威胁检测服务

快速入门

文档版本 09

发布日期 2022-12-02

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

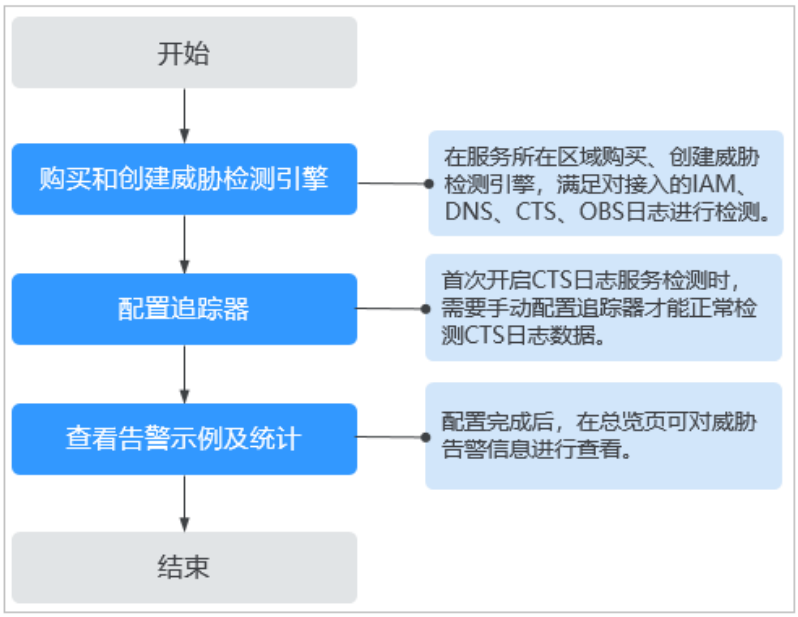
由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 威胁检测服务快速使用流程

在华为云控制台通过购买威胁检测服务，创建威胁检测引擎，配置追踪器实现威胁检测服务的使用，配置流程如图1-1所示。

图 1-1 威胁检测配置使用流程



1.1 步骤一：购买和创建威胁检测引擎

创建威胁检测引擎后，威胁检测服务将实时检测目标Region中接入的各类服务日志数据。

前提条件

已通过主账号对子账号赋予MTD权限。详细操作请参见**如何通过主账号对子账号赋予MTD权限?** 。

须知

当您使用子账号对服务进行创建检测引擎或其它操作时，需要您通过主账号对子账号进行授权才可使用子账号对MTD服务进行操作。

操作步骤详情如下：

1. 需要您创建自定义策略。

在统一身份认证控制台创建自定义策略，操作详情请参见**创建自定义策略**。

2. 需要您给用户的用户组授权。

授予用户的用户组策略权限，操作详情请参见**给用户的用户组授权**。

约束条件

- 目前仅“华南-广州”、“华东-上海一”、“华北-北京四”区域支持购买威胁检测服务。
- 在使用威胁检测服务购买威胁检测引擎时，您只能选择被检测数据的服务所在区域。

操作步骤

步骤1 **登录管理控制台**。

步骤2 单击左上角的，选择区域或项目。

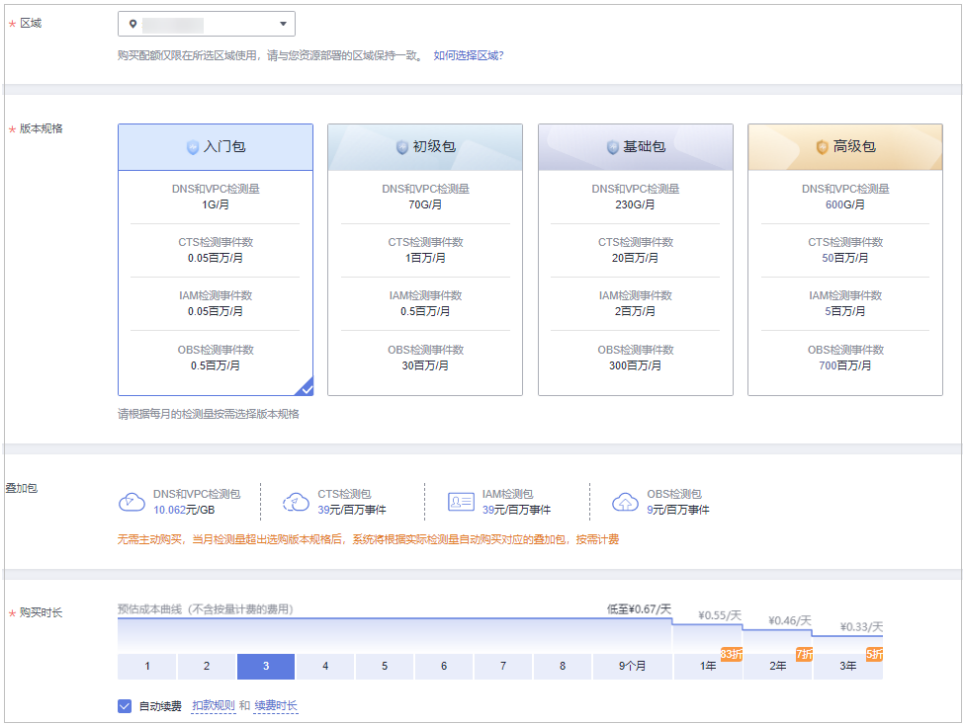
步骤3 在左侧导航树中，单击，选择“安全与合规 > 威胁检测服务”，进入威胁检测服务界面，如**图1-2**所示。

