KYLINSOFT
麒麟软件

# 银河麒麟安全中心

## 用户手册

麒麟软件有限公司

2022 年 8 月

# 目录

# 1. 概述

## 1.1 产品简介

安全中心是一款基于麒麟安全框架（KYSEC）和麒麟铠衣执行环境（KYLIN TEE）构建安全防护并行的双体系架构衍生出的图形化管理工具。提供以下防护能力：

核心安全功能层：包含可信度量、安全内存和指令流安全预检测功能，为PK体系提供安全底座，形成一体化主动免疫防御能力。

增强安全功能层：包含安全加固、账户保护、网络保护、应用执行控制和应用防护控制等功能，保障系统运行环境的安全和稳定， 进一步加固双体系安全底座。

## 1.2 产品亮点

安全中心集安全加固、账户保护、网络保护、应用保护、可信度量、安全内存和指令流安全预检测等功能于一体，全面保障系统运行环境的安全。

安全加固：提供安全服务、内核参数、安全网络、系统命令、系统审计、系统设置、潜在危险、文件权限、风险账户、磁盘检查、密码强度、账户锁定、系统安全、系统维护、资源分配等多维度的扫描与一键加固，及时发现并处理系统安全隐患。

账户保护：提供系统账户密码强度检查和账户锁定机制，实现对系统账户的统一管控，提升系统账户安全防御能力，有效防止密码被暴力破解。

网络保护：提供应用联网控制功能，实时防护未知应用网络行为，阻断主动外联及其它异常网络活动，提高网络访问安全性。

应用控制：提供应用程序执行控制功能，阻止未知软件、应用程序的恶意执行，避免木马病毒攻击，保障系统运行环境的安全可靠。

应用防护：提供进程防杀死、内核模块防卸载和文件防篡改功能，保护系统关键文件完整性，阻止系统关键应用服务异常中断。

可信度量：提供对计算子系统的主动度量（可信启动、静态度量、动态度量）和主动控制（可信策略）机制，保障系统执行环境的安全可靠。

安全内存：提供用户可配置的内存数据安全机制，保护系统内存数据安全。

指令流安全预检测：提供指令层监测漏洞攻击代码的执行功能，完全不依赖已知漏洞特征和已知攻击代码的特征，保障可信程序安全运行。

# 2. 系统安装

系统安装过程中在软件选择界面需要勾选麒麟安全增强工具分组，系统中才有安全中心的功能，如图 1 所示。


**图 1 软件选择-麒麟安全增强工具分组**

若用户在系统安装时未选择麒麟安全增强工具分组，则可以从仓库中安装对应的 ksc-defender 软件包，系统中才有安全中心的功能。

系统安装时已选择麒麟安全增强工具分组，进入系统后默认安全是关闭状态，支持用户在界面中开启安全，界面操作详情见 3.2 章节，命令行操作详情见 12.1 章节。

系统安装过程中在软件选择界面需要勾选 pks 组件分组，系统中才有 pks（安全内存、可信度量、指令流安全预检测）功能，如图 2 所示。

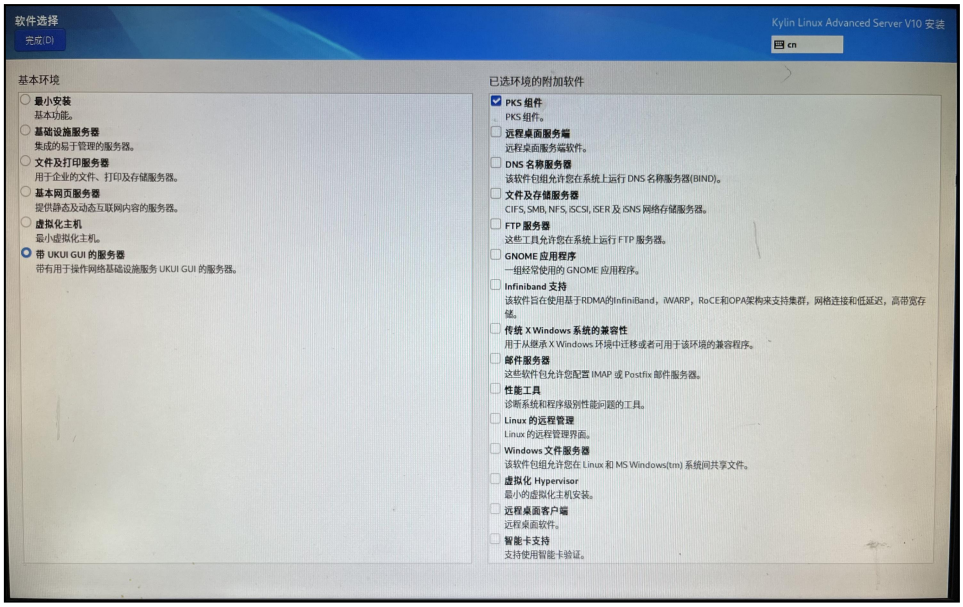


图 2 软件选择-pks 组件分组

# 3. 使用入门

## 3.1 软件位置

点击操作系统“开始菜单”，选择并点击“系统工具”菜单，选择并点击“安全中心”，打开安全中心软件界面，如图 3 所示。


图 3 开始菜单（打开安全中心）

## 3.2 安全设置

安全中心软件界面中点击≡图标，点击“设置”按钮，弹出“设置”弹窗，安全防护模式显示当前模式：自定义，支持选择安全防护设置功能，可选择关闭、推荐和安全优先及开启和关闭文件保护箱功能，如图 4 所示。

(1) 关闭：

(2) 推荐：麒麟特色安全防护机制，提供联网控制、执行控制和应用防护等功能。

(3) 安全优先：麒麟特色安全防护机制，提供联网控制、执行控制和应用防护等功能。同时，提供管理员分权功能，设立系统管理员、安全管理员和审计管理员，三元权限独立行使、相互制约。

(4) 自定义：当前模式与三种标准模式均不同，可以通过相关命令查看状态详情。

(5) 文件保护箱：可提供用户间数据隔离和加密保护功能。


**图 4 安全设置**

开启管理员分权功能时，界面伸缩展示三权管理员信息并提供新建管理员密码的功能，点击“设置密码”按钮，弹出“新建密码”弹窗，如图 5 和图 6 所示。

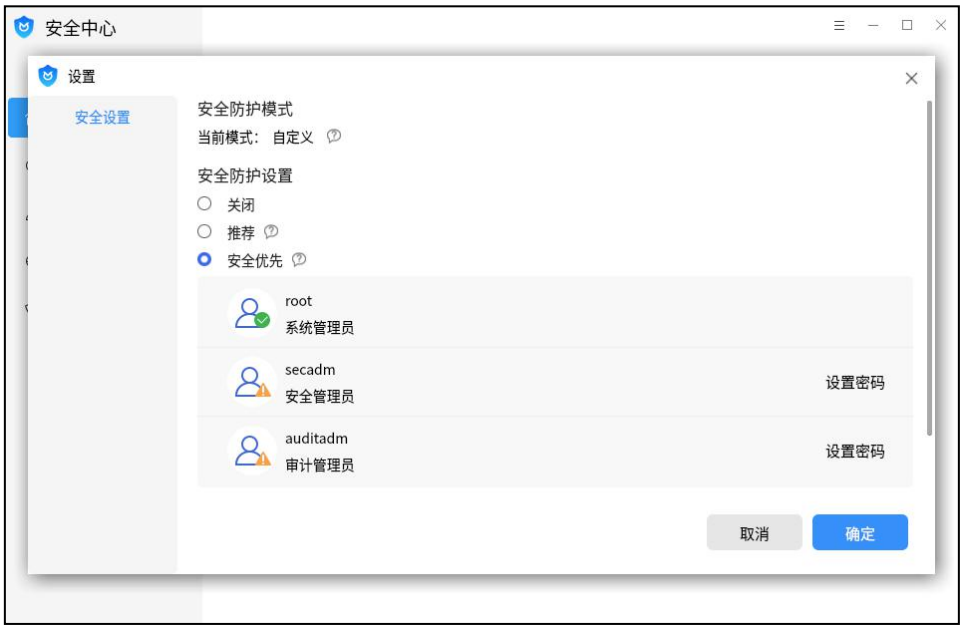


**图 5 开启管理员分权功能**

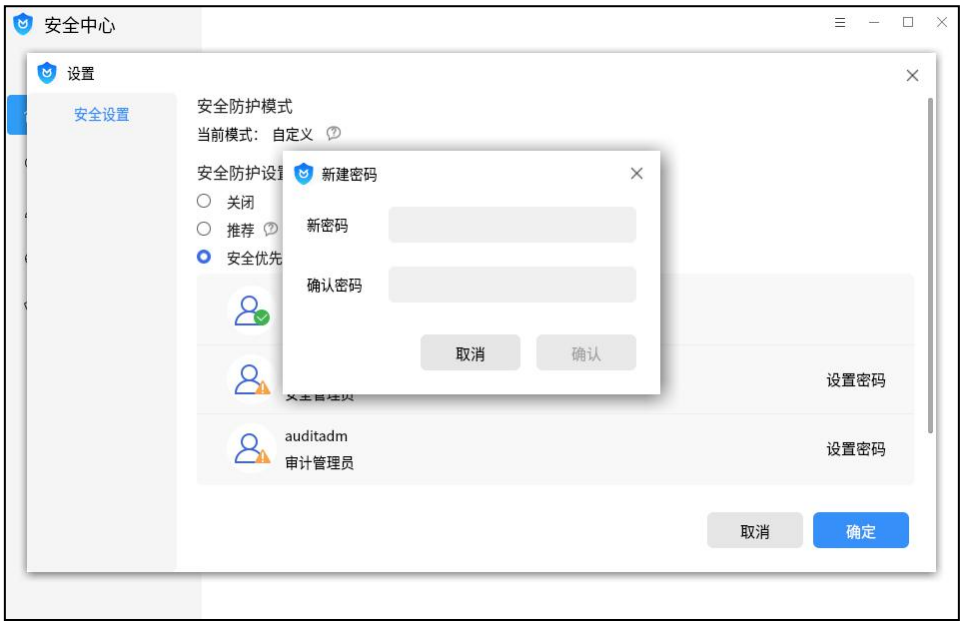


图 6 设置管理员密码

## 4. 首页

安装过程中未勾选 pks 组件，安全中心首页展示安全加固、账户保护、网络保护和应用保护四个功能模块的安全状况，可以让用户更直观了解系统当前的安全性和运行情况，同时提供各功能模块操作入口，方便用户进行功能快速跳转并对潜在风险进行及时处理，如图 7 所示。


图 7 安全中心首页（安装过程中未勾选 pks 组件）

安装过程中勾选 pks 组件，安全中心首页展示安全加固、账户保护、网络保护、应用保护、安全内存、可信度量和指令流安全预检测七个功能模块的安全状况，可以让用户更直观了解系统当前的安全性和运行情况，同时提供各功能模块操作入口，方便用户进行功能快速跳转并对潜在风险进行及时处理，如图 8 所示。


