准备两个业务应用系统。 |
| **验证流程：** | 步骤1：分别代理两个不同的业务系统，查看两个业务应用身份标识是否一致；  步骤2：登录管理平台，修改其中一个业务系统的配置，查看业务应用身份标识是否变化。 |
| **预期结果：** | 1. 步骤1中，两个业务系统的身份标识不一致； 2. 步骤2中，业务应用身份标识不变。 |
| **检验结果：** | 1. 如图，每台设备有唯一标识      1. 如图，原本的设备id，更改接入网络和设备所有权后，设备id并没有改变 |

* + - 1. 数据安全
         1. 数字水印

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 具备访问业务系统时屏幕加载数字水印。支持明文水印、矢量水印、二维码水印、盲水印等至少一种水印技术； 2. 支持自定义水印大小、显示内容等； 3. 支持显示用户名及时间。 |
| **预置条件**： | 1. 完成业务安全平台的部署及B/S应用对接。 |
| **验证流程：** | 步骤1：登录管理平台，配置水印策略，自定义水印大小、内容；  步骤2：下发水印策略给账户A；  步骤3：分别使用账户A和账户B访问业务系统，查看此时屏幕是否自动加载水印。 |
| **预期结果：** | 1. 账户A访问业务系统时，屏幕自动加载水印； 2. 账户B访问业务系统时，屏幕未加载水印。 |
| **检验结果：** | 1. 用户A访问业务系统自动加载水印，如图      1. 用户B访问业务系统时没有水印，如图 |

* + - * 1. 数据脱敏

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 系统支持数据脱敏能力，可对敏感数据进行处理展示； 2. 支持脱敏白名单功能，对特权用户不进行数据脱敏。 |
| **预置条件**： | 1. 完成业务安全平台的部署及B/S应用对接； 2. 准备普通用户A，特权用户B。 |
| **验证流程：** | 步骤1：登录管理平台，对敏感数据进行脱敏配置，如身份证号；  步骤2：对用户A与B进行不同的敏感数据权限设置，将用户B加入脱敏白名单；  步骤3：用户A访问Web应用查看敏感数据，验证敏感数据中部分内容是否被替换或隐藏；  步骤4：用户B访问Web应用查看敏感数据，验证敏感数据中部分内容是否被替换或隐藏。 |
| **预期结果：** | 1. 步骤3中，用户A访问时，敏感数据中部分内容被替换或隐藏； 2. 步骤4中，用户B访问时，敏感数据中部分内容未被替换或隐藏。 |
| **检验结果：** | 接入组织配置信息脱敏：    用户个人信息脱敏： |

* + - * 1. 安全沙箱

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 支持在安全沙箱内代理业务系统； 2. 安全沙箱数据落地加密； 3. 安全沙箱支持数据管控，包括双向隔离、数据导出、数据导入； 4. 安全沙箱内仅能访问策略允许的网络资源； 5. 安全沙箱内可使用的应用进程支持白名单模式进行管理； 6. 多安全沙箱支持； 7. 安全沙箱支持自我保护能力，可提供禁止截屏，数字水印等多种防护机制。 |
| **预置条件**： | 1. 完成业务安全平台的部署。 |
| **验证流程：** | 步骤1：登录管理平台，下发安全沙箱策略给用户A，策略内容为在安全沙箱内，仅允许通过chrome浏览器访问业务系统，数据落地在安全沙箱1中，且安全沙箱1与本地数据双向隔离；  步骤2：用户A登录系统后，查看其：   1. 是否自动拉起安全沙箱桌面； 2. 是否只能通过chrome浏览器访问业务系统； 3. 通过安全沙箱下载的数据是否加密存储在安全沙箱1中，本地存储空间不可见； 4. 安全沙箱数据是否与本地数据双向隔离；   步骤3：用户B登录系统后，查看其：   1. 是否自动拉起安全沙箱桌面； 2. 是否只能通过chrome浏览器访问业务系统； 3. 通过安全沙箱下载的数据是否加密存储在安全沙箱1中，本地存储空间不可见； 4. 安全沙箱数据是否与本地数据双向隔离。 |
| **预期结果：** | 1. 步骤2中：用户A登录系统后，自动拉起安全沙箱桌面；只能通过chrome浏览器访问业务系统；通过安全沙箱下载的数据加密存储在安全沙箱1中，本地存储空间不可见；安全沙箱数据与本地数据双向隔离； 2. 步骤3中：用户B登录系统后，不会拉起安全沙箱。 |
| **检验结果：** | 1）暂不支持此功能 |