图 1-2 威胁检测服务首页

步骤4 单击“立即购买”，进入购买页面。

步骤5 在“购买威胁检测服务”界面，选择“区域”、“版本规格”和“购买时长”，如**图1-3**所示。

图 1-3 购买威胁检测服务



1. 选择“区域”。

   MTD不支持跨区域使用，请选择需要进行威胁检测的目标区域。

2. 选择“版本规格”。

   可选“入门包”、“初级包”、“基础包”和“高级包”四种规格的检测包，不同的检测包每月所支持检测的日志量存在差异如**表 版本规格说明**所示。威胁检测服务有两种日志检测量计算方式，检测DNS和VPC服务日志按流量计算，检测CTS、IAM和OBS服务日志按事件（一个日志为一个事件）计算。

   表 1-1 版本规格说明

版本规格	DNS和VPC日志检测量	CTS日志检测事件数	IAM日志检测事件数	OBS日志检测事件数
入门包	1G/月	0.05百万/月	0.05百万/月	0.5百万/月
初级包	70G/月	1百万/月	0.5百万/月	30百万/月
基础包	230G/月	20百万/月	2百万/月	300百万/月
高级包	600G/月	50百万/月	5百万/月	700百万/月

3. “叠加包”说明。

   无需主动购买，当月检测用量超出购买的版本规格时，系统自动根据检测量购买对应叠加包，自动按需计费。

4. 选择“购买时长”。

   单击时间轴的点，选择购买时长 ，可以选择1个月～3年的时长。

须知

- 如有备案需求请购买3个月及以上时长。
- 选择购买时长后，可勾选自动续费选框开启自动续费。
  扣款规则：从可用余额扣款，自动续费规则详情请参见**自动续费规则说明**。
  续费时长：如果按月购买，单次续费为一个月，次数不限；如果按年购买，单次续费为一年，次数不限。

步骤6 阅读并勾选《华为威胁检测服务免责声明》和“叠加包使用规则”。

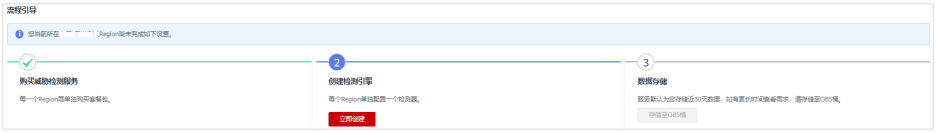
步骤7 单击页面右下角的“立即购买”，进入“订单信息确认”页面。

步骤8 确认购买信息无误，单击右下角“去支付”，进入“付款”页面。

步骤9 选择付款方式完成付款，进入“订单支付成功”页面。

步骤10 单击“返回控制台”，跳转至主控制台，按照**步骤3**重新进入威胁检测服务总览页，“流程引导”显示如**图1-4**所示，表示已购买成功，但还需要您在该区域创建检测引擎，威胁检测服务才会开始检测日志数据。

图 1-4 购买成功



步骤11 单击“创建检测引擎”下的“立即创建”，创建区域检测引擎，单击后待页面运行结束，页面右上角会提示“检测引擎创建成功”，页面会自动刷新一次，单击页面左上方流程引导的 展开流程引导，显示如**图1-5**所示，表示检测引擎创建成功，在页面右上角会显示您购买的规格包。

图 1-5 创建检测引擎成功

说明

首次创建默认开启所有日志检测。

----结束

1.2 步骤二：配置追踪器

在创建威胁检测引擎时，默认开启了CTS服务日志检测，但是此时MTD服务不能正常获取CTS服务的日志数据源，为了保证威胁检测服务能正常获取CTS服务的日志数据源，您需要配置追踪器。

