账号威胁发现

检测结果说明

腾讯云

文档目录

检测结果说明
身份安全 CEIS

最近更新时间：2023-07-13 21:11:21

本文将为您详细说明腾讯云身份安全 CEIS（Cloud Electronic Identity Security）的检测结果。

高风险类

持久证书被禁用或删除导致 API 调用报错（CertificateDisabledCauseError）

- **风险等级：**高
- **风险说明：**
  账号安全中心会在您删除或者禁用持久证书后的一段时间内，着重关注您的 API 调用情况。在这段时间内，如果出现 API 调用失败的情况，则会出现该类型的安全威胁。
- **需采取的措施：**
  请务必检查本次异常 API 调用是否是您已知的调用，如是未知调用，那么账号的持久证书可能被盗用。
- **可能造成的影响：**
  删除和禁用持久证书属于高危操作，可能会影响到您的业务。

在 GitHub上公开的持久证书出现调用（LeakedCertificateInUse）

- **风险等级：**高
- **风险说明：**
  - 账号安全中心会实时从 GitHub 上扫描公开的代码，如果发现疑似腾讯云持久证书，会进一步核实和检测。
  - 如果被公开的持久证书，出现调用 API 的行为，则会命中该规则。
- **需采取的措施：**
  请务必确认您的持久证书是否被泄露公开。
- **可能造成的影响：**
  持久证书在 GitHub 上公开，表明您腾讯云的所有资产已经受到严重威胁，请务必着重关注。

中风险类

账号登录异常（AccountAbnormalLogin）

- **风险等级：**中
- **风险说明：**
  - 账号安全中心会根据您历史的登录行为建立基准。
  - 建立基准的范围包括但不限于：登录 IP、登录设备、登录方式和登录时空习惯等。
  - 如果您的登录行为偏离基准，则会命中该规则。

- **需采取的措施：**
  请务必确认本次登录是否是您已知的登录，如果是未知登录，那么您的账号可能被盗用。
- **可能造成的影响：**
  如账号被盗用，将直接威胁到您的腾讯云资产的安全，也会影响到您部署在腾讯云上的业务的安全。

账号可能遭遇撞库攻击（AccountCollisionAttack）

- **风险等级：**中
- **风险说明：**
  您的邮箱账号可能被恶意扫描。
- **需采取的措施：**
  请务必确认本次异常登录是否是您已知的登录，如果是未知登录，那么您的邮箱账号可能存在风险，建议立即修改账号密码。
- **可能造成的影响：**
  如果账号被撞库成功，将直接威胁到您腾讯云上资产的安全。

持久证书使用异常（CertificateAbnormalUsed）

- **风险等级：**中
- **风险说明：**
  - 账号安全中心会根据您持久证书历史的调用行为建立基准。
  - 建立基准的范围包括但不限于：调用 IP、调用业务、调用 Action、调用频率以及调用时间段。
  - 如果持久证书调用 API 的行为偏离基准，则会命中该规则。
- **需采取的措施：**
  请务必检查本次异常 API 调用是否是您已知的调用，如是未知调用，那么账号的持久证书可能被盗用。
- **可能造成的影响：**
  如果持久证书被盗用，将直接威胁到您腾讯云上资产的安全，也会影响到您部署在腾讯云上业务的安全。

持久证书正在被用于执行高危操作（CertificateHighRiskAct）

- **风险等级：**中
- **风险说明：**
  安全中心检测到您的持久证书正在通过控制台或者 API 进行操作，操作类型包括但不限于：查看密钥 Key、删除持久证书、禁用持久证书、启用持久证书和新建持久证书。
- **需采取的措施：**
  请您务必检查，本次持久证书的高危操作是否符合预期。
- **可能造成的影响：**
  如果本次操作不符合您的预期，将会直接影响到您腾讯云的资产安全，也会影响到您部署在腾讯云上业务的安全。

