ALIBABA CLOUD

阿里云

云安全中心（态势感知）

威胁检测

文档版本：20220704

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.安全告警处理 05
1.1. 安全告警概述 05
1.2. 安全告警检测项 10
1.3. 查看和处理告警事件 31
1.4. 归档告警数据 35
1.5. 查看告警自动化关联分析 36
1.6. 攻击溯源 38
1.7. 设置IP拦截策略 43
1.8. 文件隔离箱 48
1.9. 一键导出事件列表 49
1.10. 安全告警设置 50
1.11. 病毒云查杀 52
1.12. 检测Linux Rootkit入侵威胁 56
2.攻击分析 60
3.AK泄露检测 64
4.云蜜罐 66
4.1. 云蜜罐概述 66
4.2. 开通云蜜罐服务 69
4.3. 配置云蜜罐 69
4.4. 查看和处理告警事件 73
4.5. 云蜜罐（公测中） 74
5.常见问题 78

1.安全告警处理

1.1. 安全告警概述

云安全中心支持实时检测您资产中的安全告警事件，覆盖网页防篡改、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250+威胁检测模型，提供全面的安全告警类型检测，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。

安全告警事件是指云安全中心检测到的您服务器或者云产品中存在的威胁，这些威胁可以是某个恶意IP对您资产进行的攻击，也可以是您资产中已被入侵的异常情况，例如**您的主机在执行恶意脚本或访问恶意下载源**等。

您可以在**威胁检测 > 安全告警处理**页面查看您资产中检测出的安全告警事件。

云安全中心支持检测的所有安全告警事件类型的更多信息，请参见安全告警类型列表。

> 说明
>
> - 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购买版本支持的防御能力。如需开通网页防篡改等防御能力，需**升级**到仅采购增值服务、防病毒版、高级版、企业版或旗舰版。升级的具体操作，请参见升级与降配。
> - 应用白名单和网页防篡改是云安全中心的增值服务。应用白名单需要申请才能开启，更多信息，请参见应用白名单；网页防篡改需要您单独购买并开通后才会开启。网页防篡改为仅采购增值服务、防病毒版、高级版、企业版和旗舰版功能，免费版不支持该功能。开通网页防篡改的具体操作，请参见网页防篡改开通服务。
> - 云产品威胁检测为企业版和旗舰版功能，企业版和旗舰版自动开启防御；免费版、防病毒版、高级版需要升级至企业版或旗舰版后才能自动开启防御。

威胁检测模型介绍

云安全中心通过250+威胁检测模型为您提供全面的威胁检测能力。您可以在**安全告警处理**页面，单击左上角 图标，查看云安全中心为您提供的威胁检测模型。威胁检测从攻击入口、载荷投递、权限提升、逃避检测等10个阶段，为您提供全链路的云上威胁检测，让风险无处遁形。

安全告警统计数据介绍

云安全中心可对您已开启的告警防御能力提供总览数据，帮助您快速了解安全告警概况、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，查看安全告警和已开启的防御项目的统计信息。

下表详细介绍了**安全告警处理**页面的统计数据。

统计项	解释	相关操作
存在告警的服务器	展示您资产中存在告警的服务器数量。	单击相应数值，可跳转到**资产中心**页面的**服务器**列表。该列表展示了已检测出安全告警的服务器的详细信息。

统计项	解释	相关操作
待处理告警总数	展示您资产中未处理告警的总数量。	在**安全告警处理**页面，您可以查看默认展示的所有**待处理**告警信息。更多信息，请参见查看和处理告警事件。
急需处理的告警	展示您资产中风险等级为**紧急**的待处理告警事件的数量。	单击相应数值，自动为您筛选出对应的告警事件，方便您集中查看和处理风险等级为**紧急**的告警事件信息。 云安全中心对安全告警风险等级的分类如下： • **紧急**：即高危风险，表示您的服务器中检测到了入侵事件（例如反弹Shell等），建议您立即查看告警事件的详情并及时进行处理。 • **可疑**：即中危风险，表示服务器中检测到了可疑的异常事件（例如可疑CMD命令序列等），建议您查看该告警事件、判断是否存在风险并进行相应处理。 • **提醒**：即低危风险，表示服务器中检测到了低危的异常事件（例如可疑端口监听等），建议您及时查看该告警事件的详情。 **说明** 建议您优先处理紧急状态的告警事件。
精准防御	展示您资产中被病毒查杀功能自动隔离的病毒告警的数量。	单击相应数值，自动为您筛选出对应的告警事件，方便您集中查看被病毒查杀功能自动隔离的所有病毒告警信息。 **说明** 病毒被自动隔离表示云安全中心已成功拦截该病毒，无需您手动进行处理。
生效IP拦截策略/全部策略	• 生效IP拦截策略：展示启用防暴力破解规则后拦截的记录数量。 • 全部策略：展示云安全中心所有的防暴力破解规则拦截的记录数量。	单击相应数值，自动展开**IP规则策略库**面板，方便您集中查看已启用或全部的IP拦截策略。IP拦截策略的更多信息，请参见设置IP拦截策略。
已隔离文件数	展示云安全中心对安全告警事件进行隔离处理后，隔离威胁文件的数量。	单击相应数值，自动展开**文件隔离箱**面板，方便您集中查看被隔离的文件信息。病毒样本文件被隔离后，将无法对业务产生危害。更多信息，请参见文件隔离箱。

安全告警类型列表

2018年12月20日起，云安全中心**免费版**只支持异常登录和其他-DDoS类型安全告警。如果您需要启用更多高级威胁检测能力，需开通云安全中心付费版。云安全中心各个版本可检测的告警类型差异，请参见功能特性。

如果您想了解云安全中心支持的告警类型涉及的具体检测项，以及对应的检测原理，请参见安全告警检测项。

下表介绍了云安全中心支持检测的所有告警类型。

告警名称	告警说明

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。可检测以下子项： • 异常文件添加 • 异常文件修改 • 异常文件删除 **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。网页防篡改为防病毒版、高级版、企业版和旗舰版功能，基础版不支持该功能。更多信息，请参见网页防篡改概述。
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，包括以下子项： • Linux系统计划任务配置文件写入 • Linux计划任务文件异常篡改 • Linux可疑命令执行 • 反弹Shell（详细信息，请参见云安全中心反弹Shell多维检测技术详解。） • Python应用执行异常指令 • 利用Windows系统文件加载恶意代码 • Windows调用mshta执行html内嵌脚本指令 • 创建异常Windows计划任务 • Windows regsvr32.exe执行异常指令 • 访问恶意下载源 • 可疑注册表配置项篡改 • 异常调用系统工具 • 执行恶意命令 • 可疑特权容器启动 • 启动项异常修改
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。 **说明** 基础版仅支持部分类型Webshell检测，云安全中心其他版本支持所有类型的WebShell检测。如果您需要执行所有类型的WebShell检测，建议您升级到防病毒版、高级版、企业版或旗舰版。升级的具体操作，请参见升级与降配。

告警名称	告警说明
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。 可检测以下子项： • ECS非合法IP登录 • ECS在非常用地登录 • ECS登录后执行异常指令序列（SSH） • ECS被暴力破解成功（SSH） 更多信息，请参见云安全中心检测和告警异常登录功能的原理。
异常事件	检测程序运行过程中发生的异常行为。
敏感文件篡改	检测是否存在对服务器中的敏感文件进行恶意修改，包含Linux共享库文件预加载配置文件的可疑篡改等行为。
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。您可通过云安全中心控制台对病毒程序进行处理。 可检测以下子项： • 访问恶意IP • 挖矿程序 • 自变异木马 • 恶意程序 • 木马程序 更多信息，请参见病毒云查杀。
异常网络连接	检测网络显示断开或不正常的网络连接状态。 可检测以下子项： • 主动连接恶意下载源 • 访问恶意域名 • 矿池通信行为 • 可疑网络外连 • 反弹Shell网络外连（详细信息，请参见云安全中心反弹Shell多维检测技术详解。） • Windows异常网络连接 • 疑似内网横向攻击 • 疑似敏感端口扫描行为（包括22、80、443、3389等常用端口）
其他	检测DDoS流量攻击等网络入侵行为和客户端异常离线。
异常账号	检测非合法的登录账号。
应用入侵事件	检测通过系统的应用组件入侵服务器的行为。
云产品威胁检测	检测您购买的其他阿里云产品中是否存在威胁，例如是否存在可疑的删除ECS安全组规则行为。

告警名称	告警说明
精准防御	**病毒查杀**功能提供了精准防御能力，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。关于如何开启该功能，请参见主动防御。
应用白名单	通过在白名单策略中设置需要重点防御的服务器应用，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。
持久化后门	检测服务器上存在的可疑计划任务，对攻击者持久入侵用户服务器的威胁行为进行告警。
Web应用威胁检测	检测通过Web应用入侵服务器的行为。
恶意脚本	检测资产的系统功能是否受到恶意脚本的攻击或篡改，对可能的恶意脚本攻击行为进行告警提示。 恶意脚本分为有文件脚本和无文件脚本。攻击者在拿到服务器权限后，使用脚本作为载体来达到进一步攻击利用的目的。利用方式包括植入挖矿程序、添加系统后门、添加系统账户等操作。恶意脚本的语言主要包括Bash、Python、Perl、Powershell、BAT、VBS。
威胁情报	利用阿里云自研的威胁情报库对访问流量、日志进行关联分析，识别出可能已经发生的威胁事件，主要包括恶意域名访问、恶意下载源访问、恶意IP访问等不易直接发现的入侵行为。
恶意网络行为	通过流量内容、服务器行为等日志综合判断的异常网络行为，包括攻击者通过开放的网络服务入侵主机、或主机沦陷后对外发起的异常网络行为。
容器集群异常	检测正在运行的容器集群安全状态，帮助您及时发现容器集群中的安全隐患和黑客入侵行为。 您需要先打开云安全中心控制台**设置**页面，在**容器K8s威胁检测**模块开启**威胁检测**开关，云安全中心才会对容器集群异常行为进行检测。更多信息，请参见容器K8s威胁检测。

告警名称	告警说明
可信异常	检测服务器的系统进程是否存在修改、启动过程是否出现异常等问题。 为了正常显示告警处理和查看资产状态，您需要为c6t等可信ECS实例配置一个ECS RAM角色并赋予足够权限。例如，您可以创建一个RAM角色，将云服务器设置为授信主体，并精确赋予它系统可信服务的访问权限。更多信息，请参见云服务器ECS实例RAM角色概述。访问系统可信服务的策略定义如下： `{ "Statement": [ { "Action": [ "yundun-systrust:GenerateNonce", "yundun-systrust:GenerateAikcert", "yundun-systrust:RegisterMessage", "yundun-systrust:PutMessage" ], "Resource": "*", "Effect": "Allow" } ], "Version": "1" }` **注意** 由于RAM用户的权限分配直接影响您的数字资产的安全性，强烈建议您阅读RAM帮助文档，并根据您的实际需要分配权限，不要给予RAM角色过多权限。

1.2. 安全告警检测项

本文列出了云安全中心威胁检测模块支持的所有告警检测项，并按照操作系统、分析对象、攻击手法等维度进行分类，帮助您更全面地了解云安全中心的威胁检测能力。

云安全中心控制台**安全告警处理**页面中，可以查看支持检测的告警类型（更多信息，请参见安全告警类型列表）。这些告警类型是云安全中心根据威胁检测引擎提供的能力，结合阿里云公网上的威胁情报和披露的最新漏洞检测得出的。本文列出了具体的告警检测项，对云安全中心支持的告警类型进行详细说明，并针对告警检测项为您介绍对应的检测原理。

适用于Linux系统的告警

告警类型	具体检测项	检测原理说明
持久化后门	篡改内核模块配置文件	检测模型发现您的服务器上有篡改内核模块配置文件行为，该行为常见于Rootkit修改配置文件以达到自启动的目的。

告警类型	具体检测项	检测原理说明
持久化后门	恶意启动项脚本	检测模型发现您服务器上的某些自启动项文件可疑，可能是恶意软件或攻击者通过计划任务、自启动脚本进行的持久化行为。
持久化后门	后门进程	检测模型发现您的服务器上存在一疑似后门的可疑进程，可能是攻击者为维持权限遗留下的持久化行为。
持久化后门	异常代码驻留内存	检测模型发现您的服务器上某进程的内存空间中疑似存在恶意指令，该进程可能为攻击者在入侵后遗留的恶意软件，或者是向正常的进程注入了恶意的代码。
持久化后门	异常进程	检测模型发现您的服务器当前运行中的程序中存在异常进程，可能是恶意程序或利用正常程序加载了恶意代码。
持久化后门	异常自启动项	检测模型发现您的服务器上存在异常的自启动项，可能是恶意软件或攻击者通过添加启动项来达到持久化的目的。
持久化后门	隐藏的内核模块	检测模型发现您的服务器上存在隐藏的内核模块，极有可能是黑客或恶意软件植入的Rootkit后门，用于维持系统权限和隐藏其他恶意行为。
持久化后门	Linux可疑计划任务	检测模型发现您服务器上存在可疑的计划任务，这可能被攻击者在入侵机器后进行的持久化行为。
持久化后门	SSH后门公钥	检测模型发现您的服务器上存在异常的SSH登录公钥，该SSH公钥历史上曾被蠕虫或黑客添加到被入侵的服务器中以达到权限维持的目的。
恶意脚本	恶意脚本代码执行	检测模型发现您的服务器上正在执行恶意的Bash、Powershell、Python等脚本代码。
恶意脚本	发现恶意脚本文件	检测模型发现您的服务器上存在恶意脚本文件，该文件极有可能是攻击者成功入侵服务器后植入的，建议您根据恶意脚本的标签检查文件内容的合法性并进行处理。
恶意进程（云查杀）	被污染的基础软件	检测模型发现您的服务器上存在被污染的基础软件，被污染的基础软件是一类特殊的恶意程序，一般是被植入了恶意代码的正常系统程序，虽然具备原始基础软件的功能但具有隐藏的恶意行为。
恶意进程（云查杀）	恶意程序	检测模型发现您的服务器上运行了恶意程序，恶意程序一般是具备多种恶意行为特征的程序，或者具备骚扰、破坏行为的第三方程序。
恶意进程（云查杀）	访问恶意IP	检测模型发现您服务器上的进程正在尝试访问一个可疑的恶意IP，这个IP可能是黑客的中控IP，矿池IP等具有高风险的IP，发起连接行为的进程可能是黑客植入的恶意文件。
恶意进程（云查杀）	感染型病毒	检测模型发现您的服务器上运行了感染型病毒，感染型病毒是一类高级恶意程序，由病毒本体将恶意代码写入正常程序文件执行，因此往往有大量原本正常程序被感染后作为宿体被检出。
恶意进程（云查杀）	黑客工具	检测模型发现您的服务器上存在黑客工具，黑客工具是攻击者在入侵过程中用于权限提升、窃取敏感数据的工具，或用于卸载安全软件的程序，或入侵后植入系统的后门程序。

告警类型	具体检测项	检测原理说明
恶意进程（云查杀）	后门程序	检测模型发现您的服务器上运行了后门程序，后门程序是植入到系统中，用于给黑客对服务器做持续入侵的持久化程序。
恶意进程（云查杀）	可疑程序	检测模型发现您的服务器上运行了可疑程序，可疑程序一般是具有一定恶意代码特征或高可疑度行为特征的、暂未明确分类的程序，需要用户结合信息判断。
恶意进程（云查杀）	勒索病毒	检测模型发现您的服务器上运行了勒索病毒，勒索病毒是一类恶性程序，会对服务器上所有关键数据文件进行加密锁定以勒索赎金。
恶意进程（云查杀）	漏洞利用程序	检测模型发现您的服务器上运行了漏洞利用程序，漏洞利用程序用于攻击或尝试攻击操作系统、应用程序的已知漏洞，用于实现提权、逃逸、任意代码执行等目的。
恶意进程（云查杀）	木马程序	检测模型发现您的服务器上存在木马程序，木马程序是专门用于侵入用户服务器的程序，一般通过伪装植入系统后会下载、释放另外的恶意程序。
恶意进程（云查杀）	蠕虫病毒	检测模型发现您的服务器上运行了蠕虫病毒，蠕虫病毒是一类用于从已攻陷服务器，向其它服务器做攻击横向移动的程序，往往包括漏洞利用、密码爆破等行为。
恶意进程（云查杀）	挖矿程序	检测模型发现您的服务器上运行了挖矿程序，挖矿程序是一类侵占服务器计算资源，进行虚拟货币挖掘的程序，服务器往往可见CPU占用飙高，以及其它相关的恶意程序。
恶意进程（云查杀）	自变异木马	检测模型发现您的服务器上运行了自变异，自变异木马是具备自变异功能的木马程序，它会改变自身hash或者将自身大量复制到不同的路径下，并后台运行起来，以躲避清理。
恶意进程（云查杀）	DDoS木马	检测模型发现您的服务器上运行了DDoS木马，DDoS木马是用于从被攻陷服务器上接受指令，对黑客指定目标发起DDoS攻击的恶意程序。
恶意进程（云查杀）	Rootkit	检测模型发现您的服务器上存在Rootkit，Rootkit是一类植入到系统底层，用于隐藏自身或其它恶意程序痕迹的恶意模块。
恶意进程（云查杀）	Rootkit内核模块	检测模型发现您的服务器上存在Rootkit，Rootkit是一类植入到系统底层，用于隐藏自身或其它恶意程序痕迹的恶意模块。
进程异常行为	篡改文件时间	检测模型发现您的服务器上有进程尝试篡改文件时间，可能是攻击者在入侵过程中通过模仿系统正常文件时间来伪造异常文件真实的创建、访问、修改时间，以达到逃避检测的目的。
进程异常行为	调用风险工具	检测模型发现您的服务器异常调用了风险工具，风险工具被攻击者用于代理、隧道、扫描工具等进一步入侵服务器的场景。
进程异常行为	反弹Shell	检测模型发现您的服务器执行了反弹Shell命令，攻击者通过该方式与自己的服务器建立了反向网络连接，通过该连接可以执行任意命令。详细信息，请参见云安全中心反弹Shell多维检测技术详解。

告警类型	具体检测项	检测原理说明
进程异常行为	访问恶意下载源	检测模型发现您的服务器正在尝试访问一个可疑的恶意下载源，可能是黑客通过弱口令或命令执行漏洞，从远程服务器下载恶意文件，危害服务器安全。
进程异常行为	访问敏感文件	检测模型通过对您服务器上的进程历史行为进行自动分析，发现该进程异常读取或修改了重要的系统文件。
进程异常行为	服务应用执行可疑命令	检测模型根据您服务器上的进程历史行为自动分析，发现该服务进程启动的命令较为可疑，可能是攻击者在利用该服务的RCE漏洞成功执行了命令。
进程异常行为	高危应用执行异常指令	检测模型发现您服务器中的高危应用（如：Web服务、数据库服务、脚本、定时任务、自启动项等）执行了可疑命令，该服务可能已被攻击者攻破并通过其执行恶意命令。
进程异常行为	可疑编码命令	检测模型发现您的服务器上执行的进程命令行高度可疑，很有可能与木马、病毒、黑客行为有关。
进程异常行为	可疑端口监听异常进程	检测模型发现您的服务器出现异常的端口监听事件，攻击者在入侵服务器后，常常会借助nc等软件建立监听端口，以此建立隐蔽通信通道实现信息窃取等目的。
进程异常行为	可疑路径	检测模型发现您的服务器上存在可疑的文件名后缀，该文件格式为可执行文件，与后缀所代表格式不匹配，常见于攻击者在入侵过程中修改可执行文件名后缀以逃避检测。
进程异常行为	可疑文件落盘执行	检测模型发现您的服务器上的某文件以一种可疑的方式被写入并执行，可能是攻击者从外部下载的恶意工具并执行。
进程异常行为	可疑行为	检测模型通过对您服务器上的历史进程行为自动分析，发现该命令较为可疑。
进程异常行为	可疑HTTP隧道信息泄漏	检测模型发现您服务器上出现利用HTTP信道将命令执行结果发送到外部服务器的行为，可能是攻击者将利用RCE漏洞执行命令的结果返回给自己的服务器。
进程异常行为	可疑SSH Tunnel端口转发隧道	检测模型发现您的服务器正在尝试建立可疑SSH Tunnel端口转发隧道。
进程异常行为	可疑Webshell写入行为	检测模型发现有可疑进程在尝试向服务器上写入Webshell文件。
进程异常行为	疑似权限提升	检测模型发现您的服务器上有进程疑似利用系统、应用漏洞来获取更高的权限，可能是攻击者在入侵过程中进行的提权行为。
进程异常行为	疑似Rootkit行为	检测模型发现你哪的服务器上有Rootkit后门正在执行可疑命令，可能是攻击者在植入Rootkit后对其下发了恶意指令来达到远程控制的目的。
进程异常行为	异常调用数据库导出工具	检测模型通过对您服务器上进程的历史行为进行分析，发现可疑调用数据库导出工具行为，可能是攻击者在攻击成功后进行数据窃取的行为。

告警类型	具体检测项	检测原理说明
进程异常行为	异常行为序列	检测模型发现您的服务器上出现了多个异常行为的序列组合，常见于各类蠕虫家族感染扩散时运行的异常行为，可能您的服务也被蠕虫病毒感染。
进程异常行为	Apache-CouchDB执行异常指令	检测模型发现您服务器上Apache-CouchDB应用执行了异常命令。
进程异常行为	FTP应用执行异常指令	检测模型发现您的FTP应用执行了异常命令，可能是攻击者通过FTP应用的弱口令，借助FTP执行BAT批处理脚本功能，执行异常命令。
进程异常行为	Java应用执行异常指令	检测模型发现您的服务器上的Java进程启动了下载恶意程序、添加后门等高危行为，很可能是因为您使用了存在漏洞的Web框架或者中间件导致。
进程异常行为	Linux计划任务文件异常篡改	检测模型发现您服务器上有进程正在尝试修改Linux计划任务文件，该行为可能是因为恶意程序、Rootkit程序正在尝试写入持久化后门代码。
进程异常行为	Linux计划任务执行异常指令	检测模型发现您服务器的计划任务执行了异常命令，可能是攻击者在入侵服务器后，为维持权限，将恶意命令写入到计划任务中。
进程异常行为	Linux可疑命令序列	检测模型发现您服务器上某进程执行了一系列可疑的命令，这些命令与攻击者入侵后通常会执行的命令序列非常相似，建议排查这些命令的父进程，可能为远控木马、存在漏洞的Web服务，或者是合法进程被注入了恶意代码。
进程异常行为	Linux可疑命令执行	检测模型发现您的服务器上执行的进程命令行高度可疑，很有可能与木马、病毒、黑客行为有关。
进程异常行为	MySQL导出功能误用写入可疑文件	检测模型发现您服务器上的MySQL应用正尝试向敏感目录写入文件，可能是攻击者通过弱口令或Web应用执行了恶意的SQL。
进程异常行为	MySQL执行异常指令	检测模型发现您的MySQL服务执行了可疑的命令，可能是由于MySQL服务存在弱口令、或Web服务被SQL注入导致。
进程异常行为	Oracle执行异常指令	检测模型发现您的服务器上的Oracle数据库执行了可疑命令，可能是因为数据库密码泄漏导致黑客远程命令执行。
进程异常行为	Postgres导出功能被误用写入可疑UDF库文件	检测模型发现您服务器上的Postgres应用正在尝试向磁盘上写入可疑so文件，可能由于Postgres存在弱口令被攻击者登录后并执行了恶意SQL，该文件可能导致您的服务器被攻击者控制。
进程异常行为	Postgresql应用执行异常指令	检测模型发现到您的Postgres服务执行了可疑的命令，可能是由于Postgres服务存在弱口令、或Web服务被SQL注入导致。
进程异常行为	Python应用执行异常指令	检测模型发现您服务器上的Python应用执行异常命令，可能是由于您服务器上通过Python搭建的Web应用存在RCE漏洞并被利用成功。
进程异常行为	Redis入侵后修改Crontab	检测模型发现您服务器上的Redis应用向磁盘写入了可疑文件，可能是攻击者通过Redis空口令或弱口令，执行了恶意SQL，该行为可使攻击者直接获取服务器权限。