本章节将介绍配置追踪器的详细操作。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 威胁检测服务”，进入威胁检测服务界面。

总览页界面提示“以下服务无法直接获取日志数据，需要您进行配置”的提示框，如图1-6所示。

图 1-6 追踪器配置提醒

步骤4 单击“创建追踪器”，跳转至CTS追踪器页面，在追踪器列表找到“追踪器类型”为“管理事件”的唯一默认追踪器，如图1-7所示。

图 1-7 管理事件追踪器

步骤5 单击目标“操作”列的“配置”，进入配置追踪器页面。

1. 在基本信息页面中，默认生成追踪器名称，无需配置。
2. 单击“下一步”，进入配置转储页面。
3. 在配置转储页面，单击“转储到LTS”后的，开启转储。

图 1-8 配置转储

4. 单击“下一步”，进入预览页面。
5. 确认无误后，单击“配置”。

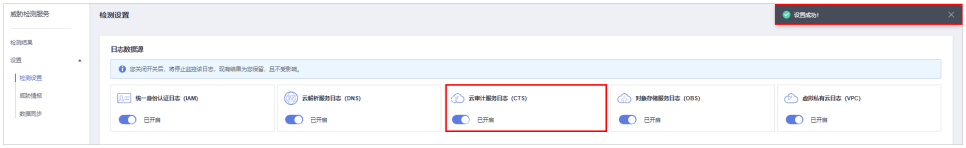
步骤6 在左侧导航树中，单击 ，选择“安全与合规 > 威胁检测服务”，返回威胁检测服务界面。

步骤7 在页面左上角选择“设置>检测设置”,进入检测设置界面，单击“云审计服务日志（CTS）”后的 ，在弹出的关闭确认窗口中单击“确认”关闭CTS日志检测，如**图 关闭云审计服务日志**所示。结束操作后，页面右上角提示“设置成功！”。

图 1-9 关闭云审计服务日志

步骤8 再次单击“云审计服务日志（CTS）”后的 ，开启CTS日志检测，页面右上角提示“设置成功！”，如**图 开启云审计服务日志**所示。

图 1-10 开启云审计服务日志



步骤9 在页面左上角选择“检测结果”进入检测结果页面，此时页面中“以下服务无法直接获取日志数据，需要您进行配置”的提示框已关闭，并且显示已开启云审计服务日志数据检测，表示配置追踪器成功。如**图 配置追踪器成功**所示。

图 1-11 配置追踪器成功

----结束

2 查看告警示例及统计

2.1 IAM 告警类型详情

Attacker

发现与历史情报相似的恶意攻击IP访问。

默认严重级别：中危。

数据源：IAM日志。

此调查结果通知您，有发现与历史情报相似的恶意攻击IP访问IAM账号。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

BlackList

发现与历史情报相似的黑名单IP访问。

默认严重级别：中危。

数据源：IAM日志。

此调查结果通知您，有发现与历史情报相似的恶意攻击IP访问IAM账号。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

CnC

发现与历史情报相似的CNC服务器IP访问。

默认严重级别：中危。

数据源：IAM日志。

此调查结果通知您，有发现与历史情报相似的恶意攻击IP访问IAM账号。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

Compromised

发现与历史情报相似的渗透IP访问。

默认严重级别：中危。

数据源：IAM日志。

此调查结果通知您，有发现与历史情报相似的恶意攻击IP访问IAM账号。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

Crawler

发现与历史情报相似的爬虫IP访问。

默认严重级别：中危。

数据源：IAM日志。

此调查结果通知您，有发现与历史情报相似的恶意攻击IP访问IAM账号。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

DDoS

发现与历史情报相似的DDoSIP访问。

默认严重级别：中危。

数据源：IAM日志。

此调查结果通知您，有发现与历史情报相似的恶意攻击IP访问IAM账号。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

Exploit

发现与历史情报相似的漏洞利用IP访问。

默认严重级别：中危。

数据源：IAM日志。

此调查结果通知您，有发现与历史情报相似的恶意攻击IP访问IAM账号。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

MaliciousSite

发现与历史情报相似的恶意网站IP访问（检测目的ip）。

默认严重级别：中危。

数据源：IAM日志。

此调查结果通知您，有发现与历史情报相似的恶意攻击IP访问IAM账号。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

Malware

发现与历史情报相似的恶意软件IP访问。

默认严重级别：中危。

数据源：IAM日志。

此调查结果通知您，有发现与历史情报相似的恶意攻击IP访问IAM账号。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

Miner

发现与历史情报相似的挖矿攻击IP访问。

默认严重级别：中危。

数据源：IAM日志。

此调查结果通知您，有发现与历史情报相似的恶意攻击IP访问IAM账号。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

