账号威胁发现

产品简介

腾讯云

文档目录

产品简介
产品概述

最近更新时间：2024-02-22 14:44:31

什么是账号威胁发现

账号威胁发现（Account Threat Discovery，ATD）为腾讯云用户提供账号安全监测服务，是腾讯云账号安全服务的子产品。账号威胁发现主要基于 操作审计（CloudAudit） 数据进行分析，快速建立用户行为基准，实时帮助用户分析 API 调用是否符合用户行为基准。与此同时，腾讯云积累多年的威胁情报源（如恶意 IP 列表等）、机器学习以及异常检测等资源和技术也会为您保驾护航。您无需部署或维护任何软、硬件，只需要在控制台进行简单操作，即可以启用威胁发现功能，持续监控用户的腾讯云账户，结合用户行为基准、情报资源以及用户自定义 IP 名单等，识别潜在威胁并确定威胁处理的优先级别。

工作原理

威胁分类

每个用户都可以通过控制台和 API 操作访问腾讯云账号下的云资源，而每种云资源下又有多种访问方式。通过分析一位用户操作一次所涉及到的步骤，威胁发现将基础威胁类型分为以下几类：

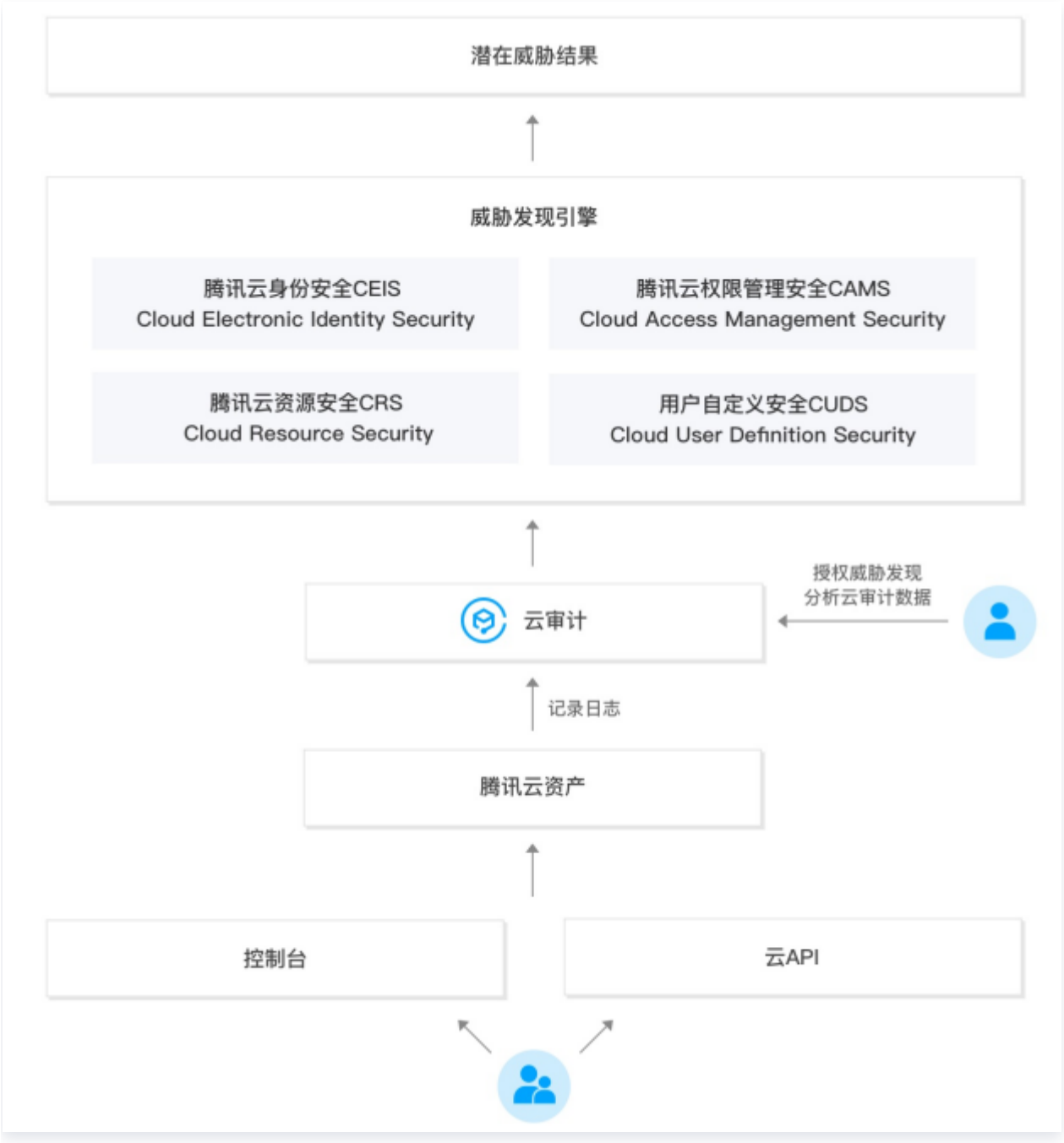
- 腾讯云身份安全 CEIS（Cloud Electronic Identity Security）
- 腾讯云权限管理安全 CAMS（Cloud Access Management Security）
- 腾讯云资源安全 CRS（Cloud Resource Security）
- 用户自定义安全 CUDS（Cloud User Definition Security）