图 8 安全中心首页（安装过程中勾选 pks 组件）

## 5. 安全加固

系统从未加固时，安全加固首页显示如图 9 所示。

图 9 安全加固首页（从未加固）

系统扫描过后，安全加固首页显示上次扫描时间、扫描持续时间、发现问题项数和完成扫描项数等信息，如图 10 所示。


图 10 安全加固首页（显示上次扫描信息）

系统加固过后，安全加固首页显示上次加固时间、加固持续时间、发现问题项数和完成加固项数等信息，如图 11 所示。


图 11 安全加固首页（显示上次加固信息）

系统还原过后，安全加固首页显示上次还原时间、还原持续时间、等待加固项数和完成还原项数等信息，如图 12 所示。


**图 12 安全加固首页（显示上次还原信息）**

## 5.1 安全加固项

安全加固项主要包含一级和二级加固项。其中，一级加固项共 15 类，包括：安全服务、内核参数、安全网络、系统命令、系统审计、系统设置、潜在危险、文件权限、风险账户、磁盘检查、密码强度、账户锁定、系统安全、系统维护、资源分配。三级加固项共 77 项，均分为风险问题项。

## 5.2 安全加固模板

点击安全加固首页“全部项”文字按钮，选择下拉框中全部项、三级项及自定义模板，支持对全部加固项进行扫描加固、支持对安全三级加固项进行扫描加固、支持对自定义加固项进行扫描加固操作，如图 13 所示。


图 13 选择安全加固模板

点击全部项中“自定义模板”文字按钮，弹出自定义模板弹窗，支持对加固模板的新增、删除和编辑等操作，其中全部项和三级项是默认模板，不可以删除和编辑，如图 14 所示。

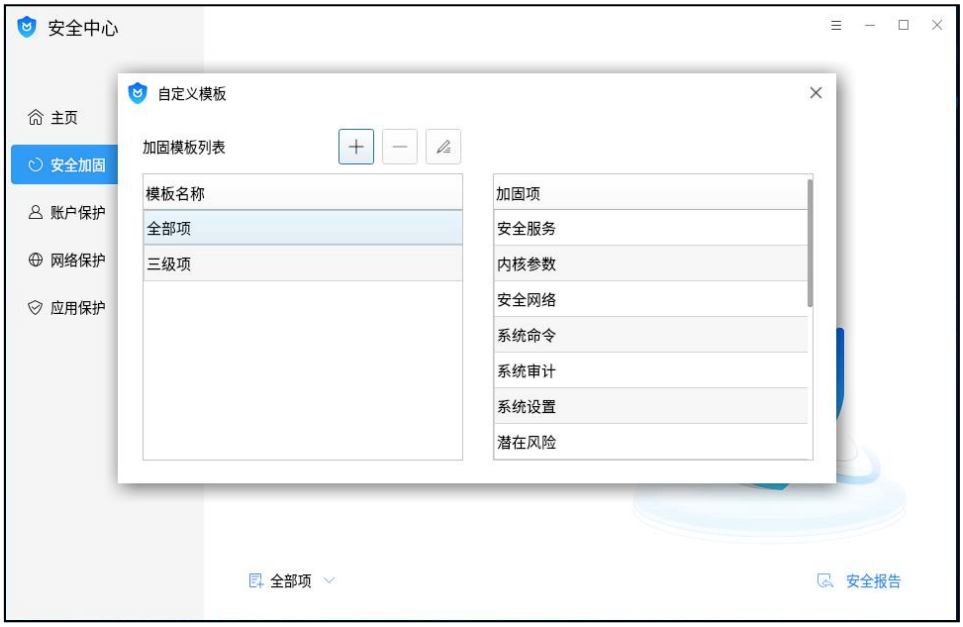


图 14 自定义安全加固模板

### 5.2.1 添加自定义模板

点击自定义模板中“添加”按钮，弹出添加模板弹窗，支持编辑自定义模板

名称、选择对应加固一类项及编辑加固项说明信息（限制 20 个字符），点击确定按钮，完成加固模板添加操作，添加的加固模板在加固模板列表中显示，如图 15 所示。

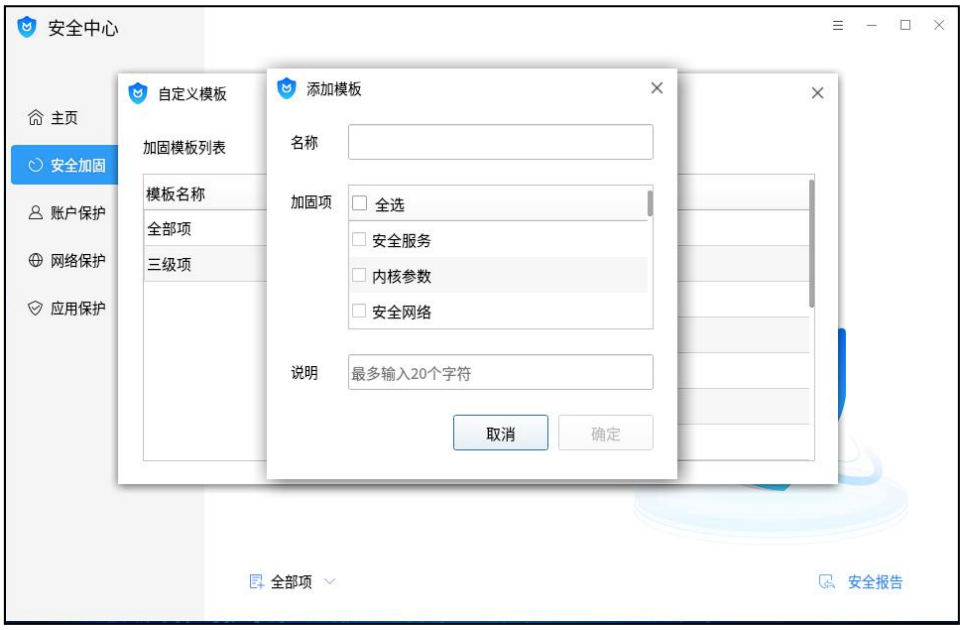


图 15 添加自定义模板

### 5.2.2 编辑自定义模板

加固模板列表中选中自定义模板，点击自定义模板中“编辑”按钮，弹出编辑模板弹窗，支持修改自定义模板名称、修改对应加固一类项及修改加固项说明信息（限制 20 个字符），点击确定按钮，完成加固模板编辑操作，如图 16 所示。

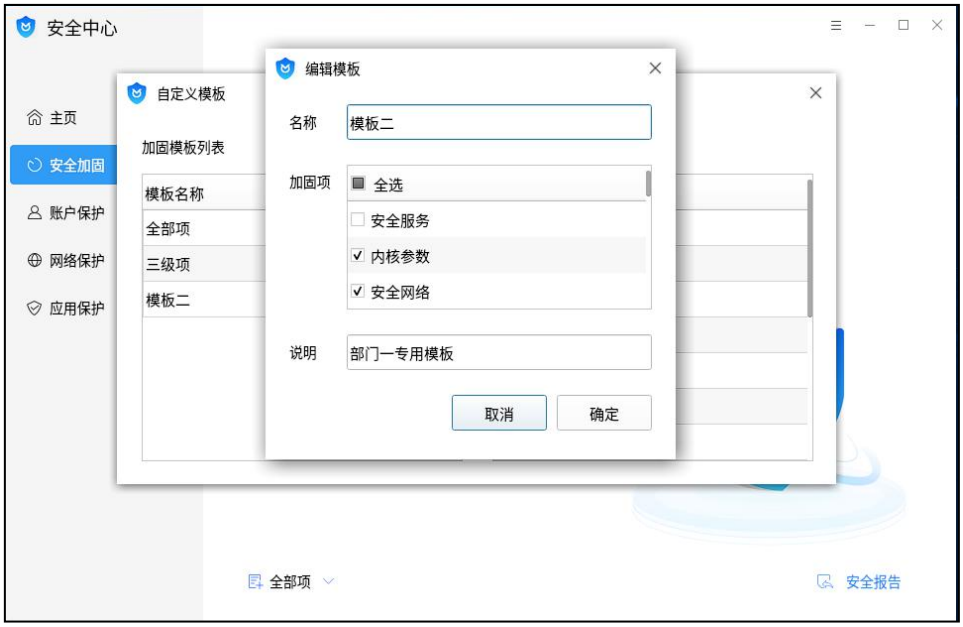

图 16 编辑自定义模板

### 5.2.3 删除自定义模板

加固模板列表中选中自定义模板，点击自定义模板中“删除”按钮，完成加固模板删除操作，如图 17 所示。

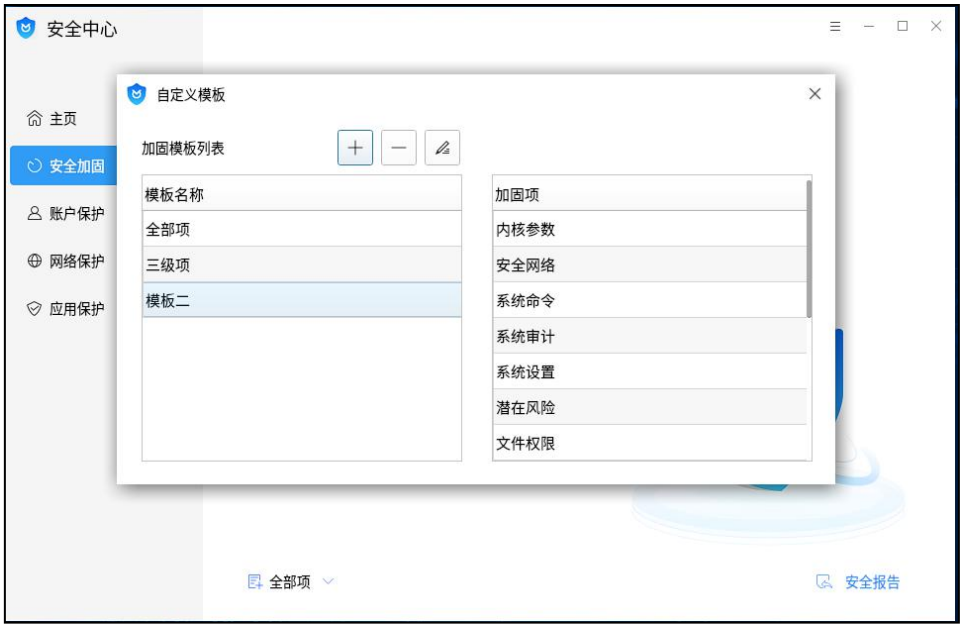


图 17 删除自定义模板

## 5.3 加固扫描

点击“开始扫描”按钮进行系统安全加固扫描，动态显示加固扫描进度，同步显示各加固项信息及扫描结果，如图 18 所示。

图 18 安全加固扫描中

如果安全加固扫描未发现任何风险问题项时，安全加固扫描页面提示“本次扫描已完成”且安全加固项状态均为无需加固，如图 19 所示。


图 19 安全加固扫描完成（未发现风险问题项）

如果安全加固扫描发现风险问题项时，安全加固扫描页面提示“本次扫描已完成，发现 XX 项问题”且存在风险问题项的安全加固项状态均为等待加固，风险问题项以红色字体提示且括号内显示风险问题小项数目，如图 20 所示。