MiningPool

发现与历史情报相似的矿池IP访问（检测目的ip）。

默认严重级别：中危。

数据源：IAM日志。

此调查结果通知您，有发现与历史情报相似的恶意攻击IP访问IAM账号。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

Payment

发现与历史情报相似的欺诈付款网站IP访问（检测目的ip）。

默认严重级别：中危。

数据源：IAM日志。

此调查结果通知您，有发现与历史情报相似的恶意攻击IP访问IAM账号。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

Phishing

发现与历史情报相似的钓鱼网站IP访问。

默认严重级别：中危。

数据源：IAM日志。

此调查结果通知您，有发现与历史情报相似的恶意攻击IP访问IAM账号。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

Proxy

发现与历史情报相似的代理IP访问。

默认严重级别：中危。

数据源：IAM日志。

此调查结果通知您，有发现与历史情报相似的恶意攻击IP访问IAM账号。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

Scanner

发现与历史情报相似的恶意扫描IP访问。

默认严重级别：中危。

数据源：IAM日志。

此调查结果通知您，有发现与历史情报相似的恶意攻击IP访问IAM账号。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

SinkHole

发现与历史情报相似的Sinkhole攻击IP访问。

默认严重级别：中危。

数据源：IAM日志。

此调查结果通知您，有发现与历史情报相似的恶意攻击IP访问IAM账号。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

Spammer

发现与历史情报相似的垃圾邮件IP访问。

默认严重级别：中危。

数据源：IAM日志。

此调查结果通知您，有发现与历史情报相似的恶意攻击IP访问IAM账号。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

Suspicious

发现与历史情报相似的可疑IP访问。

默认严重级别：中危。

数据源：IAM日志。

此调查结果通知您，有发现与历史情报相似的恶意攻击IP访问IAM账号。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

Tor

发现与历史情报相似的洋葱网络IP访问。

默认严重级别：中危。

数据源：IAM日志。

此调查结果通知您，有发现与历史情报相似的恶意攻击IP访问IAM账号。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

Zombie

发现与历史情报相似的恶意网站、僵尸网络IP访问。

默认严重级别：中危

数据源：IAM日志。

此调查结果通知您，有发现与历史情报相似的恶意攻击IP访问IAM账号。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

Bruteforce

账号存在口令方式尝试暴力破解。

默认严重级别：中危。

数据源：IAM日志。

此调查结果通知您，本IAM账号疑似受到暴力破解，请确认本账号是否存在弱口令/口令泄露风险。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

BruteforceSuccess

账号存在口令方式疑似已被暴力破解成功。

默认严重级别：高危。

数据源：IAM日志。

此调查结果通知您，本IAM账号疑似受到暴力破解，口令疑似已泄露。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

AkSkLeakage

AKSK凭据存在泄露风险。

默认严重级别：中危。

数据源：IAM日志。

此调查结果通知您，本IAM账号AK被尝试利用，请确认本账号AK和SK是否存在泄露风险。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

AkSkLeakageSuccess

AKSK凭据疑似已泄露。

默认严重级别：高危。

数据源：IAM日志。

此调查结果通知您，本IAM账号AK和SK疑似已泄露。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

BlindIpLogin

未授权IP账号登录尝试。

默认严重级别：中危。

数据源：IAM日志。

此调查结果通知您，本IAM账号被未授权IP尝试多次登录，请确认本账号是否存在弱口令/口令泄露风险

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

BlindIpLoginSuccess

未授权IP账号登录成功。

默认严重级别：高危。

数据源：IAM日志。

此调查结果通知您，本IAM账号被未授权IP登录成功，口令疑似已泄露。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

IllegalAssume

账号存在被尝试建立异常委托。

默认严重级别：中危。

数据源：IAM日志。

此调查结果通知您，本IAM账号出现异常委托行为，请确认本账号是否存在委托风险。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

IllegalAssumeSuccess

账号存在疑似已被建立异常委托成功。

默认严重级别：高危。

数据源：IAM日志。

此调查结果通知您，本IAM账号出现异常委托行为，疑似建立恶意委托。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

TokenLeakage

Token存在被恶意利用。

默认严重级别：中危。

数据源：IAM日志。

此调查结果通知您，本IAM账号出现异常Token利用，请确认本账号是否存在Token泄露风险。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

TokenLeakageSuccess

Token存在被恶意利用成功。

默认严重级别：高危。

数据源：IAM日志。

此调查结果通知您，本IAM账号出现异常Token利用，Token疑似已泄露。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