低风险类

账号高危操作（AccountHighRiskAct）

- **风险等级：**低
- **风险说明：**
  - 该规则属于着重提醒，如果是您本人或者您授权的其他人在操作，可以忽略本条提醒。
  - 该规则会帮助您归纳账号相关的高危操作，但不会判断该高危操作是否偏离基准。
- **需采取的措施：**
  - 账号绑定了新的微信、邮箱或微信公众号，请确认为本人或被授权人操作，否则您的账号存在被盗用的风险。
  - 账号中的电话、邮箱等核心信息被修改，请确认为本人或被授权人操作，否则您的账号归属可能会存在争议。
- **可能造成的影响：**
  - 账号的安全设置被修改，可能会降低账号的安全性保障。
  - 账号新增了子账号或者修改了已有子账号所在的用户组，导致您的子账号体系发生变更，最终导致账号下的云资产受到威胁。

持久证书被长期使用（CertificateUsedForLongTime）

- **风险等级：**低
- **风险说明：**
  账号安全中心会帮助您监控持久证书的使用周期。如果同一个持久证书已经使用超过180天以上，则会命中该规则。
- **需采取的措施：**
  请确认是否继续使用该持久证书。
- **可能造成的影响：**
  长期使用同一个持久证书，会大大增加信息泄露的概率。

持久证书长期未使用（CertificateUnsedForLongTime）

- **风险等级：**低
- **风险说明：**
  您创建的持久证书已经180天没有使用。
- **需采取的措施：**
  请确认是否继续保留该证书。
- **可能造成的影响：**
  长期未被使用的持久证书，建议删除或者禁用，否则会徒增信息泄露风险，进而威胁到您腾讯云的资产安全。

使用根账号持久证书调用API（CertificateUsedByRoot）

- **风险等级：**低
- **风险说明：**
  - 您使用了根账户的持久证书调用 API。
  - 根账户的持久证书就如同 Linux 操作系统的 root，可以执行操作系统中的任何操作。
  - 根账户的持久证书可以通过云 API 无限制地访问您的腾讯云资源。
- **需采取的措施：**
  请确认您是否使用了根账户的持久证书调用 API。
- **可能造成的影响：**
  根账户的持久证书可能造成您腾讯云上的资产损失，强烈建议登录子用户账户进行操作，并使用子用户持久证书访问云 API。

权限管理安全 CAMS

最近更新时间：2024-02-22 14:44:32

本文将为您详细说明腾讯云权限管理安全 CAMS（Cloud Access Management Security）的检测结果。

高风险类

CAM 权限变更导致 API 调用报错（PermissionModifyCauseError）

- **风险等级：**高
- **风险说明：**
  - 在您的账号权限发生变更后的一段时间内，账号安全中心会帮助您检测 API 的调用情况。
  - 如果 API 调用时没有权限，可能会命中该规则。
- **需采取的措施：**
  请您务必检查本次 API 调用没有权限是否符合预期，如果不符合预期，需要您及时回滚权限配置。
- **可能造成的影响：**
  API 调用失败可能会影响到您的业务。

中风险类

角色载体行为异常（RoleCarrierIsAbnormal）

- **风险等级：**中
- **风险说明：**
  - 账号安全中心会根据您角色载体的历史行为建立基准。
  - 建立基准的范围包括但不限于：调用 IP、调用资源、调用 Action、调用频率和调用时间段等。
  - 如果您角色载体的行为偏离基准，则会命中该规则。
- **需采取的措施：**
  请您务必检查本次角色载体的行为异常是否符合您的预期。
- **可能造成的影响：**
  如果本次行为异常不符合您的预期，那么您的角色载体可能存在安全问题。

删除已有角色（RoleIsDeleted）

- **风险等级：**中
- **风险说明：**
  您正在删除已经存在的角色。
- **需采取的措施：**
  请确认被删除的角色是否在使用中。

- **可能造成的影响：**
  如果您删除的角色正在使用中，可能会影响到其他服务的正常使用。
  例如：您删除了角色 CloudAudit_QCSRole，那么将会导致您操作审计中投递 COS 和投递 CMQ 的功能不可用。

低风险类

授予子账号超级权限（CAMUserGrantedSuperPermission）

- **风险等级：**低
- **风险说明：**
  您正在授予子账号超级权限。
- **需采取的措施：**
  授予子账号超级权限不符合最小权限的最佳实践，请确认授权操作。
- **可能造成的影响：**
  授予子账号超级权限可能会导致您的账号出现权限传递现象，进而威胁到您腾讯云的资产安全。