* + - 1. 资源协议支持
         1. HTTP/HTTPS

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 支持HTTP和HTTPS协议的应用接入。 |
| **预置条件**： | 1. 分别准备基于HTTP和HTTPS协议的应用各一个。 |
| **验证流程：** | 步骤1：登录管理平台，配置接入HTTP和HTTPS协议的应用各一个；  步骤2：登录系统，访问接入的应用。 |
| **预期结果：** | 1. 可正常接入并访问HTTP和HTTPS协议的应用。 |
| **检验结果：** | 1. http应用，如图   截屏2022-11-03 20.06.13  2）https应用，如图  截屏2022-11-03 20.04.47 |

* + - * 1. TCP/UDP

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 支持TCP和UDP协议的应用接入。 |
| **预置条件**： | 1. 分别准备基于TCP和UDP协议的应用各一个。 |
| **验证流程：** | 步骤1：登录管理平台，配置接入TCP和UDP协议的应用各一个；  步骤2：登录系统，访问接入的应用。 |
| **预期结果：** | 1. 可正常接入并访问TCP、UDP应用。 |
| **检验结果：** | 1. TCP应用，配置如图     访问，如图    UDP应用，配置如图    访问，如图，（通过iperf3打流） |

* + - * 1. 统一门户

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 系统支持B/S应用统一门户能力，仅显示用户有权限的全部业务应用； 2. 系统支持C/S应用统一门户能力，访问时可自动拉起相关客户端软件。 |
| **预置条件**： | 1. 完成业务安全平台的部署，准备B/S应用和C/S应用。 |
| **验证流程：** | 步骤1：管理平台配置统一门户展示的业务应用；  步骤2：登录系统，查看统一门户内的应用；  步骤3：分别访问门户中的B/S应用和C/S应用。 |
| **预期结果：** | 1. 步骤2中，系统支持统一门户，门户内的应用与管理平台配置的应用一致； 2. 步骤3中，用户可直接在门户中访问B/S应用和C/S应用，其中访问C/S应用时可自动拉起相关客户端软件。 |
| **检验结果：** | 1. 如图所示，云枢平台支持以部门、用户组、人员的维度配置应用访问策略，门户应用的可见范围与此处策略关联。   例如：配置用户A可访问全部应用，用户A登录门户，可访问全部门户应用。    用户B登录门户，没有可见应用     1. 云枢平台暂不支持唤起客户端 |

* + - * 1. 单点登录

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 支持标准协议类型单点登录，如：JWT、OIDC、CAS、Oauth2.0、SAML等； 2. 支持非标准协议类型单点登录，支持以前端密码代填、后端密码代填的方式实现SSO。 |
| **预置条件**： | 1. 准备标准协议和非标准协议的业务应用系统。 |
| **验证流程：** | 步骤1：登录管理平台，查看所支持的单点登录协议，并对标准协议业务应用系统配置单点登录，登录系统，访问业务应用，查看单点登录效果；  步骤2：对非标准协议业务应用系统配置单点登录，登录系统，访问业务应用，查看单点登录效果。 |
| **预期结果：** | 1. 步骤1中，系统支持标准协议业务系统的单点登录，包JWT、OIDC、CAS、Oauth2.0、SAML等协议； 2. 步骤2中，系统支持非标准协议业务系统的单点登录。 |
| **检验结果：** | 1. 云枢平台门户应用目前仅支持CAS协议的单点登录。CAS协议登录如下图： |

* + - 1. 全域风险感知
         1. 身份信息采集

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 产品自身具备身份信息采集及风险感知能力，包括用户、设备、应用等多个维度。 |
| **预置条件**： | 1. 完成业务安全平台的部署。 |
| **验证流程：** | 步骤1：登录系统，从用户、设备、应用等多个维度模拟触发风险；  步骤2：登录管理平台，查看风险日志等内容。 |
| **预期结果：** | 1. 风险日志内容中可看到用户、设备、应用等多个维度的风险信息。 |
| **检验结果：** | 1. 1.云枢平台的风险感知能力体现在合规检查和动态策略，有关身份和应用的维度多以动态策略中体现。如图： 2. mVRwhVD2sM   KrICxnNHmo   1. 日志审计中会有相应的处置记录，如图 |

