阿里云
云安全中心（态势感知）

威胁检测

文档版本：20190919

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。
*## *	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 安全告警处理

1.1 安全告警类型概述

云安全中心支持网页防篡改、进程异常、网站后门、异常登录、恶意进程等安全告警类型，通过全面的安全告警类型帮助您及时发现资产中的安全威胁、实时掌握您资产的安全态势。

云安全中心支持对您已开启的告警防御能力提供总览，帮助您快速了解已开启和未开启的防御项目。您可在云安全中心控制台安全告警处理页面，查看已开启和未开启的防御项目。

防御项目包含的内容参见安全告警类型。

除应用白名单和网页防篡改告警类型以外，云安全中心默认为用户开启所有的告警事件防御能力。

说明:

- 基础版用户默认只开启异常登录的防御能力。如需开通其他防御能力，需升级到高级版或企业版。有关升级的内容，参见#unique_5。
- 应用白名单和网页防篡改是云安全中心的增值服务，需要您单独购买开通后才会开启应用白名单和网页防篡改的防御。网页防篡改为高级版和企业版功能，基础版不支持该功能。应用白名单详细操作参见#unique_6；网页防篡改详细操作参见网页防篡改#unique_7。
- 云产品威胁检测为企业版功能，企业版自动开启防御；高级版需要升级至企业版后才能自动开启防御。

安全告警类型

说明:

- 2018年12月20日起，云安全中心基础版只支持异常登录和其他-DDoS类型安全告警，若您需要启用更多高级威胁检测能力，需开通云安全中心高级版和企业版服务。
- 云安全中心基础版、高级版和企业版可检测的告警类型差异参见功能特性列表。

告警名称	告警说明
网页防篡改	实时监控网站目录并通过备份恢复被篡改的文件或目录，保障重要系统的网站信息不被恶意篡改，防止出现挂马、黑链、非法植入恐怖威胁、色情等内容。 详情参见网页防篡改。 说明: 网页防篡改是云安全中心的增值服务，需要您单独购买开通后才会开启网页防篡改的防御。网页防篡改为高级版和企业版功能，基础版不支持该功能。
进程异常行为	检测资产中是否存在超出正常执行流程的行为。
网站后门	使用自主查杀引擎检测常见后门文件，支持定期查杀和实时防护，并提供一键隔离功能： · Web目录中文件发生变动会触发动态检测，每日凌晨扫描整个Web目录进行静态检测。 · 支持针对网站后门检测的资产范围配置。 · 对发现的木马文件支持隔离、恢复和忽略。
异常登录	检测服务器上的异常登录行为。通过设置合法登录IP、时间及账号，对于例外的登录行为进行告警。支持手动添加和自动更新常用登录地，对指定资产的异地登录行为进行告警。具体可参见#unique_10
异常事件	程序运行过程中发生的异常行为。
敏感文件篡改	对服务器中的敏感文件进行恶意修改。
恶意进程（病毒云查杀）	采用云+端的查杀机制，对服务器进行实时检测，并对检测到的病毒文件提供实时告警。您可通过控制台对病毒程序进行处理。详细信息参见#unique_11。
异常网络连接	网络显示断开或不正常的网络连接状态。
异常账号	非合法登录账号。
云产品威胁检测	云安全中心检测到您购买的其他阿里云产品存在的威胁。
精准防御	开启病毒查杀提供精准防御能力，可对主流勒索病毒、DDOS木马、挖矿和木马程序、恶意程序、后门程序和蠕虫病毒等类型进行防御。
应用入侵事件	通过系统的应用组件入侵服务器的告警事件。
持久化后门	检测服务器上存在的可疑计划任务，对可能被攻击者用于持久入侵用户机器的威胁进行告警提示。

告警名称	告警说明
应用白名单	通过将需要重点防御的服务器应用在白名单策略中，检测服务器中是否存在可疑或恶意进程，并对不在白名单中的进程进行告警提示。
Web应用威胁检测	云安全中心对通过Web应用入侵的行为进行检测告警。
其他	DDOS流量攻击等网络入侵行为。

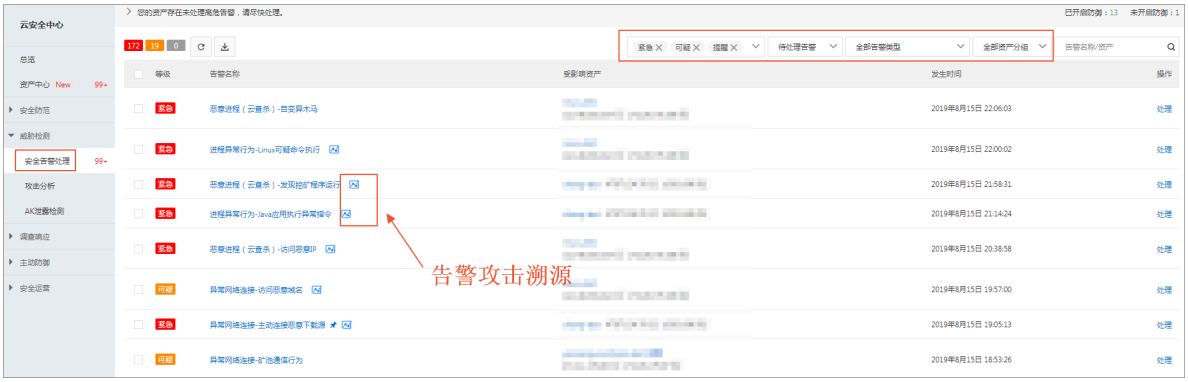
1.2 查看和处理告警事件

您可以通过阿里云云安全中心控制台查看和处理安全告警事件，并通过告警自动关联全面了解和集中处理安全威胁或入侵，并通过云安全中心提供的告警自动化溯源功能，快速定位攻击来源。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击威胁检测 > 安全告警处理。
3. 在安全告警处理列表中，查看或搜索所有检测到的入侵和威胁告警及其详细信息。