2.2 CTS 告警类型详情

NetworkPermissions

发现与历史情报相似的恶意IP尝试调用一个API，该API通常用于更改您的账户中的安全组、路由和ACL的网络访问权限。

严重级别：非固定，MTD根据告警实际威胁程度定级。

数据源：CTS日志。

此调查结果通知您，发现与历史情报相似的恶意IP尝试调用一个API，该API通常用于更改您的账户中的安全组、路由和ACL的网络访问权限。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

ResourcePermissions

发现与历史情报相似的恶意IP尝试调用一个API，该API通常用于更改您的账户中各种资源的安全访问策略。

严重级别：非固定，MTD根据告警实际威胁程度定级。

数据源：CTS日志。

此调查结果通知您，发现一个与历史情报相似的恶意IP尝试调用API，该API通常用于更改您的账户中各种资源的安全访问策略。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

UserPermissions

发现与历史情报相似的恶意IP尝试调用一个API，该API通常用于在您的账户中添加、修改或删除IAM用户、组或策略。

严重级别：非固定，MTD根据告警实际威胁程度定级。

数据源：CTS日志。

此调查结果通知您，发现一个与历史情报相似的恶意IP尝试调用API，该API通常用于在您的账户中添加、修改或删除IAM用户、组或策略。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

ComputeResources

发现与历史情报相似的恶意IP尝试调用一个API，该API通常用于启动计算资源，如ECS实例。

严重级别：非固定，MTD根据告警实际威胁程度定级。

数据源：CTS日志。

此调查结果通知您，发现一个与历史情报相似的恶意IP尝试调用API，该API通常用于启动计算资源，如ECS实例。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