* + - * 1. 环境信息采集

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 产品自身具备环境信息采集及风险感知能力，包括硬件、操作系统、网络、外设、协议等多个维度。 |
| **预置条件**： | 1. 完成业务安全平台的部署，准备上述各维度的演示设备及工具。 |
| **验证流程：** | 步骤1：登录系统，从硬件、软件、操作系统、网络、外设等多个维度模拟触发风险；  步骤2：登录管理平台，查看风险日志等内容。 |
| **预期结果：** | 1. 步骤2中，风险日志内容中可看到硬件、软件、操作系统、网络、外设等多个维度的风险信息。 |
| **检验结果：** | 1. 环境信息的风险感知能力体现在合规检查中，如图：   截屏2022-11-04 15.02.40  合规检测触发，如图    动态策略触发，如图    处理日志，如图 |

* + - * 1. 行为信息采集

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 产品自身具备行为信息采集及风险感知能力，包括位置、网络、时间等多个维度。 |
| **预置条件**： | 1. 完成业务安全平台的部署，准备上述各维度的演示设备及工具。 |
| **验证流程：** | 步骤1：登录系统，从位置、网络、时间等多个维度模拟触发风险；  步骤2：登录管理平台，查看风险日志等内容。 |
| **预期结果：** | 1. 风险日志内容中可看到位置、网络、时间等多个维度的风险信息。 |
| **检验结果：** | 1. 如图     策略触发，如图 |

* + - * 1. 第三方风险感知平台

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 产品支持对接第三方风险感知平台。 |
| **预置条件**： | 1. 完成业务安全平台的部署，准备一个第三方风险感知平台。 |
| **验证流程：** | 步骤1：对接第三方风险感知平台；  步骤2：登录系统，从设备、IP、时间段、行为、位置、账号等多个维度模拟触发风险；  步骤3：登录管理平台，查看风险日志等内容。 |
| **预期结果：** | 1. 支持对接第三方风险感知平台，且风险日志内容中可看到多维度的风险信息。 |
| **检验结果：** | 1. 云枢支持第三方风险感知平台，如支持将日志内容投递不同的第三方平台   ab |

* + - 1. 持续信任评估
         1. 规则评估

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 基于获取到的风险信息，通过规则匹配的方式进行设备、IP、时间段、行为、位置、账号等多维度的持续信任评估、输出灵活的风险决策。 |
| **预置条件**： | 1. 完成业务安全平台的部署，准备上述各维度的演示设备及工具。 |
| **验证流程：** | 步骤1：登录管理平台，分别配置上述各维度的风险规则；  步骤2：登录系统，分别模拟触发上述风险规则；  步骤3：管理平台查看风险规则触发前后信任度及风险等级的变化，如：风险日志查看等。 |
| **预期结果：** | 1. 支持设备、IP、时间段、行为、位置、账号等多维度的持续信任评估及风险决策； 2. 信任度或风险等级随风险规则触发而变化。 |
| **检验结果：** | 1. 云枢平台通过风险检查和动态策略感知风险后，有多种处置方式可选。如图，   以数据高风险为例，配置触发条件为高，如图    风险员工等级满足“高”，如图    触发动态策略，如图 |

* + - * 1. AI模型评估

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 基于获取到的风险信息，通过AI模型进行设备、IP、时间段、行为、位置、账号等多维度的持续信任评估、输出灵活的风险决策。 |
| **预置条件**： | 1. 完成业务安全平台的部署，准备上述各维度的演示设备及工具。 |
| **验证流程：** | 步骤1：登录管理平台，配置风险模型；  步骤2：登录系统，从多个维度模拟触发上述风险模型；  步骤3：管理平台查看风险模型触发前后信任度及风险等级的变化，如：风险日志查看等。 |
| **预期结果：** | 1. 支持基于AI模型进行设备、IP、时间段、行为、位置、账号等多维度的持续信任评估及风险决策； 2. 信任度或风险等级随风险模型触发而变化。 |
| **检验结果：** | 1. 非公司设备登录触发风险决策      1. 非常用网络接入触发风险决策      1. 非常用时间使用触发风险决策      1. 访问钓鱼网站触发风险决策      1. 账号异地使用触发风险决策 |

* + - 1. 动态访问控制
         1. 基于角色的访问控制

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 基于用户/用户组/角色组进行业务应用的授权； 2. 用户无法访问未授权的业务应用。 |
| **预置条件**： | 1. 完成业务安全平台的部署，准备两个相关业务应用。 |
| **验证流程：** | 步骤1：登录管理平台，对用户/用户组/角色组A授权业务应用1的访问权限，对用户/用户组/角色组B授权业务应用2的访问权限；  步骤2：使用用户A或用户组/角色组A中的用户登录系统，分别访问业务应用1和2，查看效果；  步骤3：使用用户B或用户组/角色组B中的用户登录系统，分别访问业务应用1和2，查看效果。 |
| **预期结果：** | 1. 用户A或用户组/角色组A中的用户可正常访问业务应用1，不可访问业务应用2； 2. 用户B或用户组/角色组B中的用户可正常访问业务应用2，不可访问业务应用1。 |
| **检验结果：** | 1. 用户A可访问应用1，不可访问应用2     可以访问jira，不可访问nginx     1. 用户B可访问应用2，不可访问应用1     可以访问nginx，不可访问jira |