   您也可以使用搜索和页签筛选功能快速定位到特定事件。例如，您可以通过输入告警或资产名称、筛选告警严重等级、事件状态或告警类型来搜索相关的告警事件。



   在安全告警处理页面中单击告警事件的名称，打开该告警事件的详情页面，可以查看其详情和该告警的自动化关联信息，帮助您更便捷和全面地分析威胁事件，快速定位攻击来源地址和攻击行为的路径分析。有关告警自动化关联的操作，参见#unique_13和#unique_14。

4. 在安全告警处理页面，单击处理，根据您的需求对不同告警事件执行相应处理。

- 病毒查杀/隔离：仅限对网站后门-发现后门（Webshell）文件或恶意进程（云查杀）执行结束进程、阻断或隔离的操作。确认告警信息后，单击该操作可将网站后门文件加入文件隔离箱。被隔离的文件将无法对主机造成威胁，详细信息参见文件隔离箱。

  说明:

被成功隔离的文件在30天内可执行一键恢复，过期后系统将自动清除该文件。

- 深度查杀：仅限对恶意进程（云查杀）执行深度清除病毒文件的操作。您可以单击该功能下的查看详情，查看并确认待清除列表信息。
- 阻断：仅限对恶意进程（云查杀）-访问恶意IP执行阻断的操作。

  您可以查看处理详情并设置规则有效期。

- 忽略：忽略本次告警，该告警状态将变为已处理，后续云安全中心不会再对该事件进行告警。
- 加白名单：如果告警为误报，您可以将本次告警加入白名单。告警加入白名单后该告警状态将变为已处理，后续云安全中心不会再对该事件进行告警。您可以在已处理列表中定位到该事件对其进行取消白名单的操作。

 说明：

告警误报是指系统对正常程序进行告警。常见的告警误报有 对外异常TCP发包可疑进程，提示您服务器上有进程在对其他设备发起了疑似扫描行为。

- 同时处理相同告警：对多个告警事件进行批量处理。

  注意:
  批量处理告警事件前，请详细了解告警事件的信息。

安全威胁防御限制说明

云安全中心支持安全告警实时检测与处理、漏洞检测与一键修复、攻击分析、云平台安全配置检查等功能，结合告警关联分析和攻击自动化溯源，帮助您全面加固系统和资产的安全防线。在云安全中心提供的防御能力以外，建议您也时时更新服务器安全系统补丁、配合使用云防火墙、Web应用防火墙等产品缩小网络安全威胁的攻击范围，实时预防，不让黑客有任何可乘之机。

说明:
由于网络攻击手段、病毒样本在不断的演变，实际的业务环境也有不同差异，因此无法保证能实时检测防御所有的未知威胁，建议您基于安全告警处理、漏洞、基线检查、云平台配置检查等安全能力，提升整体安全防线，预防黑客入侵和盗取或破坏业务数据。

1.3 告警自动化关联分析

云安全中心高级版和企业版支持告警自动化关联分析。您可在安全告警列表页面单击单个告警事件名称进入告警自动关联分析页面、查看和处理告警事件所有关联的异常情况并进行攻击自动溯源，帮助您对告警事件进行全方位分析和便捷处理。

功能特性

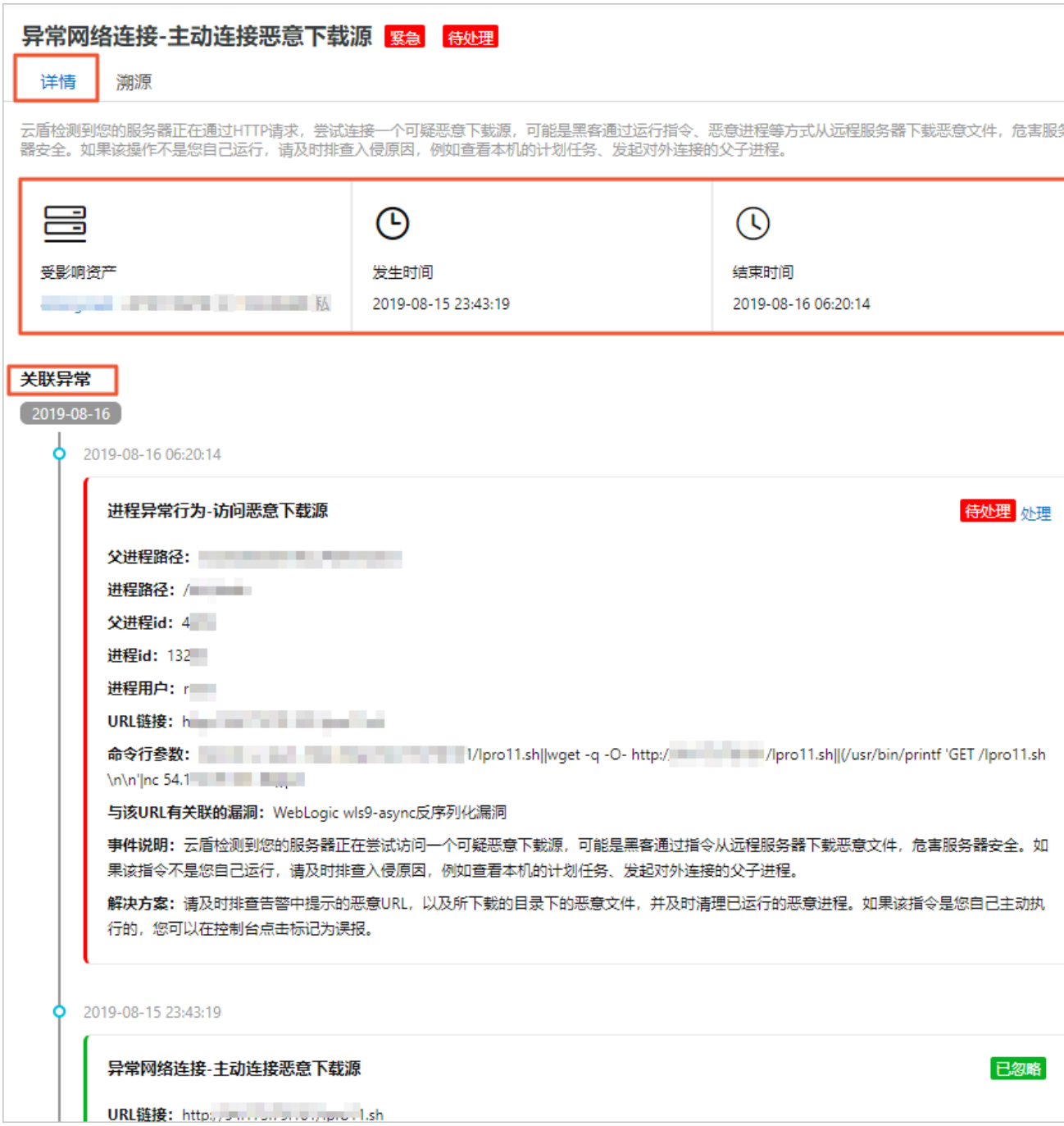
- 告警自动关联分析功能可对相关的异常事件进行实时自动化关联，挖掘出潜藏的入侵威胁。
- 告警自动化关联以告警发生的时间顺序聚合成关联的告警，帮助您更便捷地分析和处理告警事件，提升您系统的应急响应机制。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击威胁检测 > 安全告警处理。
3. 在安全告警处理列表中，单击目标告警事件名称打开告警事件详情页面。