图 20 安全加固扫描完成（发现风险问题项）

## 5.4 一键加固

点击“一键加固”按钮可对所有风险问题项进行一键式加固处理，加固过程中不能取消，如图 21 所示。


图 21 一键加固中

## 5.5 加固完成

加固完成后，系统不存在风险问题项，如图 22 所示。点击“完成”按钮返回加固首页。

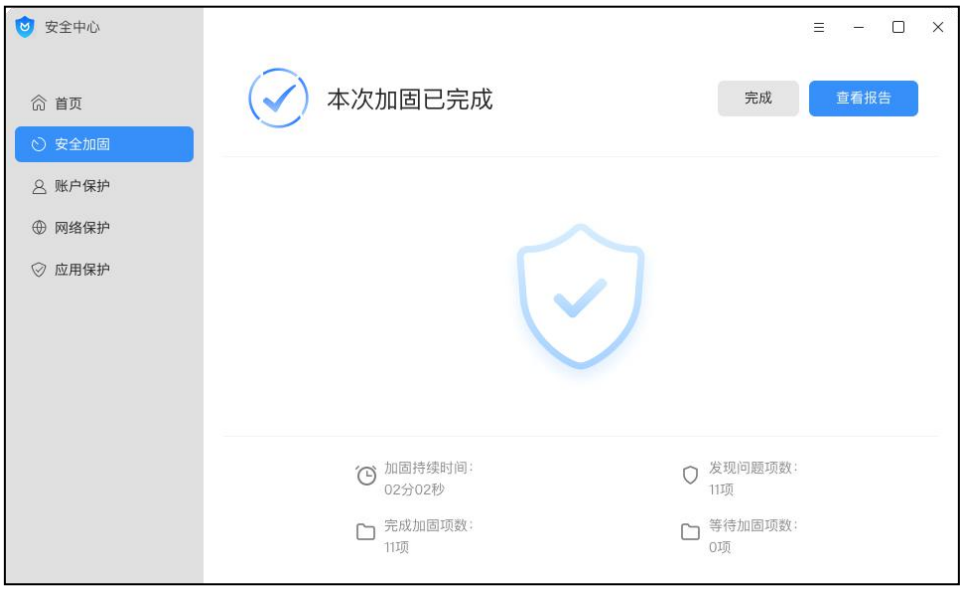


图 22 加固完成（系统暂无风险）

加固完成后，系统仍存在风险问题项，如图 23 所示。如果需要加固该项，请用户手动加固，具体加固方法可参见加固手册。

点击“完成”按钮返回加固首页。

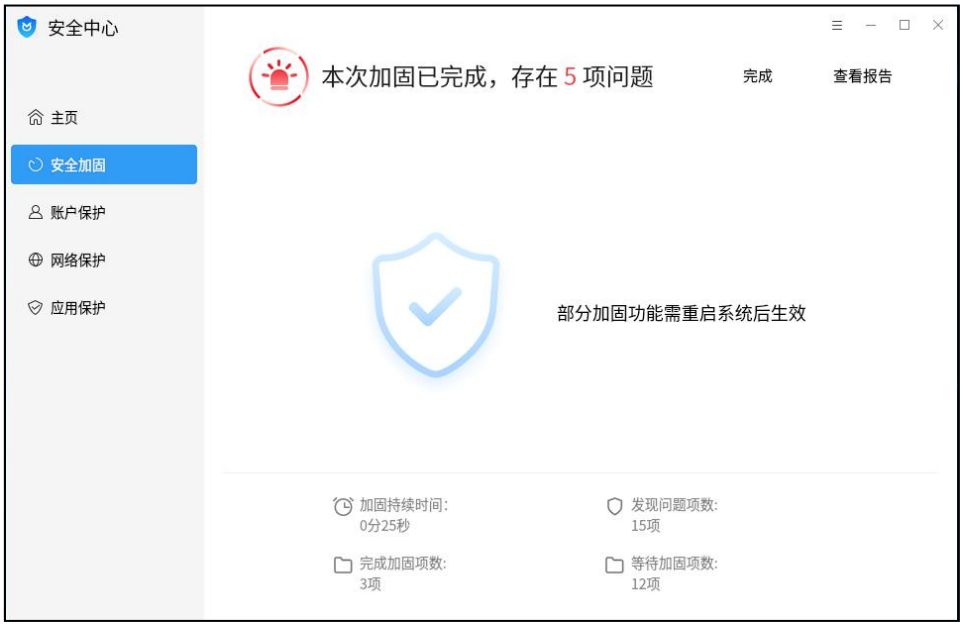


图 23 加固完成（仍存在风险问题项）

## 5.6 一键还原

点击“一键还原”按钮可对所有已加固风险问题项进行一键式还原处理，还原过程中不能取消，如图 24 所示。


图 24 一键还原中

## 5.7 还原完成

还原完成后，系统不存在已加固风险问题项，如图 25 所示。点击“完成”按钮返回加固首页。


图 25 还原完成（系统暂无风险）

还原完成后，系统仍存在已加固风险问题项，如图 26 所示。如果仍需要还原该项，请用户手动还原，具体还原方法可参见加固手册。

点击“完成”按钮返回加固首页。


图 26 还原完成（仍存在已加固风险问题项）

### 5.8 安全报告

一键加固完成后，点击“查看报告”按钮，弹出安全报告弹窗，安全报告中根据实际加固结果统计显示：无需加固 X 项、加固成功 X 项、重启生效 X 项、待加固 X 项、待手动加固 X 项、加固失败 X 项，列表中显示序号、安全加固项、详情描述及对应状态，支持对加固状态进行筛选显示，同时支持导出安全报告，如图 27 所示。


图 27 安全报告

## 6. 账户保护

安全中心提供系统账户密码强度策略配置，账户锁定策略配置功能。点击首页的“账户保护”按钮，或左侧列表中“账户保护”标签页进入，如图 28 所示。


图 28 账户保护首页

## 6.1 密码强度

密码强度功能可以开启或关闭。开启状态时，系统账户需要遵循当前密码强度策略要求；关闭状态时，系统账户无任何密码强度限制。

密码强度提供推荐、自定义两种配置模式。推荐模式：至少 8 位，包含大写字母、小写字母、数字、特殊符号中的 3 种，密码禁止包含用户名等配置策略；自定义模式：根据需要自定义相应的密码强度策略，如图 29 所示。

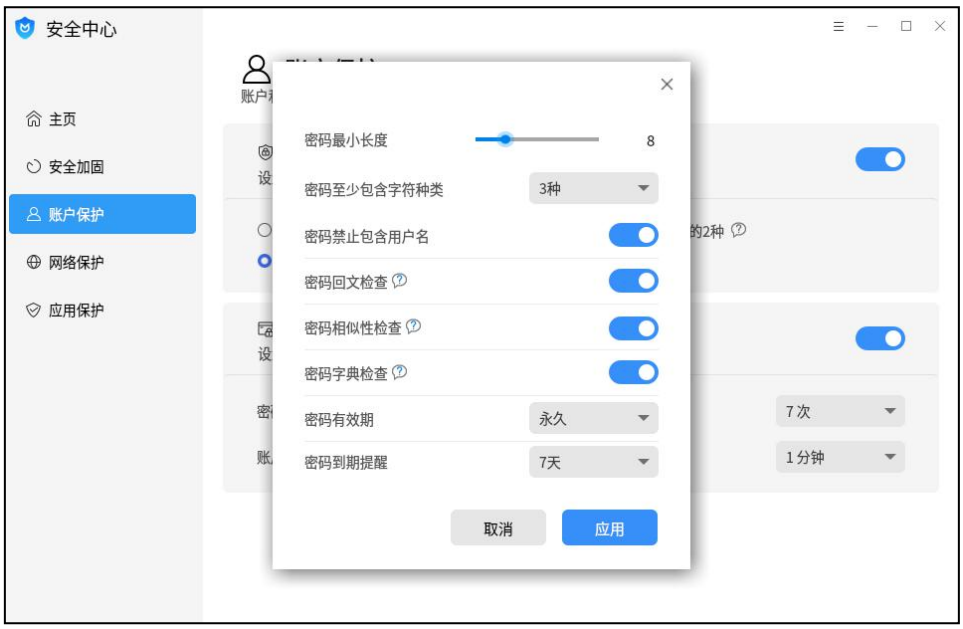


图 29 自定义密码强度策略

自定义密码强度策略配置界面提供以下设置：

（1）密码最小长度，设置范围 1 至 32 位；

（2）密码至少包含字符种类，设置范围 1 至 4 种；

（3）密码禁止包含用户名，功能可启用或关闭；

（4）密码回文检查，正读反读均相同的密码将不能设置成功，功能可启用或关闭；

（5）密码相似性检查，与原密码相似度大的密码将不能设置成功，如只改变字母大小写，功能可启用或关闭；

（6）密码字典检查，密码字典中存储着用户常用密码，与字典内字符相同的密码将不能设置成功，功能可启用或关闭；

（7）密码有效时间，包含 7 天、30 天、90 天、180 天和永久，默认为永久；

（8）密码到期提醒，包含 3 天、7 天、15 天和 30 天，当设置密码有效时间为 7 天时，密码到期提醒只能选择 3 天；

（9）密码回文检查、密码相似性检查和密码字典检查提供功能说明提示，当鼠标悬停在提示图标时显示对应项的详细说明。

### 6.2 账户锁定

账户锁定功能可以开启或关闭。开启状态时，系统账户需要遵循当前账户锁定策略要求；关闭状态时，系统账户无账户锁定限制。

账户锁定功能提供密码连续输错次数和账户锁定时间配置。密码连续输错次数：设置范围 5 至 10 次，默认为 5 次；账户锁定时间：1 分钟、3 分钟、5 分钟、10 分钟、15 分钟，默认为 10 分钟。

## 7. 网络保护

安全中心提供联网控制功能，保护系统网络安全性。点击首页“网络保护”按钮，或左侧列表中“网络保护”标签页进入，如图 30 所示。


图 30 网络保护首页

## 7.1 联网控制

设置应用联网控制策略，保护系统网络安全性。联网控制功能提供开启和关闭配置，如图 31 所示。开启：阻止未授权的应用和服务联网；关闭：允许任何应用程序联网。


图 31 联网控制

联网控制功能开启时，点击“高级配置”按钮，弹出“高级配置-联网控制”

弹窗，可以对单个应用或服务进行联网控制策略配置，提供允许和阻止，如图 32 所示。

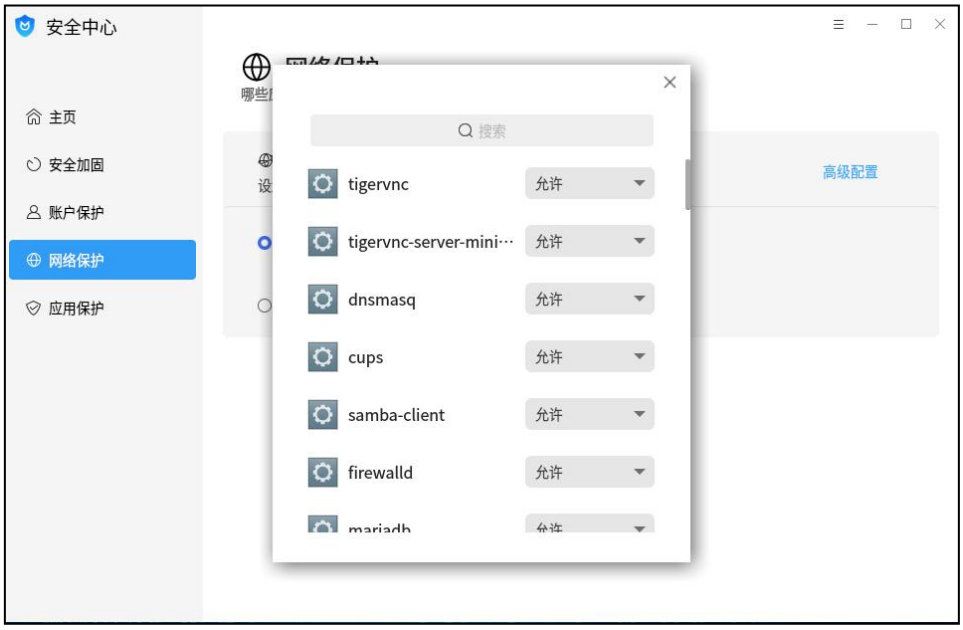


图 32 高级配置-联网控制

## 8. 应用保护

安全中心提供应用保护功能，保护您的系统免受安全威胁。点击首页“应用保护”按钮，或左侧菜单栏中“应用保护”标签页进入，如图 33 所示。


图 33 应用保护首页

## 8.1 应用程序执行控制

设置未认证应用执行策略，保护系统运行环境安全。执行控制功能提供三种模式配置，如图 33 所示。开启：阻止执行未认证的应用程序；关闭：允许执行任何应用程序。

点击“高级配置”按钮，弹出“高级配置-应用程序执行控制”弹窗，应用程序执行控制列表显示内容包括序号、文件路径、文件类型和当前状态，如图 34 所示。

（1）文件类型包括：可执行程序、共享库、可执行脚本和内核模块文件 4 种类型。

（2）当前状态包括：“被篡改”、“已损坏”和“已认证”。被篡改：表示该文件已经被篡改，并且文件类型未发生改变，此类文件可以进行认证和解除认证，也可以重新安装对应的软件包进行手动恢复；已损坏：表示该文件已经被篡改并且文件类型已被破坏，此类文件不能进行认证和解除认证，只能进行恢复或重新安装对应的软件包进行手动恢复；已认证：表示该文件未被篡改。

