

账号威胁发现 操作指南



腾讯云

【 版权声明 】

©2013–2024 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 商标声明 】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。

您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

操作指南

查看威胁事件

管理可信/威胁 IP

操作指南

查看威胁事件

最近更新时间：2024-02-19 17:34:57

本文为您介绍如何查看威胁事件。

操作步骤

1. 登录 [账号威胁发现控制台](#)，若用户第一次登录，需单击**开通应用**，开启服务应用。
服务开通以后，短时间内威胁列表中不会有数据。一旦有真实威胁发生，该列表中才会有相应的数据。
2. 单击左侧菜单栏**事件列表**进入威胁事件列表页。威胁事件按照威胁程度，分为高、中、低三类。

多个关键字用竖线“ ”分隔，多个过滤标签用回车键分隔					
全部 (2)	低严重 (2)	中严重 (0)	高严重 (0)		
威胁等级	结果类型	资源名称	上次显示时间	影响次数	操作
	CAMS:PermissionHighRiskAct	uin	2019-07-16 21:04:24	1	查看详情 反馈
	CRS:CosHighRiskAct	pref	2019-07-15 14:38:07	1	查看详情 反馈
共 2 项					
每页显示行 10 1 / 1 页					

3. 在列表中，单击对应记录右侧的**查看详情**，可以看到更多信息。

资源名称

资源类型

cam

资源地域

ap-chongqing

风险类型

影响次数 1

风险描述 [查看](#)

第一次发现时间

2019-08-26 17:13:30

最后一次发现时间

2019-08-26 17:13:30

规则名称: 授予子账号超级权限

出现该类型安全威胁的原因如下:

您正在授予子账号超级权限。

操作者UIN	事件名称	操作方式	操作类型	操作IP	操作时间	发现时间	更多详情
	绑定多个策略到用户	ConsoleCall	Write		2019-08-26 17:13:30	2019-08-26 17:17:37	查看

共 1 项

每页显示行 10

1

/ 1 页

4. 在威胁事件详情页下方，单击对应事件右侧的**查看**，页面右侧可以查看事件详情。
此处的详情与威胁详情不同点在于，威胁详情是威胁类型整体详情，此处是事件详情。

资源名称

风险类型

第一次发现时间

2019-08-26 17:13:30

资源类型

cam

影响次数

1

资源地域

ap-chongqing

风险描述

查看

最后一次发现时间

2019-08-26 17:13:30

操作者UIN	事件名称	操作方式	操作类型	操作IP	操作时间	发现时间	更多详情
	绑定多个策略到用户	ConsoleCall	Write		2019-08-26 17:13:30	2019-08-26 17:17:37	查看

共 1 项

每页显示行 10

1 / 1 页

更多详情

资源

资源名称

资源类型

cam

资源地域

ap-chongqing

关联资源

qcs::cam::uin/1...

事件

事件名称

绑定多个策略到用户

操作方式

ConsoleCall

操作类型

Write

操作时间

2019-08-26 17:17:37

操作者

操作者UIN

操作者密钥ID

密钥类型

临时密钥ID

操作者IP

IP所在国家或地区

中国

IP所在省份

广东省

IP所在城市

深圳市

IP服务提供商

中国联通

管理可信/威胁 IP

最近更新时间：2023-05-22 11:51:39

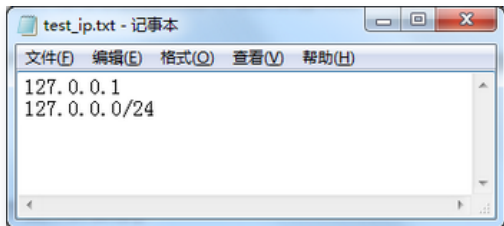
本文为您介绍如何管理可信/威胁 IP。

说明

- 可信 IP 列表：可信 IP 列表包含已列入白名单的，可与您的腾讯云环境安全通信的 IP 地址。腾讯云不会为可信 IP 列表中包含的 IP 地址生成结果。
- 威胁 IP 列表：威胁 IP 列表包含已知的恶意 IP 地址。腾讯云将为威胁 IP 列表中包含的 IP 地址生成结果。
- 若 IP 地址同时存在可信列表和威胁列表中，将优先按照可信 IP 处理。

添加列表信息

1. 将 IP 地址或 CIDR 地址一行一个，写入 TXT 文件并保存。



2. 将上述 TXT 文件上传至开放公有读权限的 COS 即可。具体操作请参见 [上传对象](#)。

3. 单击对象右侧详情，进入对象详情页。

当前路径：13 /

☐	文件名	大小	存储类型	更新时间	操作
☐	2019-07-05_105311.jpg	274.49KB	标准存储	2019-07-05 18:12:22	下载 详情 删除
☐	ceshi.txt	5B	标准存储	2019-07-18 16:04:10	下载 详情 删除
☐	test_ip.txt	13B	标准存储	2019-08-27 14:49:37	下载 详情 删除

4. 复制 COS 文件 URL。

当前路径：1 / test_ip.txt

基本信息

对象名称	test_ip.txt
对象大小	13B
修改时间	2019-08-27 14:49:37
ETag	"9110134f7f4146a8adbb"
对象地址 ①	https://1cos.ap-beijing.myqcloud.com/test_ip.txt

5. 登录 [账号威胁发现控制台](#)，单击左侧菜单栏的 **IP 清单**。

6. 根据需求，单击**添加可信 IP 列表**或**添加威胁 IP 列表**。

7. 进入弹窗填写列表名称、列表文件 URL，选择格式和同意协议。

- 列表名称：填写名称，不可与列表中的其它名称重复。
- 列表文件 URL：将步骤4复制的 URL，填写到此处。
- 选择格式：目前仅支持 TXT 格式。
- 同意协议：通过添加列表，表明您接受并同意威胁发现从此资源读取数据。

添加可信IP列表

列表名称 *

test

✓

列表文件URL *

https://1[redacted]cos.ap-bei

✓

格式 *

TXT

▼

同意协议 *

☒ 通过添加列表，表明您接受并同意威胁发现从此资源读取数据

提交

取消

8. 单击提交，等待状态跳转为“ACTIVE”，即添加成功。

列表名称	列表文件URL	格式	状态	生效时间	操作
test	https://1[redacted]cos.ap-beijing.myqcloud.com/test_ip.txt	TXT	ACTIVE	2019-08-27 16:23:46	禁用 编辑 删除

修改列表信息

单击列表右侧对应的编辑，即可修改列表信息。

⚠ 注意

若修改了 COS 文件中的 IP 列表，需要通过编辑来重新激活。

禁用与激活列表信息

- 在生效状态下，单击列表右侧对应的禁用，即可禁用 COS 文件。
- 在未生效状态下，单击列表右侧对应的激活，即可重新激活 COS 文件。

删除列表信息

- 单击列表右侧对应的删除，将弹出对话框。
- 单击确定，即可删除列表信息。