主机安全

实践教程

腾讯云

文档目录

实践教程
主机安全等保测评解读

最近更新时间：2024-11-14 10:58:12

等保标准解读

腾讯主机安全（Cloud Workload Protection，CWP）产品符合等级保护2.0标准体系主要标准。根据《网络安全等级保护基本要求》（GB/T 22239-2019），腾讯主机安全（仅限专业版、旗舰版且已购买日志分析）满足第三级及以下安全要求：

序号	等保标准章节	等保标准序号	等保标准内容	对应功能描述
1	安全区域边界—边界防护	8.1.3.1 c）	应能够对内部用户非授权联到外部网络的行为进行检查和限制。	主机安全支持对云服务器非授权恶意外联到外部恶意域名，IP 地址的行为进行检测和拦截。
2	安全区域边界—入侵防范	8.1.3.3 a）	应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。	主机安全支持检测和阻断暴破攻击，并能对常见的网络攻击进行检测，部分漏洞支持一键漏洞防御。
3	安全区域边界—入侵防范	8.1.3.3 b）	应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。	主机安全可检测云服务器系统层和应用层的主动外联和攻击行为，对进程，命令异常行为进行告警。
4	安全区域边界—入侵防范	8.1.3.3 c）	应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。	主机安全支持基于主机、网络、云平台的安全数据进行分析，实现对挖矿、勒索、木马、蠕虫等新型攻击进行检测告警。
5	安全区域边界—入侵防范	8.1.3.3 d）	当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。	主机安全在检测到暴破攻击时，会记录来源 IP、来源地、被攻击服务器 IP/名称、端口、协议、用户名、时间、破解状态、阻断状态并进行告警。
6	安全区域边界—安全审计	8.1.3.5 b）	审计记录应包括事件的日期和时间、用户、事件类型、	主机安全支持服务器登录审计，记录信息包括来源

			事件是否成功及其他与审计相关的信息。	IP、来源地、服务器 IP/名称、登录用户名、登录时间、状态、危险等级。
7	安全计算环境—身份鉴别	8.1.4.1 a）	应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。	主机安全基线检查能力支持对云服务客户登录配置和密码复杂度进行定期安全检查，对风险项进行预警并提供安全建议。
8	安全计算环境—身份鉴别	8.1.4.1 b）	应启用登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。	主机安全支持主机登录失败防御配置，可灵活设定在一定时间段内多次登录失败后锁定用户的规则。
9	安全计算环境—身份鉴别	8.1.4.1 c）	当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	主机安全支持对远程管理的不当配置进行检查，如有禁止使用 telnet 基线检查。
10	安全计算环境—访问控制	8.1.4.2 b）	应重命名或删除默认账户，修改默认账户的默认口令。	主机安全支持对账户权限配置检查，资产管理支持展示所有可登录账号，支持默认弱口令安全检查，发现风险时进行告警并提供修复建议。
11	安全计算环境—访问控制	8.1.4.2 c）	应及时删除或停用多余的、过期的账户，避免共享账户的存在。	主机安全支持对云服务器账户进行安全配置检查，资产管理支持展示所有登录账号，支持账户登录 IP 异常时进行告警，避免共享账户存在。
12	安全计算环境—安全审计	8.1.4.3 a）	应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。	主机安全支持对云服务器账户登录操作进行记录，以及高危命令、高危操作的审计。
13	安全计算环境—安全审计	8.1.4.3 b）	审计记录应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。	主机安全日志记录包括主机 IP、主机实例 ID、账户、源 IP、目的 IP、进程 ID 端口、事件类型、发生时间、动作策略等内容。

14	安全计算环境—安全审计	8.1.4.3 c）	应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	主机安全产品支持日志审计存储功能，可存储至少6个月内的日志数据，不同租户使用完全独立的日志空间，日志数据有多副本备份机制。
15	安全计算环境—入侵防范	8.1.4.4 b）	应关闭不需要的系统服务、默认共享和高危端口。	主机安全资产管理支持对云服务器上运行的服务、进程、开放的端口进行统一管控。
16	安全计算环境—入侵防范	8.1.4.4 c）	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。	主机安全支持添加主机登录 IP 地址白名单，非白名单内用户登录将被拦截。配合安全组实现云上网络管理和限制。
17	安全计算环境—入侵防范	8.1.4.4 e）	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。	主机安全支持检测 Linux 软件漏洞、Windows 系统漏洞、Web-CMS、应用漏洞、应急漏洞，评估风险级别并提供修复建议。
18	安全计算环境—入侵防范	8.1.4.4 f）	应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。	主机安全支持检测重要节点的入侵行为，主要包括恶意文件，异常登录，密码破解，恶意请求，高危命令，反弹 shell，本地提权，文件篡改等，提供告警及部分主动阻断能力。
19	安全计算环境—恶意代码防范	8.1.4.5	应采用免受恶意代码攻击的技术措施或采用主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。	主机安全支持恶意文件查杀，实时监测木马，病毒，并自动隔离。
20	安全管理中心—安全管理	8.1.5.3 a）	应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计。	主机安全支持通过控制台对云资源进行安全管理操作，能对登录行为、高危命令进行审计。

21	安全管理中心—安全管理	8.1.5.3 b）	应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。	主机安全支持通过控制台对系统中的安全策略进行配置。
22	安全管理中心—集中管控	8.1.5.3 e）	应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理。	主机安全支持漏洞集中管理，恶意代码检测和隔离。