（3）操作包括认证、解除。认证：将“被篡改”应用程序重新认证并信任，认证成功后当前状态变为“已认证”，当前应用程序可以执行；解除：将“被篡改”或“已认证”应用程序解除认证并不信任，应用程序执行控制列表会自动清除该应用程序信息，当前应用程序不可以执行；

（4）默认按照“被篡改”、“已损坏”和“已认证”的顺序依次排序。


图 34 高级配置-应用程序执行控制（简略信息）

点击“添加”按钮，弹出“添加应用程序基准值”弹框，可以添加选择单个应用程序或目录，添加目录是扫描当前目录下的所有应用程序，如图 35 所示。

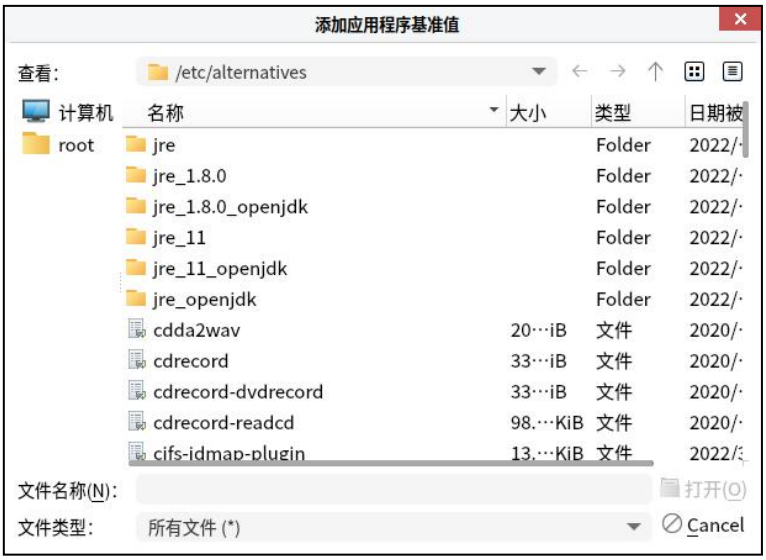


**图 35 添加应用程序基准值**

执行控制列表默认按照简略信息展示，只展示新安装应用程序信息，如图 34 所示。点击“详细信息”按钮可切换显示系统所有应用程序信息，如图 36 所示。


**图 36 高级配置-应用程序执行控制（详细信息）**

## 8.2 应用防护控制

设置系统安全防护策略，实时防护已配置的应用，保护系统关键服务运行稳

定。应用防护控制功能提供开启和关闭配置。开启时，实时防护配置应用；关闭时，无任何应用防护机制，如图 33 所示。

点击“高级配置”按钮，弹出“高级配置-应用防护控制”弹框，提供进程防杀死、内核模块文件防卸载和文件防篡改功能，如图 36 所示。

### 8.2.1 进程防杀死

进程防杀死策略配置列表显示内容包括：序号、进程号、进程名称、进程路径和防杀死保护开关。

出现多个名称相同的进程时，防杀死保护开关合并成一个，防杀死保护开启后可以同时保护这些进程，列表默认按照收起方式显示，点击展开或收起按钮进行显示切换，如图 37 至 38 所示。

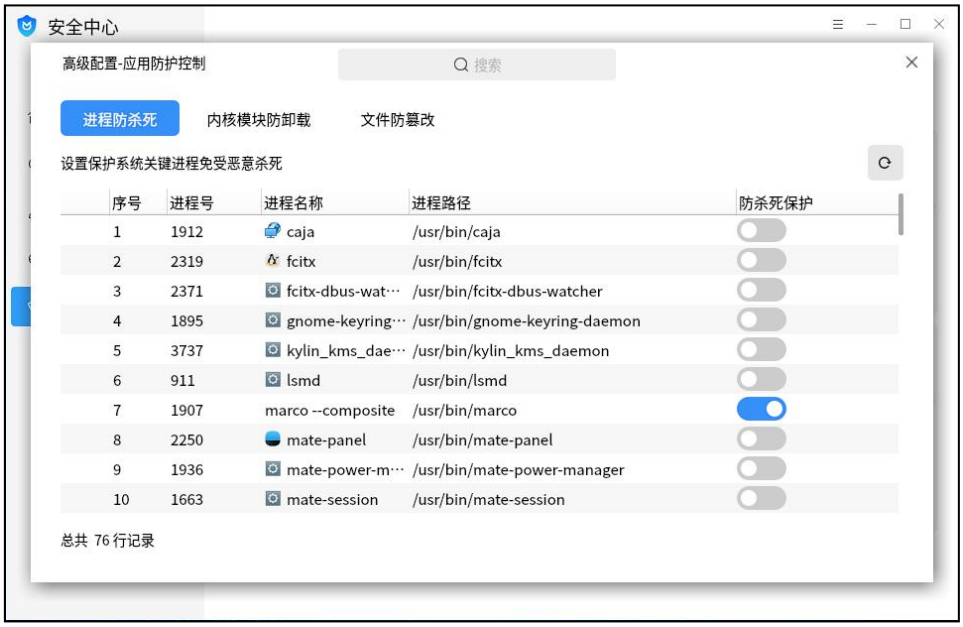


图 37 进程防杀死（默认收起）

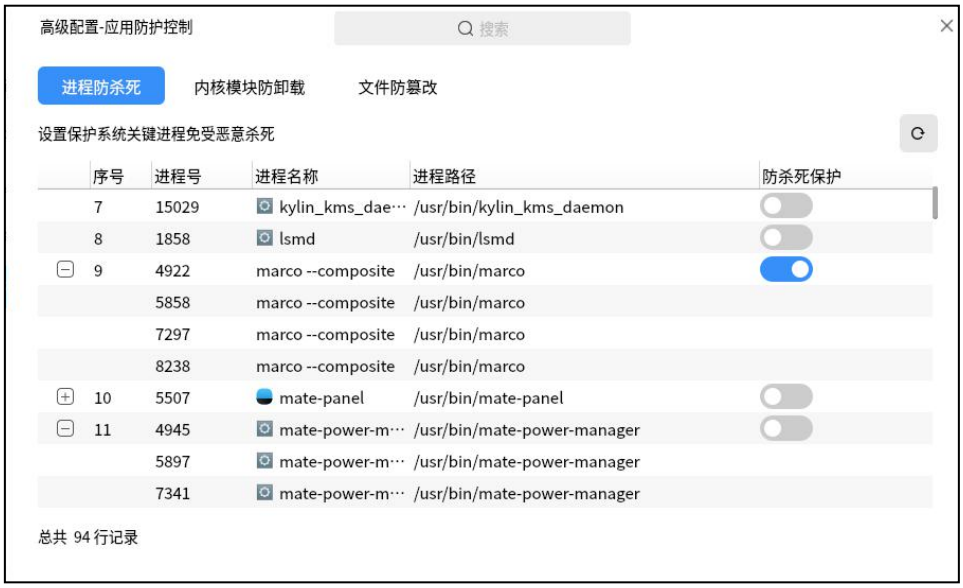


图 38 进程防杀死（展开）

### 8.2.2 内核模块防卸载

内核模块防卸载策略配置列表显示内容包括：序号、内核模块名称和防卸载保护开关，如图 39 所示。


图 39 内核模块防卸载

### 8.2.3 文件防篡改

文件防篡改策略配置列表显示示内容包括：序号、文件名称、文件路径和解除操作，解除受保护文件后，文件从列表中自动清除，如图 40 所示。

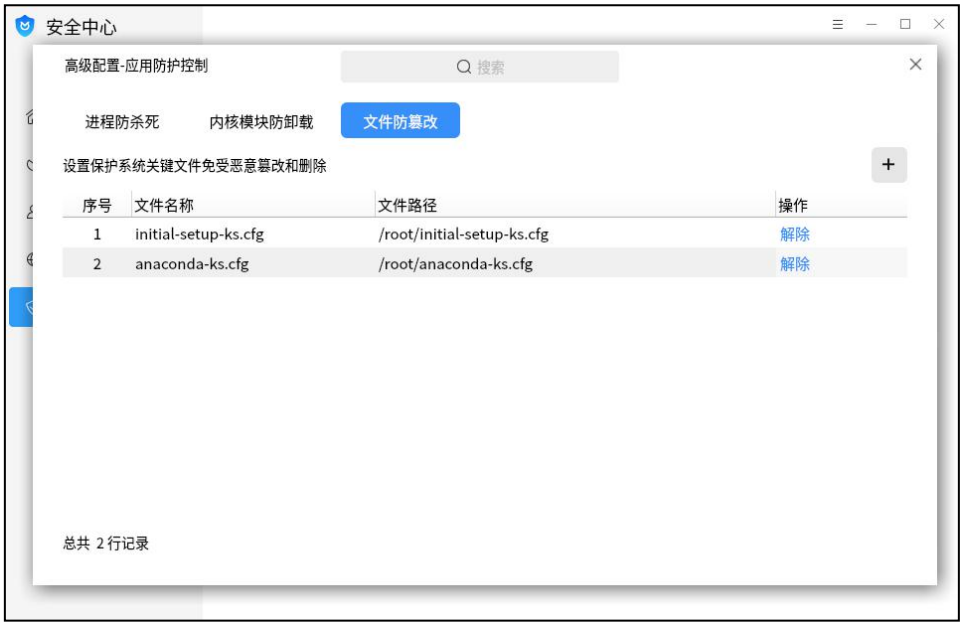


图 40 文件防篡改

点击“添加”按钮，弹出“选择需要受保护的文件”弹窗，可以自行添加需要受保护的文件，如图 41 所示。

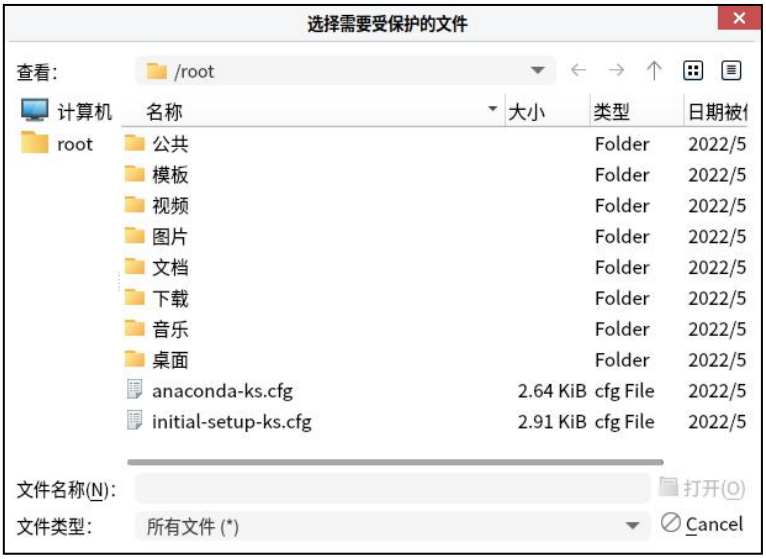


图 41 选择需要受保护的文件

## 9. 安全内存

安全内存是一款完全兼容 DDR4 RDIMM 内存系统的安全内存模组。该产品基于 DDR4 RDIMM 内存模组，由 8 Gb DDR4 SDRAM 通用内存颗粒和内建了 SAM（安全访问权限管理）机制的澜起安全寄存缓存器芯片（即“安全 RCD 芯片”）组成，