告警类型	具体检测项	检测原理说明
进程异常行为	Tomcat执行异常指令	检测模型发现您的Tomcat容器执行了异常命令，可能是攻击者通过Tomcat容器中Java应用存在的RCE漏洞或Webshell执行了恶意命令。
敏感文件篡改	篡改系统文件	检测模型发现您服务器上有进程尝试修改、替换系统文件，可能是攻击者尝试通过替换系统文件以达到躲避检测、隐藏后门等目的，请及时确认您服务器上告警的系统文件是否为真实的系统文件。
敏感文件篡改	挪移系统文件	检测模型发现您的服务器上游进程尝试挪移系统文件，可能是攻击者在入侵过程中，通过挪移被安全软件监控的系统文件来达到绕过部分检测逻辑的目的。
敏感文件篡改	Linux共享库文件预加载配置文件可疑篡改	检测模型发现您服务器上的共享库文件预加载配置文件正在被可疑篡改。
其他	云安全中心客户端异常离线	检测模型发现您服务器上的云安全中心客户端主进程AliYunDun在当天异常离线，该情况可能是因为网络不稳定导致的暂时现象，也可能是因为遭到恶意黑客入侵导致云安全中心客户端被强制卸载。请登录服务器确认云安全中心客户端进程是否处于运行状态，如果不在请及时启动。
网站后门	发现后门（Webshell）文件	检测模型在您的服务器上发现了一个可疑的Webshell文件，可能是攻击者成功入侵网站后为维持权限植入的后门文件。
异常登录	恶意IP登录	检测模型发现您的服务器被恶意IP登录成功，该IP在历史上曾被发现存在恶意攻击行为。如果不是您的登录行为，请尽快修改ECS的密码。
异常登录	恶意IP登录（FTP）	检测模型发现您服务器上的FTP应用被恶意IP登录成功，此IP在历史上曾被发现过存在恶意攻击行为。如果不是您的登录行为，请尽快修改FTP的密码。
异常登录	恶意IP登录（MySQL）	检测模型发现您服务器上的MySQL应用被恶意IP登录成功，此IP在历史上曾被发现过存在恶意攻击行为。如果不是您的登录行为，请尽快修改MySQL的密码。
异常登录	后门账户登录	检测模型发现您的服务器之前被攻击者植入了后门账户，且该后门账户刚刚被成功登录，如果不是您的操作行为，请尽快删除此账号。
异常登录	弱口令账户登录	检测模型发现您的服务器存在弱口令的账户被成功登录，这可能是攻击者或者您自己的登录行为，弱口令是攻击者最常利用的入侵手段，建议您立即加强口令的强度，防止黑客入侵。
异常登录	疑似对外发起登录扫描活动	检测模型发现您的服务器频繁对外发起爆破扫描SSH、RDP、SMB等协议的行为，可能是您的服务器已被攻击者入侵并被用于跳板来攻击其他机器。
异常登录	异常位置登录	检测模型发现您的服务器在较短时间内发生了两次用户登录，而且源自地理位置相距较远的位置。其中一个位置为您的常用登录地。发生此次行为，说明您的登录请求从一个常用位置移动到异常位置。如果不是您的登录行为，请尽快修改服务器的密码。

告警类型	具体检测项	检测原理说明
异常登录	异常账户登录	检测模型发现您将异常账户添加进管理员用户组，并检测此账户有登录行为，如果不是您的操作行为，请尽快删除此账号。
异常登录	ECS被暴力破解成功（多个无效用户）	检测模型发现您的服务器被一个IP使用多个无效的用户名尝试登录，并最后登录成功，如果不是您的登录行为，请尽快修改ECS的密码。
异常登录	ECS被暴力破解成功（RDP）	检测模型发现您的服务器正在被RDP暴力破解攻击，且攻击者在进行了一定次数的尝试后，试出了您的RDP服务密码，成功登录了系统。
异常登录	ECS登录后执行异常指令序列（SSH）	检测模型发现您的服务器在被一IP登录后，执行了一系列恶意指令，很有可能是由于您服务器的密码较弱或密码泄露被攻击者登录执行。
异常登录	ECS非常用时间登录	本次登录的时间非您定义的合法登录时间范畴，请您确认登录行为合法性。
异常登录	ECS非常用账号登录	本次登录的账号非您定义的合法账号范畴，请您确认登录行为合法性。
异常登录	ECS非常用IP登录	本次登录的IP非您定义的合法IP范畴，请您确认登录行为合法性。
异常登录	ECS在非常用地登录	本次登录的登录地非您定义的合法登录地范畴，请您确认登录的合法性。
异常网络连接	端口转发	检测模型发现您服务器上有进程正在尝试建立端口转发隧道，可能是攻击者在入侵服务器后，将该服务器作为跳板进而攻击内网的其他服务器。
异常网络连接	访问恶意域名	检测模型从DNS流量中发现您的服务器请求解析过这个风险系数高的域名，这个域名可能是远控、僵尸网络组织、矿池地址等恶意域名，意味着您的服务器可能已经沦陷并被黑客利用。
异常网络连接	可疑网络外连	检测模型发现您服务器正在访问的网络地址，疑似与中控后门、僵尸网络组织、矿池地址等地址相关。
异常网络连接	可疑Meterpreter反弹Shell连接	检测模型发现您的服务器上存在可疑进程，正在尝试利用黑客工具Meterpreter将命令控制通道反弹至攻击者的服务器。详细信息，请参见云安全中心反弹Shell多维检测技术详解。
异常网络连接	矿池通信行为	检测模型发现您的服务器存在与矿池IP通信的流量，您的服务器可能已被攻击者入侵并用于挖矿。
异常网络连接	内网扫描	检测模型发现您的服务器有进程在短时间内对多个内网IP的指定端口发起了疑似扫描行为，可能是攻击者在入侵后，尝试进行横向移动的行为。
异常网络连接	疑似内网横向攻击	检测模型发现您的服务器上存在异常的内网连接，可能是攻击者入侵服务器后，进行内网横向移动的行为。
异常网络连接	异常网络流量	检测模型通过分析您服务器的流量，发现存在异常的网络流量通信，可能是成功的漏洞利用、恶意软件通信、敏感信息泄露、可疑的代理隧道等，请根据告警详情信息做进一步判断处理。

告警类型	具体检测项	检测原理说明
异常网络连接	主动连接恶意下载源	检测模型通过HTTP流量发现您的服务器正在尝试访问一个可疑的恶意下载源，可能是黑客通过弱口令或命令执行漏洞，从远程服务器下载恶意文件，危害服务器安全。
异常网络连接	Redis执行异常指令	检测模型发现到有攻击者连接您的Redis服务后执行了恶意SQL，可能导致您的服务器被攻击者控制。
异常账号	使用可疑账号登录系统	检测模型发现到当前有用户尝试使用默认禁用、系统内置账号、或疑似黑客账号登录系统，可能是黑客的入侵行为。

适用于Windows系统的告警

告警类型	具体检测项	检测原理说明
持久化后门	可疑自启动项	检测模型发现您服务器上的某些自启动项可疑，可能是恶意软件或者黑客在入侵后进行的持久化痕迹。
持久化后门	疑似后门	检测模型发现您的服务器上存在wmi或bitsadmin后门，可能是攻击者在入侵后用来维持对您的服务器权限。
持久化后门	异常代码驻留内存	检测模型发现您的服务器上某进程的内存空间中疑似存在恶意指令，该进程可能为攻击者在入侵后遗留的恶意软件，或者是向正常的进程注入了恶意的代码。
持久化后门	异常进程	检测模型发现您的服务器当前运行中的程序中存在异常进程，可能是恶意程序或利用正常程序加载了恶意代码。
持久化后门	异常注册表项	检测模型发现您服务器上的某个注册表配置项可疑，恶意软件常常会修改某些关键注册表配置来持久化运行或干扰正常的安全防护。
持久化后门	异常自启动项	检测模型发现您的服务器上存在异常的自启动项，可能是恶意软件或攻击者通过添加启动项来达到持久化的目的。
持久化后门	CobaltStrike远控木马	检测模型发现您服务器上某个进程内存空间内存在CobaltStrike远控木马的恶意代码，可能该进程即为恶意程序或正常程序被注入了恶意指令。
恶意脚本	恶意脚本代码执行	检测模型发现您的服务器上正在执行恶意的Bash、Powershell、Python等脚本代码。
恶意脚本	发现恶意脚本文件	检测模型发现您的服务器上存在恶意脚本文件，该文件极有可能是攻击者成功入侵服务器后植入的，建议您根据恶意脚本的标签检查文件内容的合法性并进行处理。
恶意进程（云查杀）	恶意程序	检测模型发现您的服务器上运行了恶意程序，恶意程序一般是具备多种恶意行为特征的程序，或者具备骚扰、破坏行为的第三方程序。
恶意进程（云查杀）	访问恶意IP	检测模型发现您服务器上的进程正在尝试访问一个可疑的恶意IP，这个IP可能是黑客的中控IP，矿池IP等具有高风险的IP，发起连接行为的进程可能是黑客植入的恶意文件。

告警类型	具体检测项	检测原理说明
恶意进程（云查杀）	感染型病毒	检测模型发现您的服务器上运行了感染型病毒，感染型病毒是一类高级恶意程序，由病毒本体将恶意代码写入正常程序文件执行，因此往往有大量原本正常程序被感染后作为宿体被检出。
恶意进程（云查杀）	黑客工具	检测模型发现您的服务器上存在黑客工具，黑客工具是攻击者在入侵过程中用于权限提升、窃取敏感数据的工具，或用于卸载安全软件的程序，或入侵后植入系统的后门程序。
恶意进程（云查杀）	后门程序	检测模型发现您的服务器上运行了后门程序，后门程序是植入到系统中，用于给黑客对服务器做持续入侵的持久化程序。
恶意进程（云查杀）	可疑程序	检测模型发现您的服务器上运行了可疑程序，可疑程序一般是具有一定恶意代码特征或高可疑度行为特征的、暂未明确分类的程序，需要用户结合信息判断。
恶意进程（云查杀）	勒索病毒	检测模型发现您的服务器上运行了勒索病毒，勒索病毒是一类恶性程序，会对服务器上所有关键数据文件进行加密锁定以勒索赎金。
恶意进程（云查杀）	漏洞利用程序	检测模型发现您的服务器上运行了漏洞利用程序，漏洞利用程序用于攻击或尝试攻击操作系统、应用程序的已知漏洞，用于实现提权、逃逸、任意代码执行等目的。
恶意进程（云查杀）	木马程序	检测模型发现您的服务器上存在木马程序，木马程序是专门用于侵入用户服务器的程序，一般通过伪装植入系统后会下载、释放另外的恶意程序。
恶意进程（云查杀）	蠕虫病毒	检测模型发现您的服务器上运行了蠕虫病毒，蠕虫病毒是一类用于从已攻陷服务器，向其它服务器做攻击横向移动的程序，往往包括漏洞利用、密码爆破等行为。
恶意进程（云查杀）	挖矿程序	检测模型发现您的服务器上运行了挖矿程序，挖矿程序是一类侵占服务器计算资源，进行虚拟货币挖掘的程序，服务器往往可见CPU占用飙高，以及其它相关的恶意程序。
恶意进程（云查杀）	自变异木马	检测模型发现您的服务器上运行了自变异，自变异木马是具备自变异功能的木马程序，它会改变自身hash或者将自身大量复制到不同的路径下，并后台运行起来，以躲避清理。
恶意进程（云查杀）	DDoS木马	检测模型发现您的服务器上运行了DDoS木马，DDoS木马是用于从被攻陷服务器上接受指令，对黑客指定目标发起DDoS攻击的恶意程序。
恶意进程（云查杀）	Hashdump攻击异常事件	检测模型发现您的服务器上有wce、minikazi恶意软件运行，该工具可窃取系统账号HASH，导致您的账号密码泄漏。
进程异常行为	创建异常Windows计划任务	检测模型发现您的服务器上创建了异常的Windows计划任务，可能是恶意软件或攻击者在入侵过程中为维持权限而进行的行为。
进程异常行为	调用风险工具	检测模型发现您的服务器异常调用了风险工具，风险工具被攻击者用于代理、隧道、扫描工具等进一步入侵服务器的场景。
进程异常行为	调用wmic启动可疑进程	检测模型发现您服务器尝试使用wmic创建并执行程序，攻击者在入侵您服务器后，会通过创建wmic任务的方式来维持权限。

告警类型	具体检测项	检测原理说明
进程异常行为	访问恶意下载源	检测模型发现您的服务器正在尝试访问一个可疑的恶意下载源，可能是黑客通过弱口令或命令执行漏洞，从远程服务器下载恶意文件，危害服务器安全。
进程异常行为	高危应用执行异常指令	检测模型发现您服务器中的高危应用（如：Web服务、数据库服务、脚本、定时任务、自启动项等）执行了可疑命令，该服务可能已被攻击者攻破并通过其执行恶意命令。
进程异常行为	高危应用植入可疑文件	检测模型发现您服务器上的敏感服务（如Web应用等）创建了可疑的可执行文件或脚本，可能是攻击者通过漏洞攻击服务后向系统投递病毒或木马的行为。
进程异常行为	可疑的脚本操作	检测模型发现您的服务器上执行的某些与脚本相关的命令高度可疑，很有可能与恶意软件、黑客入侵有关。
进程异常行为	可疑的进程路径	检测模型发现您服务器上某个进程从一个不寻常的路径启动，常规软件通常不会在这种目录中，该进程有可能是病毒、木马、黑客入侵过程中放置的工具。
进程异常行为	可疑的进程文件名	检测模型发现您服务器上某个进程的文件名具有迷惑性后缀或是有模仿系统文件名的嫌疑，有可能是病毒、木马、黑客入侵过程中放置的工具。
进程异常行为	可疑端口监听异常进程	检测模型发现您的服务器出现异常的端口监听事件，攻击者在入侵服务器后，常常会借助nc等软件建立监听端口，以此建立隐蔽通信通道实现信息窃取等目的。
进程异常行为	可疑命令	检测模型发现您的服务器执行了可疑的信息收集命令，或启动的进程调用关系存在异常，可能与木马病毒或黑客入侵有关。
进程异常行为	可疑文件落盘执行	检测模型发现您的服务器上的某文件以一种可疑的方式被写入并执行，可能是攻击者从外部下载的恶意工具并执行。
进程异常行为	可疑注册表配置项修改	检测模型发现您服务器上有进程尝试修改注册表配置，可能是攻击者在获取服务器权限后写入后门代码或修改敏感配置。
进程异常行为	可疑CMD命令序列	检测模型发现您服务器上某进程执行了一系列可疑的命令，这些命令与攻击者入侵后通常会执行的命令序列非常相似，建议排查这些命令的父进程，可能为远控木马、存在漏洞的Web服务，或者是合法进程被注入了恶意代码。
进程异常行为	可疑procdump进程镜像转储	检测模型发现您的服务器上正在进行procdump进程镜像转储，该行为可能导致敏感数据泄漏。
进程异常行为	利用bitsadmin启动可疑进程	检测模型发现您的服务器尝试利用bitsadmin启动可疑进程，可能是攻击者利用该功能进行植入恶意程序以及执行恶意命令。
进程异常行为	利用Windows系统文件加载恶意代码	检测模型发现您的服务器执行的命令极有可能是有攻击者在利用Windows系统文件加载恶意代码，以此绕过安全软件的检测。
进程异常行为	启动项异常修改	检测模型发现您服务器上有进程正在尝试修改系统的自启动项，可能是木马病毒或攻击者通过这种方式来维持对您服务器的权限。

告警类型	具体检测项	检测原理说明
进程异常行为	使用attrib.exe修改文件的只读隐藏属性	检测模型发现您服务器上有进程正在尝试使用attrib.exe修改文件的只读隐藏属性。
进程异常行为	通过注册表添加自启动程序	检测模型发现您的服务器上有程序向注册表中添加自启动项，常见于流氓软件，含有后门的推广软件以及入侵持久化行为，也被正常软件用于开机自启动，请确认该进程路径是否为可信程序。
进程异常行为	通过FTP从远程服务器下载可疑文件到磁盘	检测模型发现您服务器上有进程正在尝试通过FTP从远程服务器下载可疑文件。
进程异常行为	通过RDP远程登录拷贝可疑文件到本地磁盘	检测模型发现有攻击者尝试通过RDP远程登录向您的服务器拷贝可疑文件，可能是因为您的服务器RDP登录密码被黑客窃取或爆破成功。
进程异常行为	系统备份异常删除	检测模型发现您服务器上有进程尝试删除系统备份文件，可能为勒索病毒为达到勒索的目的，通过删除系统的备份来阻止恢复文件。
进程异常行为	系统日志异常删除	检测模型发现您的服务器上有进程在删除系统日志，恶意软件或攻击者通常会通过清除系统日志来达到躲避检测的目的。
进程异常行为	疑似黑客工具	检测模型发现您服务器上执行的某些命令与常用的黑客工具非常类似，可能是由攻击者在入侵过程中执行的命令。
进程异常行为	疑似Windows提权操作	检测模型发现您的服务器上执行的某些命令非常可疑，极有可能是有攻击者在利用系统或应用漏洞获取更高的系统权限。
进程异常行为	异常的注册表操作	检测模型发现您的服务器上执行的某些命令操作Windows注册表的方式高度可疑，可能与恶意软件或攻击者入侵后在修改相关的配置项。
进程异常行为	异常调用数据库导出工具	检测模型通过对您服务器上进程的历史行为进行分析，发现可疑调用数据库导出工具行为，可能是攻击者在攻击成功后进行数据窃取的行为。
进程异常行为	异常调用系统工具	检测模型发现您服务器上有进程正以一种可疑方式的调用系统工具，木马病毒或黑客常常会通过这种方式绕过常规的安全软件来下载恶意文件、加载恶意代码、执行加解密操作等其他恶意操作。
进程异常行为	异常修改系统安全配置	检测模型发现您的服务器上有进程正在修改系统安全配置，可能为恶意软件或攻击者通过修改防火墙、杀毒软件配置来躲避检测。
进程异常行为	执行恶意命令	检测模型发现您的服务器上执行的进程命令行高度可疑，很有可能与木马、病毒、黑客行为有关。
进程异常行为	CobaltStrike远控恶意行为	检测模型发现您的服务器中存在CobaltStrike控制端，并正在执行恶意操作命令。
进程异常行为	FTP应用执行异常指令	检测模型发现您的FTP应用执行了异常命令，可能是攻击者通过FTP应用的弱口令，借助FTP执行BAT批处理脚本功能，执行异常命令。
进程异常行为	Java应用执行异常指令	检测模型发现您的服务器上的Java进程启动了下载恶意程序、添加后门等高危行为，很可能是因为您使用了存在漏洞的Web框架或者中间件导致。

告警类型	具体检测项	检测原理说明
进程异常行为	Lsass.exe系统安全授权程序执行异常进程	检测模型发现您的服务器上的lsass.exe进程启动了异常命令，lsass.exe进程是系统的一个安全授权服务进程，负责为登录用户进行身份鉴权和Token令牌生成，有很多系统漏洞常常针对该服务进行缓冲区溢出攻击，使得攻击者获取目标进程的完全控制权。
进程异常行为	MySQL执行异常指令	检测模型发现您的MySQL服务执行了可疑的命令，可能是由于MySQL服务存在弱口令、或Web服务被SQL注入导致。
进程异常行为	Postgresql应用执行异常指令	检测模型发现到您的Postgres服务执行了可疑的命令，可能是由于Postgres服务存在弱口令、或Web服务被SQL注入导致。
进程异常行为	Python应用执行异常指令	检测模型发现您服务器上的Python应用执行异常命令，可能是由于您服务器上通过Python搭建的Web应用存在RCE漏洞并被利用成功。
进程异常行为	regsvr32.exe执行异常指令	检测模型发现您的服务器上存在regsvr32.exe执行异常指令，可能是攻击者为了躲避系统杀软查杀，将恶意代码包装在windows ocx COM文件中，并通过regsvr32来加载到内存中运行。
进程异常行为	rundll32.exe执行异常指令	检测模型发现您的服务器上存在rundll32.exe执行异常指令，可能是攻击者为了躲避系统杀软查杀，将恶意代码包装在Windows DLL文件中，并通过rundll32.exe来加载到内存中运行。
进程异常行为	Sqlserver写可疑文件到磁盘中	检测模型发现您服务器上SQL Server应用正在尝试写入可疑文件到磁盘中，可能是因为攻击者破解了SQL Server的登录密码并执行了恶意的SQL。
进程异常行为	Sqlserver应用执行异常指令	检测模型发现您的SQL Server服务执行了可疑的命令，可能是由于SQL Server服务存在弱口令，被攻击者借助SQL Server自身的命令执行组件执行了恶意命令。
进程异常行为	Tomcat执行异常指令	检测模型发现您的Tomcat容器执行了异常命令，可能是攻击者通过Tomcat容器中Java应用存在的RCE漏洞或Webshell执行了恶意命令。
进程异常行为	Windows Defender配置修改	检测模型发现您的服务器正在通过修改注册表的方式关闭Windows Defender安全软件的部分功能，可能是攻击者在入侵服务器后使用此方法来躲避检测与防御。
进程异常行为	Windows-3389-RDP配置被修改	检测模型发现您服务器的RDP配置正在被修改，可能是攻击者在入侵服务器后，为维持权限进行的操作。
进程异常行为	Windows创建计划任务	检测模型发现到您的服务器正在创建Windows计划任务，可能由于攻击者在入侵您服务器，为维持权限而植入后门。
进程异常行为	Windows创建可疑Service服务启动项	检测模型发现您的服务器上游进程正在尝试创建可疑的Service服务启动项，该服务器可能已经被植入恶意程序，恶意程序在运行过程中会通过创建服务的方式来维持权限。
进程异常行为	Windows登录凭证窃取	检测模型发现您的服务器上某些程序修改了注册表的WDigest项，该行为常见于黑客通过修改UseLogonCredential值使系统能够明文存储登录凭证，便于攻击者后续从内存中窃取登录凭证。

告警类型	具体检测项	检测原理说明
进程异常行为	Windows调用mshta执行html内嵌脚本指令	检测模型发现您服务器上有进程在尝试调用mshta执行html内嵌脚本指令，黑客可通过这种方式向服务器植入恶意程序。
进程异常行为	Windows可疑端口转发	检测模型发现您的服务器上执行的命令可能是在转发内网的敏感端口，攻击者在内网横向移动时常常采用这种方式。
进程异常行为	Windows系统防火墙配置修改	检测模型发现有进程正在尝试修改您服务器上的Windows系统防火墙配置，请注意。
进程异常行为	Windows新增自启动项	检测模型发现您的服务器存在异常的增加自启动项的行为，可能是攻击者在入侵服务器后，为维持权限，将恶意程序添加到启动项中
进程异常行为	Windows账户异常操作	检测模型发现您服务器上的命令在操作系统账户时的上下文可疑，可能是恶意软件或者攻击者在进行用户账户的操作。
其他	云安全中心客户端异常离线	检测模型发现您服务器上的云安全中心客户端主进程AliYunDun在当天异常离线，该情况可能是因为网络不稳定导致的暂时现象，也可能是因为遭到恶意黑客入侵导致云安全中心客户端被强制卸载。请登录服务器确认云安全中心客户端进程是否处于运行状态，如果不在请及时启动。
网站后门	发现后门（Webshell）文件	检测模型在您的服务器上发现了一个可疑的Webshell文件，可能是攻击者成功入侵网站后为维持权限植入的后门文件。
异常登录	恶意IP登录	检测模型发现您的服务器被恶意IP登录成功，该IP在历史上曾被发现存在恶意攻击行为。如果不是您的登录行为，请尽快修改ECS的密码。
异常登录	恶意IP登录（FTP）	检测模型发现您服务器上的FTP应用被恶意IP登录成功，此IP在历史上曾被发现过存在恶意攻击行为。如果不是您的登录行为，请尽快修改FTP的密码。
异常登录	恶意IP登录（MySQL）	检测模型发现您服务器上的MySQL应用被恶意IP登录成功，此IP在历史上曾被发现过存在恶意攻击行为。如果不是您的登录行为，请尽快修改MySQL的密码。
异常登录	恶意IP登录（SQL Server）	检测模型发现您服务器上的SQL Server应用被恶意IP登录成功，此IP在历史上曾被发现过存在恶意攻击行为。如果不是您的登录行为，请尽快修改SQL Server的密码。
异常登录	后门账户登录	检测模型发现您的服务器之前被攻击者植入了后门账户，且该后门账户刚刚被成功登录，如果不是您的操作行为，请尽快删除此账号。
异常登录	弱口令账户登录	检测模型发现您的服务器存在弱口令的账户被成功登录，这可能是攻击者或者您自己的登录行为，弱口令是攻击者最常利用的入侵手段，建议您立即加强口令的强度，防止黑客入侵。
异常登录	疑似对外发起登录扫描活动	检测模型发现您的服务器频繁对外发起爆破扫描SSH、RDP、SMB等协议的行为，可能是您的服务器已被攻击者入侵并被用于跳板来攻击其他机器。