* + - * 1. 基于属性的访问控制

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 支持基于环境属性如：IP、时间、位置、终端环境）、实体属性如：工号、手机号、职级等）、行为属性如：读取、写入、高频访问敏感资源）等信息的访问控制。 |
| **预置条件**： | 1. 完成业务安全平台的部署，准备上述各维度的演示设备及工具。 |
| **验证流程：** | 步骤1：登录管理平台，配置基于上述属性的访问控制策略，如：仅允许可信IP段访问核心业务系统A；  步骤2：使用接入可信IP段的设备A访问业务系统1，查看效果；  步骤3：使用未接入可信IP段的设备B访问业务系统1，查看效果；  步骤4：配置其他属性的访问控制策略，查看策略是否生效。 |
| **预期结果：** | 1. 步骤2中，设备A可正常访问业务系统1； 2. 步骤3中，设备B不能访问业务系统1； 3. 步骤4中，系统支持多种属性的访问控制。 |
| **检验结果：** | 1. 控制台配置      1. 设备A可正常访问业务系统1（nginx）     设备B不可访问业务系统1     1. 其他多种属性的访问控制 |

* + - * 1. 风险分级处置

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 基于访问策略对风险进行分级，不同的风险级别对应不同的处置方式，处置结果包括阻断、放行、二次认证、动态权限伸缩、会话登出、锁定账号等至少三种。 |
| **预置条件**： | 1. 完成业务安全平台的部署，准备演示所需设备及工具。 |
| **验证流程：** | 步骤1：登录管理平台，配置访问控制策略，如：非工作时间段访问业务应用时，处置方式为阻断；  步骤2：非工作时间段内登录系统，访问业务应用，查看效果；  步骤3：修改步骤1中的处置方式分别为放行、二次认证、动态权限伸缩、会话登出、锁定账号等；  步骤4：非工作时间段内再次登录系统，访问业务应用，查看效果。 |
| **预期结果：** | 1. 步骤2中，访问业务应用时被阻断； 2. 步骤4中，支持多种处置方式，包括放行、二次认证、动态权限伸缩、会话登出、锁定账号等。 |
| **检验结果：** | 1. 云枢中的风险处理有6中，如图，针对配置的风险等级可灵活配置处置方式。   Y8fJXQVtRl  2）云枢暂不支持 |

* + - * 1. 基于策略的访问控制

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 融合基于角色的访问控制、基于属性的访问控制能力，支持风险策略的综合评估，实现资源细粒度访问控制，如：用户+IP属性的访问控制策略。 |
| **预置条件**： | 1. 完成业务安全平台的部署，准备演示所需设备及工具。 |
| **验证流程：** | 步骤1：登录管理平台，配置访问控制策略，如：仅允许用户A在可信IP段内访问业务系统1；  步骤2：使用接入可信IP段的设备登录用户A访问业务系统1，查看效果；  步骤3：使用未接入可信IP段的设备登录用户A访问业务系统1，查看效果；  步骤4：使用接入可信IP段的设备登录用户B访问业务系统1，查看效果；  步骤5：使用未接入可信IP段的设备登录用户B访问业务系统1，查看效果；  步骤6：配置其他的访问控制策略，查看策略是否生效。 |
| **预期结果：** | 1. 步骤2中，成功访问业务系统1； 2. 步骤3中，不能访问业务系统1； 3. 步骤4中，不能访问业务系统1； 4. 步骤5中，不能访问业务系统1； 5. 步骤6中，支持多种基于属性的访问控制策略。 |
| **检验结果：** | 允许用户A在可信IP段内访问业务系统1（nginx）的策略配置；  可信IP段配置信息：10.1.2.10/16     1. 使用接入可信IP段的设备登录用户A访问业务系统1，可以访问      1. 使用未接入可信IP段的设备登录用户A访问业务系统1，无法访问      1. 使用接入可信IP段的设备登录用户B访问业务系统1，无法访问      1. 使用未接入可信IP段的设备登录用户B访问业务系统1，无法访问      1. 支持多种基于属性的访问控制策略 |