支持速率达 DDR4-2666。

设备出厂用户需选配澜起（HSDIMM-Lite）安全内存，安全中心才会显示安全内存模块，安全内存界面展示内存相关的基本信息，如类型、速度、容量、防护范围等信息。其中防护范围为系统调用表，用户可根据需要开启或关闭当前的开关。如图 42 所示。


图 42 安全内存页

## 10. 可信度量

银河麒麟可信操作系统将系统结构划分为两个不同的计算域，对应为双体系架构麒麟可信执行环境( KYLIN TEE)与麒麟通用计算环境（KYLIN REE）。

双体系架构是将 CPU 核、IO 输入输出设备、内存等硬件资源隔离形成两套完整的子系统。计算部件（REE）无法访问安全部件（TEE）的内容，通过把加密密钥等数据存放在安全部件，实现了隐私数据的隔离，只有安全部件和安全应用（TA）能够访问，从而进异步保障数据的安全性。

通过可信度量、机密计算技术，实现对计算子系统的主动度量（可信启动、静态度量、动态度量）和主动控制（可信策略）。

### 10.1 可信链

基于 CPU-IP 核（即 TCM/TPCM）硬件资源构建可信根，提供可信基环境。信任链可对可信启动过程中所有环节的度量结果进行查看。如果有发现度量值改变的文件，标记为不可信，并且用户可进行查看和信任操作。如图 43 所示。


**图 43 可信度量页**

1、信任链

（1）包括可信芯片、BIOS、引导程序、操作系统、应用程序，每次系统启动后更新信任链状态，用户进入可信度量后，动态展示各个环节的度量结果。

（2）如果某个节点存在不可信的文件，则该节点标红；节点正常，则图标为蓝色；当可信芯片无法识别时，可信芯片与 BIOS 按钮置灰，无法点击。

（3）点击可信芯片可查看详情。

查看详情：包括芯片版本、规范版本、芯片厂家、芯片名称、支持算法、创建密钥、NV 存储。不同模式的可信根信息不一样，kyee 可信根详情如图 44 所示。


**图 44 kyee 可信根详情**

（4）点击 BIOS、引导程序、操作系统均可进入系统启动度量的高级配置页，，如图 45 所示。


**图 45 可信芯片详情**

（5）点击应用程序进入应用程序度量的高级配置页。

## 10.2 系统启动度量

可信启动依据信任传递的思想，实现对可信根、TPCM、可信固件 UEFI 、GRUB 引导程序、系统内核文件与关键配置文件进行逐级度量，构建完整可信信任链，为设备启动建立初态的可信执行环境。

可信启动主要展示启动度量基准库条数、本次度量失败条数、本次启动可信状态、本次度量报告时间四项信息。如图 46 所示。

（1）启动度量基准库条数：显示为当前初始化后的基准库总条数；

（2）本次度量失败条数：显示为度量值与基准库不一致的度量失败条数 ；

（3）本次启动可信状态：显示设备本次启动度量的可信或不可信状态；

（4）本次度量报告时间：显示本次的可信度量报告产生时间；


图 46 可信启动页

## 10.3 系统启动度量配置

可信启动功能提供开启和关闭两种配置模式。如图 47 所示。

（1）开启：监测到系统环境变化时，请通知我；

（2）关闭：不进行设备环境监测。

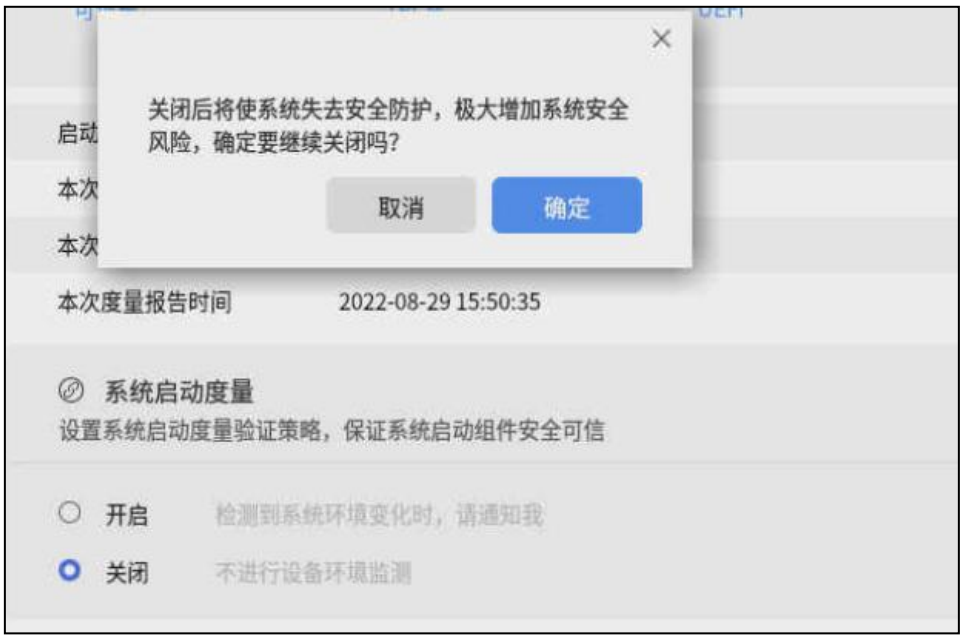


图 47 可信启动配置

## 10.4 查看度量报告

点击“查看详情”，可查看本次可信启动的度量报告日志。如图 48 所示。


图 48 查看度量报告

### 10.5 重新采集基准值

当存在度量失败项时，可通过点击“重新采集基准值”按钮并“确定”后，将会进行基准库的重新初始化，恢复对当前度量失败项的可信状态。如图 49 所示。


图 49 重新采集基准值

## 11. 指令流安全预检测

指令流安全预检测摆脱了传统安全技术对文件、流量、数据、行为等特征的依赖，采用了内存指令控制流检测技术，并与人工智能、机器学习技术深度结合，可从指令层监测漏洞攻击代码的执行，完全不依赖已知漏洞特征和已知攻击代码的特征，可发现利用未知漏洞发起的攻击。同时，在可信程序被恶意利用、及后门的检测方面，亦有着良好的效果保障可信程安全运行，发现远程漏洞攻击。如图 50 所示。


图 50 指令流安全检测页

提供检测已经在系统白名单下的程序文件因漏洞带来的指令流异常能力。分别有以下两种状态：

（1）开启：实时检测漏洞利用攻击，记录安全风险；

（2）关闭：关闭对所有指令的检测。

用户可点击“查看防护日志”，跳转到日志查看器的“指令流日志”中查看日志详情。如图 51 所示。

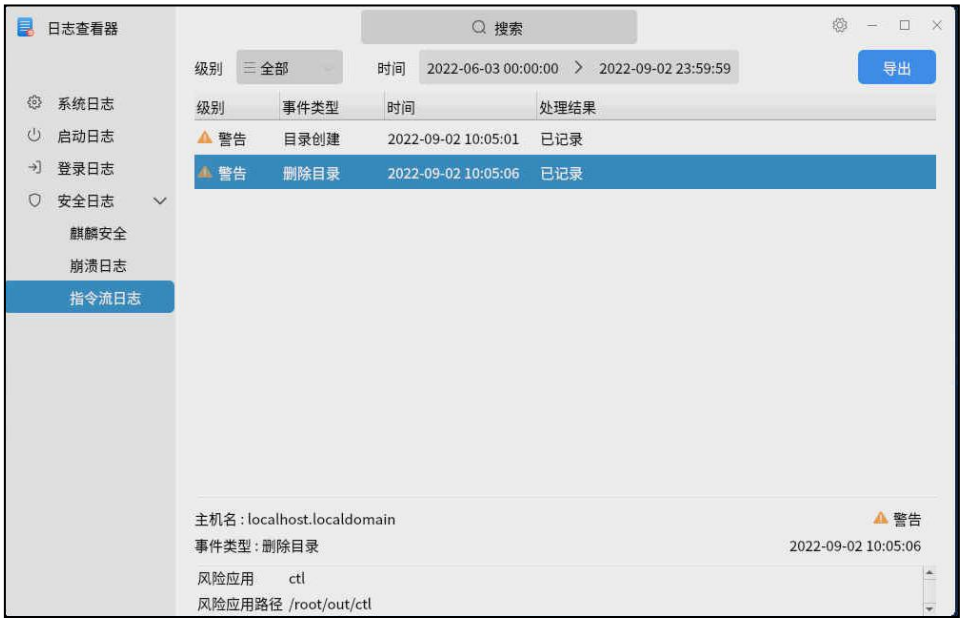


图 51 指令流日志页

# 12. 麒麟安全命令行工具

## 12.1 security-switch

### 12.1.1 功能

用于设置安全模式和获取安全模式状态。

### 12.1.2 用法

security-switch <--set|--get|--help|-h> [mode]

--set 设置安全模式

mode 安全模式

none： 关闭，disable；

default：推荐，only kysec enforcing；

strict： 安全优先，（selinux ukmcs + kysec enforcing + kysec 3adm）

更多安全模块状态设置可参考 setstatus 命令

--get 获取安全模式状态

-h,--help 显示帮助信息

### 12.1.3 示例

## 12.2 setstatus

### 12.2.1 功能

提供安全模块的开和关设置，包括 kysec、box、apparmor、selinux 等安全模块的开关。

### 12.2.2 用法

setstatus <module> [-s,--status][-f,--func][-c,--control] [-t,--temporary] [-h,--help]