PasswordPolicyChange

发现与历史情报相似的恶意IP尝试修改账户密码策略。

严重级别：非固定，MTD根据告警实际威胁程度定级。

数据源：CTS日志。

此调查结果通知您，发现一个与历史情报相似的恶意IP尝试修改账户密码策略。

修复建议：

如果此IP为您正常使用IP，请添加到MTD的白名单中。

2.3 DNS 告警类型详情

DGA

访问通过算法生成的域。此类域通常由恶意软件使用，并且可能表示虚拟机被盗用。

默认严重级别：高危。

数据源：DNS日志。

此调查结果通知您，发现一台虚拟机访问通过算法生成的域。此类域通常由恶意软件使用，并且可能表示虚拟机被盗用。

修复建议：

如果此虚拟机IP为您正常使用IP，请添加到MTD的白名单中。

Tunnel

访问通过算法生成的域隧道通信。此类域通常由恶意软件使用，并且可能表示虚拟机被盗用。

默认严重级别：高危。

数据源：DNS日志。

此调查结果通知您，发现一台虚拟机访问通过算法生成的域隧道通信。此类域通常由恶意软件使用，并且可能表示虚拟机被盗用。

修复建议：

如果此虚拟机IP为您正常使用IP，请添加到MTD的白名单中。

Adware

发现与历史情报相似的广告软件访问。

默认严重级别：中危。

数据源：DNS日志。

此调查结果通知您，发现一个与历史情报相似的恶意广告软件访问。

修复建议：

如果此虚拟机IP为您正常使用IP，请添加到MTD的白名单中。

CnC

发现与历史情报相似的CNC服务器访问。

默认严重级别：中危。

数据源：DNS日志。

此调查结果通知您，发现一个与历史情报相似的CNC服务器访问。

修复建议：

如果此虚拟机IP为您正常使用IP，请添加到MTD的白名单中。

Exploit

发现与历史情报相似的漏洞利用域名访问。

默认严重级别：中危。

数据源：DNS日志。

此调查结果通知您，发现一个与历史情报相似的漏洞利用域名访问。

修复建议：

如果此虚拟机IP为您正常使用IP，请添加到MTD的白名单中。

MaliciousSite

发现与历史情报相似的恶意网站访问。

默认严重级别：中危。

数据源：DNS日志。

此调查结果通知您，发现一个与历史情报相似的恶意网站访问。

修复建议：

如果此虚拟机IP为您正常使用IP，请添加到MTD的白名单中。

Malware

发现与历史情报相似的恶意软件访问。

默认严重级别：中危。

数据源：DNS日志。

此调查结果通知您，发现一个与历史情报相似的恶意软件访问。

修复建议：

如果此虚拟机IP为您正常使用IP，请添加到MTD的白名单中。

Miner

发现与历史情报相似的矿机访问。

默认严重级别：中危。

数据源：DNS日志。

此调查结果通知您，发现一个与历史情报相似的矿机访问。

修复建议：

如果此虚拟机IP为您正常使用IP，请添加到MTD的白名单中。

MiningPool

发现与历史情报相似的矿池访问。

默认严重级别：中危。

数据源：DNS日志。

此调查结果通知您，发现一个与历史情报相似的矿池访问。

修复建议：

如果此虚拟机IP为您正常使用IP，请添加到MTD的白名单中。

Payment

发现与历史情报相似的支付域名访问。

默认严重级别：中危。

数据源：DNS日志。

此调查结果通知您，发现一个与历史情报相似的支付域名访问。

修复建议：

如果此虚拟机IP为您正常使用IP，请添加到MTD的白名单中。

Phishing

发现与历史情报相似的钓鱼网站访问。

默认严重级别：中危。

数据源：DNS日志。

此调查结果通知您，发现一个与历史情报相似的钓鱼网站访问。

修复建议：

如果此虚拟机IP为您正常使用IP，请添加到MTD的白名单中。

Spammer

发现与历史情报相似的垃圾邮件访问。

默认严重级别：中危。

数据源：DNS日志。

此调查结果通知您，发现一个与历史情报相似的垃圾邮件访问。

修复建议：

如果此虚拟机IP为您正常使用IP，请添加到MTD的白名单中。

Suspicious

发现与历史情报相似的可疑访问。

默认严重级别：中危。

数据源：DNS日志。

此调查结果通知您，发现一个与历史情报相似的可疑访问。

修复建议：

如果此虚拟机IP为您正常使用IP，请添加到MTD的白名单中。

2.4 OBS 告警类型详情

UserFirstAccess

发现OBS中有特定用户（user）首次访问桶对象。

默认严重级别：低危。

数据源：OBS日志。

此调查结果通知您，有用户首次访问这个桶，此用户没有此桶的历史访问记录。

修复建议：

如果此用户不是此桶的授权用户，则可能表明凭据已被公开或您的OBS权限限制性不够，请修复受损的OBS存储桶的权限访问策略。

IPFirstAccess

发现OBS中有特定IP首次访问桶对象。

默认严重级别：低危。

数据源：OBS日志。

此调查结果通知您，有IP首次访问这个桶，此IP没有此桶的历史访问记录。

修复建议：

如果此IP不是此桶的授权IP，则可能表明凭据已被公开或者OBS权限限制性不够，请修复受损的OBS存储桶权限访问策略，或者增加OBS防盗链增加威胁情报。

ClientFirstAccess

发现OBS中有以新的客户端访问桶对象。

默认严重级别：低危。

数据源：OBS日志。

此调查结果通知您，有客户端首次访问这个桶，此客户端没有此桶的历史访问记录。

修复建议：

如果此用户使用的客户端，不是业务常规使用方式，请修复受损的OBS存储桶权限访问策略，或者增加OBS防盗链增加威胁情报。

UserFirstCrossDomainAccess

OBS实例的行为方式可能表明它正在被不属于您账户下的用户首次访问。

默认严重级别：低危。

数据源：OBS日志。

此调查结果通知您，有不属于您账户下的用户首次访问桶，此客户端没有此桶的历史访问记录。

修复建议：