告警类型	具体检测项	检测原理说明
异常登录	异常位置登录	检测模型发现您的服务器在较短时间内发生了两次用户登录，而且源自地理位置相距较远的位置。其中一个位置为您的常用登录地。发生此次行为，说明您的登录请求从一个常用位置移动到异常位置。如果不是您的登录行为，请尽快修改服务器的密码。
异常登录	异常账户登录	检测模型发现您服务器上的管理员组用户，从不常见的位置登录了服务器。如果不是您的操作行为，请尽快删除此账号。
异常登录	ECS被暴力破解成功（多个无效用户）	检测模型发现您的服务器被一个IP使用多个无效的用户名尝试登录，并最后登录成功，如果不是您的登录行为，请尽快修改ECS的密码。
异常登录	ECS被暴力破解成功（SSH）	检测模型发现您的服务器正在被SSH暴力破解攻击，且攻击者在进行了一定次数的尝试后，试出了您的SSH服务密码，成功登录了系统。
异常登录	ECS登录后执行异常指令序列（SSH）	检测模型发现您的服务器在被一IP登录后，执行了一系列恶意指令，很有可能是由于您服务器的密码较弱或密码泄露被攻击者登录执行。
异常登录	ECS非常用时间登录	本次登录的时间非您定义的合法登录时间范畴，请您确认登录行为合法性。
异常登录	ECS非常用账号登录	本次登录的账号非您定义的合法账号范畴，请您确认登录行为合法性。
异常登录	ECS非常用IP登录	本次登录的IP非您定义的合法IP范畴，请您确认登录行为合法性。
异常登录	ECS在非常用地登录	本次登录的登录地非您定义的合法登录地范畴，请您确认登录的合法性。
异常网络连接	端口转发	检测模型发现您服务器上有进程正在尝试建立端口转发隧道，可能是攻击者在入侵服务器后，将该服务器作为跳板进而攻击内网的其他服务器。
异常网络连接	访问恶意域名	检测模型从DNS流量中发现您的服务器请求解析过这个风险系数高的域名，这个域名可能是远控、僵尸网络组织、矿池地址等恶意域名，意味着您的服务器可能已经沦陷并被黑客利用。
异常网络连接	可疑Meterpreter反弹Shell连接	检测模型发现您的服务器上存在可疑进程，正在尝试利用黑客工具Meterpreter将命令控制通道反弹至攻击者的服务器。详细信息，请参见云安全中心反弹Shell多维检测技术详解。
异常网络连接	矿池通信行为	检测模型发现您的服务器存在与矿池IP通信的流量，您的服务器可能已被攻击者入侵并用于挖矿。
异常网络连接	内网扫描	检测模型发现您的服务器有进程在短时间内对多个内网IP的指定端口发起了疑似扫描行为，可能是攻击者在入侵后，尝试进行横向移动的行为。
异常网络连接	疑似敏感端口扫描行为	检测模型发现您服务器上的某个进程在短时间内对敏感端口发起过多的网络请求，疑似端口扫描行为。
异常网络连接	异常网络流量	检测模型通过分析您服务器的流量，发现存在异常的网络流量通信，可能是成功的漏洞利用、恶意软件通信、敏感信息泄露、可疑的代理隧道等，请根据告警详情信息做进一步判断处理。

告警类型	具体检测项	检测原理说明
异常网络连接	主动连接恶意下载源	检测模型通过HTTP流量发现您的服务器正在尝试访问一个可疑的恶意下载源，可能是黑客通过弱口令或命令执行漏洞，从远程服务器下载恶意文件，危害服务器安全。
异常网络连接	Windows异常网络连接	检测模型发现您服务器上某个进程的网络连接行为异常，很有可能与病毒、木马或黑客行为有关。
异常账号	使用可疑账号登录系统	检测模型发现到当前有用户尝试使用默认禁用、系统内置账号、或疑似黑客账号登录系统，可能是黑客的入侵行为。

适用于容器环境的告警

告警分类	具体检测项	检测原理说明
恶意进程（云查杀）	恶意程序	检测模型发现您的服务器上运行了恶意程序，恶意程序一般是具备多种恶意行为特征的程序，或者具备骚扰、破坏行为的第三方程序。
恶意进程（云查杀）	访问恶意IP	检测模型发现您服务器上的进程正在尝试访问一个可疑的恶意IP，这个IP可能是黑客的中控IP，矿池IP等具有高风险的IP，发起连接行为的进程可能是黑客植入的恶意文件。
恶意进程（云查杀）	感染型病毒	检测模型发现您的服务器上运行了感染型病毒，感染型病毒是一类高级恶意程序，由病毒本体将恶意代码写入正常程序文件执行，因此往往有大量原本正常程序被感染后作为宿体被检出。
恶意进程（云查杀）	黑客工具	检测模型发现您的服务器上存在黑客工具，黑客工具是攻击者在入侵过程中用于权限提升、窃取敏感数据的工具，或用于卸载安全软件的程序，或入侵后植入系统的后门程序。
恶意进程（云查杀）	后门程序	检测模型发现您的服务器上运行了后门程序，后门程序是植入到系统中，用于给黑客对服务器做持续入侵的持久化程序。
恶意进程（云查杀）	可疑程序	检测模型发现您的服务器上运行了可疑程序，可疑程序一般是具有一定恶意代码特征或高可疑度行为特征的、暂未明确分类的程序，需要用户结合信息判断。
恶意进程（云查杀）	勒索病毒	检测模型发现您的服务器上运行了勒索病毒，勒索病毒是一类恶性程序，会对服务器上所有关键数据文件进行加密锁定以勒索赎金。
恶意进程（云查杀）	木马程序	检测模型发现您的服务器上存在木马程序，木马程序是专门用于侵入用户服务器的程序，一般通过伪装植入系统后会下载、释放另外的恶意程序。
恶意进程（云查杀）	蠕虫病毒	检测模型发现您的服务器上运行了蠕虫病毒，蠕虫病毒是一类用于从已攻陷服务器，向其它服务器做攻击横向移动的程序，往往包括漏洞利用、密码爆破等行为。
恶意进程（云查杀）	挖矿程序	检测模型发现您的服务器上运行了挖矿程序，挖矿程序是一类侵占服务器计算资源，进行虚拟货币挖掘的程序，服务器往往可见CPU占用飙高，以及其它相关的恶意程序。

告警分类	具体检测项	检测原理说明
恶意进程（云查杀）	自变异木马	检测模型发现您的服务器上运行了自变异，自变异木马是具备自变异功能的木马程序，它会改变自身hash或者将自身大量复制到不同的路径下，并后台运行起来，以躲避清理。
恶意进程（云查杀）	DDoS木马	检测模型发现您的服务器上运行了DDoS木马，DDoS木马是用于从被攻陷服务器上接受指令，对黑客指定目标发起DDoS攻击的恶意程序。
进程异常行为	篡改文件时间	检测模型发现您的服务器上有进程尝试篡改文件时间，可能是攻击者在入侵过程中通过模仿系统正常文件时间来伪造异常文件真实的创建、访问、修改时间，以达到逃避检测的目的。
进程异常行为	存在风险的Docker远程调试接口	检测模型发现您的Docker远程调试接口对0.0.0.0开放，暴露在公网的Docker远程调试接口会迅速被蠕虫入侵，请确保该接口仅暴露在可信的网络环境中。
进程异常行为	访问恶意下载源	检测模型发现您的服务器正在尝试访问一个可疑的恶意下载源，可能是黑客通过弱口令或命令执行漏洞，从远程服务器下载恶意文件，危害服务器安全。
进程异常行为	服务应用执行可疑命令	检测模型根据您服务器上的进程历史行为自动分析，发现该服务进程启动的命令较为可疑，可能是攻击者在利用该服务的RCE漏洞成功执行了命令。
进程异常行为	可疑编码命令	检测模型发现您的服务器上执行的进程命令行高度可疑，很有可能与木马、病毒、黑客行为有关。
进程异常行为	可疑特权容器启动	检测模型发现您的服务器中有可疑的特权容器启动，特权容器会降低容器运行时的安全性，一旦被入侵者攻破将危害到宿主服务器上的其他容器和资产，请确保您的特权容器采用了可信的镜像源，并确保其运行的服务难以被入侵。
进程异常行为	可疑文件落盘执行	检测模型发现您的服务器上的某文件以一种可疑的方式被写入并执行，可能是攻击者从外部下载的恶意工具并执行。
进程异常行为	可疑行为	检测模型通过对您服务器上的历史进程行为自动分析，发现该命令较为可疑。
进程异常行为	容器发起网络扫描行为	检测模型发现您的容器内部正在主动发起可疑的网络扫描行为，可能是攻击者通过此种方法进行深入渗透和横向移动。
进程异常行为	容器高风险操作	检测模型发现您的服务器正在执行高风险的容器操作，包括通过高危权限启动容器，向容器内部映射敏感目录、文件及端口等行为。
进程异常行为	容器内部可疑命令执行	检测模型发现您的容器内部存在异常命令执行，存在入侵风险。
进程异常行为	容器内部凭证信息搜集	检测模型发现您的容器内部存在访问敏感文件行为，如：Docker/Swarm/K8s配置文件、数据库连接配置、登录凭证、API Access Key、证书及私钥文件等。请及时确认是否存在入侵事件和数据泄露风险。
进程异常行为	容器内部提权或逃逸	检测模型在您的容器中发现可疑提权脚本、指令或漏洞信息，您的容器资产很有可能已被入侵。

告警分类	具体检测项	检测原理说明
进程异常行为	容器内部信息搜集	检测模型发现您服务器上的容器内部执行了可疑命令，此类命令常见于攻击者入侵容器后在容器内部进行信息搜集行为。如果不是可信服务触发（如安全软件、管理员运维行为等），请及时重置容器。
进程异常行为	运行恶意容器镜像	检测模型发现您的服务器正在运行恶意的容器镜像，该镜像极有可能包含后门、挖矿程序、病毒或已知的严重漏洞，请及时排查并使用可信的镜像资源。
进程异常行为	Docker异常文件操作	检测模型发现您服务器上的Docker进程正在修改系统核心服务配置或敏感文件，这可能意味着攻击者利用Docker自身漏洞劫持了某些Docker服务并利用其完成容器逃逸攻击（如：CVE-2019-5736 Docker RunC逃逸漏洞、CVE-2019-14271 Docker CP逃逸漏洞），请排查当前Docker版本是否存在此类漏洞。
进程异常行为	FTP应用执行异常指令	检测模型发现您的FTP应用执行了异常命令，可能是攻击者通过FTP应用的弱口令，借助FTP执行BAT批处理脚本功能，执行异常命令。
进程异常行为	Java应用执行异常指令	检测模型发现您的服务器上的Java进程启动了下载恶意程序、添加后门等高危行为，很可能是因为您使用了存在漏洞的Web框架或者中间件导致。
进程异常行为	K8s Service Account异常行为	检测模型发现您的容器内部存在异常指令，该指令尝试通过K8s Service Account方式连接K8s API Server，请排查相关指令是否为可信服务或可信行为触发（例如安全软件、管理员运维行为等），同时请保证该账号拥有最小必要权限，以免攻击者入侵容器后可以进一步通过K8s API横向移动。
进程异常行为	Linux可疑命令序列	检测模型发现您服务器上某进程执行了一系列可疑的命令，这些命令与攻击者入侵后通常会执行的命令序列非常相似，建议排查这些命令的父进程，可能为远控木马、存在漏洞的Web服务，或者是合法进程被注入了恶意代码。
进程异常行为	Linux可疑命令执行	检测模型发现您的服务器上执行的进程命令行高度可疑，很有可能与木马、病毒、黑客行为有关。
进程异常行为	Oracle执行异常指令	检测模型发现您的服务器上的Oracle数据库执行了可疑命令，可能是因为数据库密码泄漏导致黑客远程命令执行。
进程异常行为	Tomcat执行异常指令	检测模型发现您的Tomcat容器执行了异常命令，可能是攻击者通过Tomcat容器中Java应用存在的RCE漏洞或Webshell执行了恶意命令。
容器集群异常	恶意镜像Pod启动	检测模型发现您的K8s集群中启动了含有恶意镜像的Pod，请及时排查该Image是否来自可信来源，以及Pod内部进程是否存在后门、挖矿程序等恶意程序。
容器集群异常	K8s API Server执行异常指令	检测模型发现您的K8s API执行异常指令，这意味着您的API Server凭证可能已被黑客获取并利用，请及时排查您的服务器是否已被入侵。
容器集群异常	K8s Secrets异常访问	检测模型发现您的K8s集群中存在枚举Secrets的行为，这可能意味着您的集群遭到入侵后攻击者正在窃取K8s Secrets中的敏感信息，请及时排查该操作是否由可信程序或管理员触发。

告警分类	具体检测项	检测原理说明
容器集群异常	K8s Service Account横向移动	检测模型发现您的某个Service Account请求了历史基线外的权限，或多次触发鉴权失败。这通常出现在攻击者入侵到某个Pod内部并利用本地获取到的Service Account凭证攻击API Server的过程，请及时排查。
容器集群异常	K8s匿名用户认证成功	检测模型发现您的K8s API日志中存在成功的匿名登录事件，一般情况下匿名用户不应用于K8s运维工作，允许匿名登录且暴露在公网的集群风险较高，请及时排查改操作是否由可信管理员触发，并及时清理匿名用户的访问权限。
容器集群异常	Node敏感目录挂载	检测模型发现您的Pod启动时挂载了敏感目录或文件，这可能是黑客通过挂载敏感文件从而从Pod层逃逸到Node层的持久化方式，请及时排查该行为是否为可信操作。
网站后门	发现后门（Webshell）文件	检测模型在您的服务器上发现了一个可疑的Webshell文件，可能是攻击者成功入侵网站后为维持权限植入的后门文件。
异常网络连接	可疑网络外连	检测模型发现您服务器正在访问的网络地址，疑似与中控后门、僵尸网络组织、矿池地址等地址相关。
异常网络连接	矿池通信行为	检测模型发现您的服务器存在与矿池IP通信的流量，您的服务器可能已被攻击者入侵并用于挖矿。
异常网络连接	内网扫描	检测模型发现您的服务器有进程在短时间内对多个内网IP的指定端口发起了疑似扫描行为，可能是攻击者在入侵后，尝试进行横向移动的行为。
异常网络连接	Redis执行异常指令	检测模型发现到有攻击者连接您的Redis服务后执行了恶意SQL，可能导致您的服务器被攻击者控制。

适用于阿里云平台的告警

告警类型	具体检测项	检测原理说明
云产品威胁检测	可疑的更改指定用户密码行为	检测模型发现您的云账户通过OpenAPI修改了特定用户密码，且该行为并非一高频行为，很有可能是攻击者已经获取了您的AccessKey进行恶意操作。
云产品威胁检测	可疑的枚举安全组规则行为	检测模型发现您的云账户通过OpenAPI枚举了安全组策略，且该行为并非一高频行为，很有可能是攻击者已经获取了您的AccessKey进行恶意操作。
云产品威胁检测	可疑的枚举所有用户行为	检测模型发现您的云账户通过OpenAPI枚举了用户，且该行为并非一高频行为，很有可能是黑客已经获取了您的AccessKey进行恶意操作。
云产品威胁检测	可疑的枚举指定角色权限行为	检测模型发现您的云账户通过OpenAPI枚举了指定角色权限，且该行为并非一高频行为，很有可能是黑客已经获取了您的AccessKey进行恶意操作。

告警类型	具体检测项	检测原理说明
云产品威胁检测	可疑的删除安全组规则行为	检测模型发现您的云账户通过OpenAPI删除了安全组策略，且该行为并非一高频行为，很有可能是攻击者已经获取了您的AccessKey进行恶意操作。
云产品威胁检测	可疑的修改安全组规则行为	检测模型发现您的云账户通过OpenAPI修改了安全组策略，且该行为并非一高频行为，很有可能是攻击者已经获取了您的AccessKey进行恶意操作。
云产品威胁检测	可疑的修改ECS密码行为	检测模型发现您的云账户通过OpenAPI修改了ECS密码，且该行为并非一高频行为，很有可能是黑客已经获取了您的AccessKey进行恶意操作。
云产品威胁检测	可疑的增加安全组规则行为	检测模型发现您的云账户通过OpenAPI添加了安全组策略，且该行为并非一高频行为，很有可能是攻击者已经获取了您的AccessKey进行恶意操作。
云产品威胁检测	可疑的增加SSH Key到ECS行为	检测模型发现您的云账户通过OpenAPI添加了SSH KEY，且该行为并非一高频行为，很有可能是黑客已经获取了您的AccessKey进行恶意操作。
云产品威胁检测	云助手异常命令	检测模型发现您的云账户通过云助手OpenAPI在您的服务器上调用了命令，且命令的内容较为恶意，很有可能是黑客已经获取了您的AccessKey进行恶意操作。
云产品威胁检测	ActionTrail被关闭	检测模型发现您的云账户通过OpenAP关闭了ActionTrail，这有可能是攻击者为了避免恶意行为被记录而采取的操作，为了安全我们建议您保持ActionTrail开启。
云产品威胁检测	ActionTrail被关闭OSS投递	检测模型发现您的云账户通过OpenAPI关闭了ActionTrail，这有可能是攻击者为了避免恶意行为被记录而采取的操作，为了安全我们建议您保持ActionTrail投递功能开启。
云产品威胁检测	ActionTrail被关闭SLS投递	检测模型发现您的云账户通过OpenAPI关闭了ActionTrail，这有可能是攻击者为了避免恶意行为被记录而采取的操作，为了安全我们建议您保持ActionTrail投递功能开启。

通过分析流量内容得出的告警

告警类型	具体检测项	检测原理说明
异常网络连接	访问恶意域名	检测模型从DNS流量中发现您的服务器请求解析过这个风险系数高的域名，这个域名可能是远控、僵尸网络组织、矿池地址等恶意域名，意味着您的服务器可能已经沦陷并被黑客利用。
异常网络连接	可疑Meterpreter反弹Shell连接	检测模型发现您的服务器上存在可疑进程，正在尝试利用黑客工具Meterpreter将命令控制通道反弹至攻击者的服务器。
异常网络连接	矿池通信行为	检测模型发现您的服务器存在与矿池IP通信的流量，您的服务器可能已被攻击者入侵并用于挖矿。

告警类型	具体检测项	检测原理说明
异常网络连接	异常网络流量	检测模型通过分析您服务器的流量，发现存在异常的网络流量通信，可能是成功的漏洞利用、恶意软件通信、敏感信息泄露、可疑的代理隧道等，请根据告警详情信息做进一步判断处理。
异常网络连接	主动连接恶意下载源	检测模型通过HTTP流量发现您的服务器正在尝试访问一个可疑的恶意下载源，可能是黑客通过弱口令或命令执行漏洞，从远程服务器下载恶意文件，危害服务器安全。
异常网络连接	Redis执行异常指令	检测模型发现到有攻击者连接您的Redis服务后执行了恶意SQL，可能导致您的服务器被攻击者控制。
Web应用威胁检测	成功的SQL注入攻击	检测模型通过分析HTTP流量发现您服务器上的Web服务疑似存在SQL注入漏洞并已被黑客利用。
Web应用威胁检测	高危漏洞成功利用	检测模型通过分析HTTP流量发现您的服务器存在高危Web漏洞，并且已被攻击者成功利用。
Web应用威胁检测	敏感文件泄露	检测模型通过分析HTTP流量发现您服务器上的敏感文件被外部IP通过HTTP接口直接访问，该行为可能会导致您的敏感数据泄露，从而引发攻击者进一步的攻击。
Web应用威胁检测	疑似成功的Web攻击	检测模型发现发生到您服务器的HTTP请求日志中存在命令语句，并且对应的响应中存在命令执行的结果，这意味着您的服务器的Web服务可能存在命令执行漏洞并被黑客利用。
恶意网络行为	可疑域名访问	检测模型从DNS流量中发现您的服务器请求过这个高风险的域名，表明您的服务器可能存在恶意软件感染、未授权访问或者被黑客入侵的风险问题。

通过分析文件内容的告警

告警类型	具体检测项	检测原理说明
持久化后门	Linux可疑计划任务	检测模型发现您服务器上存在可疑的计划任务，这可能被攻击者在入侵机器后进行的持久化行为。
恶意脚本	发现恶意脚本文件	检测模型发现您的服务器上存在恶意脚本文件，该文件极有可能是攻击者成功入侵服务器后植入的，建议您根据恶意脚本的标签检查文件内容的合法性并进行处理。
恶意进程（云查杀）	被污染的基础软件	检测模型发现您的服务器上存在被污染的基础软件，被污染的基础软件是一类特殊的恶意程序，一般是被植入了恶意代码的正常系统程序，虽然具备原始基础软件的功能但具有隐藏的恶意行为。
恶意进程（云查杀）	恶意程序	检测模型发现您的服务器上运行了恶意程序，恶意程序一般是具备多种恶意行为特征的程序，或者具备骚扰、破坏行为的第三方程序。
恶意进程（云查杀）	感染型病毒	检测模型发现您的服务器上运行了感染型病毒，感染型病毒是一类高级恶意程序，由病毒本体将恶意代码写入正常程序文件执行，因此往往有大量原本正常程序被感染后作为宿体被检出。

告警类型	具体检测项	检测原理说明
恶意进程（云查杀）	黑客工具	检测模型发现您的服务器上存在黑客工具，黑客工具是攻击者在入侵过程中用于权限提升、窃取敏感数据的工具，或用于卸载安全软件的程序，或入侵后植入系统的后门程序。
恶意进程（云查杀）	后门程序	检测模型发现您的服务器上运行了后门程序，后门程序是植入到系统中，用于给黑客对服务器做持续入侵的持久化程序。
恶意进程（云查杀）	可疑程序	检测模型发现您的服务器上运行了可疑程序，可疑程序一般是具有一定恶意代码特征或高可疑度行为特征的、暂未明确分类的程序，需要用户结合信息判断。
恶意进程（云查杀）	勒索病毒	检测模型发现您的服务器上运行了勒索病毒，勒索病毒是一类恶性程序，会对服务器上所有关键数据文件进行加密锁定以勒索赎金。
恶意进程（云查杀）	木马程序	检测模型发现您的服务器上存在木马程序，木马程序是专门用于侵入用户服务器的程序，一般通过伪装植入系统后会下载、释放另外的恶意程序。
恶意进程（云查杀）	蠕虫病毒	检测模型发现您的服务器上运行了蠕虫病毒，蠕虫病毒是一类用于从已攻陷服务器，向其它服务器做攻击横向移动的程序，往往包括漏洞利用、密码爆破等行为。
恶意进程（云查杀）	挖矿程序	检测模型发现您的服务器上运行了挖矿程序，挖矿程序是一类侵占服务器计算资源，进行虚拟货币挖掘的程序，服务器往往可见CPU占用飙高，以及其它相关的恶意程序。
恶意进程（云查杀）	自变异木马	检测模型发现您的服务器上运行了自变异，自变异木马是具备自变异功能的木马程序，它会改变自身hash或者将自身大量复制到不同的路径下，并后台运行起来，以躲避清理。
恶意进程（云查杀）	DDoS木马	检测模型发现您的服务器上运行了DDoS木马，DDoS木马是用于从被攻陷服务器上接受指令，对黑客指定目标发起DDoS攻击的恶意程序。
恶意进程（云查杀）	Rootkit	检测模型发现您的服务器上存在Rootkit，Rootkit是一类植入到系统底层、用于隐藏自身或其它恶意程序痕迹的恶意模块。
网站后门	发现后门（Webshell）文件	检测模型在您的服务器上发现了一个可疑的Webshell文件，可能是攻击者成功入侵网站后为维持权限植入的后门文件。

适用Fileless攻击手法的告警

告警类型	具体检测项	检测原理说明
持久化后门	疑似后门	检测模型发现您的服务器上存在wmi或bitsadmin后门，可能是攻击者在入侵后用来维持对您的服务器权限。
持久化后门	异常代码驻留内存	检测模型发现您的服务器上某进程的内存空间中疑似存在恶意指令，该进程可能为攻击者在入侵后遗留的恶意软件，或者是向正常的进程注入了恶意的代码。

告警类型	具体检测项	检测原理说明
持久化后门	异常注册表项	检测模型发现您服务器上的某个注册表配置项可疑，恶意软件常常会修改某些关键注册表配置来持久化运行或干扰正常的安全防护。
持久化后门	CobaltStrike远控木马	检测模型发现您服务器上某个进程内存空间内存在CobaltStrike远控木马的恶意代码，可能该进程即为恶意程序或正常程序被注入了恶意指令。
恶意脚本	恶意脚本代码执行	检测模型发现您的服务器上正在执行恶意的Bash、Powershell、Python等脚本代码。
进程异常行为	服务应用执行可疑命令	检测模型根据您服务器上的进程历史行为自动分析，发现该服务进程启动的命令较为可疑，可能是攻击者在利用该服务的RCE漏洞成功执行了命令。
进程异常行为	可疑注册表配置项修改	检测模型发现您服务器上有进程尝试修改注册表配置，可能是攻击者在获取服务器权限后写入后门代码或修改敏感配置。
进程异常行为	Java应用执行异常指令	检测模型发现您的服务器上的Java进程启动了下载恶意程序、添加后门等高危行为，很可能是因为您使用了存在漏洞的Web框架或者中间件导致。
进程异常行为	Linux计划任务执行异常指令	检测模型发现您服务器的计划任务执行了异常命令，可能是攻击者在入侵服务器后，为维持权限，将恶意命令写入到计划任务中。
进程异常行为	Python应用执行异常指令	检测模型发现您服务器上的Python应用执行异常命令，可能是由于您服务器上通过Python搭建的Web应用存在RCE漏洞并被利用成功。
进程异常行为	Tomcat执行异常指令	检测模型发现您的Tomcat容器执行了异常命令，可能是攻击者通过Tomcat容器中Java应用存在的RCE漏洞或Webshell执行了恶意命令。