4. 在告警事件详情页面，查看告警事件的详细信息、关联的异常事件和对告警/异常事件进行处理。

   · 查看告警详细信息：您可查看受该告警事件影响的资产信息、告警开始/结束时间、关联异常事件的详情。



   · 查看受影响资产：单击受影响资产名称，可跳转到对应资产的详情页面，方便您集中查看该资产的全部告警信息、漏洞信息、基线检查漏洞和资产指纹等信息。

- **查看和处理关联异常：您可在关联异常区域查看该告警事件关联的所有异常情况的详细信息、建议处理方案和处理方式。**

  告警事件处理方式选择，具体可参见#unique_17。

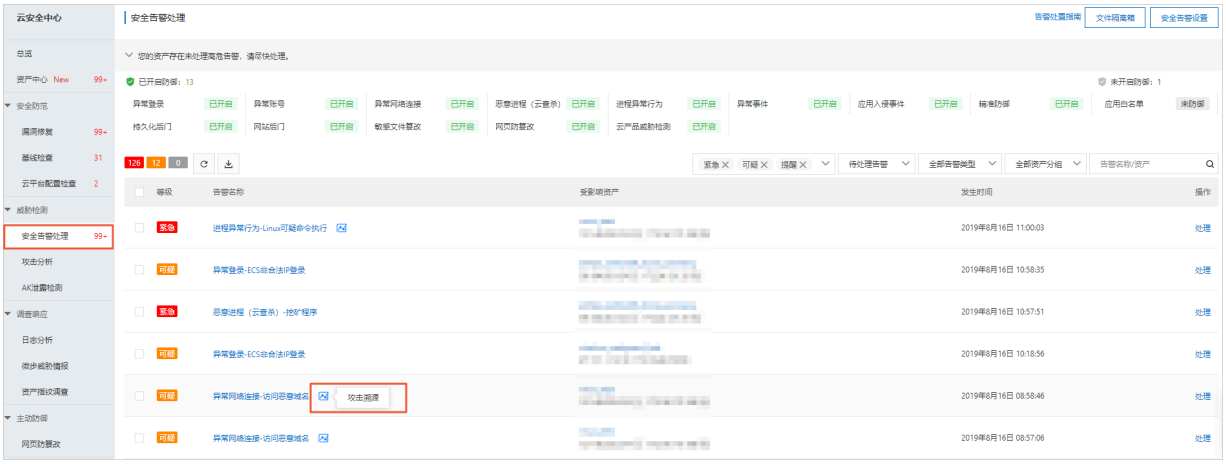
- 查看告警溯源：单击溯源，会打开该告警事件的溯源页面，详情请参见查看告警溯源和排查方案。

1.4 查看告警溯源和排查方案

云安全中心支持自动化攻击溯源，可对攻击进行自动溯源并提供原始数据预览，帮助您快速定位到攻击来源、发现入侵原因，并对弱点进行修复。

背景信息

您可在安全告警处理页面，单击攻击溯源图标，打开溯源页签查看攻击溯源详情，包括入侵原因、攻击请求的详细内容，和为您提供的排查建议。



限制条件

自动化攻击溯源是通过安全大数据关联计算产出，部分攻击行为可能由于黑客攻击未形成攻击链而无法展示溯源信息，此类情况下可直接查看告警详情。

操作步骤

1. 登录云安全中心控制台。

2. 在左侧导航栏，单击威胁检测 > 安全告警处理。
3. 在安全告警处理页面，定位到有溯源图标的告警事件，并单击告警溯源图标  ，会打开该告警事件的溯源页面。

   您可在告警溯源页面查看攻击告警名称、告警类型、影响的资源、攻击源IP、HTTP请求详情和攻击请求的详细内容。

   在溯源可视图中，您可以查看该攻击溯源事件整个链路中各个节点的信息。单击各个节点，会展示该节点的属性页面，您可以查看该节点的相关信息。

告警溯源案例

结合多种云产品日志，通过大数据分析引擎对数据进行加工、聚合、可视化，形成攻击者的入侵链路图。帮助您在最短时间内定位入侵原因、制定应急决策。适用于云环境的WEB入侵、蠕虫事件、勒索病毒、主动连接恶意下载源等场景的应急响应与溯源。