等保合规基线策略

腾讯云主机安全默认提供 等保合规基线策略，支持对基线检测项的定期检测和一键检测，帮助了解基线通过率及风险情况，提供基线和检测项的风险等级和修复建议，有助于您快速整改，满足等保合规要求。以下为等保合规支持检测项：

基线分类	基线名称	包含的检查项数量
等保二级	等保二级-CentOS 6安全基线检查	16
	等保二级-CentOS 7安全基线检查	18
	等保二级-CentOS 8安全基线检查	16
	等保二级-Ubuntu 14安全基线检查	19
	等保二级-Ubuntu 16安全基线检查	19
	等保二级-Ubuntu 18安全基线检查	21
	等保二级-Ubuntu 20安全基线检查	29
等保三级	等保三级-CentOS 6安全基线检查	27
	等保三级-CentOS 7安全基线检查	31
	等保三级-CentOS 8安全基线检查	36
	等保三级-Ubuntu 14安全基线检查	35
	等保三级-Ubuntu 16安全基线检查	33
	等保三级-Ubuntu 18安全基线检查	40
	等保三级-Ubuntu 20安全基线检查	48

	等保三级-Windows 2008安全基线检查	19
	等保三级-Windows 2012安全基线检查	19
	等保三级-Windows 2016安全基线检查	19

漏洞自动修复

最近更新时间：2025-04-03 15:58:32

本文将为您介绍自动修复漏洞的实践教程。

> **注意：**
> 自动修复漏洞可能会在您的主机上执行命令，可能影响到正在运行的应用或系统核心组件，可能影响您业务的连续性。对于核心业务主机，建议您充分考虑后再决策修复哪些漏洞及漏洞修复的先后顺序。

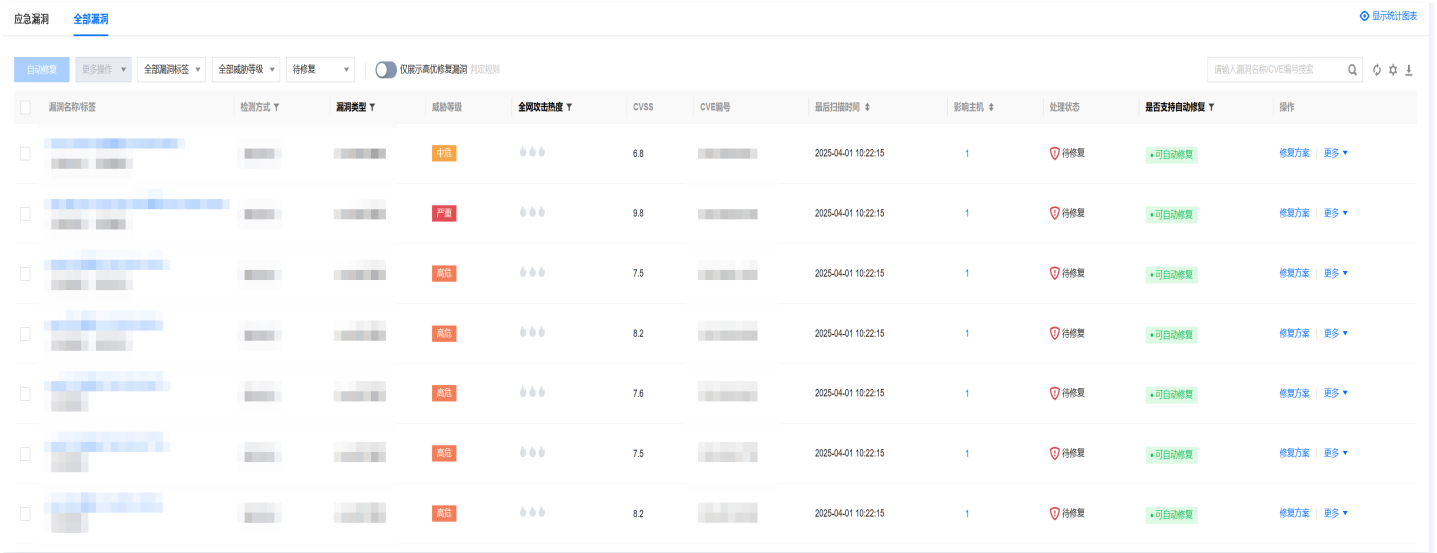
限制说明

- 支持修复的主机：仅支持腾讯云上的 CVM 服务器（主机安全客户端在线，且已绑定主机安全旗舰版授权）。
- 支持自动修复的漏洞：Linux 软件漏洞（部分）、Web-CMS 漏洞（部分）。

操作指南

1. 登录 主机安全控制台，单击左侧导航中的**漏洞管理**，底部可见漏洞检出列表。
2. 在**漏洞列表**中，分为应急漏洞、全部漏洞两类，由于均是从检出维度展示漏洞，功能差异不大，下面以**全部漏洞**作为示例，说明漏洞自动修复各个步骤。

> **说明：**
> - 漏洞修复优先级：应急漏洞 > 高优修复漏洞 > 全部漏洞。
> - 可自动修复的漏洞在操作列中有**自动修复**操作，暂不可自动修复的漏洞在操作列中有**修复方案**操作。



