ALIBABA CLOUD

阿里云

用户指南

文档版本：20220216

阿里云

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
危险	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。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会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，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	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。	单击**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。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 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。	`switch {active|stand}`

目录

1.开通免费试用

威胁情报服务支持7天免费试用，每个云账号仅可获得一次免费试用机会。

背景信息

您需要在威胁情报控制台页面获得免费试用的资格，开通免费试用后才可以使用威胁情报服务。

> **说明** 免费试用期间，您可以享受最多10次免费查询额度（包含查询IP、域名和文件的总次数）。使用了10次情报搜索后，您的免费查询额度将为0，您需要升级才可以继续使用威胁情报服务。

操作步骤

1. 登录威胁情报服务控制台。
2. 在**免费试用**对话框中单击**立即领取**。

2.概览

威胁情报概览页面为您展示近30天全球所有网上用户和您的企业已遭受的威胁的整体情况和统计数据。

操作步骤

1. 登录威胁情报控制台。
2. 在左侧导航栏单击**概览**。
3. 在**概览**页面，查看威胁情报服务检测到的全球互联网用户和您的企业已遭受的威胁事件和统计数据。

   您可以在**概览**页面执行以下操作：

   - 查看威胁情报服务的可使用量和可使用天数。
   - 查看针对全球威胁情报的统计数据。

     在**概览**页面，单击**阿里云全球情报**，查看阿里云检测到的全网用户遭受的威胁情况，包括近30天阻止的威胁事件总数、近30天威胁趋势、攻击来源地区和攻击目的地区、攻击数量排名前10的行业及其不同攻击类型的占比情况、30天IOC命中数量。

     > **说明** 30天IOC命中数量表示阿里云过去30天对安全事件划分的威胁生命周期阶段，包含初始访问、执行、持久化、特权提升等12个阶段。这12个阶段中，威胁等级从左到右依次递增，越靠近右侧（即**影响**阶段）的威胁事件，威胁程度越高。

   - 查看您企业中存在的威胁情况的统计数据。

     在**概览**页面，单击**我的企业**，查看阿里云检测到您资产中遭受的威胁情况，包括攻击来源地区和攻击目的地区、Top 5威胁事件的类型以及对应的攻击次数、30天IOC命中数量。

     > **说明** 您当前登录账号已购买了云安全中心，**我的企业**页签才会展示出来。

   - 搜索任意IP、域名或文件MD5值，确认其是否为恶意来源。

     在右上角的搜索框中输入您需要排查的IP、域名或文件MD5值后，单击搜索符号，会跳转到**搜索**页面。详细内容，请参见搜索。

3.搜索

您可以通过威胁情报搜索功能，对全网IP、域名和文件进行搜索，帮助您及时有效排查存在风险的恶意IP、域名和可疑文件。

背景信息

威胁情报服务会在搜索结果中为您展示指定IP、域名和文件的详细信息和威胁关联数据，您可以通过搜索结果中的信息判断是否存在恶意IP（仅支持IPv4）、域名或存在威胁的进程文件。

每个阿里云主账号针对每类IOC（即IP、域名或MD5）的查询上限为20次/天。如果当天的查询额度耗尽，您需要根据页面提示购买服务或申请更高权限。

> **说明** 免费试用期间，您最多有10次IP地址查询的额度。您查询过10次IP地址后，免费查询额度将为0，您需要充值续费才可以继续使用威胁情报服务。

操作步骤

1. 登录威胁情报控制台。
2. 在左侧导航栏单击**搜索**。
3. 在**阿里云威胁情报**搜索栏中输入您需要查询的可疑或恶意IP地址、域名或文件MD5值，或者上传需要检测的文件，然后单击图标进行查询。

   > **说明** 仅支持搜索单个IP地址，不支持同时搜索多个IP地址；IPv6地址暂不支持。

   执行搜索操作后，会跳转至对应的报告页面。不同的报告页面介绍如下：

   - **IP报告**

     您可以在**IP报告**页面查看该IP地址的基本信息、攻击风险程度分析等信息。详细说明如下：

     - **威胁等级**

       威胁情报服务将全球范围内的IP地址划分为正常、可疑和高危3个威胁等级。如果检索的IP地址被识别为高危等级，建议您立即对该IP地址进行处理。

     - **该可疑或恶意IP的基本信息**

       该IP地址的基本信息包括所在国家、城市、ASN编码、存在关联的域名、文件数量、IP标签等信息。

       > **说明** 威胁情报服务对该IP地址进行威胁检测和分析后，会提供该IP的风险威胁标签。标签包括暴力破解、失陷主机、僵尸网络、木马、蠕虫、矿池、Web攻击等主要威胁类型，不支持自定义。如果威胁情报判定该IP地址存在威胁，**IP标签**模块会展示红色标签和具体的标签名称为您提供警示，请您及时关注。如果威胁情报判定该IP地址是正常IP，**IP标签**模块会展示为绿色标签，并提供具体的标签名称供您参考。