- 蠕虫传播事件

  下图描述了蠕虫传播源185.234.216.52通过SSH暴力破解成功登录到主机，并通过bash执行curl指令从远端下载挖矿程序并执行。

- WEB漏洞入侵事件

  黑客通过202.144.193.8服务器发起攻击，通过WEB漏洞向Linux服务器植入恶意shell脚本和挖矿程序，同时将代码写入计划任务（crond）实现攻击持久化。您可以通过溯源页面的节点信息，清晰地了解这一过程。此外，还可以观察到攻击者的多个IP及恶意下载源URL信息。

  单击图中HTTP攻击节点查看详细信息。流量数据表明入侵者通过Apache Solr未授权访问漏洞控制API接口执行系统命令，您可以针对此漏洞进行快速修复。

1.5 文件隔离箱

云安全中心可对检测到的威胁文件进行隔离处理。被成功隔离的文件可在30天内进行一键恢复，过期后系统将自动清除被隔离文件。

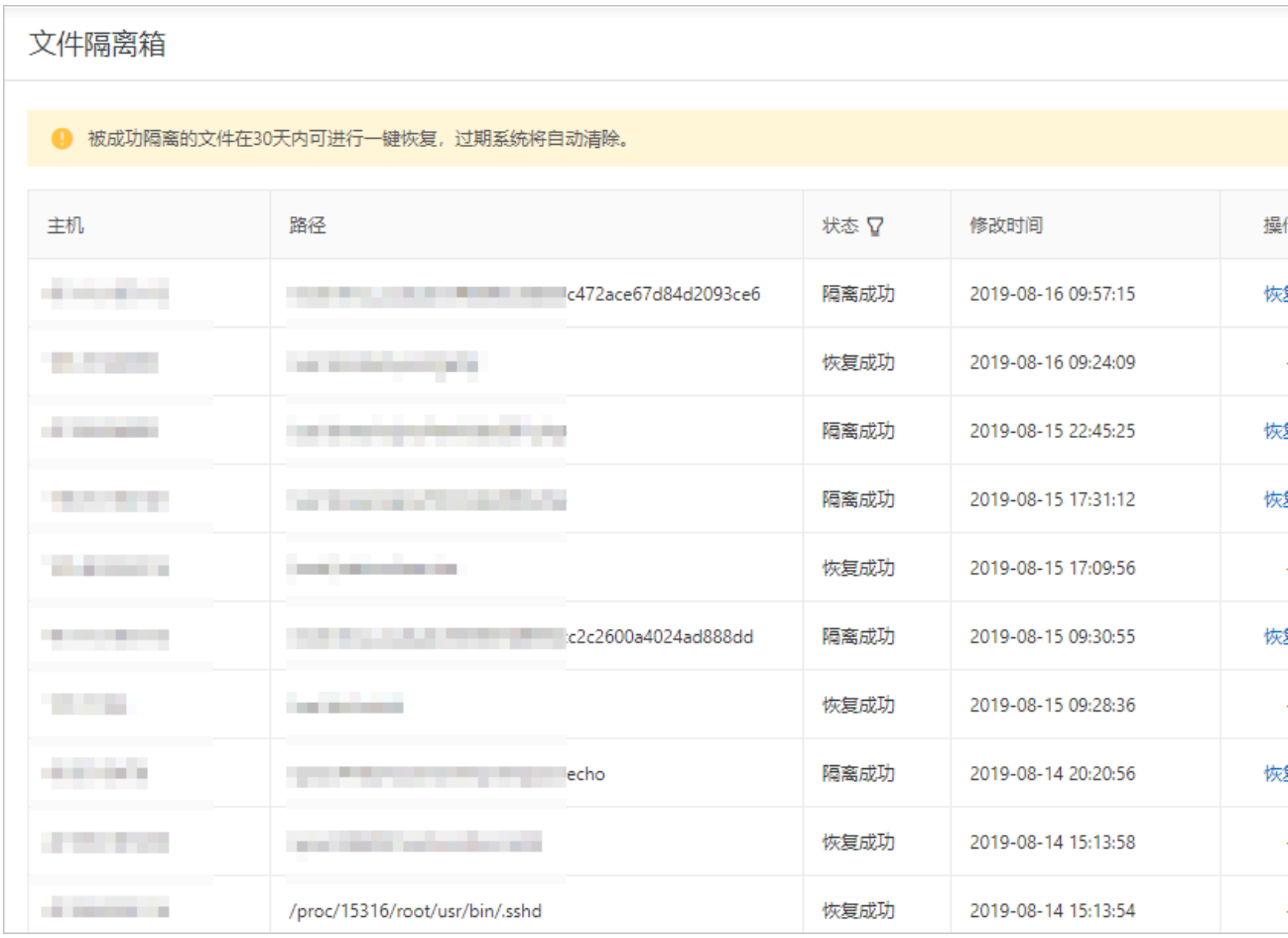
操作步骤

1. 登录云安全中心控制台。

2. 在左侧导航栏，单击威胁检测 > 安全告警处理。
3. 在安全告警处理页面单击右上角文件隔离箱。

您可在文件隔离箱进行以下操作：

- 在文件隔离箱列表中可以查看被隔离的文件主机地址、文件路径、状态和操作时间等信息。



- 单击文件隔离箱页面右侧操作栏的恢复，可以将指定的被隔离文件从文件隔离箱中恢复。恢复的文件将重新回到安全告警列表中。

1.6 一键导出事件列表

云安全中心安全告警支持一键导出告警事件详情列表。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击威胁检测 > 安全告警处理。

3. 单击安全告警处理页面危险等级栏的导出按钮  导出报表。报表导出完成后，安全告警页面右上角会提示导出完成。
4. 报表导出完成后，单击右上角导出完成提示对话框中的下载，将excel格式的报表下载到本地。

1.7 安全告警设置

安全告警设置支持手动维护常用登录地和Web目录，也允许您配置高级登录报警功能。

操作步骤

> 说明:
> 高级登录报警只有在高级版和企业版服务中提供，允许您配置更精细的异常登录检测，例如设置合法登录的IP、时间、账号。在云安全中心控制台总览页面查看您的服务器是否属于高级版或企业版。