1.3. 查看和处理告警事件

云安全中心检测出安全告警事件后，会在控制台的安全告警处理页面展示相关告警信息。您可以在安全告警处理页面查看和处理已检测出的告警事件。本文介绍如何查看和处理告警事件。

背景信息

如果告警事件未被处理，会展示在**安全告警处理**页面的**未处理**列表中。告警事件处理完成后，将从**未处理**状态转化为**已处理**。

> **说明** 云安全中心在**安全告警处理**页面为您一直保留**未处理**和**已处理**告警记录。由于待处理告警事件可能会对您的资产安全造成严重威胁，云安全中心默认为您展示**待处理告警**记录。

查看告警事件

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. 在安全告警事件列表中，查看或搜索所有检测到的入侵和威胁告警及其详细信息。

   您可以进行以下操作：

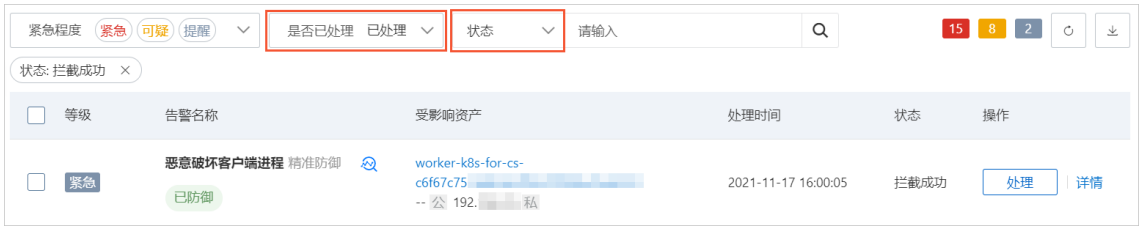
- 搜索目标告警事件
  - 可以使用告警事件列表上方提供的**紧急程度**、**是否已处理**、**过滤器**等组件筛选或搜索告警事件。
  - 您还可以使用告警事件列表左侧的**告警类型**或**ATT&CK攻击阶段**菜单筛选告警事件。
- 查看告警事件
  单击告警事件的名称，打开该告警事件的详情页面，可以查看其详情和该告警的自动化关联信息，帮助您更便捷和全面地分析威胁事件、快速定位攻击来源地址和分析攻击行为的路径。有关告警自动化关联的具体内容，请参见查看告警自动化关联分析。有关告警溯源的具体内容，请参见攻击溯源。
  将鼠标移动到告警名称右侧的标签上，查看该告警的攻击溯源或关联异常等信息。

以下是告警名称右侧标签的说明：

标签	功能	描述
	攻击溯源	云安全中心攻击溯源功能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，形成攻击者入侵的链路图，帮助您在最短时间内定位入侵原因和制定应急决策。您可以单击 图标跳转至**溯源**页面。更多信息，请参见攻击溯源。
	事件调查	事件调查是入侵调查的工作平台，可视化调查黑客攻击过程，定位攻击源IP，分析入侵原因，助力您快速掌握入侵影响面，进行安全加固。您可以单击 图标跳转至**事件调查**页面。
	关联异常	将鼠标移动到该图标上，您可以查看当前告警关联异常的数量。
	重保护模式	重保护模式是云安全中心Agent的一种防护模式，该模式适用于重大活动的安全保障，会对任何可疑的入侵行为和潜在的威胁进行告警。出现该图标说明对于该告警影响的资产，Agent防护模式为重保护模式。Agent防护模式的更多信息，请参见主动防御。
攻击入口	攻击阶段	攻击入口、载荷投递、权限提升、逃避检测、权限维持、横向移动、远程控制、数据泄露、痕迹清理、影响破坏是病毒攻击的阶段。您可以通过攻击阶段图标获当前服务器受到病毒攻击的阶段，帮助您快速掌握资产的安全状态。
已防御	已防御	表示病毒文件的恶意进程已被云安全中心实时拦截，当前已无法对您的业务造成危害，建议您尽快隔离该病毒文件。

- 查看云安全中心为您自动处理的告警。

将搜索条件**是否已处理**设置为**已处理**、**状态**选择为**拦截成功**后，查看云安全中心为您自动隔离的常见网络病毒。



处理告警事件

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. 在**安全告警处理**页面，定位到目标告警事件，单击**操作**列的**处理**。

> **说明** 如果告警事件包含多个关联异常，单击**处理**，会打开该告警事件的详情页面，您可对不同的异常事件分别进行处理。更多信息，请参见查看告警自动化关联分析。

4. 选择当前告警事件的处理方式。

   告警事件处理方式说明如下：

处理方式	说明
病毒查杀	选择**病毒查杀**，您可以选择关闭该病毒的进程并隔离源文件，病毒样本被隔离后，将无法对业务产生危害。 如果您确认该告警信息有效，可以手动选择以下选项进行处理： ○ **结束该进程的运行**：直接结束该进程的运行。 ○ **隔离该进程的源文件**：将病毒文件加入文件隔离箱，被隔离的文件将无法对服务器造成安全威胁。 **注意** 被成功隔离的文件在30天内可执行一键恢复，恢复的文件将重新回到安全告警列表中，由云安全中心继续对该文件进行监测。文件隔离30天后云安全中心会自动清除该文件。
加白名单	如果告警为误报，您可以将本次告警加入白名单，并设置加入白名单的规则。例如，选择加白名单后，您设置了*登录源IP包含10.XX.XX.198*的加白规则，则该告警状态将变为**已处理**，后续云安全中心不会再对来源于*10.XX.XX.198*的登录进行告警。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** 以上示例中的*10.XX.XX.198*为IP地址脱敏的显示效果，实际配置时请使用真实的IP地址。 加白名单操作仅对当前告警和您设置的白名单规则进行加白。执行加入白名单操作后，针对您加入白名单的事件和设置的白名单规则，云安全中心都不会再产生对应的安全告警。云安全中心支持加入白名单的对象详情，请参见安全告警可以将哪些对象加入白名单。 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。

处理方式	说明
忽略	选择**忽略**，该告警状态将更新为已忽略，当相同告警再次发生时，云安全中心将再次告警。 **说明** 如果您已确认一个或多个告警事件需要忽略或为误报，可在**安全告警处理**页面的告警事件列表中，选中一个或多个告警事件，单击列表下方的**忽略本次**或**加白名单**进行处理。
深度查杀	**深度查杀**由云安全中心安全专家团队经过对该持久化、顽固型病毒进行深度分析、测试后，推出的专项查杀能力，该操作可能存在风险，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。该处理方式还提供创建快照功能，您还可以通过创建快照备份数据，以便深度查杀清除有用数据时，可以通过快照恢复被清除数据。
关闭恶意行为防御	选择**关闭恶意行为防御**，云安全中心将停止该告警文件或告警程序所在的容器，但不会主动删除容器。在Kubernetes环境下，仅停止告警事件所在Container而不是Pod。 **注意** 选择该处理方式前，请确认该容器的停止不会影响您的正常业务，请谨慎使用该处理方式。
隔离	选择**隔离**，网站后门文件将被隔离到文件隔离箱，将无法对业务产生危害。 **注意** 被成功隔离的文件在30天内可执行一键恢复，恢复的文件将重新回到安全告警列表中，由云安全中心继续对该文件进行监测。文件隔离30天后云安全中心会自动清除该文件。
阻断	选择**阻断**，云安全中心将生成安全组防御规则，您需要配置**规则有效期**，拦截该恶意IP的访问。
结束进程	直接结束该进程的运行。
问题排查	选择**问题排查**，云安全中心的客户端问题诊断程序将在本机采集与客户端相关的网络、进程、日志等数据上报云安全中心进行分析，检查期间会占用一定的CPU和内存。 问题排查支持以下两种模式： ○ **常规模式** 常规模式将收集客户端相关日志数据上报至云安全中心进行分析。 ○ **增强模式** 增强模式将采集与客户端相关的网络、进程、日志等数据上报云安全中心进行分析。
我已手工处理	您已处理了导致该告警事件的风险问题。
同时处理相同告警	对多个告警事件进行批量处理。批量处理告警事件前，请详细了解告警事件的信息。

5. 单击**立即处理**。
   告警事件处理完成后，告警事件将从**未处理**状态转化为**已处理**状态。

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，建议您定期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、盗取或破坏业务数据。

1.4. 归档告警数据

云安全中心支持归档30天前的告警数据。您可以对历史告警数据进行归档并下载。定期归档历史告警数据，便于您查看和管理最近的告警数据。本文介绍如何使用归档告警数据功能。

背景信息

您执行归档数据操作后，云安全中心会自动归档30天前的所有历史告警数据（包括已处理和未处理的告警），并提供下载归档数据的功能。已归档的数据将无法在云安全中心控制台上进行查看。如果需要查看已归档的数据时，您要先将归档数据下载到本地。如果您从未执行过归档数据，您可以在云安全中心控制台上查看所有的告警数据。

> **说明** 如果您的账号30天前没有告警数据，云安全中心会为您在**安全告警处理**页面**归档数据**区域生成空的归档数据（文件名称*suspiciousExport_执行归档操作的日期_时间戳.zip*）。

您24小时内只能执行一次归档数据操作。归档数据下载次数不受限制。

版本限制

云安全中心所有版本用户都可使用该功能。各版本支持的功能详情，请参见功能特性。

操作步骤

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. 在**安全告警处理**页面右上角，单击**归档数据**。

   以下是归档数据的相关说明：

   - 第一次单击**归档数据**：云安全中心会自动为您归档当前时间30天前的历史告警数据并生成下载链接。
   - 不是第一次单击**归档数据**：云安全中心会自动为您归档上一次归档数据截止日期到当前时间30天前之间的告警数据并生成下载链接。

   例如，您在2020年08月13日第一次单击**归档数据**，云安全中心会为您归档2020年07月14日（2020年08月13日30天前）之前的所有告警数据（包含2020年07月14日），并生成名称为*suspiciousExport_20200813_1597282822.zip*的归档文件。您在2020年08月15日再次单击**归档数据**，云安全中心会为您归档2020年07月15日至2020年07月16日的告警数据，并生成名称为*suspiciousExport_20200815_1597455622.zip*的归档文件。

> **说明** 云安全中心24小时内最多为您归档一次告警数据。即在24小时内第一次单击**归档数据**时为您归档告警数据并生成归档文件。再次单击**归档数据**时，不会触发归档操作，仅为您打开**归档数据**对话框，您可以查看已归档的数据。

4. 在**归档数据**对话框，查看已归档的数据。

5. 单击已归档数据**下载链接**列下的**下载**，将归档数据下载到本地。

   归档数据的文件格式为XLSX。归档数据下载时间依赖于网络带宽和文件大小，一般需要2~5分钟。

   下载完成后，您可以在归档数据文件中，查看历史告警的告警ID、告警名称、告警详情、告警等级、状态、影响资产、影响资产备注名称、影响概况和告警发生时间。

> **说明** 告警状态为**已经过期**说明在告警发生30天内，您未对该告警做任何处理。建议您及时对云安全中心检测到的安全告警事件进行处理。

6. 单击**确定**。

1.5. 查看告警自动化关联分析

云安全中心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。

前提条件

- 仅支持企业版和旗舰版用户使用告警自动化关联分析功能，免费版、防病毒版和高级版用户需要升级到企业版或旗舰版才能使用该功能。
- 已开启自动化告警关联分析功能。具体操作，请参见自动化告警关联分析。

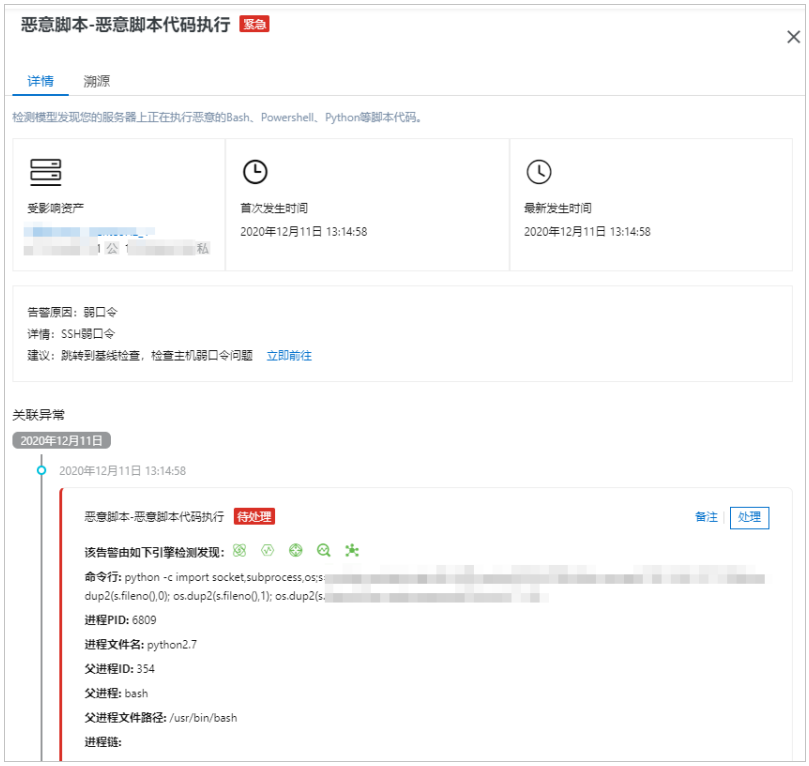
背景信息

- 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。
- 告警自动化关联分析聚合后的告警以 图标标识。

操作步骤

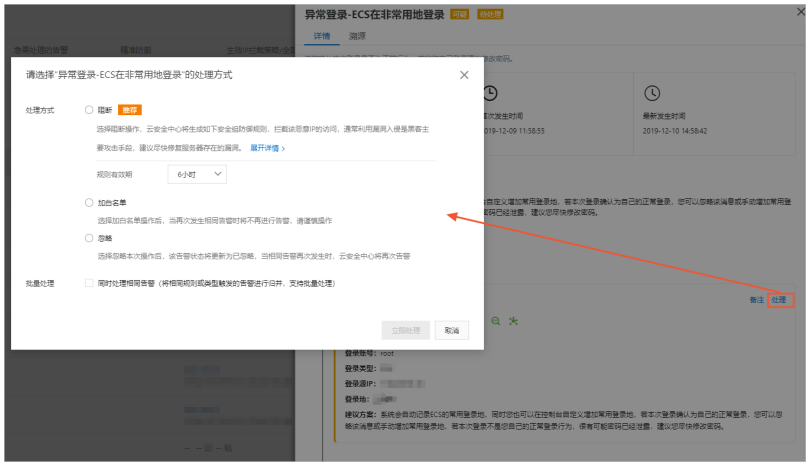
1. 登录云安全中心控制台。

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，单击目标打开告警事件详情页面。
4. 在告警事件详情页面，查看和处理该告警事件的详细信息、关联的异常事件和对告警的异常事件进行处理。
   - 查看告警详细信息
     您可查看该告警事件的**受影响资产**、**首次发生时间**、**最新发生时间**、**告警原因**和**关联异常**。



   - 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。
   - 查看告警原因
     查看告警出现的原因和处理建议，您可以单击**立即前往**跳转至**漏洞修复**、**基线检查**等页面，查看并处理漏洞、基线检查风险项信息。
   - 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和建议方案。您可以执行以下操作处理异常：

- 单击各关联异常区域右侧的**处理**，选择处理方式，处理不同异常事件。
  告警事件处理方式选择的更多信息，请参见查看和处理告警事件。



- 单击各关联异常区域右侧的**备注**，可为该关联异常事件添加备注信息。

单击备注信息右侧的 × 图标，即可删除备注信息。

- 查看告警**溯源**
  单击**溯源**页签，打开该告警事件的溯源页面。溯源的更多信息，请参见攻击溯源。

1.6. 攻击溯源

云安全中心支持自动化攻击溯源，可对攻击事件进行自动化溯源并提供原始数据预览。

背景信息

云安全中心攻击溯源功能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，形成攻击者入侵的链路图，帮助您在最短时间内定位入侵原因和制定应急决策。攻击溯源适用于云环境下的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。

云安全中心会在检测到威胁后10分钟，生成自动化攻击溯源的链路。建议您在告警发生10分钟后，再查看该告警相关的攻击溯源信息。

目前，云安全中心攻击溯源已支持所有安全告警类型。详细了解安全告警类型，请参见安全告警类型列表。

仅企业版支持自动化攻击溯源，基础版、基础杀毒版、高级版用户需升级到企业版才能使用该功能。

> **说明** 安全告警触发后超过3个月，该告警的自动化攻击溯源信息将被自动清除。请您及时查看告警事件的攻击溯源信息。

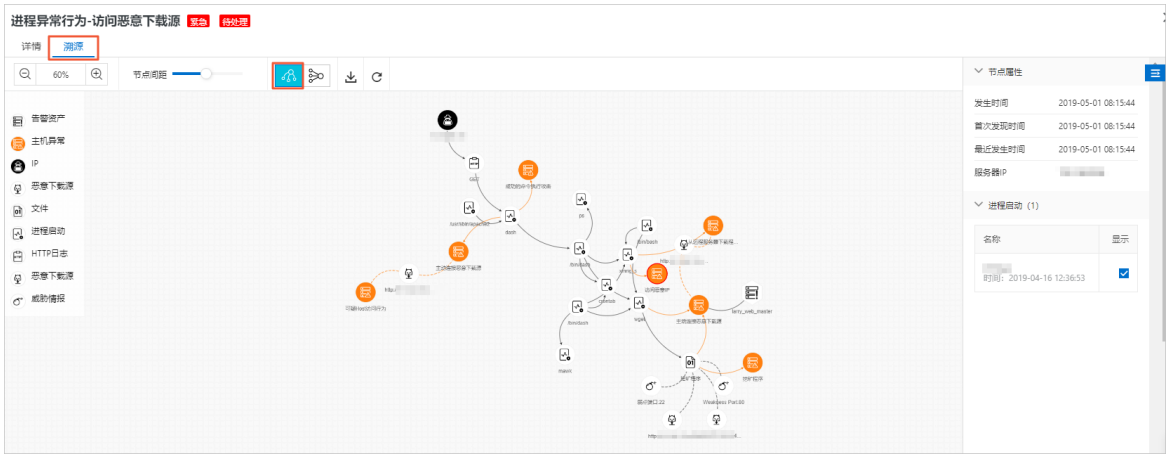
限制说明

- 自动化攻击溯源是由安全大数据关联计算得出，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。
- 对于恶意进程（云查杀）这类告警，由于云安全中心会对此类攻击执行自动处理（告警状态为**已防御**），因此默认不提供恶意进程（云查杀）的攻击溯源信息。