-h,--help 显示帮助信息

module 安全模块名

kysec：麒麟安全框架，提供联网控制、应用执行控制和应用防护等功能

selinux：selinux 是一种基于域-类型模型的强制访问控制安全系统

box：文件保护箱提供用户间数据隔离和加密保护功能，支持国密算法

apparmor：apparmor 是一种基于文件或目录的强制访问控制安全系统

-s,--status 设置安全模块的状态

安全模块为 kysec 时取值：

disable 关闭

enforcing 强制模式

permissive 宽松模式

安全模块为 selinux 时取值：

disable 不生效

enforcing 强制模式

permissive 宽松模式

安全模块为 box 时取值：

disable 关闭

enable 开启

安全模块为 apparmor 时取值：

disable 关闭

enable 开启

-f，--func 安全模块下的子功能，子功能状态依赖安全模块的状态，无子功能无需设置

安全模块为 kysec 时取值：

execctl 执行管控子模块

netctl 应用联网管控子模块

ppro 进程防杀死子模块

fpro 文件保护子模块

kmod 模块防卸载子模块

-c，--control 子功能管控状态

execctl：on/off　　on 表示开启，在 kysec 为 enforcing 状态时，阻止执行未认证或已篡改的应用程序；在 kysec 为 permissive 状态时，允许执行任何应用程序并记录执行日志。off 表示关闭，允许执行任何应用程序且不记录执行日志

ppro：on/off　　on 表示开启，off 表示关闭

kmod：on/off　　on 表示开启，off 表示关闭

fpro：on/off　　on 表示开启，off 表示关闭

devctl：on/off　　on 表示开启，off 表示关闭

-t，--temporary 临时生效(只支持 selinux、kysec 模块的 permisive 和 enforcing 状态间，kysec 子模块状态的切换)

### 12.2.3 示例

1）设置 kysec 的状态为 enforcing

```
[root@localhost ~]# setstatus kysec -s enforcing
安全模块状态设置改变，需要重启系统才能生效！
```

**图 52 设置 kysec 状态为 enforcing**

2）设置 kysec 的状态为临时 permissive

```
[root@localhost ~]# setstatus kysec -s permissive -t
[root@localhost ~]# getstatus
KySec status: permissive
        execTl  : on
        netctl  : on
        fpro    : on
        kmod    : on
        ppro    : on
selinux status: disable
apparmor status: disable
box status: disable
```

**图 53 设置 kysec 状态为 permissive**

3）设置 kysec 的状态为临时 enforcing

```
[root@localhost ~]# setstatus kysec -s enforcing -t
[root@localhost ~]# getstatus
KySec status: enforcing
        execTl  : on
        netctl  : on
        fpro    : on
        kmod    : on
        ppro    : on
selinux status: disable
apparmor status: disable
box status: disable
```

**图 54 设置 kysec 临时状态**

4）设置 kysec 的执行管控为关闭状态

```
[root@localhost ~]# setstatus kysec -f execTl -c off
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# getstatus
KySec status: enforcing
        execTl  : off
        netctl  : on
        fpro    : on
        kmod    : on
        ppro    : on
selinux status: disable
apparmor status: disable
box status: disable
```

**图 55 设置子模块 execTl 的状态**

5）设置 kysec 的状态为 disable

```
[root@localhost ~]# setstatus kysec -s disable
kysec已成功设置为disable，此设置将使系统失去安全防护，极大增加系统安全风险！
```

**图 56 设置 kysec 状态为 disable**

## 12.3 getstatus

### 12.3.1 功能

获取安全模块状态。

### 12.3.2 用法

getstatus [-m | --module module] [-h |--help]

-h,--help 显示帮助信息

-m,--module 安全模块名，不带参数显示全部

kysec：麒麟安全，提供联网控制、应用执行控制和应用防护等功能

selinux：selinux 是一种基于域-类型模型的强制访问控制安全系统

box：文件保护箱提供用户间数据隔离和加密保护功能，支持国密算法

apparmor：apparmor 是一种基于文件或目录的强制访问控制安全系统

### 12.3.3 示例

1) 获取安全模块状态

```
[root@localhost ~]# getstatus
KySec status: enforcing
        execTl  : on
        netctl  : on
        fpro    : on
        kmod    : on
        ppro    : on
selinux status: disable
apparmor status: disable
box status: disable
```

**图 57 获取安全状态**

2) 获取 kysec 安全模块状态

```
[root@localhost ~]# getstatus -m kysec
KySec status: enforcing
        execTl  : on
        netctl  : on
        fpro    : on
        kmod    : on
        ppro    : on
```

**图 58 获取 kysec 状态**

3) 获取 selinux 安全模块状态

```
[root@localhost ~]# getstatus -m selinux
selinux status: disable
```

图 59 获取 selinux 状态

## 12.4 kysec_set

### 12.4.1 功能

安全模块策略设置。

### 12.4.2 用法

kysec_set <module> [-R] [-c] [-v] <value> [-f|-P] <path|pkgname>

-h, --help 显示帮助信息

module 安全模块

execti: 执行管控

fpro: 文件保护

netctl: 应用程序联网控制

ppro: 进程保护

kmod: 模块防卸载

execti: 执行管控

-R, --recursive: 递归目录

-v, --value 标签值

original: 系统原始标记

verified: 第三方可执行标记

trusted: 可信文件标记

kysoft: 软件包安装标记

parent: 追溯标记

unknown:  未知文件标记

-f, --file  文件或目录路径，设置文件或目录下文件的标记

-P, --package  已安装的软件包名称，设置软件包中文件的标签

-c, --clean  清除设置的标签

fpro:  文件保护

-v, --value  标签值

readonly:  文件只读

none:  取消只读

-f, --file  文件或目录路径，设置文件或目录下文件的标记

-P, --package  已安装的软件包名称，设置软件包中文件的标签

-c, --clean  清除设置的标签

netctl:  应用程序联网控制

-v, --value  设置是否联网

allow:  允许联网

deny:  拒绝联网

warning:  拒绝并弹窗

-n,--name  应用程序名

-f, --file  应用程序文件路径

ppro:  进程保护

-v, --value  设置进程不可被杀死

allow:  允许杀死

deny: 防杀死

-f, --file 进程程序文件路径

-p, --pid 进程号

kmod: 模块防卸载

-v, --value 设置模块不可被卸载

allow: 允许被卸载

deny: 防卸载

-f, --file 模块文件路径

-n, --name 模块名(可通过 lsmod 查看)

### 12.4.3 示例

1）递归添加执行控制白名单列表

```
[root@localhost ~]# kysec_set exectl -R -v verified -f /usr/sbin/
```

**图 60 对目录下的文件设置标记**

2）按照文件路径添加模块防卸载

```
[root@localhost ~]# kysec_set kmod -v deny -f /lib/modules/4.19.90-51.0.v2207.ky
10.x86_64/kernel/sound/soundcore.ko.xz
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# kysec_get kmod -l
模块名称：soundcore, 防卸载保护：开
```

**图 61 添加模块防卸载**

3）按照文件路径添加应用程序拒绝联网

```
[root@localhost ~]# kysec_set netctl -v deny -f /usr/sbin/sshd
[root@localhost ~]#
```

**图 62 设置应用程序联网状态**

4）按照文件路径添加程序进程防杀死

```
[root@localhost ~]# kysec_set ppro -v deny -f /usr/sbin/security-reinforce-daemon
[root@localhost ~]#
```

图 63 添加进程防杀死

5）

## 12.5 kysec_get

### 12.5.1 功能

安全模块策略获取。

### 12.5.2 用法

-h, --help 显示帮助信息

-m, --module 显示某一模块的帮助信息

execti: 执行管控

fpro: 文件保护

netctl: 应用程序联网控制

ppro: 进程保护

kmod: 模块防卸载

execti: 执行管控

-R, --recursive: 递归目录

-f, --file 文件或目录路径

-P, --package 已安装的软件包名称

-p, --pid 进程号，获取进程的标签

fpro: 文件保护

-R, --recursive: 递归目录

-f, --file 文件或目录路径

-P, --package 已安装的软件包名称

netctl: 应用程序联网控制

-l, --list 产看列表

-f, --file 应用程序文件路径

ppro: 进程保护

-l, --list 查看列表

-f, --file 进程程序文件路径

-p, --pid 进程号，获取进程保护状态

kmod: 模块防卸载

-l, --list 查看列表

-f, --file 模块文件路径

-n, --name 模块名

### 12.5.3 示例

1）根据文件路径查看执行管控白名单信息

```
[root@localhost ~]# kysec_get exectl -f /usr/share/locale/
exectl: /usr/share/locale/locale.alias: original
```

**图 64 执行管控白名单信息**

2）查看进程防杀死列表

```
[root@localhost ~]# kysec_get ppro -l
pid: 928, 进程名称：auditd, 进程路径：/usr/sbin/auditd, 防杀死保护：开
pid: 922, 进程名称：kyseclogd, 进程路径：/usr/sbin/kyseclogd, 防杀死保护：开
pid: 1428, 进程名称：kysec-sync-daemon, 进程路径：/usr/sbin/kysec-sync-daemon, 防杀死保护：开
pid: 2232, 进程名称：marco, 进程路径：/usr/bin/marco, 防杀死保护：开
pid: 2278, 进程名称：pulseaudio, 进程路径：/usr/bin/pulseaudio, 防杀死保护：开
```

**图 65 进程防杀死列表**

3）根据文件路径查看文件只读保护

```
[root@localhost ~]# kysec_get fpro -f /etc/
fpro: /etc/mtab: none
fpro: /etc/fstab: none
fpro: /etc/crypttab: none
fpro: /etc/netconfig: none
fpro: /etc/my.cnf: none
fpro: /etc/virc: none
fpro: /etc/cron.allow: none
fpro: /etc/Trolltech.conf: none
fpro: /etc/uid_list: readonly
fpro: /etc/.productinfo: none
fpro: /etc/issue: none
fpro: /etc/issue.net: none
fpro: /etc/kylin-release: none
fpro: /etc/DIR_COLORS: none
fpro: /etc/os-release: none
fpro: /etc/rhashrc: none
fpro: /etc/system-release: none
fpro: /etc/papersize: none
```

**图 66 文件只读保护**

4）根据模块名查看模块防卸载信息

```
[root@localhost ~]# kysec_get kmod -n soundcore
模块名称：soundcore, 防卸载保护：开
```

**图 67 模块防卸载信息**

5）查看应用程序联网列表信息

```
[root@localhost ~]# kysec_get netctl -l
netctl: tigervnc:       允许
netctl: tigervnc-server-minimal:        允许
netctl: dnsmasq:        允许
netctl: cups:   允许
netctl: samba-client:   允许
netctl: firewalld:      允许
netctl: mariadb:        允许
netctl: nfs-utils:      允许
netctl: net-snmp:       允许
netctl: rpcbind:        允许
netctl: ntp:    允许
netctl: dhcp:   允许
netctl: telnet: 允许
netctl: systemd-udev:   允许
netctl: gvfs:   允许
netctl: gnupg2: 允许
netctl: sssd:   允许
netctl: openldap-servers:       允许
netctl: firefox:        允许
```

**图 68 应用程序联网列表信息**

## 12.6 security-reinforce

### 12.6.1 功能

安全加固命令提供安全服务、安全网络、磁盘检查、潜在危险、系统安全等16大类安全加固检查项，同事符合操作系统安全三级技术要求，为用户提供加固扫描、一键加固、一键还原和安全报告等功能。

### 12.6.2 用法

security-reinforce [-h|--help]