CAM 权限高危操作（PermissionHighRiskAct）

- **风险等级：**低
- **风险说明：**
  - 账号安全中心会根据您历史的操作 CAM 行为建立基准。
  - 建立基准的范围包括但不限于：操作 IP、操作方式和操作时空习惯等。
  - 如果您的操作行为偏离基准，则会命中该规则。
- **需采取的措施：**
  请您务必检查本次高危操作是否是您本人或被授权人操作，如果是未知操作，那么您的账号可能被盗用。
- **可能造成的影响：**
  如果本次操作不是您的已知操作，将可能威胁到您账户的整体安全。

授予角色超级权限（RoleGrantedSuperPermission）

- **风险等级：**低
- **风险说明：**
  您正在授予角色超级权限。
- **需采取的措施：**
  授予角色超级管理员权限不符合最小权限的最佳实践，请确认授权操作。
- **可能造成的影响：**
  授予角色超级管理员权限可能会导致您的账号出现权限传递现象，进而威胁到您腾讯云的资产安全。

子账号添加子账号（CAMUserAddSubaccount）

- **风险等级：**低
- **风险说明：**
  您的子账号正在添加子账号。
- **需采取的措施：**
  请您确认本次添加子账号的操作是否符合预期。
- **可能造成的影响：**
  您的子账号如果在您不知情的情况下添加子账号，可能会出现权限传递现象。

资源安全 CRS

最近更新时间：2024-02-22 14:44:32

本文将为您详细说明腾讯云资源安全 CRS（Cloud Resource Security）的检测结果。

中风险类

操作审计停止跟踪集（CloudAuditStopLogging）

- **风险等级：**中
- **风险说明：**
  您的操作审计跟踪集被停止。
- **需采取的措施：**
  请确认本次操作是否符合您的预期。
- **可能造成的影响：**
  跟踪集是操作审计持久存储访问行为的功能，如果您的跟踪集被停止，那么您的访问行为将不能被持久化存储。

操作审计删除跟踪集（CloudAuditDeletedAudit）

- **风险等级：**中
- **风险说明：**
  您的操作审计跟踪集被删除。
- **需采取的措施：**
  请确认本次操作是否符合您的预期。
- **可能造成的影响：**
  跟踪集是操作审计持久存储访问行为的功能，如果您的跟踪集被删除，那么您的访问行为将不能被持久化存储。

低风险类

无服务器云函数高风险操作（ScfHighRiskAct）

- **风险等级：**低
- **风险说明：**
  - 账号安全中心会根据您历史操作 SCF 的行为建立基准。
  - 建立基准的范围包括但不限于：操作 IP、操作方式和操作时空习惯等。
  - 如果您的操作行为偏离基准，则会命中该规则。
- **需采取的措施：**
  请您务必检查本次 SCF 相关的高危操作是否是您本人或被授权人操作，如果是未知操作，那么您的账号可能被盗用。
- **可能造成的影响：**

如果本次操作不是您的已知操作，将可能会威胁到您 SCF 的安全。

容器高风险操作（TkeHighRiskAct）

- **风险等级：**低
- **风险说明：**
  - 账号安全中心会根据您历史操作 TKE 的行为建立基准。
  - 建立基准的范围包括但不限于：操作 IP、操作方式和操作时空习惯等。
  - 如果您的操作行为偏离基准，则会命中该规则。
- **需采取的措施：**
  请您务必检查本次 TKE 相关的高危操作是否是您本人或被授权人操作，如果是未知操作，那么您的账号可能被盗用。
- **可能造成的影响：**
  如果本次操作不是您的已知操作，将可能会威胁到您 TKE 的安全。

云硬盘高风险操作（CbsHighRiskAct）

- **风险等级：**低
- **风险说明：**
  - 账号安全中心会根据您历史操作 CBS 的行为建立基准。
  - 建立基准的范围包括但不限于：操作 IP、操作方式和操作时空习惯等。
  - 如果您的操作行为偏离基准，则会命中该规则。
- **需采取的措施：**
  请您务必检查本次 CBS 相关的高危操作是否是您本人或被授权人操作，如果是未知操作，那么您的账号可能被盗用。
- **可能造成的影响：**
  如果本次操作不是您的已知操作，将可能会威胁到您 CBS 的安全。