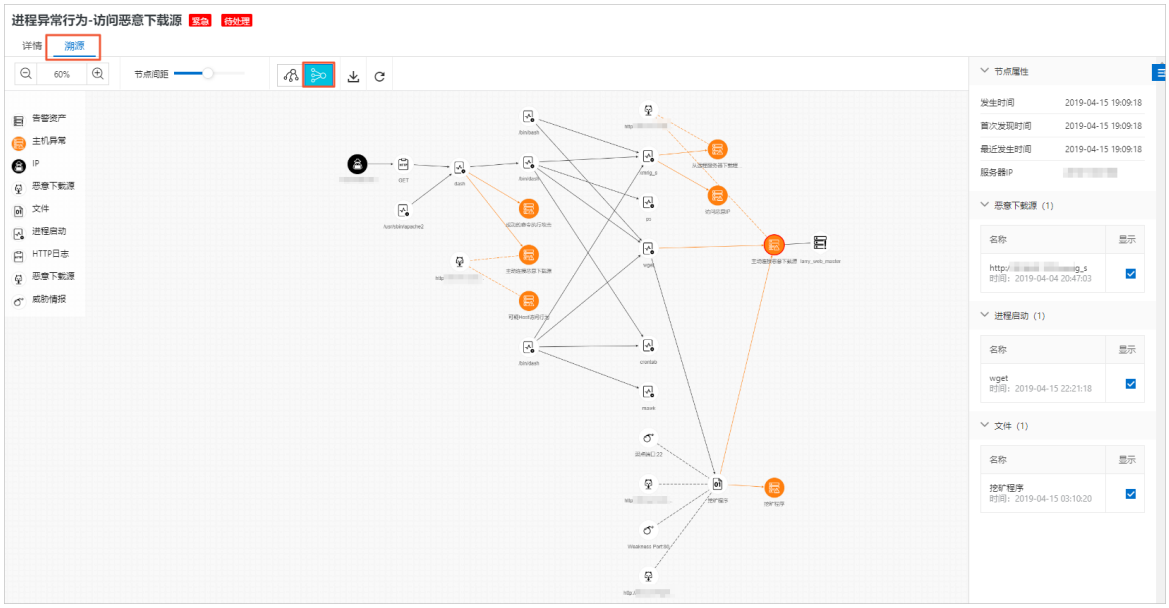
操作步骤

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，并单击溯源 图标。

   单击**溯源**，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。

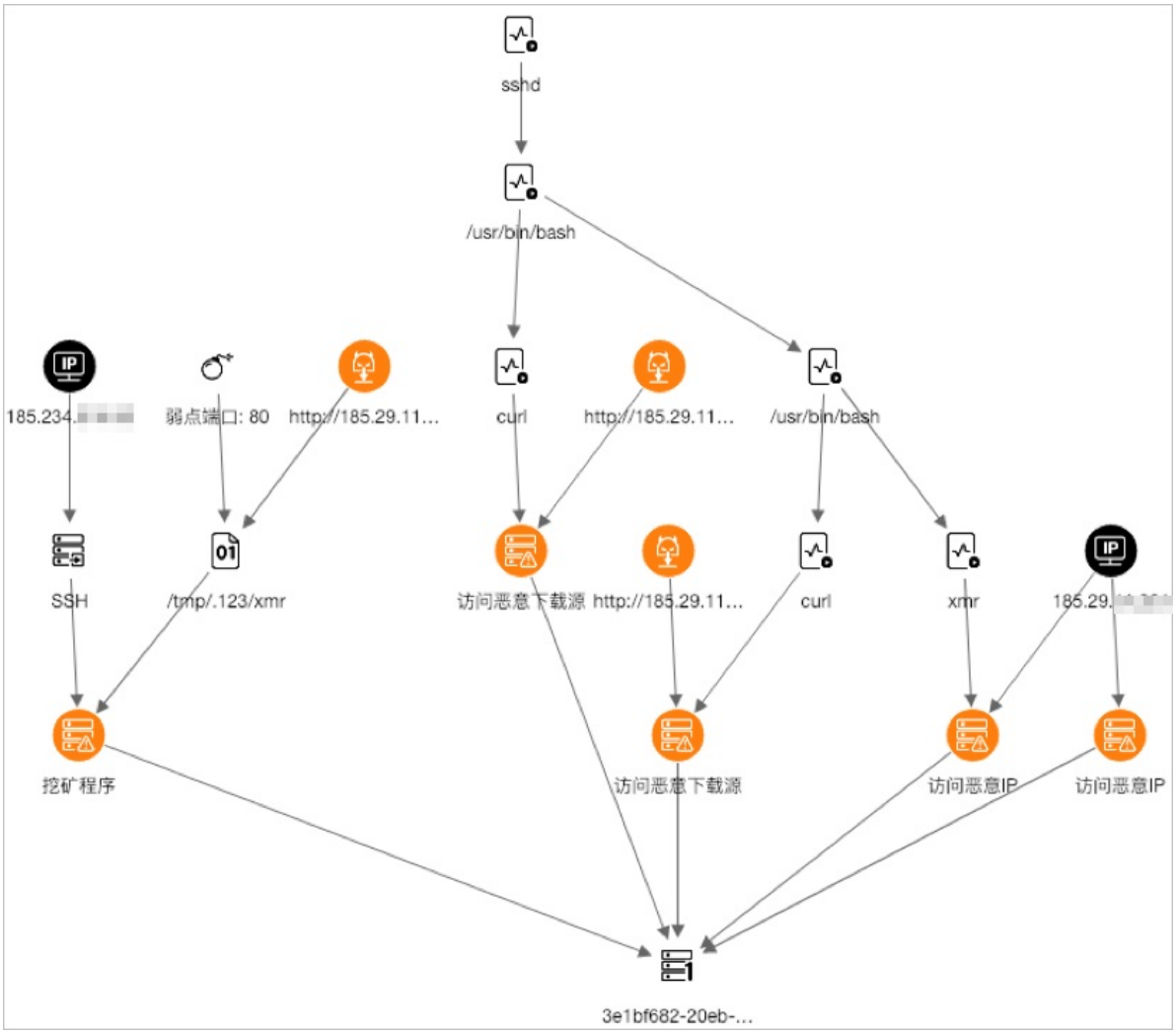


在溯源可视图中，您可以查看该攻击溯源事件整个链路中各个节点的信息。单击各个节点展示该节点的**节点属性**页面，您可以查看该节点的相关信息。



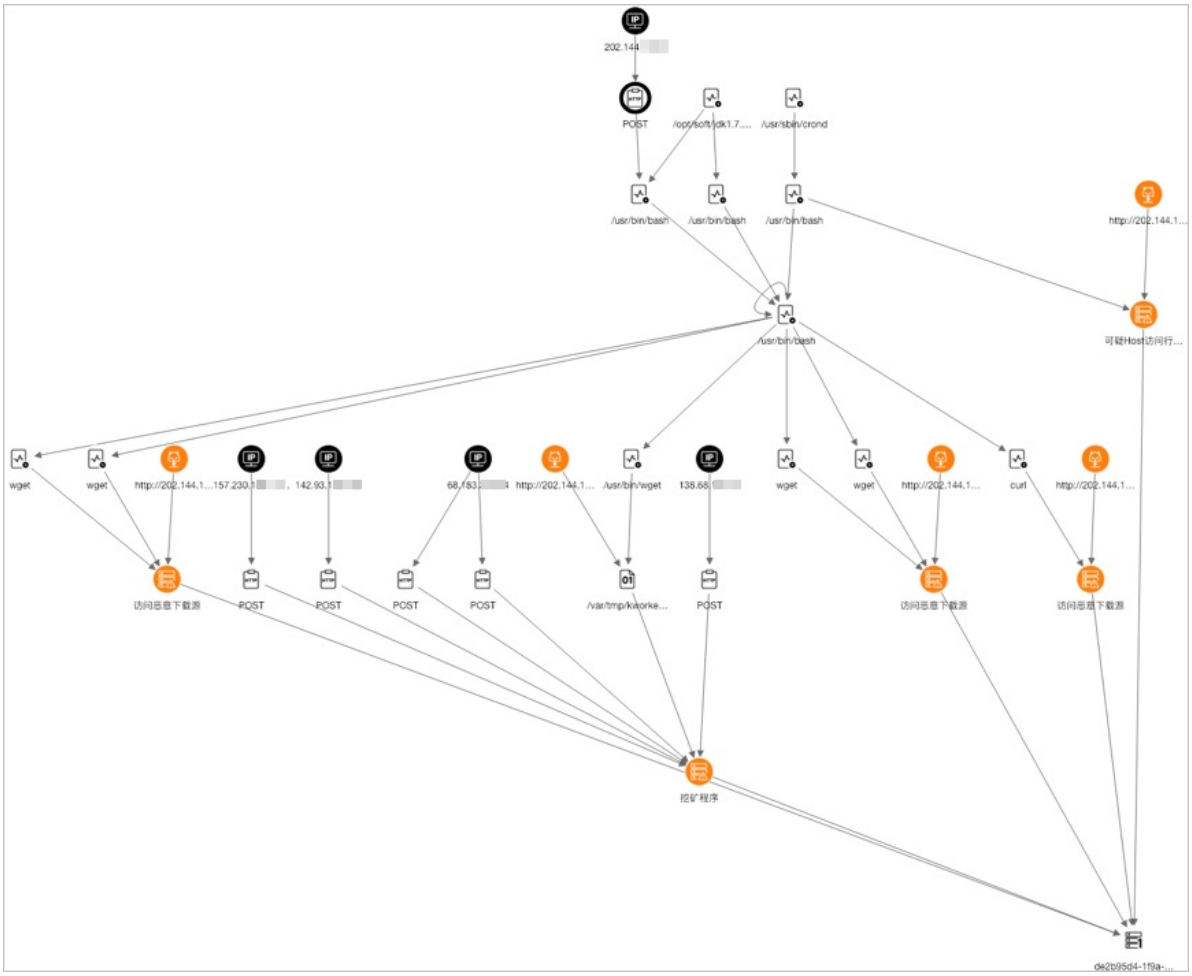
告警溯源案例

- 蠕虫传播事件
  下图描述了蠕虫传播源（例如：`185.234.*.*`）通过SSH暴力破解成功登录到服务器，并通过bash执行curl指令从远端下载挖矿程序并在服务器中执行该挖矿程序。

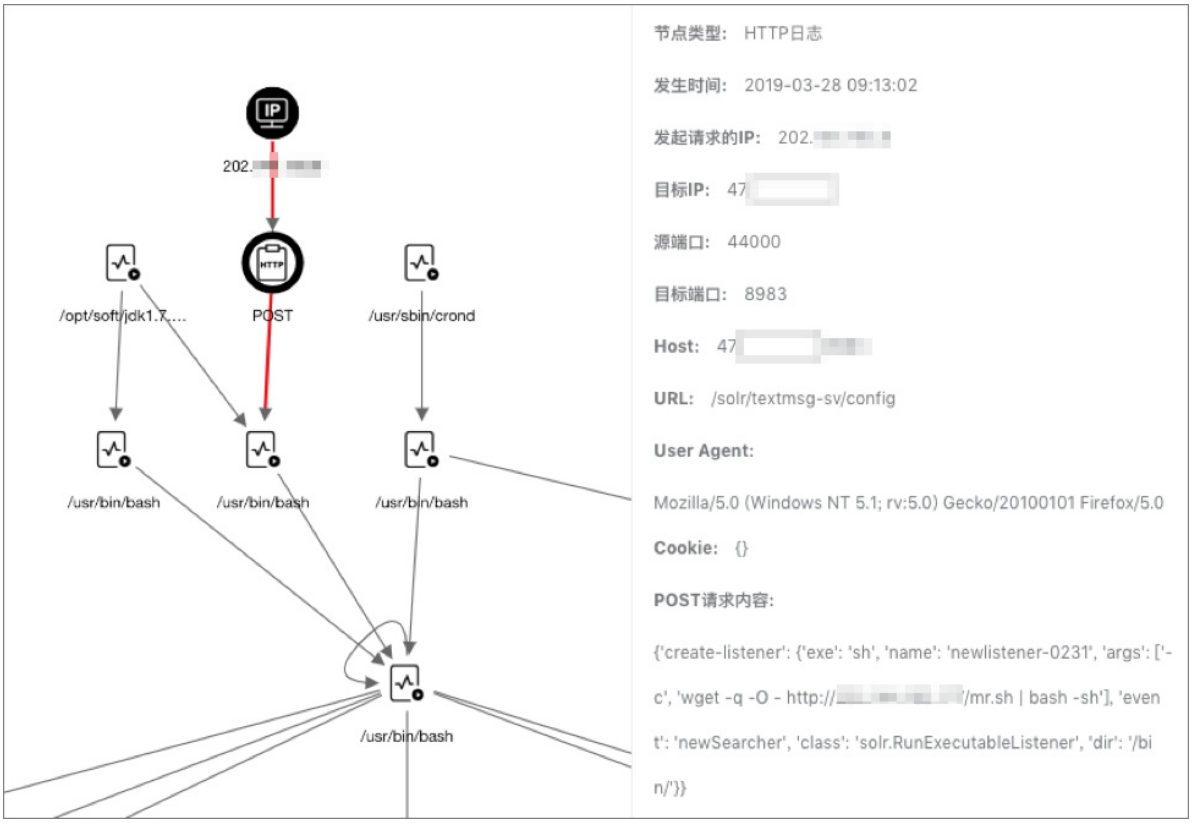

sshd
/usr/bin/bash
185.234.
弱点端口: 80
http://185.29.11...
curl
http://185.29.11...
/usr/bin/bash
SSH
/tmp/.123/xmr
访问恶意下载源
http://185.29.11...
curl
xmr
185.29.
挖矿程序
访问恶意下载源
访问恶意IP
访问恶意IP
3e1bf682-20eb-...

- Web漏洞入侵事件

下图描述了黑客通过服务器（例如：`202.144.*.*`）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，您可以针对此漏洞快速进行修复。



1.7. 设置IP拦截策略

云安全中心支持通过设置IP拦截策略达到防止暴力破解的目的。本文介绍如何启用或禁用IP拦截策略，以及如何新建、编辑自定义IP拦截策略。

背景信息

云安全中心支持系统内置和用户自定义两种IP拦截策略，具体介绍如下：

- 系统规则：即您在**安全告警设置 > 防暴力破解**页面添加了防御规则后，该规则触发了IP拦截，就会自动生成IP拦截策略。系统规则创建后默认为**已启用**状态。防暴力破解防御规则中设置的指定时长内登录失败次数决定了系统规则的产生条件（即触发IP拦截的条件），禁止登录时长决定了系统规则的生效时长。详细内容，请参见配置防暴力破解规则。

- 自定义规则：即您在**IP规则库 > 自定义规则**页面添加的拦截策略。您可以根据实际业务的需要，自定义IP拦截规则，拦截恶意IP对云上资产的访问。自定义规则可以设置拦截的IP地址以及该恶意IP访问的服务器等。自定义规则创建后默认为**已禁用**状态，需要手动开启。详细内容，请参见启用或禁用IP拦截策略。

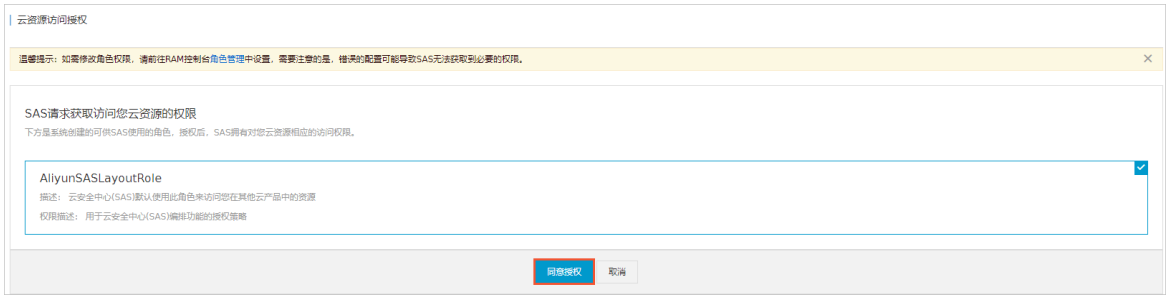
新建自定义IP拦截策略

如果您发现防暴力破解没有拦截某些恶意IP对您服务器的访问，您可以创建自定义IP拦截策略，拦截该IP的访问。

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. 在**安全告警处理**统计数字区域，单击**生效IP拦截策略/全部策略**下的数字，展开**IP规则策略库**面板。

4. 单击**自定义规则**页签。
5. （可选）首次新建IP拦截策略需要授权，将鼠标移动到**新建策略**上并单击**立即授权**。

6. （可选）在**云资源访问授权**页面，单击**同意授权**并返回**IP规则库 > 自定义规则**页签。



7. 在**自定义规则**页签下，单击**新建策略**。
8. 在**新建IP拦截策略**面板，配置相关参数。

配置项说明如下：

配置项	说明
拦截对象	输入需要拦截的IP地址。
全部资产	选择新建IP拦截策略应用的服务器。支持同时选择多台服务器。您可以在搜索框中输入服务器名称或服务器IP地址搜索指定服务器。 **说明** 仅支持选择阿里云ECS服务器。

配置项	说明
规则方向	设置拦截流量的方向，可选择**入方向**或**出方向**。
所属安全组	该IP拦截策略关联的安全组，默认为**云安全中心拦截组**。该策略启用时会在此安全组中自动创建相应规则，该策略过期或禁用后会自动删除该规则。
过期时间	设置该策略的有效时间。策略过期后，该策略状态将变为**已禁用**。

9. 单击**确定**。

   新建IP拦截策略创建成功后默认为**已禁用**状态，如果您需要该策略立即生效，您需要手动启用该策略。详细信息，请参见启用或禁用IP拦截策略。

启用或禁用IP拦截策略

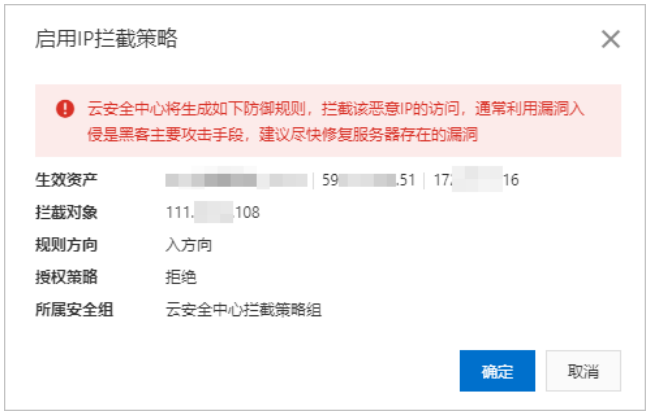
根据实际场景需要，您可对存在暴力破解风险的IP启用相应的防暴力破解规则。如果确认拦截策略拦截了正常流量，您可以禁用该策略。禁用策略后，云安全中心不会再拦截该策略中拦截对象的访问，该IP将可以正常访问您的服务器。

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. 在**安全告警处理**统计数字区域，单击**生效IP拦截策略/全部策略**下的数字，展开**IP规则策略库**面板。

4. 在**IP规则策略库**面板上，定位到需要设置的IP拦截策略，启用或禁用该IP拦截策略。

   如果您需要启用或禁用自定义IP拦截策略，请单击**自定义规则**切换到自定义规则页签。

   - **启用**：打开**策略状态**开关，在**启用IP拦截策略**对话框中单击**确定**。启用后该IP拦截策略会生效并且状态将变更为**已启用**，云安全中心会根据该IP拦截策略定义的拦截规则拦截恶意流量。



> **说明** 如果您启用了已到期的自定义IP拦截策略，该策略的有效期将变更为启用时间后两小时。如果您需要修改该策略的有效期，建议您编辑该策略后再执行启用操作。更多信息请参见编辑IP拦截策略。

- **禁用**：关闭**策略状态**开关，在**禁用IP拦截策略**对话框中单击**确定**。禁用后该IP拦截策略将失效并且状态将变更为**已禁用**，云安全中心不会再拦截策略中设置的IP地址对指定服务器的访问。

编辑IP拦截策略

仅支持编辑自定义IP拦截策略，不支持编辑内置的IP拦截策略。

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. 在**安全告警处理**统计数字区域，单击**生效IP拦截策略/全部策略**下的数字，展开**IP规则策略库**面板。

4. 单击**自定义规则**页签。
5. 定位到需要编辑的IP拦截策略并单击其**操作**列的**编辑**。

> **注意** 仅支持编辑已禁用状态的IP拦截策略。如果需要编辑已启用状态的IP拦截策略，您可以禁用该IP拦截策略后，再编辑该策略。

6. 在**编辑IP拦截策略**面板上，修改该拦截策略的生效资产和过期时间。

7. 单击**确定**。

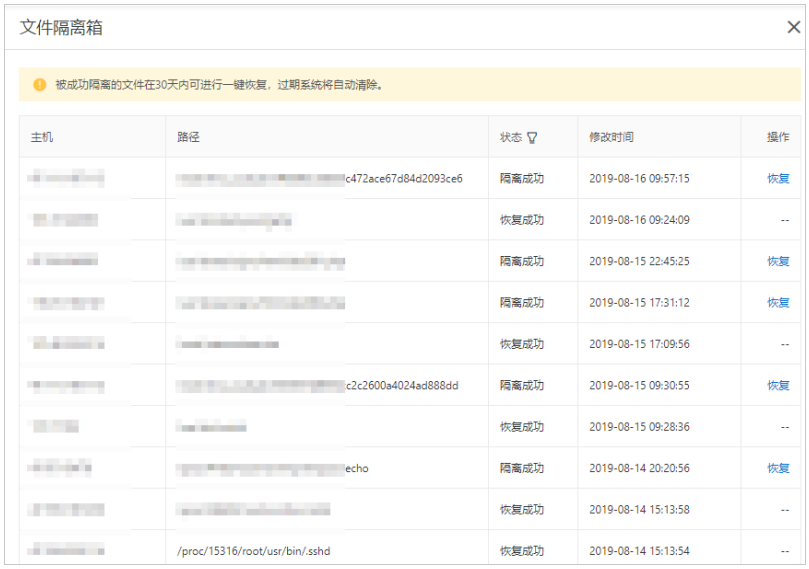
   云安全中心将按照您修改后的生效资产和过期时间执行IP拦截任务。

1.8. 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，被成功隔离的文件会添加到安全告警处理页面的文件隔离箱中。被成功隔离的文件可在30天内进行一键恢复，且隔离30天后系统将自动清除被隔离文件。本文介绍了如何查看隔离文件和解除文件隔离。

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**页面右上角，单击**文件隔离箱**。
4. 在**文件隔离箱**面板，查看被隔离的文件或恢复被隔离的文件。
   - 在文件隔离箱列表中可以查看被隔离文件的主机地址、路径、状态和修改时间信息。



- 单击待恢复文件操作列的**恢复**，并在**提示**对话框中单击**确定**，可以将指定的被隔离文件从文件隔离箱中移除。恢复的文件将重新显示在安全告警列表中。

> **注意** 恢复操作仅支持在文件被隔离30天内进行。云安全中心将自动清除被隔离超过30天的文件。

相关文档

是否可以自动隔离WebShell文件？

1.9. 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。本文介绍了导出告警事件列表的具体操作。

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**页面右侧 图标，导出安全告警事件列表。

报表导出完成后，**安全告警处理**页面右上角会提示**导出完成**。

4. 在**安全告警处理**页面右上角**导出完成**对话框中，单击**下载**。
   安全告警事件文件会下载到本地。

1.10. 安全告警设置

安全告警设置功能支持手动维护服务器的常用登录地、常用登录IP、常用登录时间、常用登录账号、防暴力破解、Web目录定义以及加入白名单规则，可帮助您建立更精细化的威胁防护规则并对这些规则进行统一的管理，从而及时发现资产中的安全威胁，实时掌握资产的安全态势。

背景信息

在**安全告警设置**面板为服务器配置常用登录地、常用登录IP、常用登录时间、常用登录账号、防暴力破解、Web目录定义以及加入白名单规则后，触发规则产生的告警事件会展示在**安全告警处理**页面的告警列表中。为了您的资产安全，建议您及时处理相关的告警事件。具体操作，请参见查看和处理告警事件。

版本限制说明

云安全中心各版本对安全告警设置面板上的功能的支持情况如下。

> **说明** 下表使用到的标识的说明如下：
> - ×：表示该版本不支持使用此功能。
> - √：表示该版本支持使用此功能。

功能名称	免费版	防病毒版	高级版	企业版	旗舰版
常用登录地	√	√	√	√	√
常用登录IP	×	×	√	√	√
常用登录时间	×	×	√	√	√
常用登录账号	×	×	√	√	√
防暴力破解	×	×	√	√	√
Web目录定义	√	√	√	√	√
告警处置规则	√	√	√	√	√

管理常用登录地、IP、时间及账号

您可以在**安全告警设置**面板对**常用登录地**、**常用登录IP**、**常用登录时间**、**常用登录账号**进行配置。配置完成后，云安全中心会对服务器的非指定的登录情形告警。

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. 在**安全告警处理**页面，单击右上角**安全告警设置**。
4. 在**安全告警设置**面板，管理**常用登录地**、**常用登录IP**、**常用登录时间**、**常用登录账号**。

   常用登录地、**常用登录IP**、**常用登录时间**、**常用登录账号**配置的操作步骤基本相同。下文以管理**常用登录地**为例，为您介绍这些功能配置的操作步骤，其他几种规则的配置本文不再赘述。

   i. 在**常用登录地**页签，单击**常用登录地**区域右侧的**管理**。

ii. 在**常用登录地**面板，您可以根据业务需要选择一个地区作为常用登录地，然后选择该规则生效的服务器，单击**确定**，完成添加。

云安全中心支持编辑和删除已成功添加的常用登录地。

- 单击目标常用登录地右侧的**编辑**，修改该登录地的生效服务器。
- 单击目标常用登录地右侧的**删除**，删除该常用登录地配置。

配置防暴力破解规则

云安全中心提供防暴力破解功能，支持配置自定义暴力破解防御规则。配置防暴力破解规则后，登录服务器时，在某个时间范围内登录服务器的失败次数超过限定次数将被禁止登录一段时间。防暴力破解功能，可有效防止您服务器账号的密码被暴力破解。

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. 在**安全告警处理**页面，单击右上角**安全告警设置**，并单击**防暴力破解**页签。
4. 如果您是首次使用防暴力破解功能，您需要进行**防暴力破解**授权操作。
   i. 将鼠标悬停在**防暴力破解**区域右侧的置灰**管理**上，在弹出的提示框中单击**去授权**。
   ii. 单击**同意授权**。
5. 单击**防暴力破解**区域右侧的**管理**。

   云安全中心的免费版、防病毒版用户需要升级到高级版以上的版本才能使用此功能。
6. 在**防暴力破解**面板，配置防暴力破解规则。

   云安全中心提供默认防暴力破解规则：同一服务器10分钟内登录失败次数超过80次，禁止登录6小时。您可以选择对应服务器，直接使用该默认防御规则。您也可以参考以下表格中的配置说明自定义防御规则。

配置项	说明
防御规则名称	设置防暴力破解自定义规则名称。
防御规则	设置防暴力破解的规则。即登录服务器时，在某个时间范围内登录服务器的失败次数超过限定次数将被禁止登录一段时间。例如：1分钟内登录失败次数超过3次，禁止登录30分钟。
设置为默认策略	设置该防御规则是否为默认策略。设置为默认策略后，未添加防御规则的服务器将默认应用该规则。 **说明** 选中**设置为默认策略**后，无论您是否在**请选择对应的服务器**中选择了服务器，当前策略都会对所有未添加防御规则的服务器生效。
请选择对应的服务器	设置防御规则生效的服务器。支持直接选择云安全中心防护的服务器，或根据服务器名称和IP筛选指定服务器。

7. 单击**确定**。

> **注意** 每台服务器仅支持配置一个防暴力破解规则。
>
> - 如果该规则中设置生效的服务器未配置其他任何防御规则，该防暴力破解规则添加成功。
> - 如果该规则中设置生效的服务器已配置了其他防暴力破解规则，且您确定要更换为当前配置的规则，请在**确认防御规则变更**页面，单击**确认**。
> - 如果原防暴力破解规则的生效服务器配置了新防御规则，则原防暴力破解规则的生效服务器数量会相应减少。

您在**安全告警设置**面板的**防暴力破解**页签添加了防御规则后，该规则触发了IP拦截，就会自动生成IP拦截策略。IP拦截策略的更多信息，请参见设置IP拦截策略。

管理自定义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。当黑客通过已知网站后门进行异常连接行为时，云安全中心会进行主动拦截，并会生成告警事件展示在**安全告警处理**页面的告警列表中。

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. 在**安全告警处理**页面，单击右上角**安全告警设置**，并单击**Web目录定义**页签。
4. 单击**Web目录定义**区域右侧的**管理**。
5. 输入常用的Web路径，然后选择生效服务器，该路径所对应的Web目录会被添加到检测列表中。

   > **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。

6. 单击**确定**，完成添加。

管理告警处置规则

如果您在处理告警事件时选择处理方式为加白名单，对应的处理方式会展示在**安全告警设置**面板的**告警处置规则**列表中。您可以在**安全告警设置**面板，编辑或删除该规则。

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. 在**安全告警处理**页面，单击右上角**安全告警设置**。
4. 在**安全告警设置**面板，单击**告警处置规则**页签。
5. 在**告警处置规则**区域，您可以对目标规则进行**编辑**和**删除**。
   - **编辑告警处置规则**
     a. 定位到您要编辑的规则，单击**操作**列的**编辑**。
     b. 在**编辑规则**面板，修改该告警处置规则生效的服务器。
     c. 单击**确定**，完成修改。
   - **删除告警处置规则**
     a. 定位到您要删除的规则，单击**操作**列的**删除**。
     b. 单击**确定**，完成删除。

1.11. 病毒云查杀

云盾云安全中心病毒查杀（以下简称“云查杀”）集成了中国及中国以外地域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，实时服务百万云上服务器。