* + - 1. 安全管理平台
         1. 账户管理

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 本地账户管理：支持本地账户的创建、批量导入、修改、删除等，提供用户组及组织机构管理能力，并可针对用户组进行授权； 2. 第三方账户管理系统对接：支持通过Radius、LDAP等方式对接第三方认证体系，支持同步第三方对应的账户、组织架构等信息。 |
| **预置条件**： | 1. 完成业务安全平台的部署，准备第三方账户管理系统，如4A、IAM等。 |
| **验证流程：** | 步骤1：登录管理平台，对账户进行创建、批量导入、修改、删除等操作，查看效果；  步骤2：创建组织结构及用户组，并对用户组进行业务应用授权；  步骤3：分别使用用户组中的用户访问授权的业务系统，查看效果；  步骤4：使用系统与第三方账户管理系统对接，如：4A、IAM等；  步骤5：查看账户信息、组织架构同步情况。 |
| **预期结果：** | 1. 步骤1中，管理平台支持账户创建、批量导入、修改、删除等基础功能； 2. 步骤2中，管理平台支持组织结构和用户组管理及基于用户组的应用授权； 3. 步骤3中，用户组中的用户可成功访问授权的业务系统； 4. 步骤5中，系统支持与第三方账户管理系统对接，可进行账户信息、组织架构同步。 |
| **检验结果：** | 1. 云枢平台支持创建自定义账户以及接入第三方的身份源。如图，     自定义组织支持单个人员添加和批量人员导入，如图，  截屏2022-11-03 19.33.37  支持人员的修改和删除，如图，    支持创建用户组，如图，  截屏2022-11-03 19.34.50  应用访问权限可根据人员部门用户组精确分配，如图 |

* + - * 1. 设备管理

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 管理平台支持对设备通过分组或标签的形式进行归类管理； 2. 管理平台支持展示设备名称、设备指纹、操作系统类型、设备IP、上线时间等信息； 3. 支持对全部设备的管理维护，将设备与账户进行绑定，实现身份安全可控，如设备锁定。 |
| **预置条件**： | 1. 完成业务安全平台的部署，准备移动和PC设备各一台。 |
| **验证流程：** | 步骤1：登录管理平台，查看是否可对设备通过分组或标签的形式进行归类管理；  步骤2：查看设备相关信息；  步骤3：对设备进行管理操作，如：锁定移动端的设备，分别使用移动端设备和PC端设备登录系统，查看效果。 |
| **预期结果：** | 1. 步骤1中，管理平台支持对设备通过分组或标签的形式进行归类管理； 2. 步骤2中，管理平台展示终端设备的相关信息，包括设备名称、设备指纹、操作系统类型、设备IP、上线时间等； 3. 步骤3中，移动端设备不能登录系统，PC端设备可正常登录系统。 |
| **检验结果：** | 云枢平台的设备支持分组分类管理，如图，  tEkmIpTrfy  可查看某一台设备详情信息，如图    可对设备进行，删除、隔离、挂失、卸载操作。 |

* + - * 1. 资源管理

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 应用管理：支持本地应用的创建、修改、删除、应用授权等全生命周期的管理。 |
| **预置条件**： | 1. 完成业务安全平台的部署。 |
| **验证流程：** | 步骤1：登录管理平台，对应用进行创建、批量导入、修改、删除等操作，查看效果。 |
| **预期结果：** | 1. 步骤1中，管理平台支持应用创建、修改、删除、授权等基础功能。 |
| **检验结果：** | 1. 云枢平台支持完善的应用管理能力，如图，   截屏2022-11-03 19.37.43  添加应用，如图，  Xox7bxkeEe |

* + - * 1. 策略管理

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 支持终端安全基线策略、动态访问控制策略、认证策略等策略的管理； 2. 支持对策略的全生命周期管理，包括：策略添加，修改，删除等。 |
| **预置条件**： | 1. 完成业务安全平台的部署。 |
| **验证流程：** | 步骤1：登录管理平台，查看是否具备终端安全基线策略、动态访问控制策略、认证策略等策略的管理能力；  步骤2：对相关策略进行添加，修改，删除等操作。 |
| **预期结果：** | 1. 步骤1中，支持终端安全基线策略、动态访问控制策略、认证策略等策略的管理； 2. 步骤2中，支持对策略的全生命周期管理，包括：策略添加，修改，删除等。 |
| **检验结果：** | 1. 合规检查策略，如图   截屏2022-11-03 19.39.58  安全基线，如图  截屏2022-11-03 19.40.45  访问控制策略，如图  截屏2022-11-03 19.41.22 1  动态决策策略，如图  截屏2022-11-03 19.41.56 |