1. 登录云安全中心控制台。
2. 在左侧导航栏选择威胁检测 > 安全告警处理。
3. 单击页面右上角安全告警设置，完成以下配置：
   - 添加常用登录地
     a. 单击常用登录地右侧的添加按钮。
     b. 选择要添加的常用登录地点，然后选择添加应用的服务器。
     c. 单击确定，完成添加。
     您可以编辑和删除已成功添加的常用登录地。
     - 单击一个常用登录地下的编辑，修改该登录地的生效服务器。
     - 单击一个常用登录地下的删除，删除该常用登录地配置。
   - 配置高级登录报警

     说明:

使用高级登录告警，您可以进一步指定合法的登录IP、时间段、和账号，云安全中心会对指定外的登录情形进行告警。以下功能的操作类似常用登录地配置，您可以参考上文进行添加、编辑、删除。

- 单击合法登录IP右侧的切换开关，开启/关闭登录IP检查，开启后通过非指定IP登录会触发报警。
- 单击合法登录时间右侧的切换开关，开启/关闭登录时间检查，开启后在非指定时间登录会触发报警。
- 单击合法账号右侧的切换开关，开启/关闭登录账号检查，开启后使用非指定账号登录会触发报警。

· 自定义Web目录

云安全中心会自动检测您服务器资产中的Web目录，并进行动态检测和静态扫描；您也可以手动添加服务器中的其它Web目录进行检测扫描。

a. 单击Web目录定义右侧的添加。

b. 输入一个合法的Web路径，然后选择生效服务器，该路径将被添加为扫描路径的服务器。

说明:
出于性能效率考虑，不支持直接添加root目录作为Web目录。

c. 单击确定，完成添加。

相关文档

#unique_10

1.8 病毒云查杀

云盾云安全中心病毒查杀（以下简称“云查杀”）集成了国内外多个主流的病毒查杀引擎，并利用阿里云海量威胁情报数据和自主研发的基于机器学习、深度学习异常检测模型，为用户提供全面和实时的病毒检测和防护服务。

目前云查杀每天检测数亿文件，实时服务百万云上主机。

云查杀检测能力

云安全中心采用云+端的查杀机制，客户端负责采集进程信息，上报到云端控制中心进行病毒样本检测。若判断为恶意进程，支持用户进行停止进程、隔离文件等处理。

- 深度学习检测引擎（自主研发）：云盾深度学习检测引擎，使用深度学习技术，基于海量攻防样本，专门打造的一款适用于云环境的恶意文件检测引擎，智能识别未知威胁，是传统病毒查杀引擎的有力支撑。
- 云沙箱（自主研发）：真实还原云上环境，监控恶意样本攻击行为，结合大数据分析、机器学习建模等技术，自动化检测和发现未知威胁，提供有效的动态分析检测能力。
- 集成国内外主流病毒查杀引擎：云查杀集成国内外多款优秀的杀毒引擎，可对病毒进行实时更新。
- 威胁情报检测：基于云盾威胁情报数据，配合主机异常行为检测模型，实现多维度检测异常进程和恶意行为。

云查杀覆盖的病毒类型

云查杀是阿里云安全技术与攻防专家经验融合的最佳实践，从数据的采集、脱敏、识别、分析、隔离到恢复已形成安全闭环，同时支持用户在云安全中心控制台中进行隔离和恢复处理。

云查杀覆盖以下病毒类型：

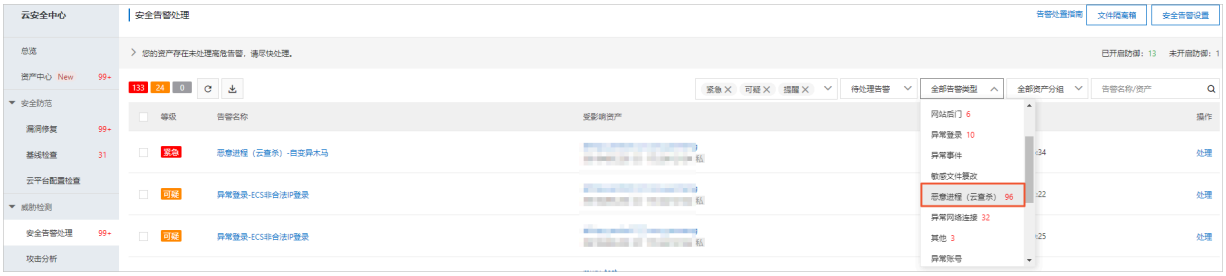
病毒类型	病毒描述
挖矿程序	非法占用服务器资源进行虚拟货币挖掘的程序。
蠕虫病毒	利用网络进行复制和传播的恶意程序，能够在短时间内大范围传播。
勒索病毒	利用各种加密算法对文件进行加密，感染此病毒一般无法解密，如WannaCry等。
木马程序	特洛伊木马，可受外部用户控制以窃取本机信息或者控制权、盗用用户信息等的程序，可能会占用系统资源。
DDoS木马	用于控制肉鸡对目标发动攻击的程序，会占用本机带宽攻击其他服务器，影响用户业务的正常运行。
后门程序	黑客入侵系统后留下的恶意程序，通过该程序可以随时获得主机的控制权或进行恶意攻击。
病毒型感染	运行后感染其他正常文件，将可能携带有感染能力的恶意代码植入正常程序，严重时可能导致整个系统感染。
恶意程序	其他威胁系统和数据安全的程序，例如黑客程序等。