步骤1：查看漏洞详情

单击**自动修复**，打开漏洞详情弹窗。

步骤2：选择需要修复的主机

1. 在受影响的服务器列表中选择您要修复的主机，单击**修复**。

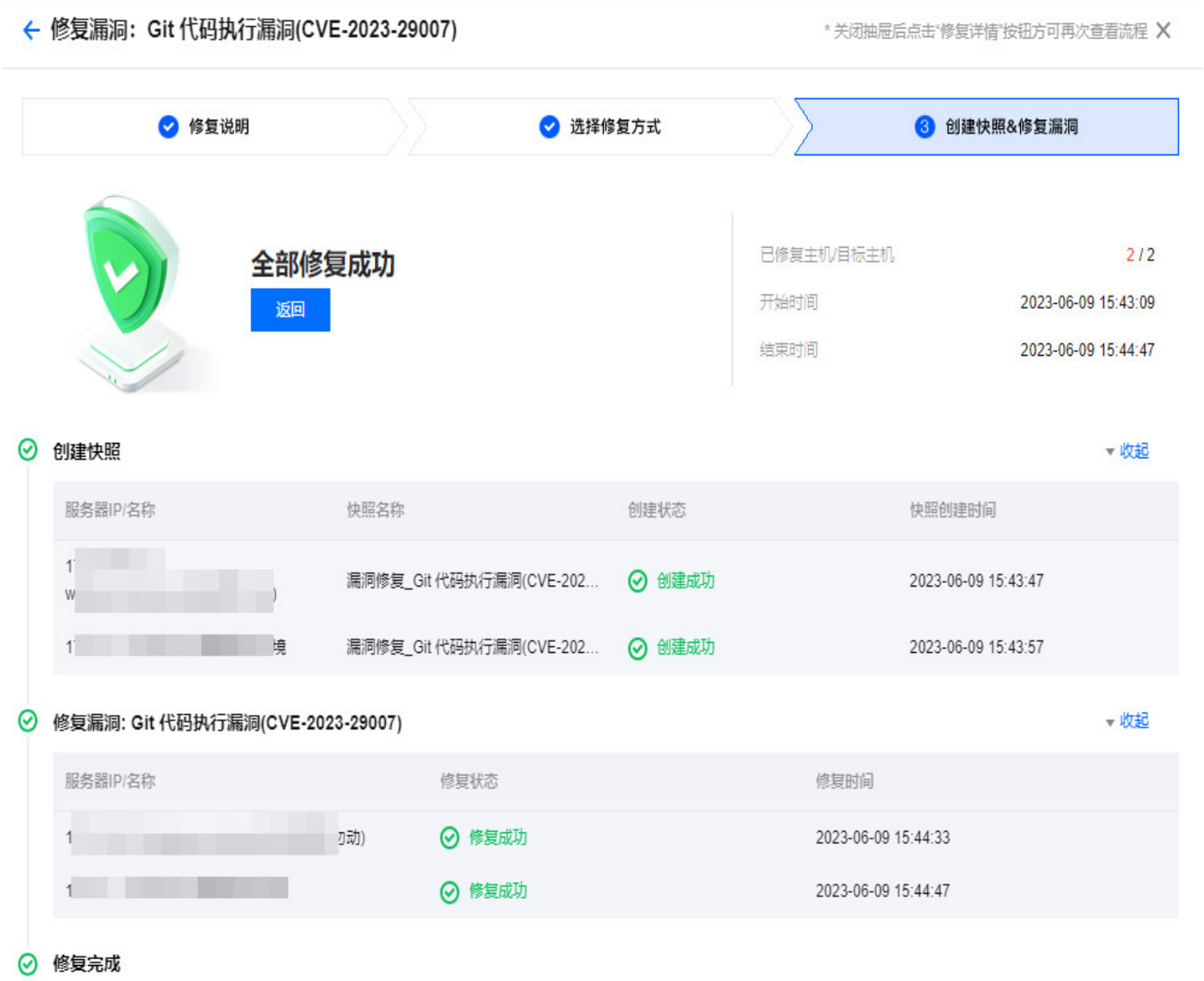
2. 在确认修复弹窗中，单击**确定**，进入修复漏洞页面。

步骤3：选择是否创建快照

1. 在修改漏洞页面，确认修复主机范围，单击**下一步**。
2. 根据实际需求选择修复方式：
   - 自动创建快照并修复：支持设置快照名称、快照保存时长（3天、7天、15天，建议保留7天时间，以便在有需求的情况下及时回滚）。
   - 不创建快照直接修复：若今日所选修复主机均已创建过快照，此选项将变为可选状态。

步骤4：开始修复

单击**确认修复**开始修复漏洞，您可查看当前修复的情况。



步骤5：查看主机状态变更

返回**漏洞详情**，关注主机状态变更。若漏洞修复失败，状态则为修复失败；若漏洞修复成功，状态则变更为已修复。

- 漏洞修复后，若对您的业务产生了较大影响，您可单击**回滚**操作，将引导前往 云服务器 > **快照列表**，选择您修复前创建的快照进行回滚。回滚成功后，请重启服务器，对漏洞进行重新扫描。
- 漏洞修复后，可进行**重新扫描**操作，再次验证漏洞是否已修复。
- 漏洞修复后，也可单击**修复详情**操作，查看修复的具体过程。

扫码安全登录

最近更新时间：2025-05-29 11:32:32

扫码安全登录功能允许用户仅通过微信扫码验证即可完成服务器登录，无需输入密码。该功能有效防止黑客的暴力破解攻击，从而进一步提高服务器的安全性，同时也增加了登录的便利性。本文将向您介绍扫码安全登录的实践教程。