* + - * 1. 日志审计

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 具备日志审计功能，包括但不限于用户日志、管理员日志、应用日志、流量日志、终端日志、风险日志等； 2. 日志中所展示的字段，包括但不限于用户、设备、IP、时间、事件等信息； 3. 支持通过syslog/API接口推送/拉取日志。 |
| **预置条件**： | 1. 完成业务安全平台的部署。 |
| **验证流程：** | 步骤1：登录管理平台，查看是否支持用户日志、管理员日志、应用日志、流量日志、终端日志、风险日志等；  步骤2：查看日志中展示的字段；  步骤3：开启syslog/API服务，配置推送/拉取内容、时间及日志服务器等信息；  步骤4：查看日志服务器是否获取日志。 |
| **预期结果：** | 1. 管理平台可查看用户日志、管理员日志、应用日志、流量日志、终端日志、风险日志等； 2. 日志中包括以下字段：用户、设备、IP、时间、事件等； 3. 日志服务器可获取到相关的日志。 |
| **检验结果：** | 1. 内网访问日志，如图   SAl8l2vFrj  动态决策日志，如图  ISuTeF2YX0  合规检查日志，如图，  IMGbVp7Xqt  安全审计日志，如图  截屏2022-11-03 19.44.22  操作日志，如图  截屏2022-11-03 19.44.52 |

* + 1. 性能效率
       1. 传输特性
          1. 传输效率

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 支持加密隧道高效传输，加密隧道数据传输速率达到非隧道传输数据传输速率的70%以上。 |
| **预置条件**： | 1. 完成业务安全平台的部署，准备传输速率检验工具。 |
| **验证流程：** | 步骤1：未登录系统，直接通过业务应用原始路径进行访问，检验并记录传输速率；  步骤2：登录系统，访问同一业务应用，检验并记录传输速率；  步骤3：对比隧道传输效率与非隧道传输效率。 |
| **预期结果：** | 1. 加密隧道数据传输速率达到非隧道传输数据传输速率的70%以上。 |
| **检验结果：** | 1. 以github为例，未连接云枢时，如图      1. 开启云枢访问以后，如图 |

* + - 1. 时间特性
         1. 界面响应及数据处理时间

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 系统响应一个用户操作的时间满足规定的目标； 2. 系统完成一个作业或一个异步进程的周转时间满足规定的目标。 |
| **预置条件**： | 1）完成业务安全平台的部署。 |
| **验证流程：** | 步骤1：打开管理平台界面；  步骤2：启动任意一个数据处理功能，查看系统实现这一功能所用的时间是否符合预期。 |
| **预期结果：** | 1）系统响应用户操作的时间符合预期；  2）系统完成两个任务的周转时间与单独执行时满足规定的目标。 |
| **检验结果：** | 1. 数据处理以日志审计为例，数据量较大的情况下，如图     多次刷新加载，时间符合预期，如图 |

* + - 1. 资源利用性
         1. 静默状态所消耗资源

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：  1）静默状态下，所消耗的系统资源（CPU负载、内存使用、磁盘利用率）符合规定的目标，系统占用CPU不能超过10%，内存占用不超过16G，磁盘占用不超过30G。 |
| **预置条件**： | 1）完成业务安全平台的部署。 |
| **验证流程：** | 步骤1：使系统处于静默状态；  步骤2：检验系统资源占用率。 |
| **预期结果：** | 1）实验结果符合要求。 |
| **检验结果：** | 1. 云枢客户端资源占用率如图 |

* + 1. 安全性
       1. 安全身份
          1. 身份唯一标识

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：  1）对用户身份进行标识和鉴别，身份标识具有唯一性。 |
| **预置条件**： | 1）完成业务安全平台的部署。 |
| **验证流程：** | 步骤1：检验产品是否对其用户进行唯一性标识，如不允许创建重名用户。 |
| **预期结果：** | 1）产品确保在用户进行操作之前，对用户进行唯一的身份识别。 |
| **检验结果：** | 1. 云枢平台每个用户都有唯一的用户id，但是这个id只能后台查看。如图     用户可感知的唯一性体现在添加用户是手机号和邮箱重复提示用户已存在，如图 |