打开终端，输入security-reinforce，回车，显示如图所示信息：

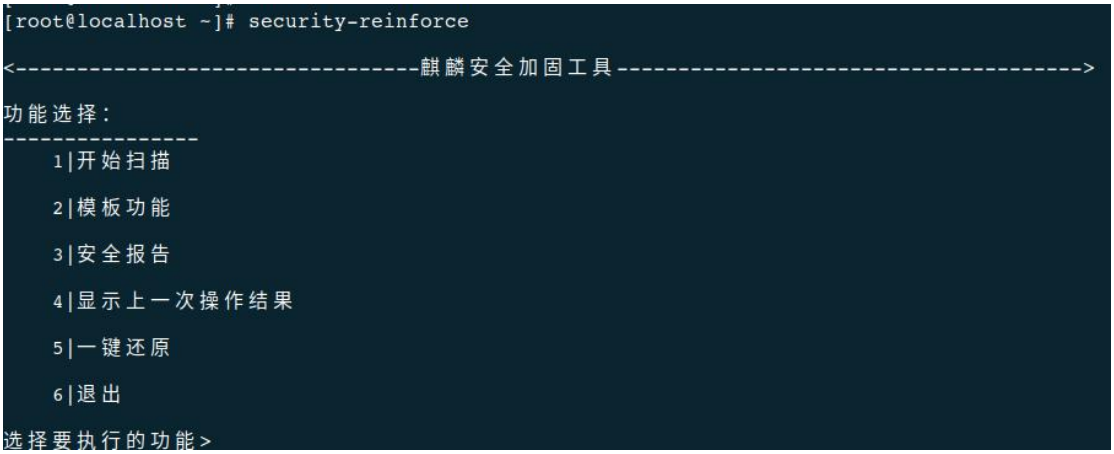


**图 69 安全加固命令帮助信息**

### 12.6.3 示例

1）模板功能

图43输入2，回车，进入模板功能

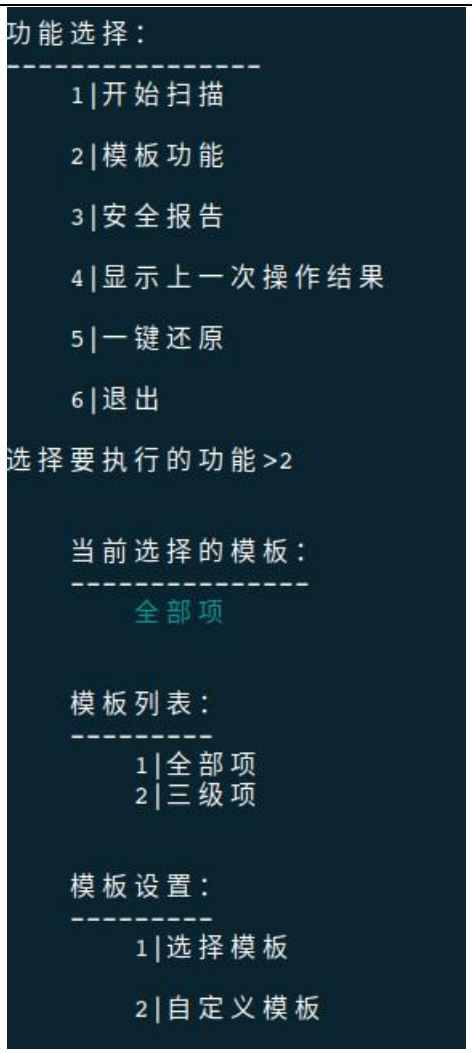
功能选择：
1|开始扫描
2|模板功能
3|安全报告
4|显示上一次操作结果
5|一键还原
6|退出
选择要执行的功能>2
当前选择的模板：
全部项
模板列表：
1|全部项
2|三级项
模板设置：
1|选择模板
2|自定义模板

**图 70 模板功能**

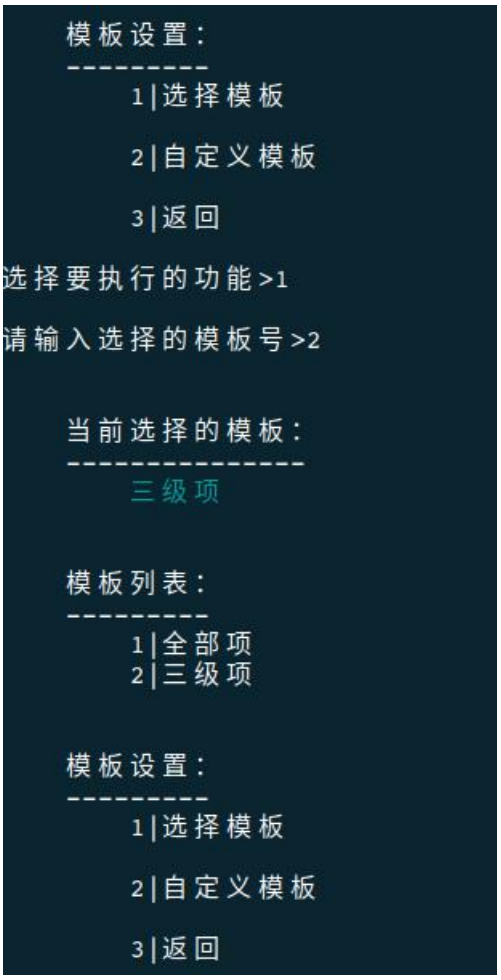
模板设置：
1|选择模板
2|自定义模板
3|返回
选择要执行的功能>1
请输入选择的模板号>2
当前选择的模板：
三级项
模板列表：
1|全部项
2|三级项
模板设置：
1|选择模板
2|自定义模板
3|返回

**图 71 选择模板**

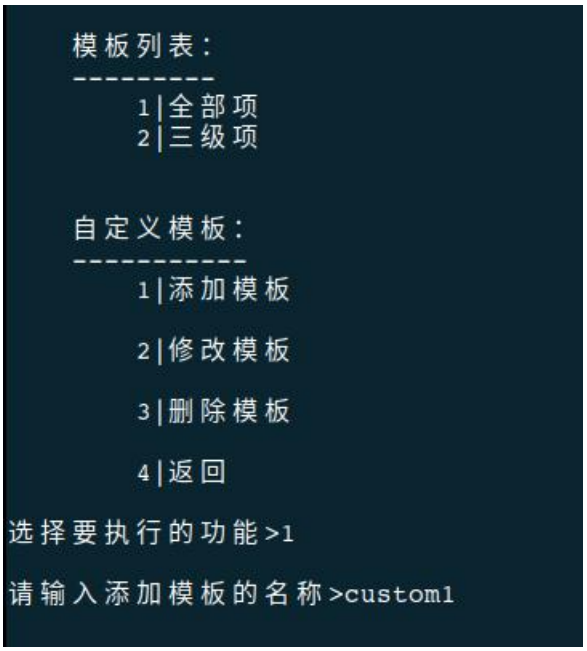
模板列表：
1|全部项
2|三级项
自定义模板：
1|添加模板
2|修改模板
3|删除模板
4|返回
选择要执行的功能>1
请输入添加模板的名称>custom1