注意：

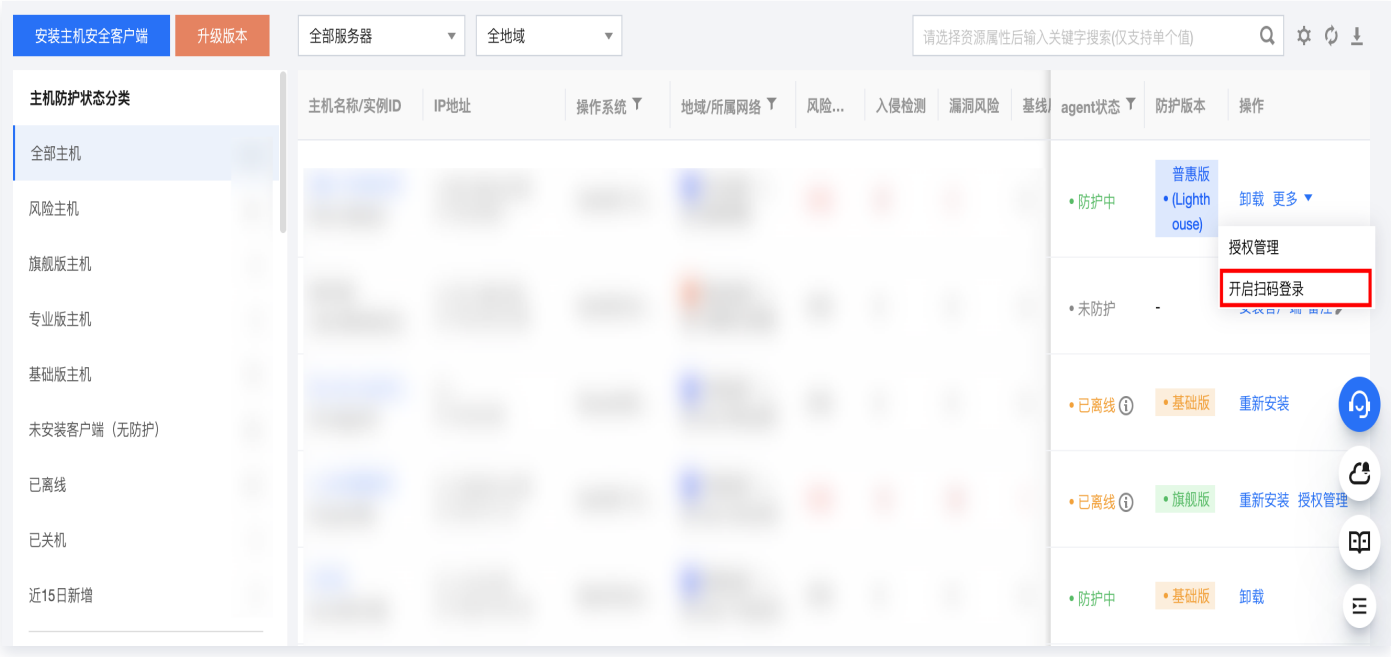
- 启用扫码登录后，将用微信扫码验证腾讯云账号的方式替代密码登录，这可能会影响到相关自动化业务。同时，在使用 SSH 相关的协议时，虽然支持 SCP、SFTP、RSYNC、GIT、MOSH 等场景，但暂不支持基于 SSHFS 协议的文件夹挂载等场景。
- **对于核心业务的主机，建议您充分考虑后再决策是否更改登录方式。**

限制说明

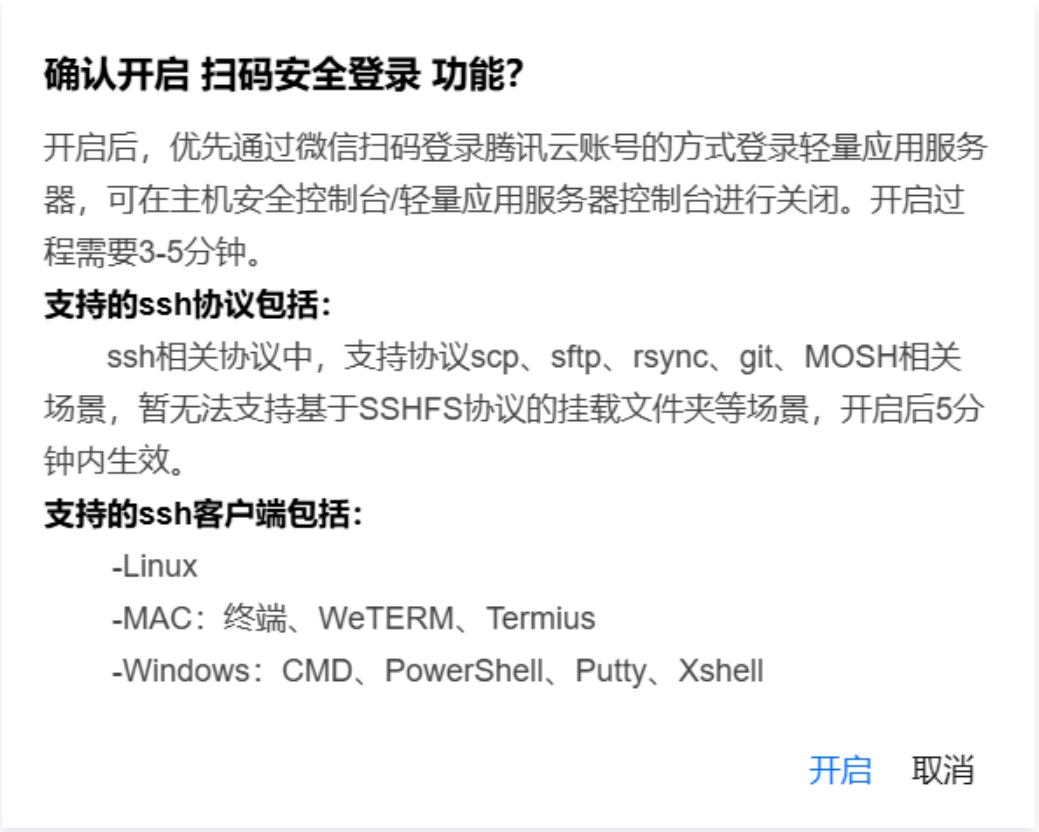
- 支持的主机类型：仅限于腾讯云上的 CVM/Lighthouse 服务器（要求主机安全客户端在线）。
- 支持的登录用户：机器所属的腾讯云子账号及其主账号，或经 CAM 授权的其他腾讯云账号。
- 支持 SSH 客户端：CMD、PowerShell、Putty、Xshell、终端、WeTERM、Termius 等。