云查杀的优势

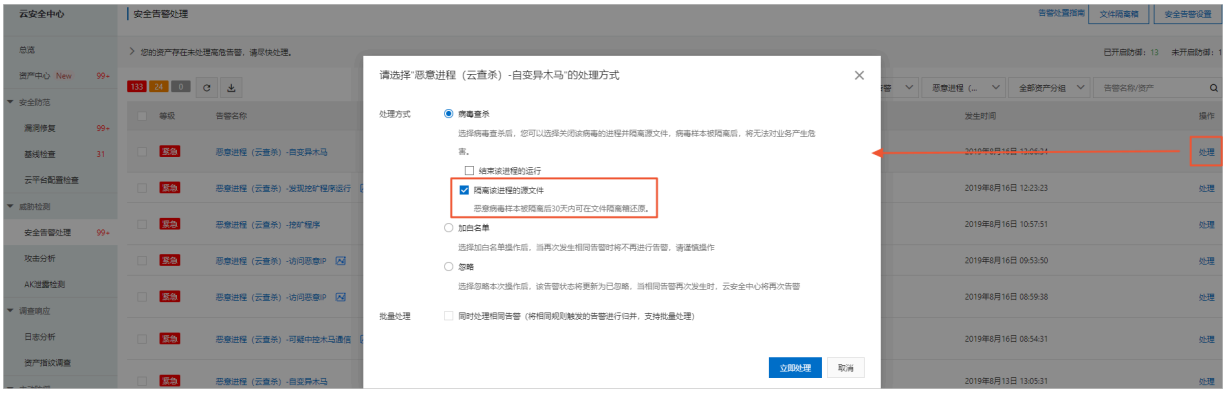
- 自主可控：基于自主研发的深度学习、机器学习能力及大数据攻防经验，并结合多引擎检测能力，为用户提供全面、实时的病毒检测服务。
- 轻量：客户端服务仅占用1%的CPU、50MB内存，不影响业务的运行。
- 实时：获取进程启动日志，实时监控病毒程序的启动。
- 统一管理：云安全中心控制台支持对所有主机进行统一管理，实时查看所有主机的安全状态。

云查杀应用案例

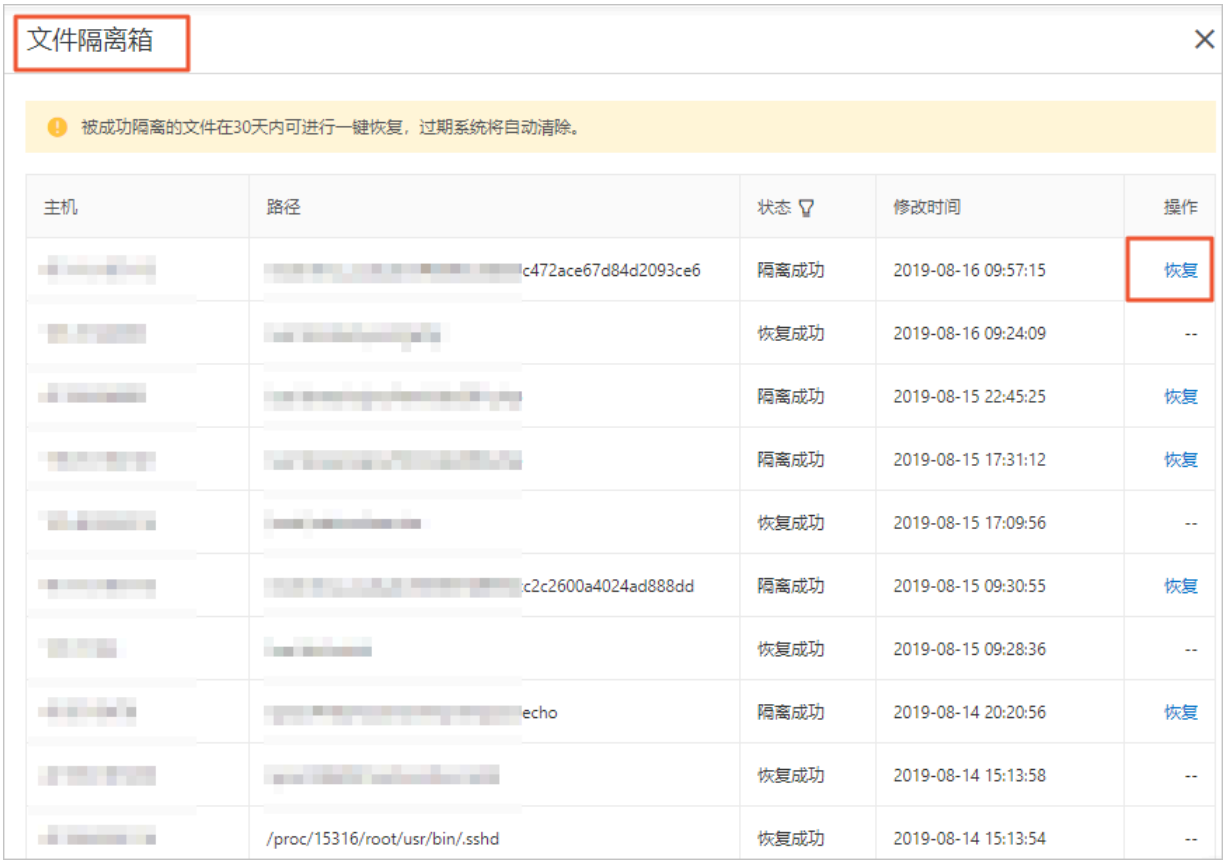
检测



隔离



恢复



安全威胁防御限制说明

云安全中心支持安全告警实时检测与处理、漏洞检测与一键修复、攻击分析、云平台安全配置检查等功能，结合告警关联分析和攻击自动化溯源，帮助您全面加固系统和资产的安全防线。在云安全中心提供的防御能力以外，建议您也时时更新服务器安全系统补丁、配合使用云防火墙、Web应用防火墙等产品缩小网络安全威胁的攻击范围，实时预防，不让黑客有任何可乘之机。

说明:

由于网络攻击手段、病毒样本在不断的演变，实际的业务环境也有不同差异，因此无法保证能实时检测防御所有的未知威胁，建议您基于安全告警处理、漏洞、基线检查、云平台配置检查等安全能力，提升整体安全防线，预防黑客入侵和盗取或破坏业务数据。