Redis 高风险操作（RedisHighRiskAct）

- **风险等级：**低
- **风险说明：**
  - 账号安全中心会根据您历史操作 Redis 的行为建立基准。
  - 建立基准的范围包括但不限于：操作 IP、操作方式和操作时空习惯等。
  - 如果您的操作行为偏离基准，则会命中该规则。
- **需采取的措施：**
  请您务必检查本次 Redis 相关的高危操作是否是您本人或被授权人操作，如果是未知操作，那么您的账号可能被盗用。
- **可能造成的影响：**

如果本次操作不是您的已知操作，将可能会威胁到您 Redis 的安全。

MongoDB 高风险操作（MongodbHighRiskAct）

- **风险等级：**低
- **风险说明：**
  - 账号安全中心会根据您历史操作 MongoDB 的行为建立基准。
  - 建立基准的范围包括但不限于：操作 IP、操作方式和操作时空习惯等。
  - 如果您的操作行为偏离基准，则会命中该规则。
- **需采取的措施：**
  请您务必检查本次 MongoDB 相关的高危操作是否是您本人或被授权人操作，如果是未知操作，那么您的账号可能被盗用。
- **可能造成的影响：**
  如果本次操作不是您的已知操作，将可能会威胁到您 MongoDB 的安全。

动态加速网络高风险操作（DsaRiskAct）

- **风险等级：**低
- **风险说明：**
  - 账号安全中心会根据您历史操作 DSA 的行为建立基准。
  - 建立基准的范围包括但不限于：操作 IP、操作方式和操作时空习惯等。
  - 如果您的操作行为偏离基准，则会命中该规则。
- **需采取的措施：**
  请您务必检查本次 DSA 相关的高危操作是否是您本人或被授权人操作，如果是未知操作，那么您的账号可能被盗用。
- **可能造成的影响：**
  如果本次操作不是您的已知操作，将可能会威胁到您 DSA 的安全。

内容分发网络高风险操作（CdnRiskAct）

- **风险等级：**低
- **风险说明：**
  - 账号安全中心会根据您历史操作 CDN 的行为建立基准。
  - 建立基准的范围包括但不限于：操作 IP、操作方式和操作时空习惯等。
  - 如果您的操作行为偏离基准，则会命中该规则。
- **需采取的措施：**
  请您务必检查本次 CDN 相关的高危操作是否是您本人或被授权人操作，如果是未知操作，那么您的账号可能被盗用。
- **可能造成的影响：**

如果本次操作不是您的已知操作，将可能会威胁到您 CDN 的安全。

专线接入高风险操作（DcRiskAct）

- **风险等级：**低
- **风险说明：**
  - 账号安全中心会根据您历史操作 DC 的行为建立基准。
  - 建立基准的范围包括但不限于：操作 IP、操作方式和操作时空习惯等。
  - 如果您的操作行为偏离基准，则会命中该规则。
- **需采取的措施：**
  请您务必检查本次 DC 相关的高危操作是否是您本人或被授权人操作，如果是未知操作，那么您的账号可能被盗用。
- **可能造成的影响：**
  如果本次操作不是您的已知操作，将可能会威胁到您 DC 的安全。

私有网络高风险操作（VpcRiskAct）

- **风险等级：**低
- **风险说明：**
  - 账号安全中心会根据您历史操作 VPC 的行为建立基准。
  - 建立基准的范围包括但不限于：操作 IP、操作方式和操作时空习惯等。
  - 如果您的操作行为偏离基准，则会命中该规则。
- **需采取的措施：**
  请您务必检查本次 VPC 相关的高危操作是否是您本人或被授权人操作，如果是未知操作，那么您的账号可能被盗用。
- **可能造成的影响：**
  如果本次操作不是您的已知操作，将可能会威胁到您 VPC 的安全。

MariaDB 高风险操作（MariadbRiskAct）

- **风险等级：**低
- **风险说明：**
  - 账号安全中心会根据您历史操作 MariaDB 的行为建立基准。
  - 建立基准的范围包括但不限于：操作 IP、操作方式和操作时空习惯等。
  - 如果您的操作行为偏离基准，则会命中该规则。
- **需采取的措施：**
  请您务必检查本次 MariaDB 相关的高危操作是否是您本人或被授权人操作，如果是未知操作，那么您的账号可能被盗用。
- **可能造成的影响：**