步骤1：配置登录方式

1. 登录 主机安全控制台，在左侧导航栏，单击**主机列表**。
2. 在主机列表中，右侧找到对应实例，在操作项中选择**更多**，单击**开启扫码登录**。



3. 单击**开启**，开启后该服务器优先通过微信扫码登录腾讯云账号的方式登录。

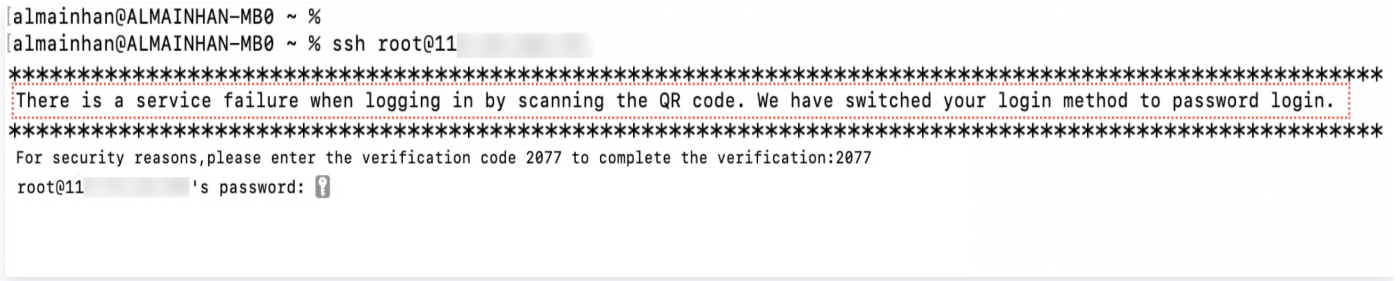


步骤2：终端发起登录

1. 开启扫码登录后，SSH 命令行输入实例 IP 后弹出二维码，使用微信扫码将会进入腾讯云助手小程序进行身份认证，完成认证后即可完成登录。

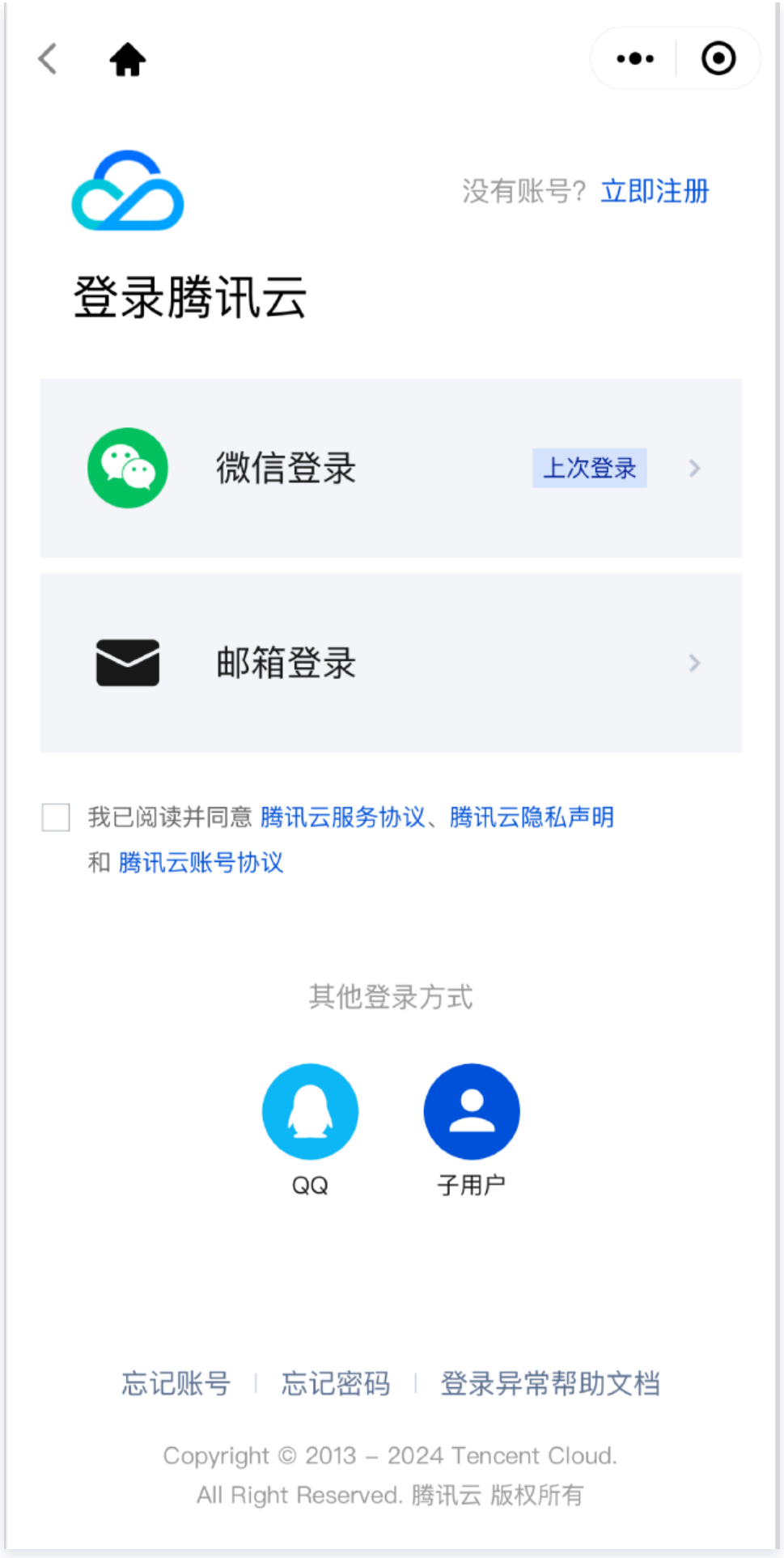
> **说明：**
> 如果二维码显示有问题，请通过下方提供的 URL 在网页中打开二维码图片。