     - **威胁概述**

       威胁概述页签为您展示了该IP地址的Top 5攻击偏好、攻击数量、攻击风险程度分类和威胁活动信息。

- **攻击路径测绘**

  攻击路径测绘页签为您展示了该IP地址的情报来源、首次发现时间、最后活跃时间和威胁标签。

- **RDNS**

  RDNS页签展示了该IP的反向域名解析信息，包括首次发现时间、最后活跃时间、关联度、以及对应域名的一级标签。域名展示顺序按照域名的关联度由高到低展示。

- **相关样本**

  相关样本页签展示了该IP的访问样本和下载样本信息，包括文件MD5、扫描时间、家族标签、威胁等级。

- **相关URL**

  相关URL页签展示了该IP的所有相关URL、发现时间、威胁等级。

- **域名报告**

  您可以在**域名报告**页面查看该域名是否存在威胁和对应的威胁等级、域名的Whois信息、域名注册时间和有效期、域名的威胁详情等信息。详细说明如下：

  - **威胁等级**

    威胁情报服务将全球范围内的域名划分为正常、可疑和高危3个威胁等级。如果检索的域名被识别为高危等级，建议您立即对该域名进行处理。

  - **报告摘要信息**

    报告摘要信息包括该域名历史上检测出的恶意IP数量、域名上的恶意URL地址、该域名的恶意子域名数量、与该域名进行过恶意通信的样本数量、该域名的注册时间和过期时间。报告摘要中如果有项目为空，表示当前该项未产生检测结果。

  - **域名的标签**

    威胁情报服务对该域名行威胁检测和分析后，会提供该域名的风险威胁标签。标签包括暴力破解、失陷主机、僵尸网络、木马、蠕虫、矿池、Web攻击等主要威胁类型，标签不支持自定义。如果威胁情报判定该域名存在威胁，**域名标签**模块会展示红色标签和具体的标签名称为您提供警示，请您及时关注。绿色标签表示该文件的基础属性，为您了解该域名提供更多信息。

  - **威胁详情**

    在**威胁详情**页签下的**概述**页签中，展示了该域名的攻击风险程度分类和威胁活动信息。

    在**威胁详情**页签下的**详情**页签中，展示了该域名的威胁情报来源、首次发现时间、最后活跃时间和威胁标签。

- **MD5文件报告**

  您可以在**MD5文件报告**页面查看该文件是否存在威胁和对应的威胁等级、文件报告摘要、静态威胁分析、域名的威胁详情等信息。详细说明如下：

  - **威胁等级**

    威胁情报服务将文件划分为正常、可疑和高危3个威胁等级。如果检索的文件被识别为高危等级，建议您立即对该文件进行处理。

- **报告摘要信息**

  报告摘要信息包括该文件的文件标签、文件名称（即MD5值）、首次发现时间等。

  > **说明** 威胁情报服务对该文件行威胁检测和分析后，会提供该文件的风险威胁标签。标签包括暴力破解、失陷主机、僵尸网络、木马、蠕虫、矿池、Web攻击等主要威胁类型，标签不支持自定义。如果威胁情报判定该文件存在威胁，**文件标签**模块会展示红色标签和具体的标签名称为您提供警示，请您及时关注。绿色标签表示该文件的基础属性，为您了解该文件提供更多信息。

- **静态威胁分析和动态威胁分析结果**

  静态威胁分析采用阿里云自研的威胁检测引擎，有效检测出二进制文件（例如：病毒）和脚本文件（例如：Webshell等）。威胁情报服务使用威胁标签对静态威胁分析结果进行标签分类，标签类别包括恶意、正常、可疑、未检测（表示当前文件不适用于检测引擎），帮助您更精准地判断威胁的类型。

  动态威胁分析是指使用沙箱模拟运行该文件时，监控到的释放文件、发起网络连接和DNS请求这三种动态行为的记录。对于这些相关文件、IP和域名，如果已经被威胁情报服务识别为恶意，则会展示对应的标签信息，帮助您分析该恶意文件可能会涉及到的影响，并进一步发现该文件关联的恶意文件、IP和域名。标签类别包括恶意、正常、可疑、未检测（表示当前文件不适用于指定的检测引擎）。

  > **说明** **释放文件**表示将该文件写入到其他路径；**网络连接**表示该文件与网络进行通信的信息；**DNS请求**表示该文件访问的域名信息。

热门IOC示例表示当天用户搜索量排名前10的IP、域名和文件MD5值。

4. （可选）如果有存在误报或漏洞的情况，您可以在对应报告页面，单击页面右上角的**IOC反馈**，反馈至阿里云威胁情报团队进行进一步分析。

4.资产暴露面

4.1. 资产管理

您可以将需要关注的IP、域名和URL资产导入到威胁情报服务中进行统一管理。

操作步骤

1. 登录威胁情报控制台。
2. 在**资产管理**页面，单击左上角**资产导入**。
3. 在**资产导入**面板中，导入指定的资产信息。

   支持手动导入、模板导入、云账号导入三种方式。