图 72 添加模板-模板命名

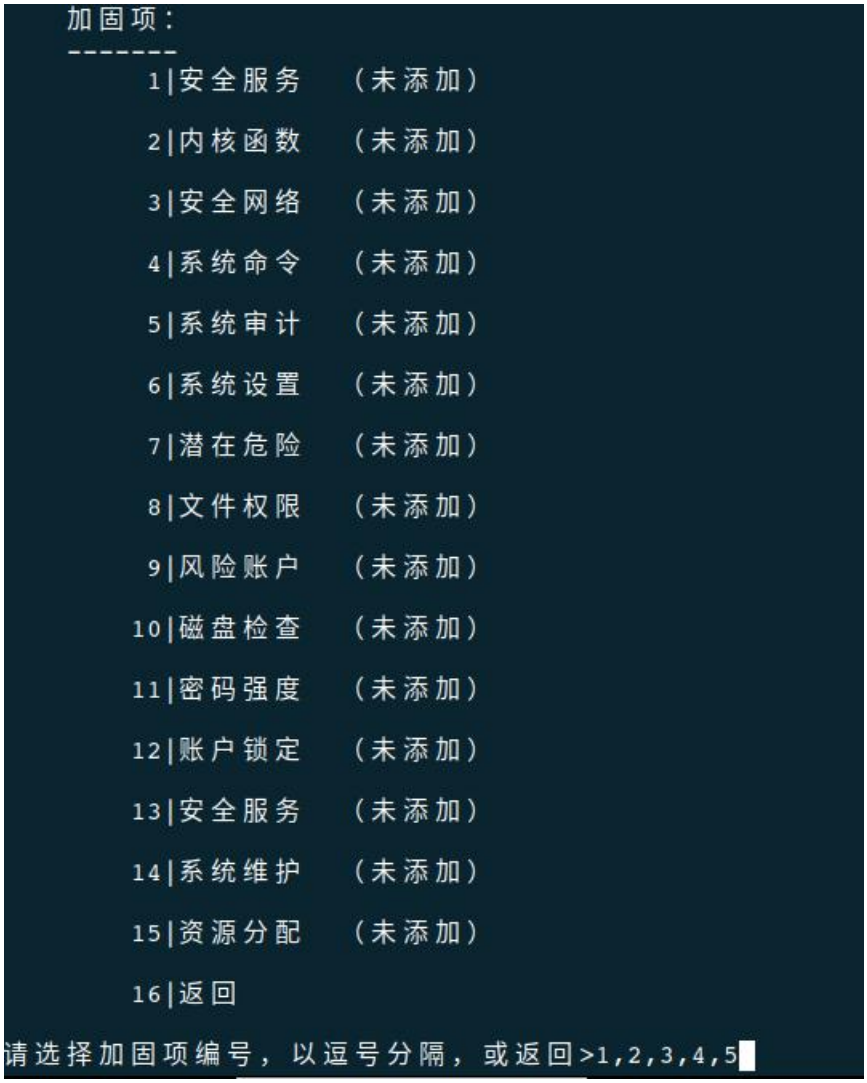


图 73 添加模板-选择加固项

2）加固扫描

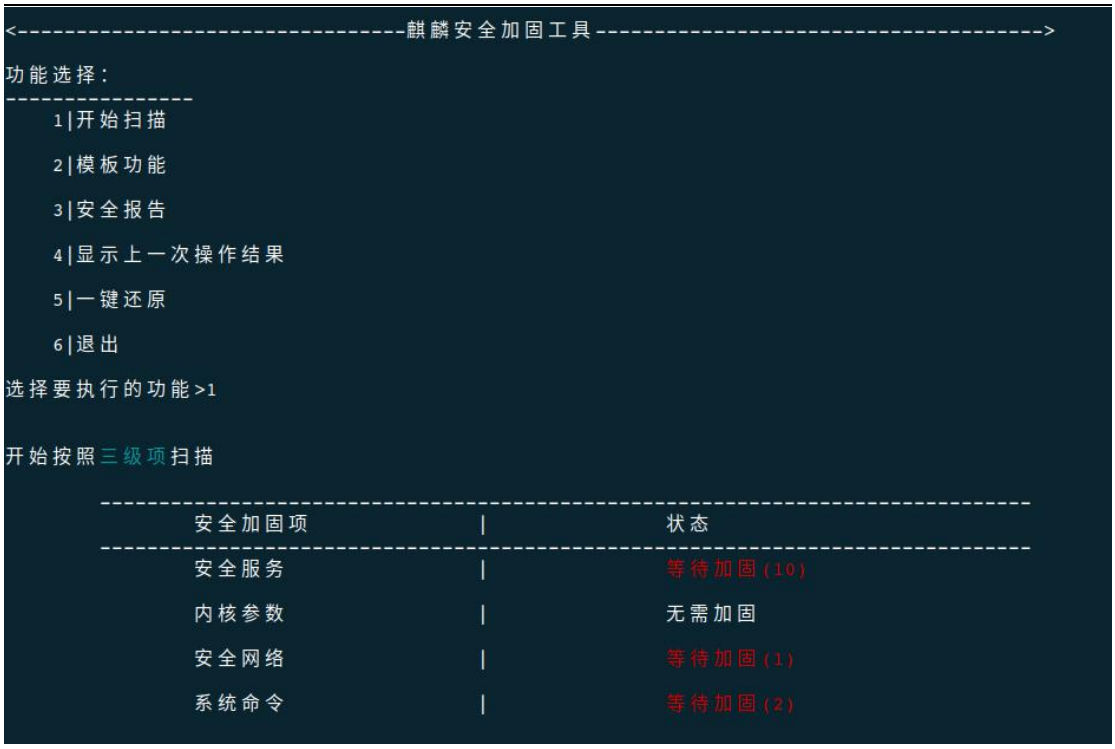


**图 74 加固扫描**

3）安全报告


**图 75 安全报告**

4）一键加固

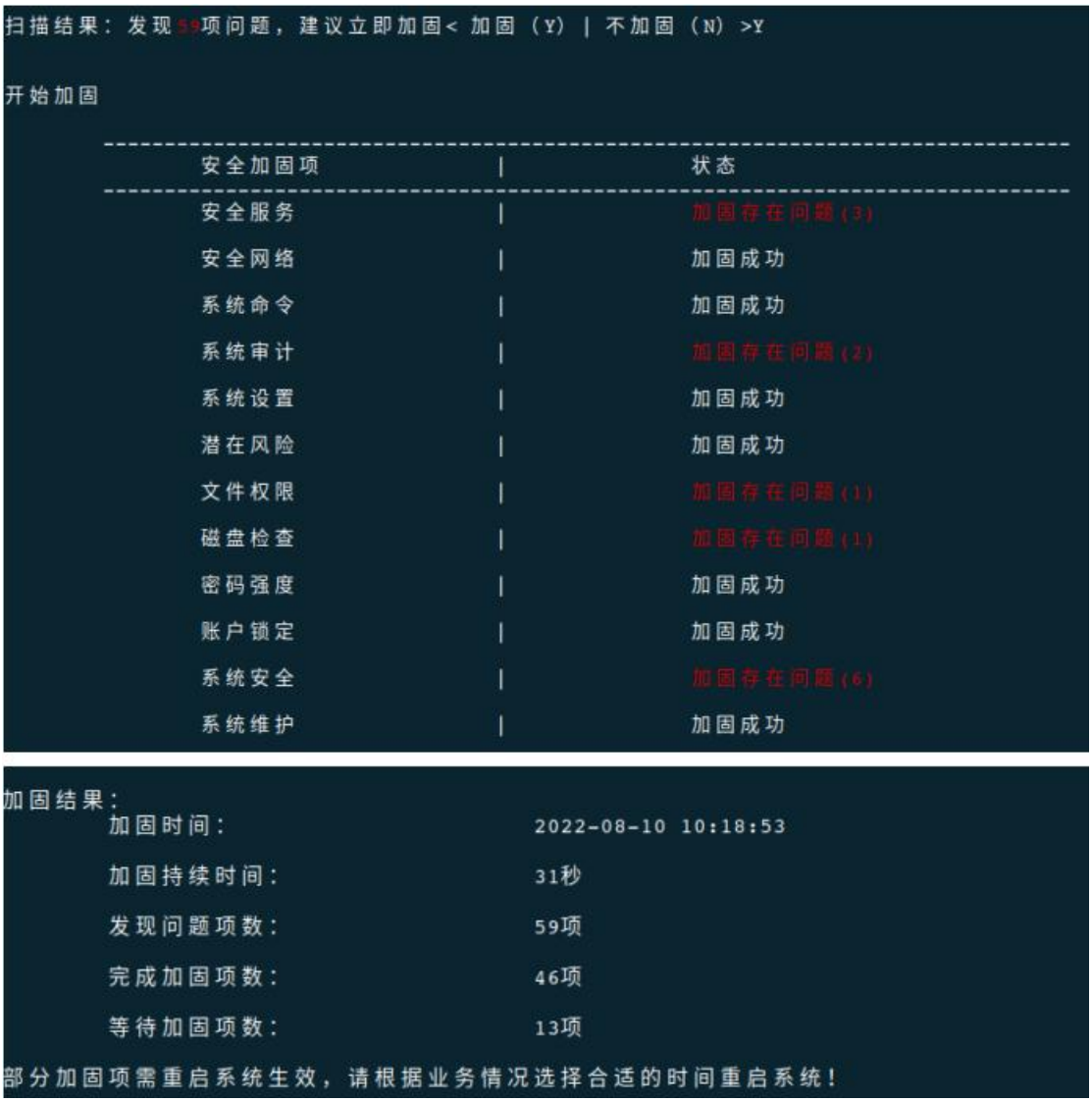


**图 76 一键加固**

5）一键还原

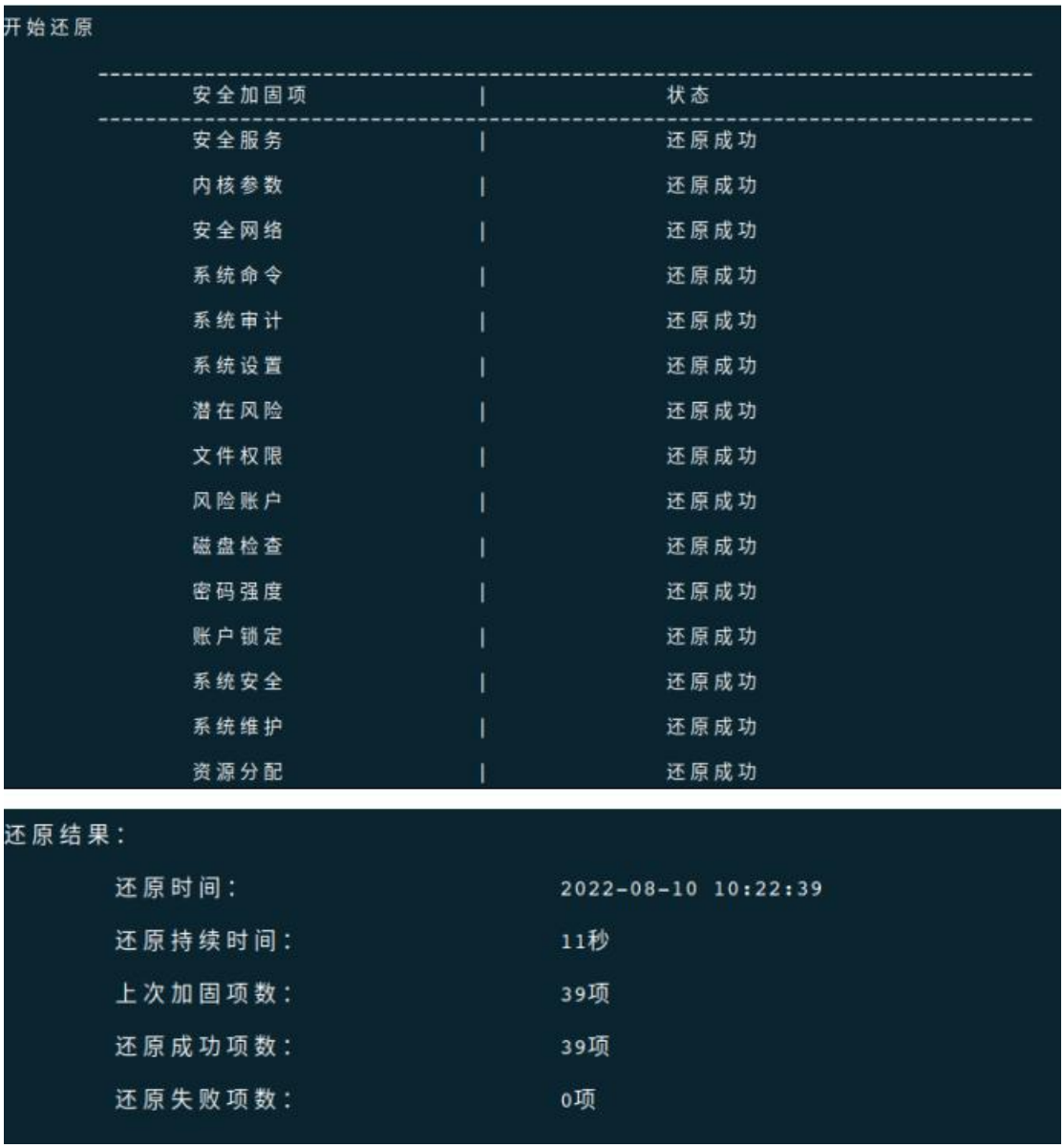


**图 77 一键还原**

6）显示上次操作结果

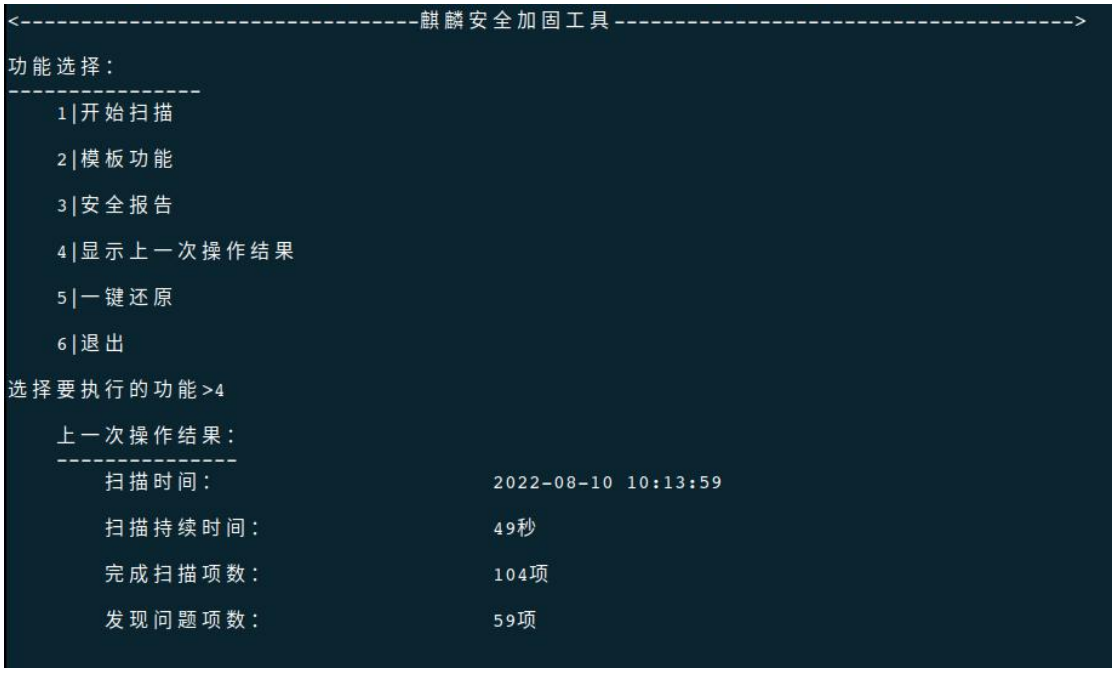


图 78 显示上次操作结果