2. 扫码登录服务异常时将自动降级到常规的密码登录，并增加人机校验兜底策略，输入随机数完成认证后可通过密码登录的方式完成登录。

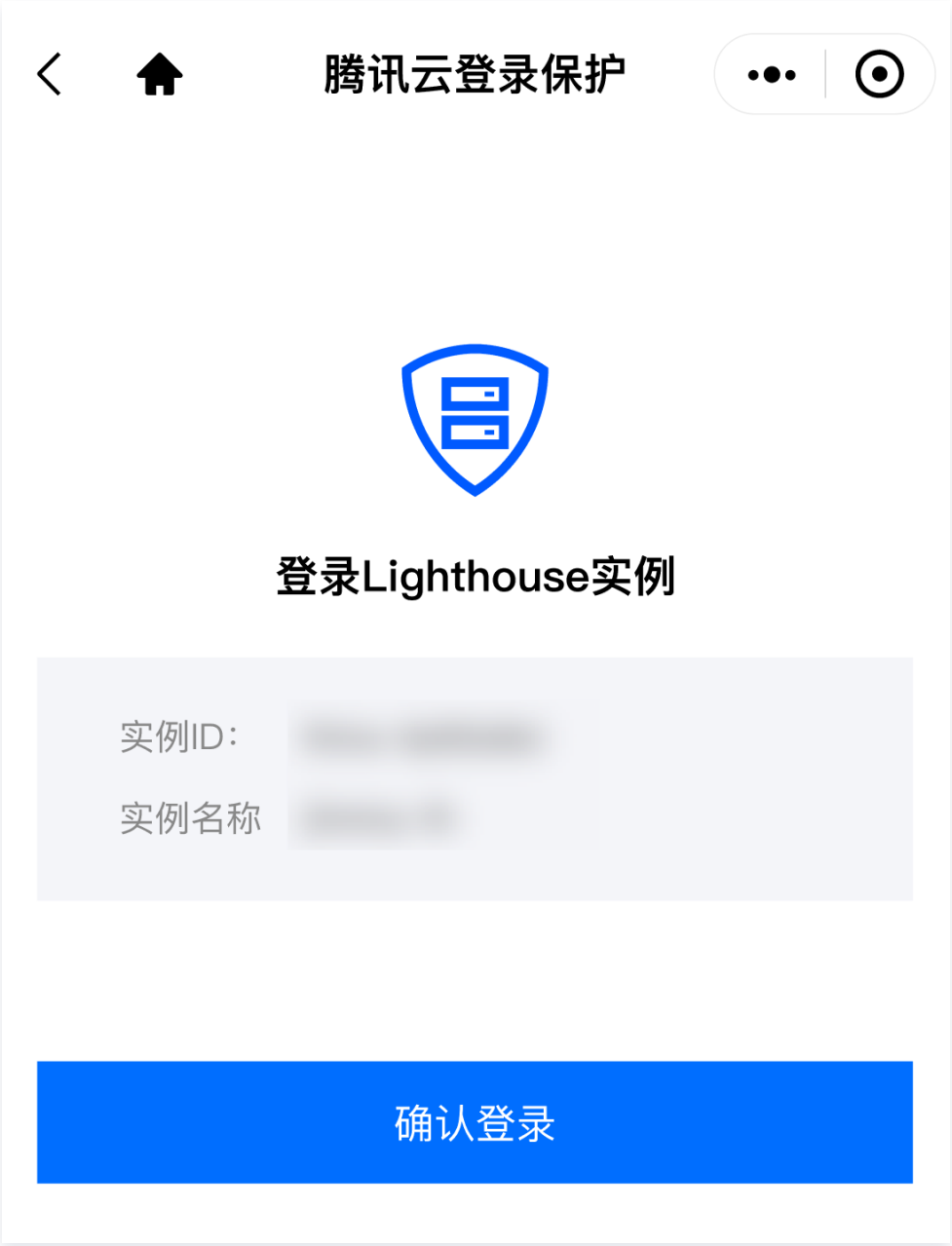


步骤3：小程序验证

1. 扫码后打开腾讯云助手，选择登录方式登录腾讯云账号以完成校验。


没有账号？立即注册
登录腾讯云
微信登录
上次登录
邮箱登录
我已阅读并同意 腾讯云服务协议、腾讯云隐私声明
和 腾讯云账号协议
其他登录方式
QQ
子用户
忘记账号
忘记密码
登录异常帮助文档
Copyright © 2013 – 2024 Tencent Cloud.
All Right Reserved. 腾讯云 版权所有