如果此用户不是此桶的授权用户，则可能表明凭据已被公开或您的OBS权限限制性不够，请修复受损的OBS存储桶权限访问策略。

UserAccessFrequencyAbnormal

发现用户访问特定桶的频率出现异常。

默认严重级别：低危。

数据源：OBS日志。

此调查结果通知您，您账户下的用户访问这个桶的频率出现异常。

修复建议：

如果此用户访问OBS频次异常属于非正常使用，则可能表明您的OBS权限限制性不够，请修复受损的OBS存储桶权限访问策略。

IPAccessFrequencyAbnormal

发现特定IP访问特定桶的频率出现异常。

默认严重级别：低危。

数据源：OBS日志。

此调查结果通知您，此IP访问这个桶的频率出现异常。

修复建议：

如果此IP访问OBS频次异常属于非正常使用，则可能表明您的OBS权限限制性不够，请修复受损的OBS存储桶权限访问策略。

UserDownloadAbnormal

发现用户下载行为异常。

默认严重级别：低危。

数据源：OBS日志。

此调查结果通知您，此用户在这个桶的下载量出现异常。

修复建议：

如果此用户下载异常行为属于非正常使用，则可能表明凭据已被公开或您的OBS权限限制性不够，请修复受损的OBS存储桶权限访问策略。

UserIPDownloadAbnormal

发现用户使用特定IP下载行为异常。

默认严重级别：低危。

数据源：OBS日志。

此调查结果通知您，此用户使用特定IP在这个桶的下载量出现异常。

修复建议：

如果此用户使用此IP下载异常行为属于非正常使用，则可能表明凭据已被公开或您的OBS权限限制性不够，请修复受损的OBS存储桶权限访问策略。

UnauthorizedAccess

发现非授权访问。

默认严重级别：低危。

数据源：OBS日志。

此调查结果通知您，在此时间段范围，这个桶的API 操作出现多次权限错误。

修复建议：

如果此用户是此桶的授权用户，则可在权限访问策略添加权限，否则在OBS防盗链增加黑名单。

UserHourLevelAccessAbnormal

发现用户小时时段访问异常。

默认严重级别：低危。

数据源：OBS日志。

此调查结果通知您，在和历史每天的同一时间段范围内，这个桶的API 操作频率出现异常。

修复建议：

如果此访问方式异常，不是业务常规使用方式，请修复受损的OBS存储桶的权限访问策略。

IPSwitchAbnormal

IP切换异常。

默认严重级别：低危。

数据源：OBS日志。

此调查结果通知您，在此时间段范围内，这个桶被多个IP操作访问API，使用IP的数量和您历史行为不一致。

修复建议：

如果此访问方式异常，不是业务常规使用方式，则可能表明您的OBS权限限制性不够，请修复受损的OBS存储桶权限访问策略，或者增加OBS防盗链增加威胁情报。

2.5 VPC 告警类型详情

DDoSTcpDns

在租户侧网络场景下，检测到某些ECS可能正在基于DNS协议进行Dos攻击，端口为53。

默认严重等级：高危。

数据源：VPC流日志。

此调查结果通知您，检测到某些ECS可能正在基于DNS协议进行Dos攻击，端口为53。

修复建议：如果此事件为异常行为，则您的ECS有可能遭到攻击，请查看端口为53的进程是否出现异常，并清除任何发现的恶意软件，如有必要，建议您终止当前ECS，根据需要使用新ECS来做代替。

DDoSTcp

在租户侧网络场景下，检测到某些ECS可能正被用于TCP协议进行DoS攻击，使入口 | 出口流量会瞬间暴增。

默认严重等级：高危。

数据源：VPC流日志。

此调查结果通知您，检测到某些ECS可能正被用于TCP协议进行DoS攻击，使入口 | 出口流量会瞬间暴增。

修复建议：如果此事件为异常行为，则您的ECS有可能遭到攻击，请查看是否存在可疑进程，并清除任何发现的恶意软件，如有必要，建议您终止当前ECS，根据需要使用新ECS来做代替。

DDoSUdp

在租户侧网络场景下，检测到某些ECS可能正被用于UDP协议进行DoS攻击，使入口| 出口流量会瞬间暴增。

默认严重等级：高危。

数据源：VPC流日志。

此调查结果通知您，检测到某些ECS可能正被用于UDP协议进行DoS攻击，使入口| 出口流量会瞬间暴增。

修复建议：如果此事件为异常行为，则您的ECS有可能遭到攻击，请查看是否存在可疑进程，并清除任何发现的恶意软件，如有必要，建议您终止当前ECS，根据需要使用新ECS来做代替。

DDoSTcp2Udp

在租户侧网络场景下，检测到某些ECS可能正在TCP端口上使用UDP协议进行DoS攻击。 例如，端口80常用于tcp通信，但某个时间点发现80端口被用于udp通信，并使入口| 出口流量会瞬间暴增。

默认严重等级：高危。

数据源：VPC流日志。

此调查结果通知您，检测到某些ECS可能正在TCP端口上使用UDP协议进行DoS攻击。例如，端口80常用于tcp通信，但某个时间点发现80端口被用于udp通信，并使入口| 出口流量会瞬间暴增。

修复建议：如果此事件为异常行为，则您的ECS有可能遭到攻击，请查看是否存在可疑进程，并清除任何发现的恶意软件，如有必要，建议您终止当前ECS，根据需要使用新ECS来做代替。

DDoSUnusualProtocol

在租户侧网络场景下，检测到某些ECS可能正在使用异常协议进行DoS攻击。例如除了常见协议TCP、UDP、ICMP、IPv4、IPv6、STP等等以外的协议，出现在流量中，需要引起高度重视。

默认严重等级：高危。

数据源：VPC流日志。

此调查结果通知您，检测到某些ECS可能正在使用异常协议进行DoS攻击。例如除了常见协议TCP、UDP、ICMP、IPv4、IPv6、STP等等以外的协议，出现在流量中，需要引起高度重视。

修复建议：如果此事件为异常行为，则您的ECS有可能遭到攻击，请查看是否存在可疑进程，并清除任何发现的恶意软件，如有必要，建议您终止当前ECS，根据需要使用新ECS来做代替。