如果本次操作不是您的已知操作，将可能会威胁到您 MariaDB 的安全。

云服务器高风险操作（CvmRiskAct）

- **风险等级：**低
- **风险说明：**
  - 账号安全中心会根据您历史操作 CVM 的行为建立基准。
  - 建立基准的范围包括但不限于：操作 IP、操作方式和操作时空习惯等。
  - 如果您的操作行为偏离基准，则会命中该规则。
- **需采取的措施：**
  请您务必检查本次 CVM 相关的高危操作是否是您本人或被授权人操作，如果是未知操作，那么您的账号可能被盗用。
- **可能造成的影响：**
  如果本次操作不是您的已知操作，将可能会威胁到您 CVM 的安全。

负载均衡高风险操作（ClbRiskAct）

- **风险等级：**低
- **风险说明：**
  - 账号安全中心会根据您历史操作 CLB 的行为建立基准。
  - 建立基准的范围包括但不限于：操作 IP、操作方式和操作时空习惯等。
  - 如果您的操作行为偏离基准，则会命中该规则。
- **需采取的措施：**
  请您务必检查本次 CLB 相关的高危操作是否是您本人或被授权人操作，如果是未知操作，那么您的账号可能被盗用。
- **可能造成的影响：**
  如果本次操作不是您的已知操作，将可能会威胁到您 CLB 的安全。

对象存储高风险操作（CosRiskAct）

- **风险等级：**低
- **风险说明：**
  - 账号安全中心会根据您历史操作 COS 的行为建立基准。
  - 建立基准的范围包括但不限于：操作 IP、操作方式和操作时空习惯等。
  - 如果您的操作行为偏离基准，则会命中该规则。
- **需采取的措施：**
  请您务必检查本次 COS 相关的高危操作是否是您本人或被授权人操作，如果是未知操作，那么您的账号可能被盗用。
- **可能造成的影响：**

如果本次操作不是您的已知操作，将可能会威胁到您 COS 的安全。

云数据库高风险操作（CdbRiskAct）

- **风险等级：**低
- **风险说明：**
  - 账号安全中心会根据您历史操作 TencentDB 的行为建立基准。
  - 建立基准的范围包括但不限于：操作 IP、操作方式和操作时空习惯等。
  - 如果您的操作行为偏离基准，则会命中该规则。
- **需采取的措施：**
  请您务必检查本次 TencentDB 相关的高危操作是否是您本人或被授权人操作，如果是未知操作，那么您的账号可能被盗用。
- **可能造成的影响：**
  如果本次操作不是您的已知操作，将可能会威胁到您 TencentDB 的安全。

批量计算高风险操作（BatchRiskAct）

- **风险等级：**低
- **风险说明：**
  - 账号安全中心会根据您历史操作 Batch 的行为建立基准。
  - 建立基准的范围包括但不限于：操作 IP、操作方式和操作时空习惯等。
  - 如果您的操作行为偏离基准，则会命中该规则。
- **需采取的措施：**
  请您务必检查本次 Batch 相关的高危操作是否是您本人或被授权人操作，如果是未知操作，那么您的账号可能被盗用。
- **可能造成的影响：**
  如果本次操作不是您的已知操作，将可能会威胁到您 Batch 的安全。

弹性伸缩风险操作（AsRiskAct）

- **风险等级：**低
- **风险说明：**
  - 账号安全中心会根据您历史操作 AS 的行为建立基准。
  - 建立基准的范围包括但不限于：操作 IP、操作方式和操作时空习惯等。
  - 如果您的操作行为偏离基准，则会命中该规则。
- **需采取的措施：**
  请您务必检查本次 AS 相关的高危操作是否是您本人或被授权人操作，如果是未知操作，那么您的账号可能被盗用。
- **可能造成的影响：**

如果本次操作不是您的已知操作，将可能会威胁到您 AS 的安全。

用户自定义安全 CUDS

最近更新时间：2023-07-13 21:11:21

本文将为您详细说明用户自定义安全 CUDS（Cloud User Definition Security）的检测结果。

命中威胁 IP（OccursOnThreatIP）

- **风险等级：**高
- **风险说明：**
  您的账号下存在不安全操作：调用方的 IP 命中了您自定义的威胁 IP。
- **需采取的措施：**
  请确认本次操作是否符合您的预期。
- **可能造成的影响：**
  受到已知威胁源的威胁，将可能威胁到您账户的整体安全。