* + - * 1. 登录失败处理

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：  1）管理平台及客户端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。 |
| **预置条件**： | 1）完成业务安全平台的部署。 |
| **验证流程：** | 步骤1：尝试连续多次失败登录产品，触发产品的登录失败处理功能，检查产品采用何种机制防止用户进一步进行尝试。 |
| **预期结果：** | 1）输入错误口令达到设定的最大失败次数后，产品终止可信主机或用户建立会话的过程，并对该失败用户做禁止访问处理。 |
| **检验结果：** | 1. 云枢平台登录失败次数过多（10次）后，账号密码登录会被限制，提示“登录错误次数过多”，如图 |

* + - * 1. 会话超时处理

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：  1）管理平台及客户端具有会话超时处理功能。 |
| **预置条件**： | 1）完成业务安全平台的部署。 |
| **验证流程：** | 步骤1：登录系统后，在超时限定时间内无任何操作，查看会话是否自动退出。 |
| **预期结果：** | 1）登录系统后，在超时限定时间内无任何操作，会话自动退出。 |
| **检验结果：** | 1. 云枢平台支持过期强制登录功能，如图   VZJaQbW9BW |

* + - * 1. 口令复杂度

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：  1）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。 |
| **预置条件**： | 1）完成业务安全平台的部署。 |
| **验证流程：** | 步骤1：检验产品是否提供了口令复杂度校验机制，是否不允许用户设置弱口令，如空口令、纯数字等。 |
| **预期结果：** | 1）产品提供了口令复杂度校验机制。 |
| **检验结果：** | 1. 主账号创建子账号，首次登录时设置子账号登录密码，要求满足口令复杂度，如图 |

* + - * 1. 默认口令强制修改

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：  1）当产品中存在默认口令时，强制用户对默认口令进行修改，以减少用户身份被冒用的风险。 |
| **预置条件**： | 1）完成业务安全平台的部署。 |
| **验证流程：** | 步骤1：产品存在默认口令时，检查产品是否提示并强制用户对默认口令进行修改。 |
| **预期结果：** | 1）产品存在默认口令时，产品能提示并强制用户对默认口令进行修改。 |
| **检验结果：** | 合规检测强制用户对弱口令进行修改，不修改会强制断开内网且无法连接 |

* + - 1. 安全管理
         1. 可信主机

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：  1）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地址。 |
| **预置条件**： | 1）完成业务安全平台的部署。 |
| **验证流程：** | 步骤1：验证产品是否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地址。 |
| **预期结果：** | 1）产品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地址。 |
| **检验结果：** | 指定IP白名单才能访问控制台进行管理  vO3jrIHL6P |

* + - * 1. 管理通道加密

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：  1）远程管理过程中，管理端与产品之间的所有通信数据应非明文传输。 |
| **预置条件**： | 1）完成业务安全平台的部署。 |
| **验证流程：** | 步骤1：验证产品在远程管理过程中，管理端与产品之间的所有通信数据是否为非明文传输。 |
| **预期结果：** | 1）产品在远程管理过程中，管理端与产品之间的所有通信数据为非明文传输。 |
| **检验结果：** | 1. 本地IP地址：10.\*.\*.65，服务端测试IP地址：81.\*\*.\*\*\*.94（敏感数据已加密处理）   2nIWMsS61C |

* + - * 1. 集中管理

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：  1）支持集中管理，通过集中管理平台实现监控运行状态、下发安全策略。 |
| **预置条件**： | 1）完成业务安全平台的部署。 |
| **验证流程：** | 步骤1：验证产品是否支持集中管理，是否能通过集中管理平台实现监控运行状态、下发安全策略。 |
| **预期结果：** | 1）产品支持集中管理，并通过集中管理平台实现监控运行状态、下发安全策略。 |
| **检验结果：** | 1. 专线机器系统使用状态及运行状态   t3sM1VmdTa |

* + - * 1. 管理员三权分立

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：  1）应区分管理员角色，能划分为系统管理员、安全管理员和系统审计员；  2）系统管理员负责对软件环境日常运行的管理和维护，以及对系统的备份和操作系统恢复；系统审计员负责对系统中的日志进行安全审计；  3）安全管理员负责业务配置、应用管理、授权管理等管理操作。  4）系统审计员负责对系统中的日志进行安全审计。 |
| **预置条件**： | 1）完成业务安全平台的部署。 |
| **验证流程：** | 步骤1：验证产品是否区分管理员角色，是否能划分系统管理员、安全管理员和系统审计员；  步骤2：验证三类管理员的权限是否符合上述要求，是否相互制约。 |
| **预期结果：** | 1）产品能区分管理员角色，能划分为系统管理员、安全管理员和系统审计员；  2）三类管理员的权限符合上述要求，且三类管理员角色权限相互制约。 |
| **检验结果：** | 1. 云枢平台有9中默认角色，另外可根据需要灵活配置角色赋予相应的权限。如图      1. 每种角色都有与角色相对应的权限，如图      1. 用该角色的子账号登录云枢平台，只有该角色的功能权限，如图 |
|  |  |