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。
- **集成中国及中国以外地域主流病毒查杀引擎**：云查杀集成中国及中国以外地域多款优秀的杀毒引擎，可对病毒库进行实时更新。
- **威胁情报检测**：基于云盾威胁情报数据，配合服务器异常行为检测模型，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，同时支持用户在云盾控制台中对云查杀结果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服务器信息或者控制权、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服务器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，为您提供全面、实时的病毒检测服务。
- **轻量**：Agent客户端仅占用1%的CPU、50 MB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服务器进行统一管理，实时查看所有服务器的安全状态。

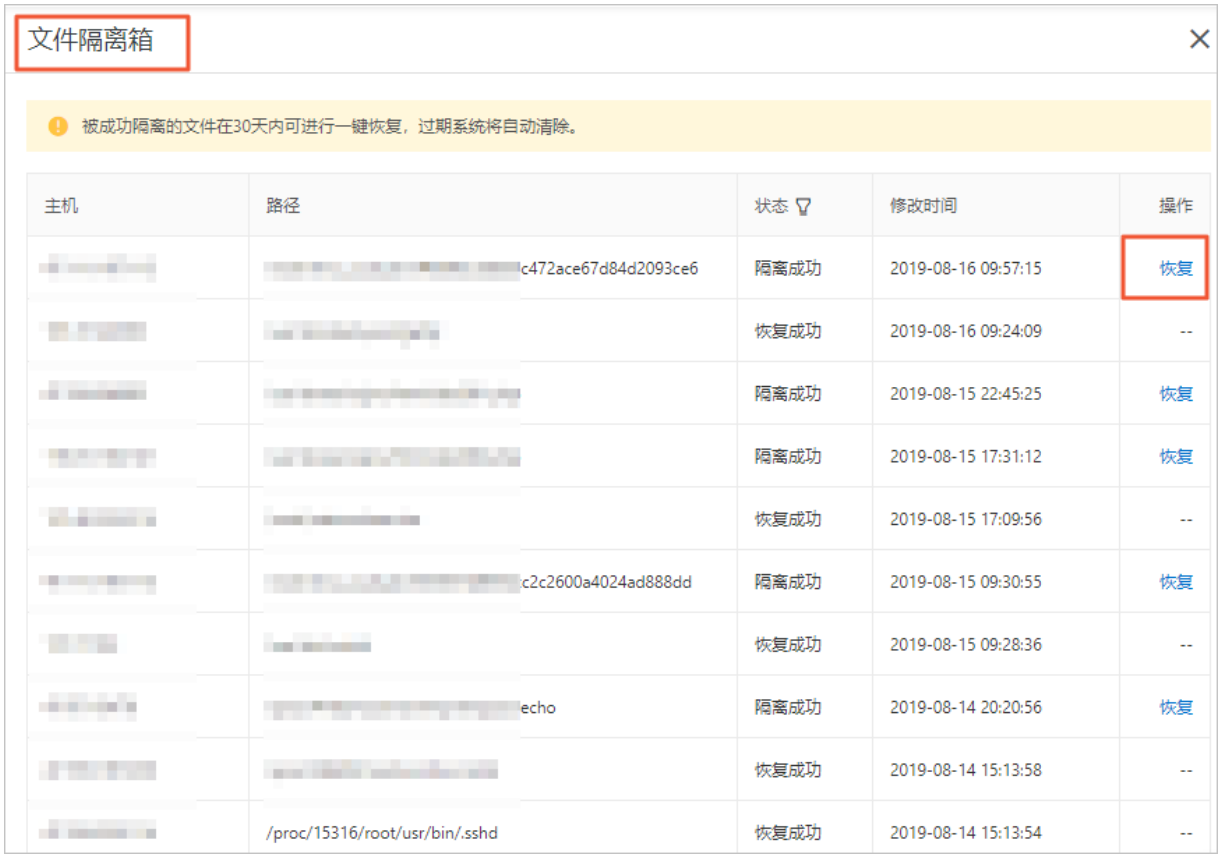
云查杀应用案例

检测

隔离


请选择"感染型病毒-恶意进程（云查杀）"的处理方式
病毒防御功能全新发布，为您提供安全体检功能，一键查杀服务器恶意病毒，点击前往
处理方式
病毒查杀
选择病毒查杀后，您可以选择关闭该病毒的进程并隔离源文件，病毒样本被隔离后，将无法对业务产生危害。
结束该进程的运行
隔离该进程的源文件
恶意病毒样本被隔离后30天内可在文件隔离箱还原。
加白名单
选择加白名单操作后，当再次发生相同告警时将自动进入已处理列表中，不再进行告警通知，请谨慎操作
忽略
选择忽略本次操作后，该告警状态将更新为已忽略，当相同告警再次发生时，云安全中心将再次告警
我已手工处理
该告警为可疑的异常行为，建议您根据处置建议进行排查，排查后点击立即处理后，该告警状态将更新为已处理。
立即处理
取消

恢复


文件隔离箱
被成功隔离的文件在30天内可进行一键恢复，过期系统将自动清除。
主机
路径
状态
修改时间
操作
c472ace67d84d2093ce6
隔离成功
2019-08-16 09:57:15
恢复
恢复成功
2019-08-16 09:24:09
--
隔离成功
2019-08-15 22:45:25
恢复
隔离成功
2019-08-15 17:31:12
恢复
恢复成功
2019-08-15 17:09:56
--
c2c2600a4024ad888dd
隔离成功
2019-08-15 09:30:55
恢复
恢复成功
2019-08-15 09:28:36
--
echo
隔离成功
2019-08-14 20:20:56
恢复
恢复成功
2019-08-14 15:13:58
--
/proc/15316/root/usr/bin/.sshd
恢复成功
2019-08-14 15:13:54
--

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，建议您定期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、盗取或破坏业务数据。

1.12. 检测Linux Rootkit入侵威胁

云安全中心企业版支持Linux Rootkit入侵威胁检测功能，帮助您及时发现资产是否被Rootkit入侵。

背景信息

Rootkit泛指所有黑客在已入侵的服务器上，为了实现自身或其它恶意行为而隐藏的恶意程序。Rootkit往往采用与操作系统机制相关的底层技术实现，用于与人工审计、安全软件分析进行对抗，因此往往涉及对受害服务器的内核、驱动进行注入和篡改。

Rootkit危害

Linux服务器的Rootkit是一类近些年有很大发展的高级对抗性恶意程序。通常，Linux Rootkit特指以Linux内核模块（LKM）形式加载到操作系统中，从内核态实现更高权限的操作，或直接对内核态代码进行篡改，从而劫持整个系统正常程序的运行。借助Rootkit，黑客可以实现对任意目录、文件、磁盘内容、进程、网络连接与流量的隐藏、窃取和篡改，并提供隐蔽的后门可供黑客直接登录到受害服务器执行更多操作。

如果服务器被植入了Rootkit，该服务器就会被黑客完全控制并且无法察觉。例如，在Linux服务器中较为常见的Reptile Rootkit，可以向目标系统安装一个名为reptile_module的内核态驱动模块，并将自身隐藏，实现以下目的：

- 黑客用户提权
- 隐藏文件和目录
- 隐藏进程
- 隐藏TCP/UDP连接
- 开机持久化隐藏
- 文件内容读写篡改
- ICMP/UDP/TCP类型后门
- 带文件传输功能的反弹Shell
- 代码与模块混淆

检测难点与现状

相比Rootkit的公开流行和发展，其检测技术在业界并没有成型的产品和成熟的方案。现有的工具例如Chkrootkit和Rkhunter，仅根据特定几种已知类型Rootkit的文件等特征判断，无法发现存在隐藏痕迹的、新型的Rootkit。而类似Volatility的内存取证方案，需要采集待检测服务器的全系统快照，并依赖于定制的或特定功能的插件，导致其无法被非安全专业人员或云服务器用户使用。

云安全中心Rootkit检测方案介绍

为了对云服务器实现Rootkit精准检测，云安全中心推出了一套轻量级的方案，以取证的方式，尝试发现潜在的Rootkit存在痕迹与影响。同时，保证对目标服务器的资源消耗极低，避免带来潜在的稳定性风险。

为发现任何形式隐藏、混淆的Rootkit，Rootkit检测功能针对通用Rootkit的原理，即总是存在对内核态函数（系统调用、VFS函数及底层功能函数）的挂钩（hook）、篡改和劫持，对系统内存镜像进行必要数据的采集检查，来确定Rootkit的存在与属性，判断被篡改劫持的系统功能，推断Rootkit本身的功能作用，从而尽可能准确地判定Rootkit，并向用户告警传递以上信息。

作为一种取证扫描形式的检测技术，本检测方案可定时对目标服务器所有历史上被植入且仍然存活的Rootkit内核模块进行全量检出，但不包括Rootkit植入进行时的行为检测。关于疑似Rootkit植入行为，以及用于植入的Rootkit内核模块文件（.ko文件），云安全中心提供“进程异常行为”、“恶意进程（云查杀）”、“持久化后门”等类型的告警检测。

Rootkit检测与推送范围

云安全中心企业版每天定时检测您资产中是否存在Rootkit威胁，检测出威胁时会自动发送告警通知，无需您主动启用或触发检测。非企业版用户或未检测出Rootkit威胁的用户不会收到相关告警。

> **说明** 如果您在安全告警设置中未选择任何关注等级，您将不会收到告警通知。具体内容，请参见通知。

Rootkit告警信息解读

如果您的资产中检测到Rootkit内核模块，云安全中心控制台会推送以下告警信息。

告警参数说明详见以下表格。

参数	说明
Rootkit内核模块名称	指从内核态内存中，定位到的隐藏的内核模块名称。正常的内核模块载入后会在lsmod命令输出中列出，而隐藏的模块名则在此列表中隐藏。
Rootkit篡改的内核函数	指在扫描中，发现被篡改、劫持的内核态函数名。这其中包括了作为内核功能入口的系统调用函数、VFS抽象层函数以及更底层的函数等。这种篡改既包括对正常函数指针的替换，也包括对正常内核代码的改写。这些劫持后真正被执行的代码，都存在于上述命名的隐藏内核模块的内存地址空间内。
Rootkit特征影响	指根据上述定位的篡改的目标，分析归纳出的Rootkit作用功能。现在包括如下分类标签：目录或文件隐藏、进程隐藏、文件内容隐藏、目录或文件防删除、网络隐藏、用户提权、进程劫持、信号劫持或后门开关、文件防改写或输入窃取、工作目录劫持。不同的Rootkit可能包括其中一项或多项标签。

支持检测的Rootkit列表

云安全中心Rootkit检测功能支持检测Linux 2.6.32以上内核、64位服务器。实际测试中选取了GitHub上较活跃维护的Rootkits-List-Download列表，筛选其中开源或开放的Linux LKM型Rootkit。当前，云安全中心已全部可检出其中仍然有效的Rootkit。

支持检测的完整的Rootkit列表及状态如下。

Rootkit	测试系统	内核	结果
f0rb1dd3n/Reptile 1.0	CentOS 7.6	3.10.0	检出
f0rb1dd3n/Reptile 2.0	Ubuntu 16.04	4.4.0	检出
Eterna1/puszek-rootkit	Ubuntu 16.04	4.4.0	检出
m0nad/Diamorphine	Ubuntu 16.04	4.4.0	检出
citypw/suterusu	CentOS 7.6	3.10.0	检出
Xingyiquan	CentOS 6.10	2.6.32	检出
bones-codes/the_colonel	CentOS 6.10	2.6.32	检出
miagilepner/rickrolly	CentOS 6.10	2.6.32	检出
matteomattia/moo_rootkit	CentOS 6.10	2.6.32	已失效
ivyl/rootkit	CentOS 6.10	2.6.32	检出
QuokkaLight/rkduck	Ubuntu 16.04	4.4.0	检出
falk3n/subversive	CentOS 6.10	2.6.32	检出
a7vinx/liinux	CentOS 6.10	2.6.32	检出
varshapaidi/Kernel_Rootkit	CentOS 7.8	3.10.0	已失效
hanj4096/wukong	CentOS 7.8	3.10.0	检出
NinnOgTonic/Out-of-Sight-Out-of-Mind-Rootkit	CentOS 6.10	2.6.32	已失效
joshimhoff/toykit	CentOS 6.10	2.6.32	已失效
jiayy/lkm-rootkit	CentOS 6.10	2.6.32	已失效
nurupo/rootkit	CentOS 6.10	2.6.32	检出
trimpsyw/adore-ng	CentOS 7.8	3.10.0	检出
PinkP4nther/Sutekh	AliyunLinux	4.19.91	检出

> **说明** 当前，对于已经在云上发现的多种非开源、并已有一定受害影响面的Rootkit，云安全中心已支持全部检出。具体检测列表后续披露。

高级对抗型Rootkit检测

在云服务器的大量分析中，已经发现有部分对抗型Rootkit，用于对抗类似Volatility的一般内核内存取证形式的扫描检测。我们目前的检测机制，已经支持对这类混淆和对抗的绕过。这类对抗型Rootkit，一般会尝试在已隐藏模块的基础上，进一步在载入内核的内存数据中，擦除包括模块头部数据在内的痕迹。对这种情况，我们仍然能够检测出上述内核函数篡改以及对应的特征影响，但其内核模块名称已经无法还原提取，此时用户接收到的告警如下所示。

2.攻击分析

云安全中心支持攻击分析功能，为您全面展示您资产受到的攻击并对攻击行为进行分析。本文介绍了攻击分析的统计信息，包括攻击次数、攻击类型分布、攻击来源TOP 5、被攻击资产TOP 5和攻击详情列表。

版本限制

仅企业版和旗舰版支持该功能，其他版本用户需要升级到企业版或旗舰版才可使用该功能。购买和升级云安全中心服务的具体操作，请参见购买云安全中心和升级与降配。各版本的功能详情，请参见功能特性。

背景信息

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。云安全中心检测到基础攻击后会自动进行拦截和处理，并在**攻击分析**页面为您展示攻击相关的数据，针对这些攻击无需您做任何处理。如果涉及风险较高的攻击事件，您可对指定攻击来源的地址进行进一步分析或排查。建议您根据自身业务需求，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。

您可在云安全中心控制台的**威胁检测 > 攻击分析**页面，查看您资产受到的攻击详情，具体包括以下内容：

- 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TOP 5：攻击次数排名前5位的攻击来源IP地址。
- 被攻击资产TOP 5：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。

在**攻击分析**页面，您可以设置时间范围查看以下攻击分析结果。您可以快速查看当天、最近7天或最近30天内的攻击分析结果，也可以选择**自定义时间**，查看最近30天内任意时间范围的攻击分析结果。

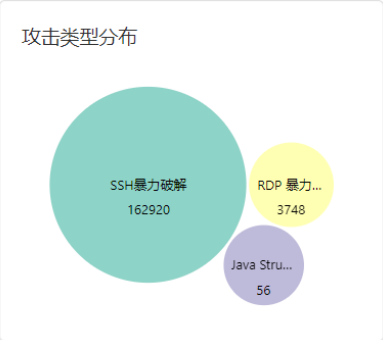
> **说明**
>
> - 新购买的云产品，需等待云安全中心自动完成该产品的网络攻击数据同步后（攻击数据同步需要3小时左右的时间），才可查看相关的攻击分析信息。
> - 攻击分析数据来源于云安全中心、阿里云云平台、Web应用防火墙（前提是已开通Web应用防火墙服务）。

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TOP 5

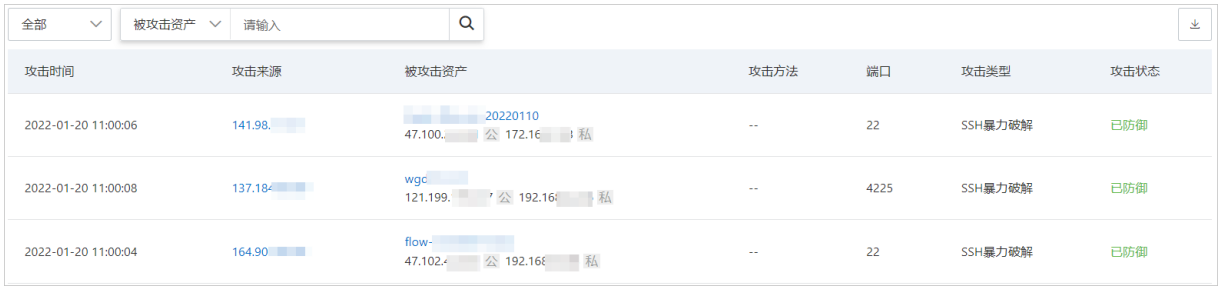
您可在**攻击来源TOP 5**区域，查看攻击次数排名前五的攻击来源IP地址及其对应的攻击次数。

被攻击资产TOP 5

您可在**被攻击资产TOP 5**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10,000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

参数	说明
攻击时间	攻击发生的时间。
攻击来源	发起攻击的源IP地址和区域。
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。
端口	被攻击的端口号，仅攻击类型为SSH暴力破解时会显示被攻击的端口号。
攻击类型	攻击事件的类型，例如SSH暴力破解、代码执行等。
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**安全告警处理**页面中。

在攻击详情列表中您可以执行以下操作。

- 搜索查看攻击事件
  您可通过攻击详情列表上方搜索条件，筛选指定的攻击类型、被攻击资产、攻击来源和端口，搜索目标的攻击事件并查看其详细信息。

- 查看攻击来源详情
  鼠标移动到**攻击来源**IP地址处，可查看该攻击来源的详细信息，包括威胁程度、发现时间、最后活跃时间、攻击来源的国家地区和威胁标签。您可以单击**详情**跳转至威胁情报控制台该攻击来源IP的**IP报告**页面，查看该攻击来源IP的更多详细信息和威胁关联数据。更多信息，请参见搜索。

- 查看被攻击资产信息

鼠标移动到**被攻击资产**名称处可查看该资产的基本信息。

- 导出攻击事件列表

  单击攻击事件列表左上方的 图标，将云安全中心检测出的攻击事件统一导出并保存到本地。导出的文件为Excel格式。

- 关闭拦截规则

  在攻击事件列表中，**中国蚁剑Webshell通信**、**中国菜刀Webshell通信**和**XISE Webshell通信**这三类攻击事件的**攻击类型**列，会显示 图标，鼠标悬停在该图标上，可以看到**关闭拦截规则**对话框。如果您的系统不需要云安全中心自动拦截此类可疑攻击行为，您可以单击**去恶意行为防御配置**，前往恶意行为防御页面关闭该系统防御规则。

相关文档

攻击分析页面的数据来源是哪些产品？

3.AK泄露检测

云安全中心实时检测GitHub等平台公开源代码中的AccessKey信息，可识别出AccessKey是否泄露，并提供相应的告警，帮助您及时发现并处理可能外泄的AccessKey信息。

背景信息

企业员工如果将不可公开的公司源码上传至GitHub等平台，会导致企业的AccessKey信息在代码中直接外泄。

云安全中心AK泄露检测功能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等平台进行实时检测，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AccessKey信息并提供实时告警，帮助您及时规避数据外泄的风险。

> **说明** 云安全中心所有版本用户都默认开启AK泄露检测功能。

版本限制

云安全中心所有版本用户都可使用该功能。各版本支持的功能详情，请参见功能特性。

设置AK泄露告警通知

云安全中心支持对AK泄露情报提供告警通知，通知的方式包括短信、邮件、站内信。

云安全中心默认开启AK泄露告警通知。您也可以根据需要，在云安全中心控制台**设置**页面的**通知**页签中，自定义**AccessKey泄露情报**的**通知时间**和**通知方式**。设置后，只有在您设置的时间段会收到通知，避免其余时间受到不必要的通知干扰。详细内容，请参见通知。

> **注意**
>
> - 已设置时间段外发生外泄事件时，您无法第一时间收到通知。
> - 收到AK泄露告警通知后，请确保您已处理了所有的AK泄露来源，并且在云安全中心控制台对该AK告警事件进行处理（即选择**我已手动删除**、**我已手动禁用AK**或**加白名单**）。否则云安全中心将会持续为您发送告警通知。

查看和处理AK泄露事件

1. 登录云安全中心控制台，在左侧导航栏，选择**威胁检测 > AK泄露检测**。
2. 在**AK泄露检测**页面，查看并处理AccessKey泄露事件。
   - **查看AccessKey泄露情报统计数据**
     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、AccessKey异常调用告警的次数、检测平台。
     单击**AccessKey异常调用告警**下的数字，可以跳转到**安全告警处理**页面查看检测出的AccessKey异常调用告警。
   - **搜索指定AccessKey泄露情报**
     在搜索框输入AccessKey ID，快速定位到想要查看的记录。
   - **查看AccessKey泄露检测详情**
     您可以在AK泄露检测列表中，选择一个检测记录，单击其操作列的**详情**，查看详细的情报信息。
   - **处理检测出的AK泄露事件**
     您可以在AK泄露检测列表中定位到具体事件，单击其操作列的**处理**，对AK泄露事件进行处理。处理建议如下：

- 在日志服务控制台，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），确认是否存在AK泄漏的情况。
- 在**AccessKey泄露详情**页面的**相关推荐**中，查看具体的处理方案并进行相应的处理。处理完成后，您需要在**处理方式**模块进行手动确认。**处理方式**包含**我已手动删除**、**我已手动禁用AK**、**加白名单**三种。

  > **说明** 您针对该AK泄露已处理了所有的AK泄露来源、并手动确认**处理方式**后，该AK泄露事件的状态会变为**已处理**，云安全中心将不会针对该AK泄露事件为您继续发送告警通知。

  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。
  需要恢复检测时，您可从**已处理**列表进入AccessKey泄露详情页，进行**取消白名单**操作。

- **导出AccessKey泄露检测报表**

  在**AccessKey泄露检测**页面，单击图标，在出现**导出完成**提示后，单击**下载**，将Excel格式的报表下载到本地。

相关文档

AK和账密防泄漏最佳实践

设置告警通知

4.云蜜罐

4.1. 云蜜罐概述

云安全中心的云蜜罐功能可以为您提供云内外的攻击发现、攻击反制等能力。您可以在阿里云VPC、已接入云安全中心的服务器实例上创建云蜜罐实例，来防御您服务器在云内外受到的真实攻击，加固您服务器的安全防护。

背景信息

传统防御方式的主旨是将攻击者拒之门外，然而随着攻击手段的多样化、隐蔽化、复杂化，传统的防御方式往往疲于应付，比如利用0day漏洞的APT攻击，传统的基于规则和特征库的安全产品很难察觉。出现问题时安全运维人员只能做事后修补，而实际上攻击者早已渗透到内网并潜伏。企业需要一种技术手段，主动对抗攻击行为，采取有利于防守方的技术措施，对攻击者形成震慑，保护数据安全。

蜜罐是一个攻击诱骗系统，通过使用蜜罐模拟一个或多个易受攻击的主机和服务，给攻击者提供一个容易被攻击的目标，伪装成用户的业务应用，使攻击者误认为是欲攻击的目标对象。由于蜜罐并没有向外界提供真正有价值的服务，因此所有试图与其进行连接的行为均可认为是可疑的，同时，让攻击者在蜜罐上耗费时间，可以延缓对真正自标的攻击，捕获更多攻击者的信息进行反制，使目标系统得到保护。

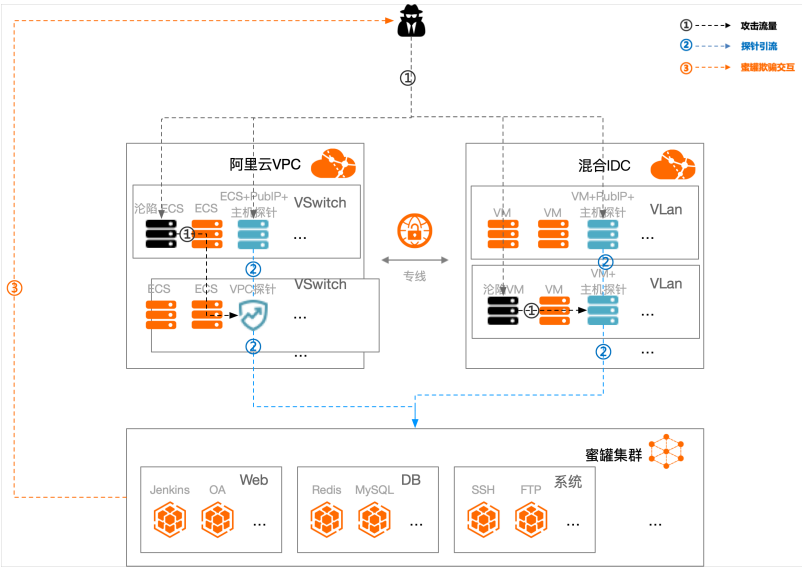
云蜜罐的原理

虽然蜜罐转守为攻，但是传统蜜罐的缺点也很明显：几乎不可实现高真实、低成本、高覆盖的蜜罐服务。为弥补传统防御方式、传统蜜罐方案的不足，云安全中心的云蜜罐技术应运而生。