2. 成功登录腾讯云账号，单击**确认登录**，校验该账号登录服务器的权限后，通过验证完成登录。



恶意文件处理

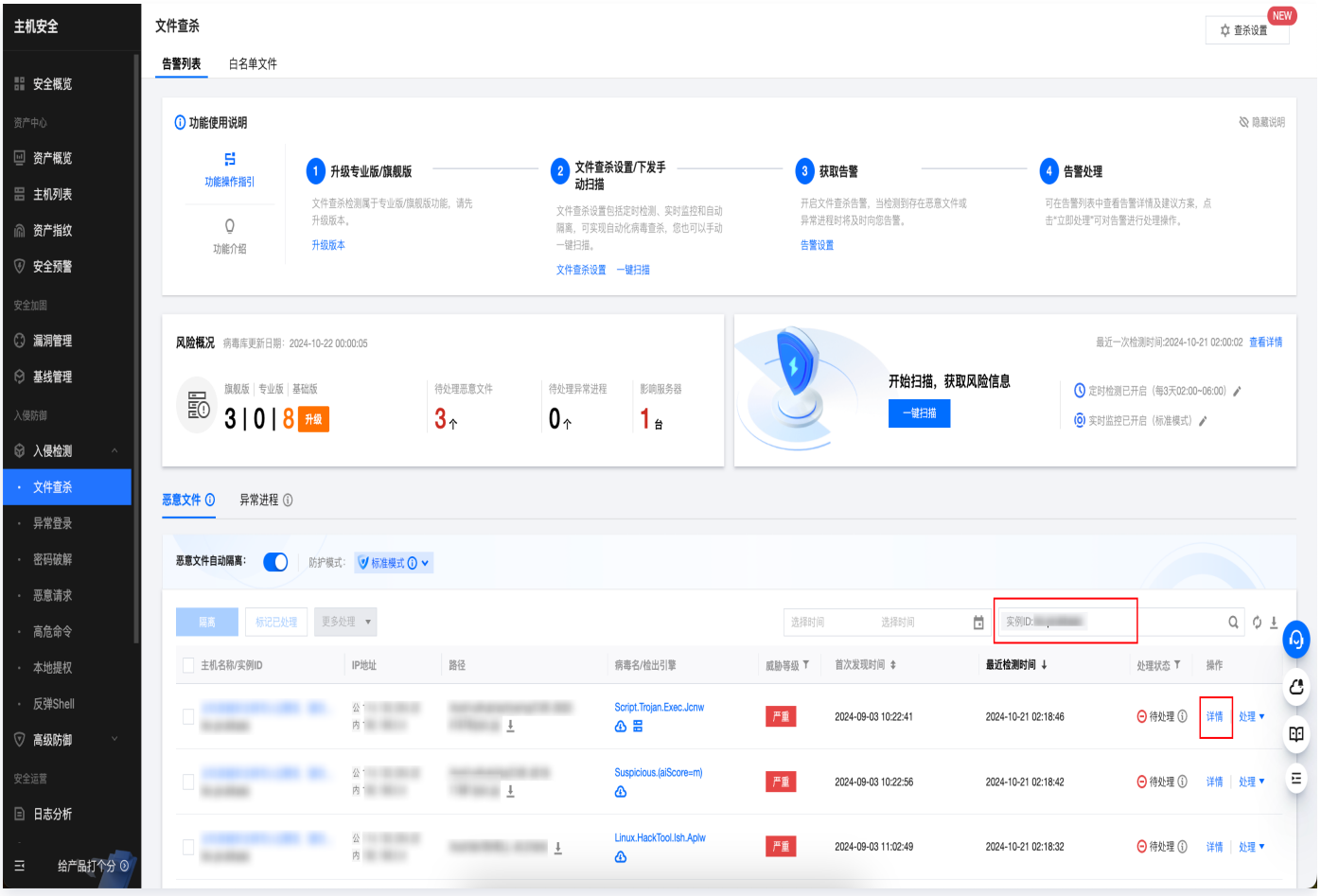
最近更新时间：2025-04-29 10:58:42

当用户腾讯云账号下的服务器被检出存在恶意文件，主机安全若发现该文件没有命中文件白名单，则会触发实时告警。

处理步骤

在收到恶意文件告警后，请按照下列步骤进行操作：

1. 登录 主机安全控制台 ，在左侧导航栏，选择**入侵检测** > **文件查杀**。
2. 在文件查杀页面，通过告警资产**实例 ID** 进行搜索，定位到具体告警并单击**详情**。



3. 查看告警详情后，请确认该恶意文件是否误报，若是误报，请执行步骤4，若不是误报，请执行步骤5。

> **说明：**
> 该恶意文件是否误报，可结合以下几种方式判定：
> - 联系业务团队判断该文件是否是业务正常运行所需文件。
> - 查询威胁情报，判断该文件是否被外网标记为恶意样本。
> - 该文件行为是否导致进一步触发更多告警。