JunkMail

在租户侧网络场景下，检测到某些ECS正在基于端口25，跟远程主机通讯并发送垃圾邮件。

默认严重等级：中危。

数据源：VPC流日志。

此调查结果通知您，检测到某些ECS正在基于端口25，跟远程主机通讯并发送垃圾邮件。

修复建议：如果此事件为异常行为，则您的ECS有可能遭到攻击，请查看端口25是否被开启，如有必要请在安全组关闭端口25，并清除任何发现的恶意软件。

UnusualNetworkPort

在租户侧网络场景下，检测到某些ECS可能正在使用异常端口与远程主机通信，可能从事非法活动。异常端口可能来自于任何自定义开放端口。

默认严重等级：中危。

数据源：VPC流日志。

此调查结果通知您，检测到某些ECS可能正在使用异常端口与远程主机通信，可能从事非法活动。异常端口可能来自于任何自定义开放端口。

修复建议：如果此事件为异常行为，则您的ECS有可能遭到攻击，请查看是否存在可疑进程，并清除任何发现的恶意软件，如有必要，建议您终止当前ECS，根据需要使用新ECS来做代替。

UnusualTrafficFlow

在租户侧网络场景下，检测到某些ECS生成大量的网络出口流量，此网络出口流量偏离了正常基线值，并全部流向到远程主机。

默认严重等级：中危。

数据源：VPC流日志。

此调查结果通知您，检测到某些ECS生成大量的网络出口流量，此网络出口流量偏离了正常基线值，并全部流向到远程主机。

修复建议：如果此事件为异常行为，则您的ECS有可能遭到攻击，请查看是否存在可疑进程，并清除任何发现的恶意软件，如有必要，建议您终止当前ECS，根据需要使用新ECS来做代替。

Cryptomining

在租户侧网络场景下，检测到某些ECS可能正在访问与挖矿活动相关联的IP，可能从事非法活动。

默认严重等级：高危。

数据源：VPC流日志。

此调查结果通知您，检测到某些ECS可能正在访问与挖矿活动相关联的IP，可能从事非法活动。

修复建议：如果此事件为异常行为，则您的ECS有可能遭到攻击，请查看是否存在可疑进程，并清除任何发现的恶意软件，如有必要，建议您终止当前ECS，根据需要使用新ECS来做代替。

CommandControlActivity

VPC检测到ECS存在当前IP被用于向高危网络发送消息。

默认严重等级：高危。

数据源：VPC流日志。

此调查结果通知您，MTD 发现当前IP正在访问已知命令和控制相关联的IP，从事非法活动。

修复建议：如果此事件为异常行为，则您的ECS有可能遭到攻击，请查看是否存在可疑进程，并清除任何发现的恶意软件，如有必要，建议您终止当前ECS，根据需要使用新ECS来做代替。

PortDetection

VPC侦测到ECS存在端口探测数量异常。

默认严重等级：高危。

数据源：VPC流日志。

此调查结果通知您，检测到某些ECS正在探测大量IP上的活跃端口，属于慢攻击探测远程端口。

修复建议：如果此事件为异常行为，则您的ECS有可能遭到攻击，请查看是否存在可疑进程，并清除任何发现的恶意软件，如有必要，建议您终止当前ECS，根据需要使用新ECS来做代替。

PortScan

VPC侦测到ECS存在端口扫描访问数量异常。

默认严重等级：中危。

数据源：VPC流日志。

此调查结果通知您，检测到某些ECS正在扫描远程资源的出站端口，可能从事非法活动。

修复建议：如果此事件为异常行为，则您的ECS有可能遭到攻击，请查看是否存在可疑进程，并清除任何发现的恶意软件，如有必要，建议您终止当前ECS，根据需要使用新ECS来做代替。

A 修订记录

发布日期	修改记录
2022-10-26	第七次正式发布。 优化**步骤一：购买和创建威胁检测引擎**章节内容。
2022-01-14	第六次正式发布。 增加检查VPC能力，优化内容描述。 将**步骤一：购买和创建威胁检测引擎**和**步骤二：配置追踪器**合入**威胁检测服务快速使用流程**。 修改**查看告警示例及统计**。
2021-12-13	第五次正式发布。 修改**查看告警示例及统计**。
2021-11-17	第四次正式发布。 修改**步骤一：购买和创建威胁检测引擎**
2021-10-30	第三次正式发布。 购买时新增入门包和初级包的选择说明。
2021-09-29	第二次正式发布。 补充OBS告警类型描述。
2021-07-10	第一次正式发布。