2 攻击分析

云安全中心企业版支持攻击分析，为您全面展示您资产受到的攻击并对攻击行为进行分析。

攻击分析基于阿里云平台的安全防护能力，为您提供基础攻击检测和防护。建议您根据自身业务需求，可考虑从防火墙和业务安全方面构建更精细化的纵深防护体系。

您可通过云安全中心控制台攻击分析页面查看您资产受到的攻击详情。

说明：

对于新购买的云产品，需等待数据同步完成后才可看到新购云产品相关的攻击分析信息。

攻击分析页面包含以下模块信息：

- 攻击时间范围：获取当天、最近7天或30天内的攻击详情。
- 攻击次数：指定时间范围内资产被攻击的总次数。
- 攻击类型分布：攻击类型和对应的攻击次数。
- 攻击来源TOP5：攻击次数排名前5位的攻击来源IP地址。
- 被攻击资产TOP5：被攻击次数排名前5位的资产信息。
- 攻击详情列表：所有攻击事件的详细信息，包含攻击发生的时间、攻击源IP地址、被攻击的资产信息、攻击类型和攻击状态。

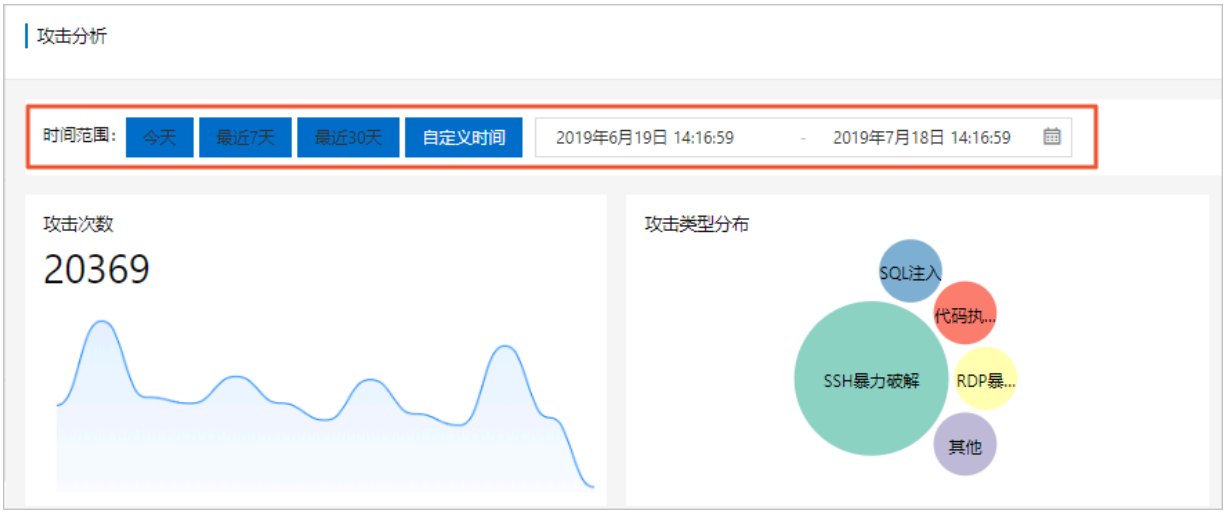
说明：

攻击分析数据来源于云安全中心、阿里云云平台、Web应用防火墙（前提是已开通Web应用防火墙服务）。

攻击时间范围

您可在攻击分析页面通过指定攻击发生的时间范围筛选和查看指定时间范围内发生的攻击事件及其详情。

攻击时间范围可选择今天、最近7天内、最近30天内或自定义时间段。

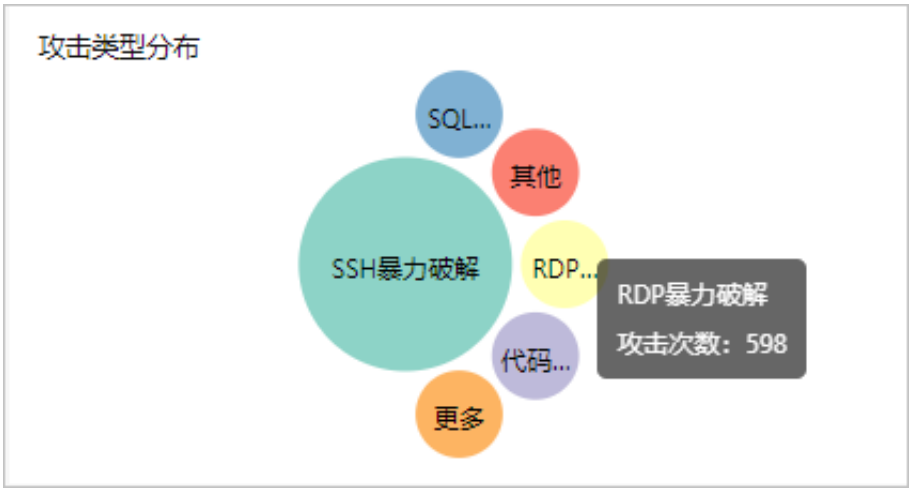


攻击次数

您可在攻击次数区域查看指定时间范围内资产被攻击的总次数曲线图和攻击次数峰谷值。鼠标悬浮在曲线图上可展示攻击发生的日期、时间和次数值。

攻击类型分布

您可在攻击类型分布区域查看攻击类型名称和该类型攻击发生的总次数。



攻击来源TOP5

您可在攻击来源TOP5区域查看攻击您资产次数排名前5的攻击源IP地址及其攻击次数。

被攻击资产TOP5

您可在被攻击资产TOP5区域查看您资产中被攻击次数排名前5的资产公网IP地址及其被攻击次数。

攻击详情列表

您可在攻击详情列表中查看您资产受到的攻击详细信息，包含攻击发生的时间、攻击源IP地址、被攻击的资产信息、攻击类型、攻击方法和攻击状态。

说明:
攻击详情列表展示攻击数据上限为10000条。如需查看更多数据可切换时间范围查看指定时间范围内的全部攻击数据。

攻击详情参数表

内容	描述
攻击时间	攻击发生的时间。
攻击来源	攻击的源IP地址。
被攻击资产	被攻击资产的名称和公网、私网IP地址。
攻击方法	发起攻击采用的HTTP请求方法：POST或GET。
攻击类型	攻击事件的类型，如SSH暴力破解、代码执行等。