- 联系 安全专家服务 。

4. 明确是误报，请将该文件加入白名单，后续再次检出此文件将被忽略，不会产生告警，并联系我们 反馈误报 。

5. 明确不是误报，请参考告警详情中的修复建议进行处理。

- 可单击**隔离**，对该文件进行隔离并结束相关进程的操作，该告警处理状态将变为“已隔离”。
- 可登录该主机，找到对应文件，手动进行删除或隔离并结束相关进程，然后在控制台对该告警标记已处理，该告警处理状态将变为“已处理”。

6. 在文件查杀页面，单击右上角的**查杀设置**，建议开启自动隔离开关，检出恶意文件则立即自动隔离。

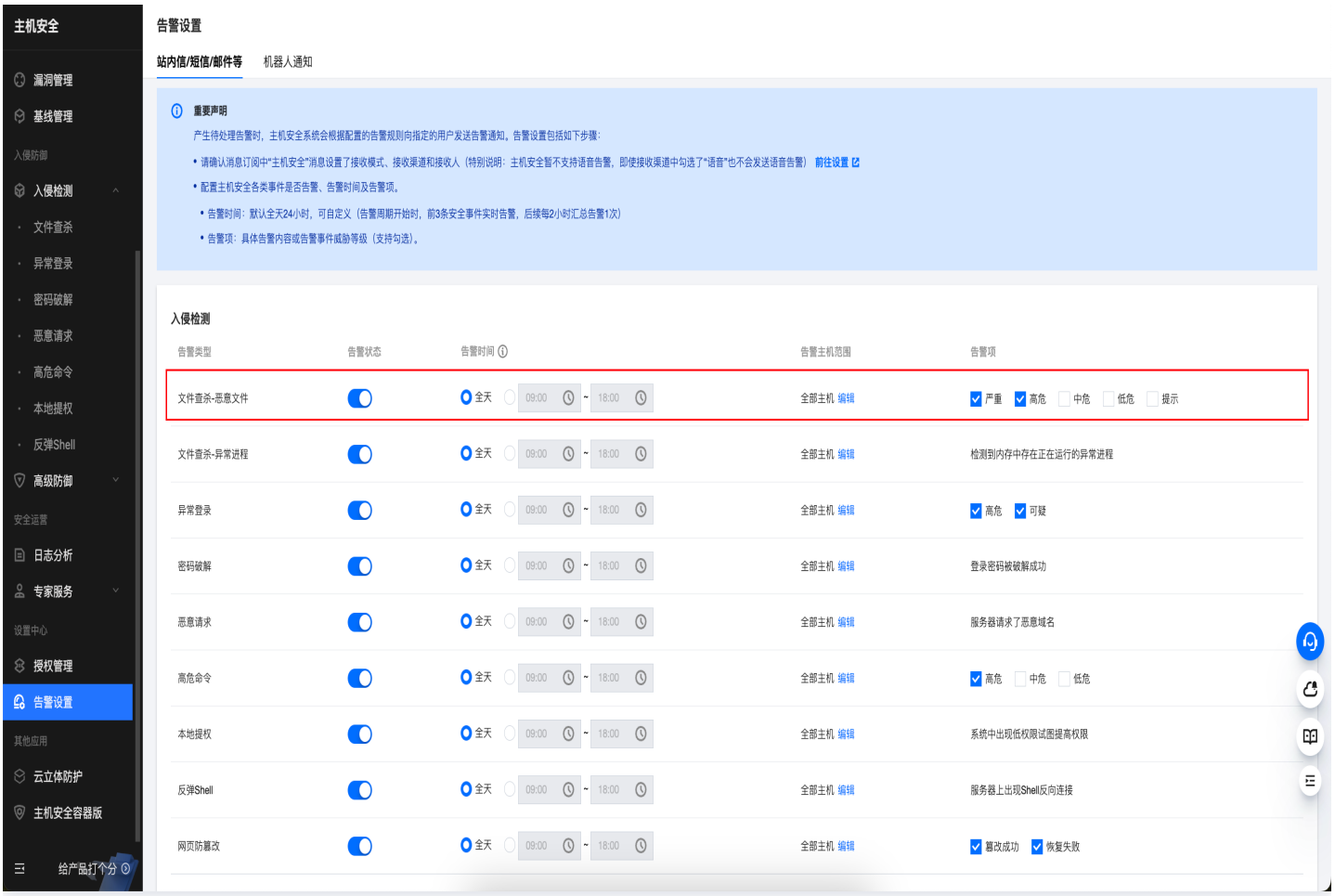
说明：

- **并非所有检出的恶意文件均能被自动隔离，部分恶意文件仍需用户手动确认隔离，建议检查文件查杀中的告警列表，确保已全部处理。**
- **若出现误隔离，请在已隔离列表中对文件进行恢复。**
- **开启或关闭自动隔离，均需要进行配置，实际生效存在几分钟延迟。**

热点问题

恶意文件在哪里配置告警?

在 告警设置页面，配置**文件查杀-恶意文件**的告警时间、告警范围和告警项。



恶意文件如何设置定期检测?

在 文件查杀页面，单击右上角的**查杀设置**，打开查杀设置弹窗，进行定时扫描设置。

若文件已被删除，再次对进行恶意文件扫描，原告警处理状态会变成什么？

原告警处理状态将变为“已清理”。