原理说明

当用户想重启 A 账号下的某个 CVM 实例：

1. 登录账号 A。在登录时需要验明正身，此时会产生一连串的校验日志，CEIS 异常检测便会对验明正身的过程进行异常检测。
2. 验明正身后，需要找到对应的 CVM 实例并尝试执行重启操作。
   2.1 执行重启操作前，需要校验当前用户是否具备重启 CVM 实例的权限，此时也会产生一连串的检验日志，CAMS 异常检测便会对这次权限验证的过程进行异常检测。
   2.2 开始执行重启操作，CRS 便会对这次执行重启的逻辑进行异常检测。
3. 此外，账号威胁发现还会根据用户自己上传的 IP 列表进行数据分析，即用户自定义安全 CUDS（Cloud User Definition Security）。

整体工作原理如下图所示：



风险等级

账号威胁发现根据威胁事件的危害程度，将事件分为高、中、低三个等级，定义原则如下：

- 高风险：需要马上修复，否则将对用户的资产或业务产生重大影响。
- 中风险：需要用户及时确认是否真的存在问题，如问题存在，需马上修复，否则会对用户的资产造成影响。
- 低风险：用户的操作不符合最佳安全事件，需尽快确认并按照最佳安全事件进行修改，否则可能存在安全风险。

产品功能

最近更新时间：2024-02-22 14:44:31

账户级别检测

账号威胁发现的数据源是操作审计数据。只要授权使用账号威胁发现服务，系统便会对账号的操作审计数据进行账户级别分析，包括该账号下子账号和协作者的行为分析。

自定义 IP 列表

账号威胁发现除了内置的检测算法和评测标准，还支持用户自定义可信 IP 列表和威胁 IP 列表。账号威胁发现基于自定义的 IP 列表对用户的操作行为进行实时检测，并对命中威胁 IP 列表的事件进行风险定级和落地。

威胁事件反馈

用户可以通过反馈功能，将使用异常检测算法时出现的问题反馈到后台。账号威胁发现会根据用户反馈，及时调整检测算法，快速建立起对用户有效的异常检测算法。

风险评估修复

账号威胁发现在预定义威胁类型时，也会针对威胁类型进行详尽的分析和演算，为用户提供专业的风险评估结果和快速的风险修复手段。用户可以利用风险评估修复功能，快速评估潜在威胁对自身账户的影响，并找出有效的修复手段。

快速开关服务

用户需要开通此项服务时，只需在控制台进行简单操作即可。账号威胁发现开通后，系统便会对用户的账户进行持续监控。用户无需使用该服务时，只需在控制台上单击关闭即可。

> **警告：**
> 账号威胁发现关闭后，会把未归档的威胁检测结果一并删除，且不可恢复。

产品优势

最近更新时间：2024-02-22 14:44:31

简单授权全面监控

账号威胁发现在获得用户简单授权后，将持续分析用户操作审计数据中的操作行为数据，从账户、权限、资源和自定义安全四个维度，对账户的 API 调用进行全面监控。

安全事件集中管理

账号威胁发现能监控主账号、主账号下的子账号、协作者的操作行为，并将发现的安全事件分为高、中、低三个等级，统计归纳到系统上。用户可在控制台查看所有安全事件，实现安全事件的集中便捷管理。

安全威胁快速响应

开通服务后，账号威胁发现会实时获取用户行为数据，并利用实时数据分析引擎和离线数据分析引擎，帮助用户快速发现潜在威胁事件。同时，账号威胁发现还会分析每种威胁类型的触发原因和影响结果，评估当前潜在威胁可能造成的影响，并提供修复建议，协助用户快速修复当前威胁。

应用场景

最近更新时间：2023-07-13 17:03:42

账户安全管理

企业全面上云后，随着在腾讯云上使用的业务和资源不断增加，使用场景不断深化，子账号和协作者数量不断扩张，维护云账户安全和资产安全显得更加困难。账号威胁发现可以帮助您进行账号级别分析，及早发现潜在安全威胁，保障企业账号安全。

操作安全管理

企业自身实现持续监控和分析账户操作行为，需要充分了解日志字段组成和触发场景，十分耗时且未必准确。当业务迁移到云上后，账户的操作行为收集就会变得简单。账号威胁发现能充分了解每一次 API 调用的场景和执行结果，并结合威胁信息、异常检测和机器学习等资源和算法，帮助您轻松掌握潜在威胁，高效智能地解决安全问题。

使用限制

最近更新时间：2023-07-13 17:03:42

使用账号威胁发现服务的注意事项如下表所示：

资源	默认限制	说明
探测器	1个	目前仅支持创建1个探测器，且用户不能请求增加探测器的数量。
可信 IP 集合	6个	用户可以上传6个可信 IP 集合，单个 IP 集合中有效 IP 数量不超过2000个。
威胁 IP 集合	6个	用户可以上传6个威胁 IP 集合，单个 IP 集合中有效 IP 数量不超过25000个。
文件大小	3.5MB	单个用户上传的可信 IP 列表和威胁 IP 列表的文件总大小不能超过3.5MB。
威胁发现结果保存时间	90天	检测结果默认存储90天，且最长时长为90天。如需延长存储时长，可使用归档服务。
IP 文件存储位置	COS	IP 文件必须存储在腾讯云的 COS 上，且为公有读。
IP 文件后缀	TXT	目前仅支持 TXT 的文件。