* + - 1. 自安全性
         1. 系统加固

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：  1）进行必要的裁剪，不提供多余的组件或网络服务。 |
| **预置条件**： | 1）完成业务安全平台的部署。 |
| **验证流程：** | 步骤1：查看产品文档，并验证产品的支撑系统是否进行了必要的裁剪，是否不提供多余的组件或网络服务。 |
| **预期结果：** | 1）产品支撑系统进行了必要的裁剪，不提供多余的组件或网络服务。 |
| **检验结果：** | 1. 部署服务器管控服务信息   img_v2_8917881f-0ee7-4b50-8c41-d9f85e700bfg |

* + - * 1. 漏洞自查

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：  1）不含已知中、高风险安全漏洞。 |
| **预置条件**： | 1）完成业务安全平台的部署。 |
| **验证流程：** | 步骤1：对产品进行安全性检验，验证是否不含已知的中、高风险安全漏洞。 |
| **预期结果：** | 1）产品不含已知中、高风险安全漏洞。 |
| **检验结果：** | 1. 云枢平台提供漏洞修复功能，如图。并且漏洞库会定时更新。   截屏2022-11-03 19.52.10 |

* + - * 1. 系统监控

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 可对自身环境进行安全监测，对安全监测项可进行配置； 2. 支持对服务器系统异常，如CPU、内存、硬盘、插拔硬件等进行监测； 3. 支持对服务器应用异常，如端口启停、关键文件修改等进行监测； 4. 支队对服务器网络异常，如网络上下行流量进行监控； 5. 发现异常时可通过邮件等形式实时告警。 |
| **预置条件**： | 1. 完成业务安全平台的部署； 2. 已配置安全监测项的配置规则。 |
| **验证流程：** | 步骤1：登录管理平台，对安全监测项可进行配置；  步骤2：分别模拟触发各安全监测项配置策略；  步骤3：查看是否接收到告警通知，并查看告警内容是否准确。 |
| **预期结果：** | 1. 当服务器出现系统异常，如CPU、内存、硬盘使用率超过预设置阈值、发生硬件插拔时，产生邮件等形式告警通知管理员； 2. 当服务器出现应用异常，如打开或关闭端口号、预配置的关键文件被修改时，产生邮件等形式告警通知管理员； 3. 当服务器出现网络异常，如网卡流量超过预配置阈值时，产生告警通知，产生邮件等告警通知管理员； 4. 告警通知内容可准确描述告警异常。 |
| **检验结果：** | 1. 云枢平台支持很多类型的监控告警，且阈值和时间都可以自定义设置，如图，例如，组织同步异常、专线联通异常、专线连通数异常、专线宽带异常、专线CPU使用率异常、专线内存使用率异常。   截屏2022-11-03 19.53.10 |

* + - 1. 密码要求
         1. 保密性

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 对系统中重要数据应采用经核准的密码算法、技术和产品进行加密存储。 |
| **预置条件**： | 1. 完成业务安全平台的部署及资源配置。 |
| **验证流程：** | 步骤1：查看后台管理系统存储的数据是否加密存储；  步骤2：查看后台管理系统配置，查看数据加密所采用的算法和技术。 |
| **预期结果：** | 1. 后台管理系统具备数据加密功能，且密码算法和技术合规有效。 |
| **检验结果：** | 1. 加密数据部分展示（mobile/email/pwd） |

* + - * 1. 完整性

|  |  |
| --- | --- |
| **能力要求：** | 产品应具备如下能力：   1. 对系统中重要数据应采用经核准的密码算法、技术和产品进行完整性保护。 |
| **预置条件**： | 1. 完成业务安全平台的部署及资源配置。 |
| **验证流程：** | 步骤1：查看后台管理系统存储的数据是否进行完整性保护；  步骤2：查看后台管理系统配置，查看数据加密所采用的算法和技术。 |
| **预期结果：** | 1. 后台管理系统具备数据完整性保护功能，且密码算法和技术合规有效。 |
| **检验结果：** | 1. 数据存储采用加密存储的方式 |

|  |  |  |
| --- | --- | --- |
|  | **此页为报告最后一页** |  |