内容	描述
攻击状态	攻击事件当前所处的状态。云安全中心在检测到攻击事件的同时基于云平台防御能力对常见攻击进行防御，已防御的攻击事件状态为已防御。异常入侵事件将会展示在安全告警中。

您可在攻击详情列表右上方通过筛选指定的攻击类型、被攻击资产或攻击源IP地址，搜索指定的攻击事件并查看其详细信息。

鼠标放到被攻击资产名称可显示该资产的基本信息。

3 AK泄露检测

云安全中心可以检测在Github等第三方代码托管网站上的公开代码中可能包含的您资产的登录账号和密码信息。

背景信息

阿里云云安全中心企业版支持AK泄露检测功能，基础版和高级版不支持该功能。基础版和高级版用户需先升级至企业版，才可使用AK泄露检测服务。

功能说明

因企业制度不规范或管理困难，企业员工有权限（或无意识地）将公司源码上传至Github等代码托管平台，导致企业的数据库连接地址和密码以及服务器登录密码等在代码中直接外泄。

云安全中心使用搭建在网络空间中的威胁情报采集系统，通过网络爬虫对Github等第三方代码托管网站进行实时监控，捕获并判定被公开的源代码（多为企业员工私自上传并不小心公开）中是否含有ECS、RDS、Redis、MySQL等用户资产的登录名和密码等信息，帮助企业规避数据外泄。

云安全中心AK和账密泄露检测功能支持检测AK（AccessKey）信息。

> 说明:
> 如果用户在云安全中心控制台的安全运营 > 设置 > 通知页面，设置AccessKey泄露情报的通知时间是`8:00-20:00`，这种情况下，`8:00-20:00`以外时间检测到的AK泄露情报，只能在以后的这个时间段通知。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击威胁检测 > AK泄露检测。

3. 您可以在AK泄露检测页面，进行以下操作。

- 查看AccessKey泄露情报列表

  您可以查看云安全中心检测到的所有信息泄露情报：AccessKey泄露次数及检测列表、检测平台、最近一次检测时间。

- 搜索指定AccessKey泄露情报

  在搜索框输入AccessKey ID可以快速定位到想要查看的记录。

- 执行立即检测

  您可以在AccessKey泄露检测页，单击立即检测，检测最新的AccessKey泄露情报。

- 查看AccessKey泄露检测详情

  您可以选择一个记录，单击其操作列下的详情，查看详细的情报信息。

- 处理检测出的AK泄露事件

  您可以根据AccessKey泄露详情页面的相关推荐，尽快确认数据泄露事件以及参考建议方案对AK泄露进行处理。

  - 您可以前往日志检索平台，搜索对应的服务器访问日志（例如，检索日志源Web访问日志，指定URI字段为包含AK应用文件的文件路径），确认数据是否泄漏。
  - 处理方式包含手动删除、手动禁用AK、加白名单三种，您可根据实际情况选择合适的处理方式。

    您可以在AccessKey泄露检测列表，单击一个检测记录右侧操作列下的处理，选择处理方式。

    如果选择加入白名单处理，该检测项处理状态变为已加白名单，并进入已处理列表。需要回复检测时，可以从已处理列表，进入AccessKey泄露详情页进行取消白名单操作。

说明:

建议您禁止员工将公司源代码托管在GitHub等代码平台，或使用私有的Github代码托管来管理代码，搭建企业内部的代码托管系统，防止源代码和敏感信息泄露。

- 导出AccessKey泄露检测报表

  您可以单击AccessKey泄露检测列表右上角的导出按钮。报表导出完成后，安全告警页面右上角会提示导出完成。单击右上角导出完成提示对话框中的下载，将excel格式的报表下载到本地。

4 RDS SQL注入威胁检测

云安全中心企业版支持RDS SQL注入威胁检测功能，帮助您及时发现资产中是否存在RDS SQL注入隐患。

背景信息

RDS SQL注入是数据库攻击的常见方式之一。SQL注入会导致数据泄露、篡改或对敏感数据的非法操作，威胁您资产的数据安全。

> 说明:
> 云安全中心基础版和高级版不支持云产品威胁检测-RDS SQL注入功能。

步骤一：开通RDS SQL洞察

1. 登录RDS管理控制台。
2. 在左侧导航栏单击实例列表 > 基本信息。
3. 在实例列表页面中单击需要开通RDS SQL洞察功能的数据库实例。
4. 在左侧导航栏单击SQL洞察 > 立即开通。
5. 选择您所需要的RDS日志存储时长。

   SQL洞察试用版只能查询当天的日志数据，建议选择非试用版。

> 说明:
> 开通非试用版SQL洞察功能会收取RDS相关使用费用，选择30天或以上，按小时扣费，每小时每GB 0.008元。无需使用SQL洞察时，可关闭该功能。RDS SQL洞察详细说明参见#unique_26。

步骤二：开启RDS SLS日志投递

1. 登录SLS管理控制台。
2. 在接入数据模块单击RDS审计-云产品，进行RDS审计数据接入。
3. 在RDS审计页面新建或选择您想存放SQL洞察数据相关的项目Project和日志库Logstore。
4. 在RDS审计实例列表中，定位到需要开启SQL注入检测的SQL实例，单击开通投递。

5. 单击下一步完成数据接入配置，将RDS相关日志数据同步到SLS日志服务中。

步骤三：开启云安全中心RDS SQL注入威胁检测

目前，RDS SQL注入威胁检测功能需要人工开通，您可以提交工单联系阿里云开通此功能。

步骤四（可选步骤）：查看SQL注入告警

您的资产开启了RDS SQL注入威胁检测功能后，您可在云安全中心安全告警处理页面，查看和处理云安全中心为您检测到的RDS SQL注入告警事件。