云安全中心的云蜜罐功能提供了以下功能和服务。

- 云原生的VPC黑洞功能
  将VPC内部流量中，目的IP不可达的，导流至VPC黑洞探针，再由VPC黑洞探针上面的配置转发规则，转发至相应的蜜罐服务。
- 通用的主机探针方案
  在业务主机上部署Agent进行流量转发，负载低、无应用侵入、安全稳定，支持大多数主流硬件和系统。
- 丰富的蜜罐服务
  高低交互蜜罐，其中低交互可以覆盖所有端口，高交互内置几十种常见的、易被攻击者攻击的蜜罐服务，覆盖Web、数据库、系统服务、特殊缺陷、自定义服务五大类型。
- 可定制化蜜罐
  可基于docker实现自定义蜜罐，实现最高级别的业务模拟。

VPC黑洞方案与主机探针方案结合，实现低IP成本、低计算资源成本下高IP覆盖。丰富的蜜罐服务与可定制化蜜罐组成的统一的蜜罐集群，实现高真实度的同时，实现蜜罐类型的高覆盖。



云蜜罐的安全性

因为安全产品带入的稳定性问题、安全性的问题常有曝光，因此云蜜罐在设计之初就考虑了自身产品的性能、稳定性与安全性，确保在实现功能的同时，保证低负载、高稳定、高安全。

性能影响

- VPC黑洞功能
  不占用主机、网络资源。
- 主机探针
  纯异常端口流量转发，占用系统资源较小。

稳定性影响

- VPC黑洞功能
  VPC黑洞功能会针对扫描流量进行模拟交互，如果有通过扫描的资产探测软件，可能会造成误报。
- 主机探针
  主机探针需要占用主机端口，因此需要合理规划主机探针所安装的主机端口分配。

安全性影响

- 主机探针的安全性
  主机探针与管理中心只存在导流与功能控制交互，即使管理节点被攻陷，也没有渠道通过探针控制主机。
- 蜜罐逃逸的安全性
  每个用户独享一套蜜罐集群，且内置docker逃逸检测。
- 网络安全性
  通过网络隔离，即使蜜罐集群被攻陷，也不能通过蜜罐和探针的通道攻击客户原网络。

支持的环境

云蜜罐支持阿里云、非阿里云（其他云、传统线下环境）等各种网络环境。

- 在阿里云环境，云安全中心和网络团队合作开发的VPC黑洞蜜罐功能，可以将VPC内部流量中，目的IP不可达的流量黑洞，再接入蜜罐服务，实现低成本、高覆盖的蜜罐服务。
- 在非阿里云环境，云蜜罐支持低负载、安全可靠的主机探针导流模式，将可疑流量导流至后端蜜罐集群。

使用限制

主机探针的使用限制

主机探针仅支持在云安全中心的**资产中心**中维护的服务器实例。

VPC黑洞探针的使用限制

VPC黑洞探针目前仅支持阿里云的以下地域。

- 华北1（青岛）
- 华北2（北京）
- 华北3（张家口）
- 华北5（呼和浩特）
- 华北6（乌兰察布）
- 华东1（杭州）
- 华东2（上海）
- 华南1（深圳）
- 华南2（河源）
- 华南3（广州）
- 西南1（成都）
- 中国（香港）
- 日本（东京）
- 新加坡
- 澳大利亚（悉尼）
- 印度尼西亚（雅加达）
- 印度（孟买）
- 美国（弗吉尼亚）
- 美国（硅谷）
- 英国（伦敦）
- 阿联酋（迪拜）
- 德国（法兰克福）

公测版与正式版的云蜜罐功能说明

如果您是在2022年04月20日之前开通过云蜜罐功能，则您使用的是公测版云蜜罐功能。云蜜罐已于2022年04月20日发布正式版，您可在控制台开通使用。

公测版将于2022年06月30日前停止服务，如果您想继续使用云蜜罐功能，建议您开通正式版云蜜罐。

> **说明** 公测版在产品说明中可看到公测字样，目前公测阶段已完成，未开通公测版的用户可使用正式版云蜜罐。

公测版与正式版云蜜罐的功能对比如下：

版本	应用场景	蜜罐类型	引流方式	收费标准
公测版	阿里云VPC内网横向入侵检测	低交互	VPC黑洞	公测期间免费试用

版本	应用场景	蜜罐类型	引流方式	收费标准
正式版	阿里云、非阿里云（其他云、传统IDC等）环境 • 内网横向入侵检测 • 公网威胁情报收集 • 攻防场景溯源反制	• 低交互 • 高交互 • 自定义	• VPC黑洞 • 主机探针 • 诱饵	收费。具体收费标准，请参见收费标准。

公测版升级到正式版的注意事项

正式版不支持从公测版直接升级。公测版和正式版的数据、功能不可并存使用，已配置公测版的用户升级为正式版数据将不会保留，需要重新进行配置。正式版需要付费开通后才能使用。

- 如果您想使用正式版的云蜜罐产品，您需要将公测版云蜜罐功能下已创建的云蜜罐实例全部删除。删除公测版云蜜罐中的存量实例后，单击页面右上角的**立即开启高交互蜜罐**，即可开通正式版云蜜罐功能。开通正式版云蜜罐的具体操作，请参见开通云蜜罐服务。
- 如果您想继续使用公测版云蜜罐功能，请参考云蜜罐（公测中）文档。

4.2. 开通云蜜罐服务

使用云安全中心的云蜜罐功能前，您需要购买并开通该服务。

收费标准

云蜜罐按照探针的数量来收费，云蜜罐有两种探针类型：

- VPC探针
  VPC探针部署在阿里云VPC上，1个VPC有且只能有1个VPC探针。
- 主机探针
  主机探针可以部署在任意主机上，1个主机有且只能部署1个主机探针。

在收费标准上，这两种探针并无差别。云蜜罐最低标准为20个探针起售，最多可购买500个。若超过500个，可以提交工单联系技术支持进行扩容。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**威胁检测 > 云蜜罐**。
3. 在**云蜜罐**页面，单击**立即购买**跳转到**变配**页面。
4. 在**变配**页面，将**云蜜罐**配置为**是**，并设置**云蜜罐授权数**。
5. 单击**立即购买**。

后续步骤

开通云蜜罐功能后，您就可以开始为您的服务器或VPC部署云蜜罐。具体操作，请参见配置云蜜罐。

4.3. 配置云蜜罐

您可以使用云蜜罐功能，通过在您的阿里云VPC、服务器上部署云蜜罐，检测您服务器在云内、云外受到的真实攻击，甚至溯源反制攻击者，提升安全感知和威慑能力。本文介绍如何配置云蜜罐。

前提条件

已开通云蜜罐功能。具体操作，请参见开通云蜜罐服务。

配置流程概述

首先您需要创建一个管理节点，其次再创建一个蜜罐，然后将创建的蜜罐与管理节点关联，最后通过在目标服务器或VPC中安装探针，将访问该服务器或VPC的流量转发至云蜜罐，通过转移攻击者目标，让攻击者在蜜罐中攻击真实伪装应用，从而延长攻击时间，记录完整攻击行为和溯源，为安全运营者及防守方提供先人一步的主动防御手段。

配置云蜜罐的步骤如下：

- 步骤一：新增管理节点
- （可选）蜜罐模板
- 步骤二：新增蜜罐
- 步骤三：新增探针

步骤一：新增管理节点

管理节点是提供蜜罐服务的系统，探针转发的流量最终会进入管理节点中配置的各种蜜罐服务上。管理节点是整个系统的核心与基础。

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**威胁检测 > 云蜜罐**。
3. 单击**云蜜罐**页面右上角的**配置管理**，进入**配置管理**页面。
4. 在**管理节点**页签下，单击**新建节点**。

   新建管理节点的配置项说明如下：

配置项	说明
管理节点名称	设置管理节点的名称。
分配探针数	设置该管理节点的探针数。分配探针数不能小于20，不能超过100。设置的探针数超过100时，系统会自动设置为100。建议每个C段安装2~3个主机探针，每个VPC安装1个VPC黑洞探针。 **说明** 探针的作用是流量导流，云蜜罐支持主机探针通过安装在主机上，进行端口流量导流至蜜罐服务。VPC黑洞探针安装在VPC上，将目标IP不存在的且为内网IP的流量，导入至蜜罐服务。主机探针VPC黑洞探针
放行网段	设置该管理节点与主机探针的放行网段，即允许探针的哪些出口IP访问该管理节点。默认配置为0.0.0.0/0。最多支持设置100个放行网段。服务过程中探针需要和管理节点进行通信，请确保探针的出口IP在放行网段内。
允许蜜罐访问外网	设置该管理节点是否允许蜜罐访问外网。 **注意** 开启此功能，可能存在安全风险，攻击者可以成功入侵蜜罐后进行强攻击；不开启的情况下，仅支持攻击检测，适用于内网场景。

5. 单击**确定**。

   您可以在管理节点列表中查看您新建的管理节点。新建的管理节点的**管理节点状态**为**准备中**，这个状态会持续5分钟左右，请您耐心等待。

（可选）蜜罐模板

蜜罐模板功能可针对不同蜜罐类型配置不同的自定义属性，构造出符合业务场景的蜜罐，以模拟出更真实的应用。其中可以自定义的蜜罐类型包括但不限于网站title、OA背景图、Web页面数据等。您可根据您的业务需要定制蜜罐模板。

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**威胁检测 > 云蜜罐**。
3. 单击**云蜜罐**页面右上角的**配置管理**，进入**配置管理**页面。
4. 在**蜜罐模板**页签的左侧选择蜜罐类型，然后单击**新建模板**。
5. 在**创建模板**面板上，配置蜜罐模板相关信息。

   蜜罐模板的配置项说明如下：

配置项	说明
模板名称	设置蜜罐模板的名称。
管理节点	选择部署云蜜罐的管理节点。即您步骤一中新建的管理节点。

> **说明** 蜜罐模板的其他配置项的设置，因选择的蜜罐类型不同配置也稍有差别。如果您需要设置这部分配置项，具体设置方法，您可以提交工单咨询阿里云技术支持。

6. 单击**确定**。

步骤二：新增蜜罐

蜜罐是蜜罐服务的基础单位，系统默认有许多的内置蜜罐镜像，通过蜜罐镜像创建对应的蜜罐实例，从而提供蜜罐服务。

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**威胁检测 > 云蜜罐**。
3. 单击**云蜜罐**页面右上角的**配置管理**，进入**配置管理**页面。
4. 在**蜜罐管理**页签下，单击**新建蜜罐**。

   新建蜜罐的配置项说明如下：

配置项	说明
名称	设置蜜罐的名称。
管理节点	选择部署云蜜罐的管理节点。即您步骤一中新建的管理节点。

配置项	说明
蜜罐类型	选择蜜罐的类型。支持选择的蜜罐的大类有以下几种： ○ Web ○ 高级 ○ 特殊缺陷 ○ 系统服务 ○ 数据库
自定义蜜罐配置	配置蜜罐的自定义属性。支持针对不同蜜罐类型配置不同的自定义属性，构造出符合业务场景的蜜罐，以模拟出更真实的应用。其中可以自定义的蜜罐类型包括但不限于网站title、OA背景图、Web页面数据等。 您也可以通过提前配置**蜜罐模板**，然后通过**导入模板配置**的方式，添加自定义蜜罐配置。 关于**自定义蜜罐**、**蜜罐模板**的配置操作，您可以提交工单咨询阿里云技术支持。

5. 单击**确定**。

步骤三：新增探针

探针是导流的工具，功能是将主机、网络中的异常流量导流至蜜罐服务，有VPC探针和主机探针两种类型。

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**威胁检测 > 云蜜罐**。
3. 单击**云蜜罐**页面右上角的**配置管理**，进入**配置管理**页面。
4. 在**探针管理**页签下，单击**新增探针**。

   支持新增主机探针和VPC黑洞探针。

   ○ 新增主机探针的配置项说明如下：

配置项	说明
探针名称	设置探针的名称。
管理节点	选择部署探针的服务器对应的管理节点。即您步骤一中新建的管理节点。
部署主机	选择部署探针的服务器。
配置服务	设置访问流量转发的蜜罐的名称和监听端口。
开启检测项	选择是否开启检测项，支持以下检查项： ■ ping扫描检测 ■ ARP欺骗检测

   ○ 新增VPC黑洞探针的配置项说明如下：

> **注意** 仅支持在阿里云VPC下创建蜜罐实例，不支持在其他网络下创建。每个VPC下仅支持创建一个蜜罐实例。目前仅支持在部分地域部署VPC黑洞探针。详细信息，请参见使用限制。

配置项	说明
探针名称	设置探针的名称。
管理节点	选择探针部署的服务器对应的管理节点。即您步骤一中新建的管理节点。
部署VPC	选择部署探针的VPC。
配置服务	设置访问流量转发的蜜罐的名称和监听端口。

5. 单击**确定**。

后续步骤

云蜜罐配置后，云蜜罐通过探针监测转移攻击者目标，让攻击者在蜜罐中攻击真实伪装应用，并会记录这些攻击的信息形成告警事件。您可以通过查看和处理告警事件，提升您的服务器和VPC的安全防御。具体操作，请参见查看和处理告警事件。

4.4. 查看和处理告警事件

云蜜罐部署后，云蜜罐会诱捕您服务器在云内外受到的真实攻击，并将攻击数据生成告警事件展示在云蜜罐页面。为了您的服务器的安全，建议您及时查看和处理告警事件。本文介绍如何查看和处理告警事件。

查看告警事件

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**威胁检测 > 云蜜罐**。
3. 在云蜜罐页面查看告警事件。

   云蜜罐页面分为总览和告警列表两个区域。

   - 总览
     在总览区域，您可以查看**管理节点健康状态**、**已授权探针数量**、**未使用探针数量**、**已部署主机探针数量**等信息。
     当您的云蜜罐探针数量不足时，您可以单击**升级配置**，购买足够的云蜜罐探针数量。
   - 告警列表
     在告警列表区域，您可以查看云蜜罐诱捕的黑客攻击所产生的安全告警事件的详细信息。包括告警事件的**风险等级**、**风险概述**、**攻击来源**等信息。
     单击目标告警事件**操作**列的**查看日志**，进入**事件日志**，可以查看该告警事件相关的详细的日志记录列表。单击目标日志**操作**列的**详情**，可查看日志详情，包括攻击事件的**基础信息**和**攻击时间线**，进一步了解攻击事件的详细信息。

处理告警事件

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**威胁检测 > 云蜜罐**。
3. 处理告警事件。

   您可以通过查看告警事件，根据告警事件详情选择合适的方式处理告警事件。

- 加入白名单

  > **注意** 将告警事件处理方式设置为加白名单后，与该告警事件相同的攻击信息将不会在产生告警事件上显示在告警事件列表，为了您的资产安全，请您谨慎操作。

  如果通过查看告警事件详情，确认该告警事件为正常的业务，您可以单击告警事件**操作**列的**处理**，处置方式选择**加白名单**。

  > **说明** 将告警事件加入白名单后，如果后续业务中，您想再次上报该告警事件，您可以在已处理的告警事件列表中，单击目标告警事件**操作**列的**处理**，对告警事件执行**取消白名单**的操作。

- 标记为已处理
  如果通过查看告警事件详情，确认该告警事件为黑客攻击行为，您需要对您的服务器或VPC中对存在的安全风险进行加固。加固完成后，您可以单击该告警事件**操作**列的**处理**，处置方式选择**标记为已处理**。

4.5. 云蜜罐（公测中）

云安全中心云蜜罐为您提供云上攻击收集、分析和告警能力。您可以在阿里云VPC下创建蜜罐实例，来诱捕您服务器在云上受到的真实攻击，加固您服务器的安全防护。本文介绍如何创建蜜罐实例并查看蜜罐捕捉到的安全风险。

版本限制

仅企业版和旗舰版支持该功能，其他版本用户需要升级到企业版或旗舰版才可使用该功能。购买和升级云安全中心服务的具体操作，请参见购买云安全中心和升级与降配。各版本的功能详情，请参见功能特性。

限制条件

- 仅支持在阿里云VPC下创建蜜罐实例，不支持在其他网络下创建。每个VPC下仅支持创建一个蜜罐实例。
- 云蜜罐功能公测中，目前支持在以下地域和可用区内的VPC和交换机下创建蜜罐实例。

地域	城市	地域ID
华北1	青岛	cn-qingdao
华北2	北京	cn-beijing
华北3	张家口	cn-zhangjiakou
华北5	呼和浩特	cn-huhehaote
华北6	乌兰察布	cn-wulanchabu
华东1	杭州	cn-hangzhou
华东2	上海	cn-shanghai
华南1	深圳	cn-shenzhen
华南2	河源	cn-heyuan

地域	城市	地域ID
华南3	广州	cn-guangzhou
西南1	成都	cn-chengdu
中国香港	香港	cn-hongkong
亚太东北1	东京	ap-northeast-1
亚太东南1	新加坡	ap-southeast-1
亚太东南2	悉尼	ap-southeast-2
亚太东南5	雅加达	ap-southeast-5
亚太南部1	孟买	ap-south-1
美国东部1	弗吉尼亚	us-east-1
美国西部1	硅谷	us-west-1
英国	伦敦	eu-west-1
中东东部1	迪拜	me-east-1
欧洲中部1	法兰克福	eu-central-1

注意 如果已有的VPC和交换机未在以上地域和可用区内，您可以提交工单并附上VPC及对应地域和可用区的信息申请试用云蜜罐功能。在审核通过后，云安全中心会为您开通该功能。

- 云安全中心默认为您提供3个授权数，创建一个蜜罐实例会消耗一个授权数，即您最多可以创建3个蜜罐实例。您可以在**创建蜜罐**面板查看可用授权数。如果您需要更多的授权数，请提交工单申请。

创建蜜罐实例

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**威胁检测 > 云蜜罐**。
3. 在**云蜜罐**页面，单击**蜜罐状态**页签。
4. 在**蜜罐状态**页签下，单击**创建蜜罐**。
5. 在**创建蜜罐**面板，配置地域、VPC和交换机信息。

6. 单击**确定**。
   创建完成后，该蜜罐状态会变为**正在运行**，该蜜罐会诱捕您VPC里的攻击行为，发现安全风险时会发送告警信息。您可以在**风险总览**页面查看发现的告警信息。更多信息，请参见查看蜜罐风险总览。您还可以对已创建的蜜罐执行以下操作：
   - 暂停蜜罐：如果需要暂停正在运行中的蜜罐的诱捕行为，您可以单击该蜜罐**操作**列的**暂停**。
   - 开启蜜罐：如果需要为暂停诱捕的蜜罐重新开启诱捕行为，您可以单击该蜜罐**操作**列的**开启**。
   - 删除蜜罐：如果不再需要某个蜜罐，您可以单击该蜜罐**操作**列的**删除**。执行删除操作后，该蜜罐实例状态为**删除中**。删除操作完成后，将释放当前正在使用的授权数。

     > **说明** 删除蜜罐后，该蜜罐在删除前上报的告警信息仍会保留，您可以在**风险总览**页面查看相应告警信息。

查看蜜罐风险总览

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**威胁检测 > 云蜜罐**。
3. 在**风险总览**页签下，查看Top 5风险VPC、Top 5风险资产和告警列表。
   以下是Top 5风险VPC、Top 5风险资产和告警列表的介绍：
   - Top 5风险VPC：展示今天、近一周或近一月风险数排名前5的VPC信息。
   - Top 5风险资产：展示今天、近一周或近一月风险数排名前5的资产信息。

- 告警列表：展示蜜罐在您资产中检测到的告警信息，包告警风险等级、事件名称、最新发生时间和受影响资产。支持使用事件名称及风险等级筛选告警信息。

  > **说明** Top 5风险VPC和Top 5风险资产中的VPC和服务器资产存在较大的安全风险，建议您及时处理相关风险。

4. 单击需查看的告警**操作**列的**详情**，查看该告警详细信息。

   您可以查看以下信息：

   - **受影响资产**：单击受影响资产名称，可以跳转到该资产详情页面，查看该资产的漏洞、基线等风险信息。
   - **首次发生时间**：首次检测到该告警的时间。
   - **更新时间**：最近一次检测到该告警的时间。
   - **关联异常**：和该告警关联的异常情况。支持查看该告警事件关联的所有异常情况的详细信息和建议解决方案。

5.常见问题

本文汇总了威胁检测的常见问题。

- **安全告警问题**
  - Rootkit告警支持实时检测吗？
  - 如何判断资产中是否存在挖矿威胁？
  - 未开启病毒拦截，我的服务器遭受挖矿攻击，该如何处理？
  - 我不小心将挖矿告警加入了白名单，该如何取消？
  - 如何查看我已开启了哪些防御能力？
  - 如何确认病毒自动拦截已生效？
  - phpinfo为什么会产生告警，是否为误报？
  - 是否可以自动隔离WebShell文件？
  - 云安全中心WebShell检测的原理是什么？
  - 为什么安全告警中涉及到我服务器中常用的文件，是误报吗？
  - 云安全中心如何发现黑客入侵行为？
  - 常见的黑客入侵行为有哪些？
  - 安全告警可以将哪些对象加入白名单？
  - 常见告警处理方法有哪些？
  - 为什么某些告警状态为已过期数据？
- **异常登录问题**
  - 正常登录服务器，云安全中心提示异常登录，如何避免这种情况？
  - 多次输错服务器登录密码后才成功登录服务器，触发了ECS被暴力破解登录告警，我该怎么办？
  - 设置了常用IP、时间及账号，并且正常登录，依然会提示异常登录怎么办？
  - 产生异常登录告警时，登录是成功了还是被拦截了？
  - 异常登录告警已确定为黑客登录，我该怎么办？
  - 出现ECS登录后执行异常指令序列（SSH）告警时，该操作是否已经被执行？
  - 发生异常登录告警时，对应服务器应该查看什么日志？
- **攻击分析**
  - 攻击分析页面的数据来源是哪些产品？
- **暴力破解问题**
  - 如何查看服务器被暴力破解的次数或拦截情况？
  - 如何预防服务器被暴力破解？
  - 误操作导致防暴力破解生效怎么办？
  - 防暴力破解支持防护Web应用或网站吗？
  - 被暴力破解成功之后该怎么处理？
  - 为什么修改22端口后仍然出现密码暴力破解提示？
  - 为什么安全组或者防火墙规则已经屏蔽了RDP服务的3389端口，但RDP还是有被暴力破解的记录？
  - ECS登录弱口令是指系统层面的RDP或者SSH扫描吗？
  - 如何处理SSH、RDP远程登录被拦截？

- AK泄露检测问题
  - 高危敏感信息泄露处置方案

Rootkit告警支持实时检测吗？

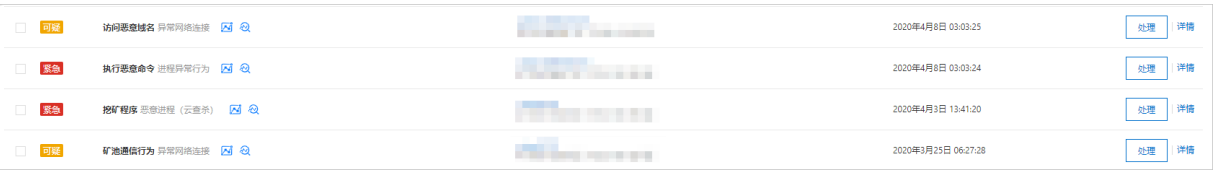
不支持。

云安全中心通过定时任务，触发对内存的扫描，来判断是否存在Rootkit威胁。如果存在Rootkit威胁，会产生Rootkit告警。Rootkit检测详细信息，请参见检测Linux Rootkit入侵威胁。

如何判断资产中是否存在挖矿威胁？

如果您服务器的CPU使用率明显升高，例如达到80%以上，并且出现未知进程持续向外发送网络包的情况，可以判定您的服务器中存在挖矿威胁。

云安全中心防护的资产被挖矿程序入侵时，云安全中心会向您发送告警短信或邮件，您可以在云安全中心控制台**威胁检测 > 安全告警处理**页面处理挖矿事件告警。**挖矿程序**如果关联了其他告警事件，例如**矿池通信行为**、**访问恶意域名**等，建议您一并处理关联的告警事件。如何查看和处理关联告警，请参见查看告警自动化关联分析。



未开启病毒拦截，我的服务器遭受挖矿攻击，该如何处理？

在云安全中心控制台**安全告警处理**页面，定位到相应告警，单击其操作列**处理**，选择**病毒查杀**、**隔离该进程的源文件**和**结束该进程的运行**后单击**立即处理**。在**设置**页面，打开**防病毒**开关。

