阿里云
安全众测

产品简介

文档版本：20181112

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止：** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告：** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明：** 您也可以通过按**Ctrl** + **A**选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

1 什么是先知（安全众测）

先知（安全众测）是一个帮助企业建立私有应急响应中心的平台。

先知（安全众测）是一个帮助企业建立私有应急响应中心的平台（帮助企业收集漏洞信息）。企业加入先知（安全众测）平台后，可自主发布奖励计划，激励先知平台的安全专家来测试和提交企业自身网站或业务系统的漏洞，保证安全风险可以快速进行响应和修复，防止造成更大的安全损失。

旨在为企业建立高效完善的安全应急响应中心（Security Response Center）。企业通过入驻先知（安全众测）平台，可以借助先知平台众多优质、可信的白帽子及时发现现有业务的安全问题，包括业务逻辑漏洞、权限问题等安全工具无法有效检测的漏洞等，尽早发现存在的漏洞可以有效地减少企业可能的损失。并且，随着业务的不断发展，通过白帽子的持续安全检测可以及时发现新业务的安全问题。先知平台会为所有入驻企业的漏洞严格保密，从而避免漏洞被恶意宣传。

说明：

白帽子指通过先知平台参与漏洞提交过程的安全专家，能够识别计算机系统或网络系统中的安全漏洞，但并不会恶意利用，而是报告漏洞，帮助企业在被其他人恶意利用之前修补漏洞，维护计算机和互联网安全。

功能描述

- **自主设定奖励计划**

  企业可以自由设定高、中、低危漏洞的奖励金额和奖励范围，安全专家可实时查看到奖励计划。

- **漏洞收集**

  加入先知（安全众测）平台后，外部安全专家可通过先知平台给企业提交漏洞，提交后将由平台进行审核，您也可同步看到进度

- **免费审核漏洞**

  公测期间，外部安全专家提交的漏洞，平台免费为企业进行审核，审核后将通知企业进行漏洞修复

- **协助漏洞修复**

  先知平台会协助用户进行修复漏洞，若可以提供修复方案，平台会给企业提供参考的漏洞修复方案

2 应用场景

先知（安全众测）平台的应用场景。

企业经常被其他平台曝光漏洞，对声誉会造成很大影响，甚至造成直接金钱损失。因此，企业需要建立一个漏洞收集渠道，以免外部白帽子将漏洞提交到其他平台。

企业加入先知（安全众测）平台后，可自主发布奖励计划，吸引先知平台上的白帽子提交漏洞。同时，先知平台不会公开任何漏洞细节。

3 产品优势

先知（安全众测）平台的优势。

私有的安全中心

- 不公开任何漏洞标题及细节
- 不进行漏洞负面炒作和公关
- 完全自定义漏洞奖励标准

可靠的安全专家

- 100% 支付宝实名认证的安全专家
- 共享阿里巴巴集团安全应急响应中心（ASRC）安全专家团队和能力
- 漏洞提交者可靠，漏洞影响可追踪

公正的漏洞运营

- 共享阿里巴巴集团漏洞运营团队的安全能力
- 漏洞审核流程私密、公正
- 奖金评定、等级确定双重审核

可信的先知平台

- 建立安全专家与企业联系的桥梁
- 加入先知（安全众测）平台，共建互联网生态圈
- 信任、闭环、共赢的先知平台

4 名词解释

先知（安全众测）相关的名称解释。

白帽子

白帽子指通过先知平台参与漏洞提交过程的安全专家。白帽子能够识别计算机系统或网络系统中的安全漏洞，但并不会恶意利用，而是报告漏洞，帮助企业在被其他人恶意利用之前修复漏洞，维护计算机和互联网安全。

先知称号

白帽子通过提交漏洞可获得先知称号，最终根据获得的积分来决定先知的等级，所以可以看到“四级先知”、“五级先知”等名词。

奖励计划

加入先知（安全众测）平台的企业可以设置奖励计划，即企业高、中、低危漏洞分别对外展示奖励金额，最终先知平台的运营人员也会根据这个奖励金额来决定发放多少钱给白帽子。

奖励系数

高、中、低危漏洞均对应固定范围的贡献值，加入先知（安全众测）平台的企业只需要设定奖励系数即可。例如，高危漏洞基础贡献值为 60-80 分，企业设置奖励系数为 10，则最终高危漏洞奖励计划的金额范围是 600-800 元。