我不小心将挖矿告警加入了白名单，该如何取消？

在云安全中心控制台**安全告警处理**页面，将筛选条件改为**已处理**，可以看到已经处理过的全部告警。定位到相应告警，单击其操作列**取消白名单**，即可恢复该告警。

如何查看我已开启了哪些防御能力？

云安全中心支持对您已开启的防御能力提供总览，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。

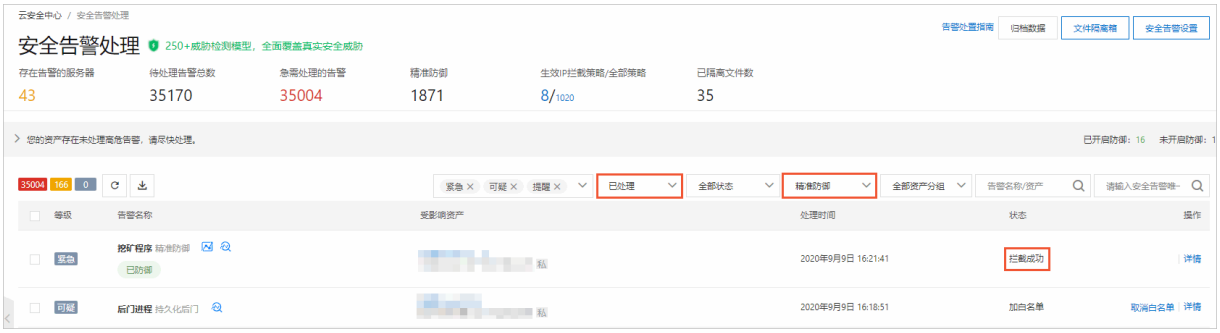
已开启的防御项默认不展示，您可在安全告警处理页面单击 > 图标，展开防御能力列表。

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购买版本支持的告警事件防御能力。

> **说明**
>
> - 如需开通网页防篡改等防御能力，需**升级**到防病毒版、高级版、企业版或旗舰版，并购买网页防篡改增值服务。有关开通网页防篡改的内容，请参见开通服务。网页防篡改详细操作，请参见启用网页防篡改保护。
> - 目前应用白名单功能处于邀测阶段，您可通过云安全中心控制台**应用市场 > 概况**提交开通试用的申请。应用白名单详细操作，请参见应用白名单。
> - 云产品威胁检测为企业版和旗舰版功能，企业版和旗舰版自动开启防御；免费版、防病毒版、高级版需要升级至企业版或旗舰版后才能自动开启防御。

如何确认病毒自动拦截已生效？

在云安全中心控制台**设置**页面开启了**防病毒**后，您可以在**安全告警处理**页面，将筛选条件更改为**精准防御**、**已处理**，看到防御状态为**拦截成功**说明病毒自动拦截已生效。



云安全中心如何发现黑客入侵行为？

云安全中心发现的所有黑客入侵行为，是通过扫描检测和阿里云安全工程师分析客户流量数据并加以验证得出的。

常见的黑客入侵行为有哪些？

云安全中心提供的告警检测项已经覆盖了常见的黑客入侵行为，包括后门、暴力破解、挖矿等。详细内容，请参见安全告警类型列表。

phpinfo为什么会产生告警，是否为误报？

不是误报。

phpinfo包含大量敏感信息，例如网站绝对路径等，具有较高的风险性，可能存在被黑客利用的风险。大部分黑客第一步都会上传phpinfo从而为进一步渗透获取更多信息。如果您确认该文件是您业务所需的正常文件，您可以在云安全中心控制台**安全告警处理**页面处理该告警时选择**加入白名单**。

是否可以自动隔离WebShell文件？

不可以。由于WebShell文件可能涉及您业务方面的信息，需要您判断后手动隔离。被隔离的文件可以在文件隔离箱中找到，且30天内可以恢复。关于文件隔离箱的更多信息，请参见文件隔离箱。

云安全中心WebShell检测的原理是什么？

云安全中心采用主机+网络双重检测机制，检测PHP、ASP、JSP等类型的网站脚本文件。以下是两种检测机制的介绍：

- 主机检测：实时监控主机上网站目录文件的变化。
- 网络检测：通过还原后门文件及分析网络协议进行检测。

为什么安全告警中涉及到我服务器中常用的文件，是误报吗？

这种情况不属于误报。如果您服务器中常用的文件生成时间存在改动、文件内容包含明显的后门语句，云安全中心也会进行相应告警。您排查后根据实际情况进行处理即可。

安全告警可以将哪些对象加入白名单？

安全告警处理功能支持对恶意进程（云查杀）类的告警进行加白名单的操作。加入白名单操作仅针对当前告警事件中的访问源进行加白。支持加入白名单的告警类型详见以下表格。

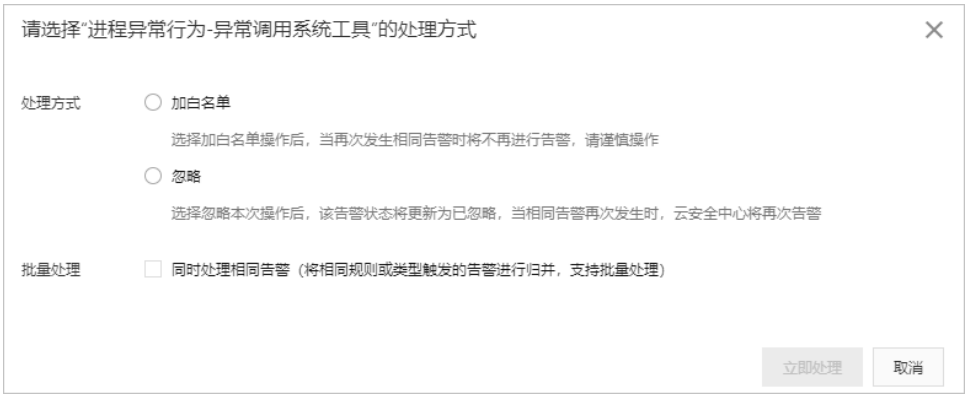
告警类型	加白对象
恶意进程（云查杀）	基于文件MD5值加白
异常登录	对异常登录的IP加白
访问恶意IP、矿池通信行为	基于IP加白
访问恶意域名	基于域名加白
访问恶意下载源、主动连接恶意下载源	基于URL加白
WebShell	基于Web目录配置加白
恶意脚本	基于MD5和路径加白
云产品威胁检测	支持在控制台配置加白规则
进程异常行为	基于命令行加白
持久化后门	基于文件MD5和特征加白
敏感文件篡改	基于文件路径加白
应用入侵事件	基于命令行加白
Web应用威胁检测	基于域名或URL加白
异常网络连接	基于进程命令行、目标IP、目标端口加白。如果有部分字段缺失，仅对已有字段加白。

常见告警处理方法有哪些？

本部分内容介绍云安全中心常见告警的处理方法。

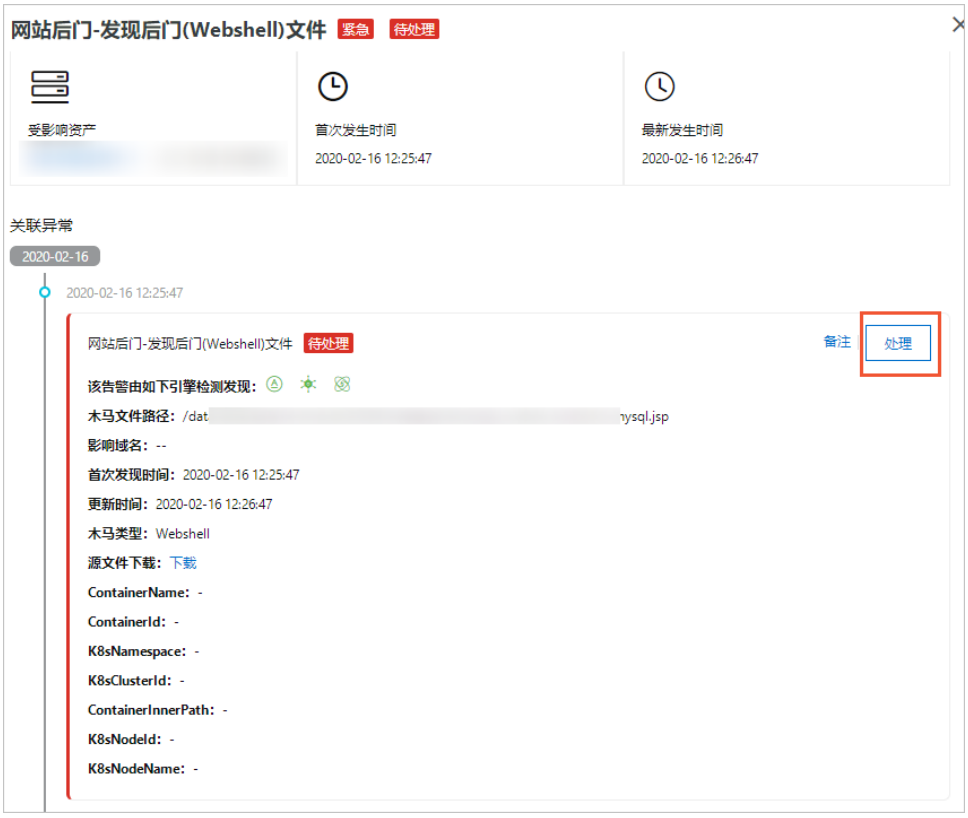
- **进程异常行为告警处理**

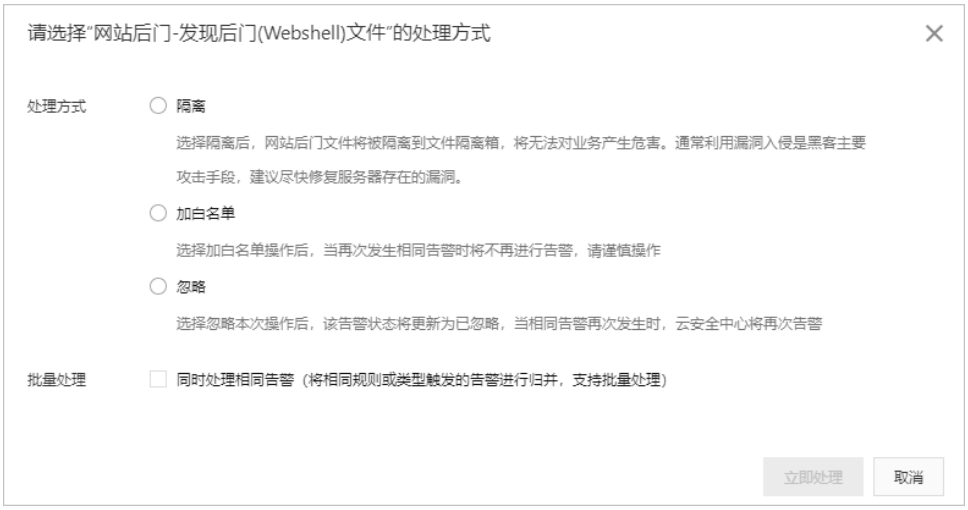
查看告警，确认该行为是否为正常业务操作。如果是正常业务操作，单击**处理**并选择**加白名单**；如果不是正常业务行为，要结合其它告警处理安全事件，安全事件处理完毕后，在控制台单击**处理**并选择**忽略**。



- **网站后门处理**

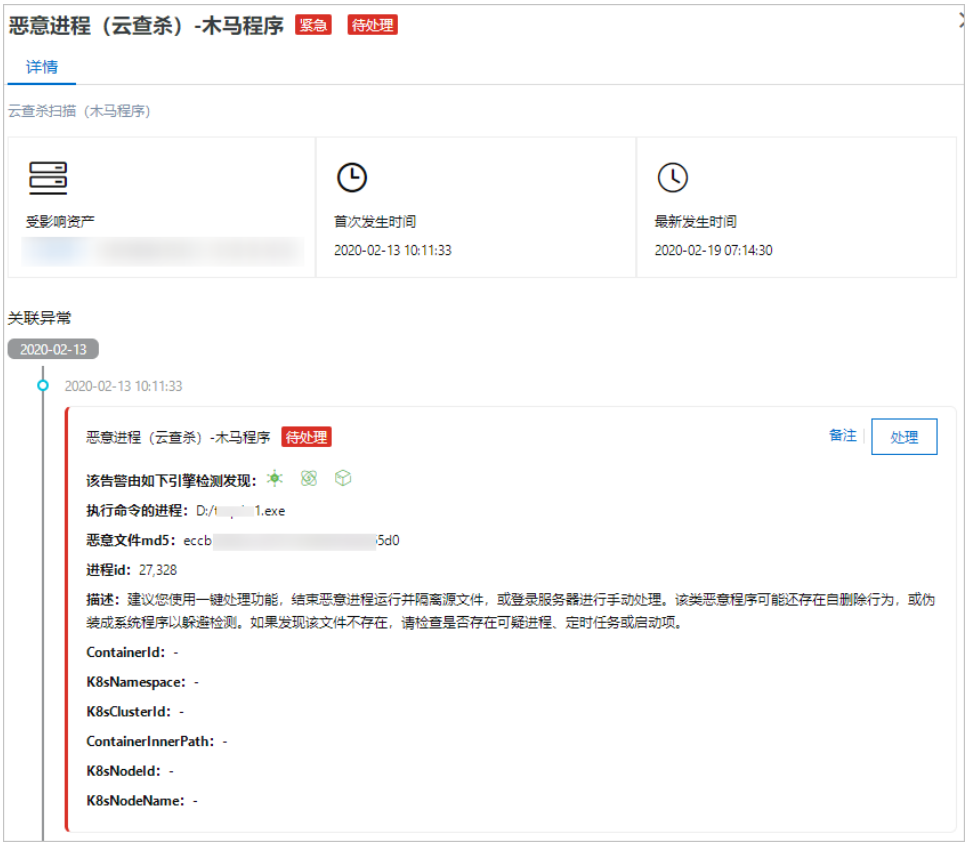
确认对应的文件是否为正常业务文件。如果是正常业务文件，单击**处理**并选择**加白名单**；如果不是正常的业务文件请单击**处理**并选择**隔离**。





- **恶意进程（云查杀）**

建议您使用病毒查杀功能，结束恶意进程运行并隔离源文件，或登录服务器进行手动处理。该类恶意程序可能还存在自删除行为，或伪装成系统程序以躲避检测。如果发现该文件不存在，请检查是否存在可疑进程、定时任务或启动项。



- **异常网络连接**

若为正常业务流量，请单击**处理**并选择**加白名单**；若不是正常业务流量，请依据具体告警采用云防火墙、WAF进行针对性拦截，处理完毕后选择**忽略**，该事件将移置已处理中。

为什么某些告警状态为已过期数据？

如果告警最后一次发生时间距离现在超过30天，云安全中心会将该告警状态置为**已过期**。如果后续再次检测到该告警发生，云安全中心会更新该告警发生时间为最新检测到的时间，并将该告警的状态置为**未处理**。

正常登录服务器，云安全中心提示异常登录，如何避免这种情况？

通过使用云安全中心控制台**安全告警处理**页面的**安全告警设置**功能，设置常用登录IP、时间及账号，支持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。

多次输错服务器登录密码后才成功登录服务器，触发了ECS被暴力破解登录告警，我该怎么办？

由于服务器密码复杂度较高，可能会存在多次输错ECS服务器登录密码后，才成功登录服务器的情况。该行为会被云安全中心的防暴力破解模型判定为ECS密码被暴力破解，并产生ECS被暴力破解登录告警。您在确认是误操作触发该告警后，可以忽略该告警。忽略告警的具体操作，请参见处理告警事件。

设置了常用IP、时间及账号，并且正常登录，依然会提示异常登录怎么办？

这种情况应先判断告警类型是否为非合法IP登录、在非常用地登录还是非常用账号登录。登录IP、登录地、账号、时间都是影响登录告警的因素，不存在优先级关系，只要其中一个因素存在异常，都会触发告警。

产生异常登录告警时，登录是成功了还是被拦截了？

产生异常登录告警表示已经登录成功，但是这个登录行为被云安全中心判定为可疑行为，所以产生该可疑行为的告警事件。

异常登录告警已确定为黑客登录，我该怎么办？

在云安全中心控制台**安全告警处理**页面，定位到该告警并单击操作列的**处理**，选择阻断12小时并单击**立即处理**，即可立马阻断该黑客的入侵。建议您立即修改密码，并检查服务器是否存在其他未知账号和其他未知公钥，防止SSH免密登录。

出现ECS登录后执行异常指令序列（SSH）告警时，该操作是否已经被执行？

该命令已经被执行，请您及时更新服务器登录密码，并检查服务器是否有其他异常行为，例如启动了未知进程。

发生异常登录告警时，对应服务器应该查看什么日志？

您可以查看服务器*/var/log/secure*目录下的信息。例如执行命令 `grep 10.80.22.22 /var/log/secure` 。

如何查看服务器被暴力破解的次数或拦截情况？

在云安全中心控制台**威胁检测 > 攻击分析**页面，可以查看SSH暴力破解拦截成功的信息。

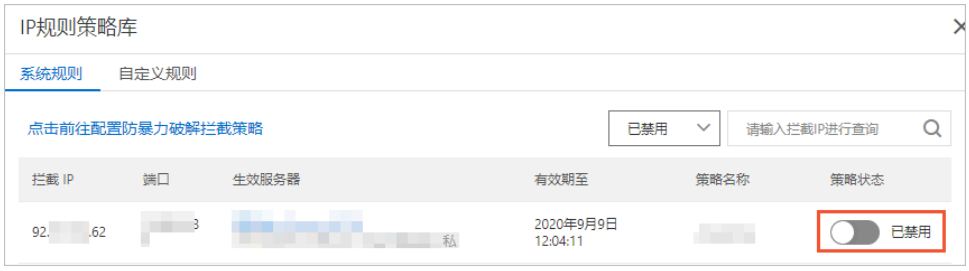
如何预防服务器被暴力破解？

您可以通过设置常用登录IP、或采取证书登录方式，避免该情况发生。设置常用登录IP的方法，请参见安全告警设置。

误操作导致防暴力破解生效怎么办？

如果在设置了防暴力破解规则后，由于登录失败次数太多，导致防暴力破解规则生效，无法登录服务器，您可以参考以下方法解除禁止登录：

在云安全中心控制台**安全告警处理**页面，单击**生效IP拦截策略/全部策略**下的数字，在**IP规则策略库**页面，找到对应的拦截规则，将该规则的**策略状态**置为**已禁用**。



防暴力破解支持防护Web应用或网站吗？

不支持。

防暴力破解支持对使用RDP和SSH协议登录的服务器进行防护，不支持防护Web应用或网站。

被暴力破解成功之后该怎么处理？

如果您的服务器密码被暴力破解成功，攻击者很有可能已经入侵并登录您的服务器并留下恶意程序。您可以在云安全中心控制台**威胁检测 > 安全告警处理**页面查看是否存在暴力破解成功相关的告警。

如果您的资产中存在**ECS被暴力破解成功**类似告警，则表示您的相应服务器已被暴力破解成功，建议您尽快参考以下步骤加固您的服务器安全：

- **处理被暴力破解成功相关告警**

在云安全中心控制台**威胁检测 > 安全告警处理**页面，单击告警操作列的**处理**，在告警处理页面选择**阻断**后，单击**立即处理**。云安全中心将为您生成安全组防御规则，拦截恶意IP的访问。更多信息，请参见查看和处理告警事件。

- **修改服务器用户密码**
  请尽快更换您服务器被暴力破解成功的用户密码，建议您使用复杂密码。
- **使用云安全中心基线检查功能进行风险检测**
  使用云安全中心的基线检查功能全面检测您的服务器安全，并根据建议处理风险项。

> **说明** 仅高级版、企业版和旗舰版支持基线配置检查功能。

为什么修改22端口后仍然出现密码暴力破解提示？

如果您将Linux服务器上的SSH服务的默认端口从22修改为其它端口，您仍然可能收到云安全中心安全告警功能提示的密码暴力破解告警信息。

云安全中心异常登录事件检测会根据尝试登录SSH服务的频繁度，检测是否存在暴力破解攻击行为。因此，即使您已修改SSH服务的默认端口，当恶意攻击者尝试暴力破解您的SSH服务时，云安全中心仍然能正常检测到攻击行为并为您提示告警信息。

如果您的服务器被暴力破解成功，建议您及时对服务器进行安全加固。详细内容，请参见被暴力破解成功之后该怎么处理？

为什么安全组或者防火墙规则已经屏蔽了RDP服务的3389端口，但RDP还是有被暴力破解的记录？

由于Windows登录审核机制的原因， $IPC 、RDP、SAMBA服务的登录审核过程被记录在同一个日志里面，且未区分具体登录方式。所以，在已经屏蔽了RDP服务端口还出现RDP被暴力破解记录时，您需要检查是否还开启了其它两个服务。

检查方法是查看ECS是否有监听135、139、445等端口并且外网IP均可访问，并且查看Windows安全类日志是否在该时段有对应的登录记录。

ECS登录弱口令是指系统层面的RDP或者SSH扫描吗？

弱口令包含两种，一种是RDP和SSH的弱口令，一种是类似CMS管理员后台登录的弱口令。

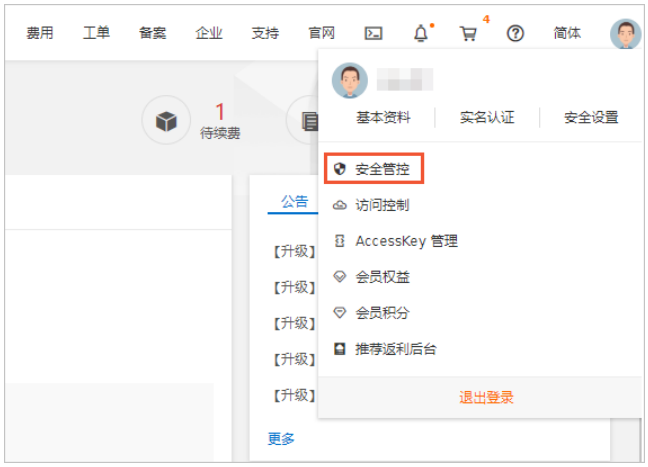
如何处理SSH、RDP远程登录被拦截？

如果您发现当前IP无法远程连接（SSH、RDP）云上服务器，您可以在安全管控管理控制台将登录IP加入到服务器白名单，防止其访问服务器时被拦截。

参照以下步骤，将登录IP地址添加到服务器白名单：

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**设置**，在**设置**页签中的**安全管控**模块，单击**设置**，跳转到安全管控管理控制台。

> **说明** 您也可以将鼠标移至阿里云管理控制台右上角的账户图标，在悬浮菜单中单击**安全管控**进入安全管控管理控制台。



3. 在安全管控管理控制台左侧导航栏，定位到**白名单管理 > IP白名单**页面，单击**添加**。
4. 在**源IP**文本框中输入需要加入IP白名单的IP地址，并配置允许该IP地址登录的服务器。从左侧服务器框中选择目标服务器（可多选），并单击右向箭头，将其添加到右侧白名单配置生效的**已选**服务器框中。

5. 配置完成后，单击**确定**。

高危敏感信息泄露处置方案

企业或个人用户在使用GitHub、码云等中国及中国以外地域代码托管平台时，其托管的源代码中已被发现或可能存在以下敏感信息：阿里云账号AccessKey、RDS账号密码、ECS自建数据库或邮箱的账号密码等。上述账号密码信息在被他人获取后，可以**被直接用来访问用户的阿里云资源和数据资源**，导致企业或个人敏感信息泄露。

如果企业使用ECS自行搭建部署了数据库服务，开发人员可能在数据库连接配置文件里面写入数据库连接密码、邮箱密码等高危敏感信息。如果黑客通过GitHub获取泄露的账号密码，并成功通过认证，则可以轻易获取企业数据，给企业带来极大的安全风险。

解决方案：

- （推荐）使用**私有的**Github代码仓库来管理代码，或搭建企业内部的代码托管系统，防止源代码泄露和敏

感信息泄露。

- 如果发现阿里云AccessKey等高危敏感信息泄露，应立即登录阿里云控制台，禁用并重置AccessKey（或直接删除）；同时尽快删除GitHub托管代码。
- 定期前往日志服务控制台，搜索对应的服务器访问日志，检查数据是否泄漏。例如，检索日志源Web访问日志，选择URI字段，检查包含有AccessKey应用文件的文件路径等。
- 建立企业内部的安全运维规范和开发红线，培训内部IT人员，提高其安全意识，防止信息泄露。

AccessKey的更多信息，请参见阿里云AccessKey。

攻击分析页面的数据来源是哪些产品？

攻击分析页面展示的数据，是云安全中心自动为您识别并拦截基础攻击事件后统计的攻击数据。这些攻击数据是云安全中心防护的云资产的相关数据。您可以在资产中心页面查看哪些资产是受到云安全中心防护的。