威胁检测服务

用户指南

文档版本 10

发布日期 2022-10-26

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 威胁检测服务使用

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。

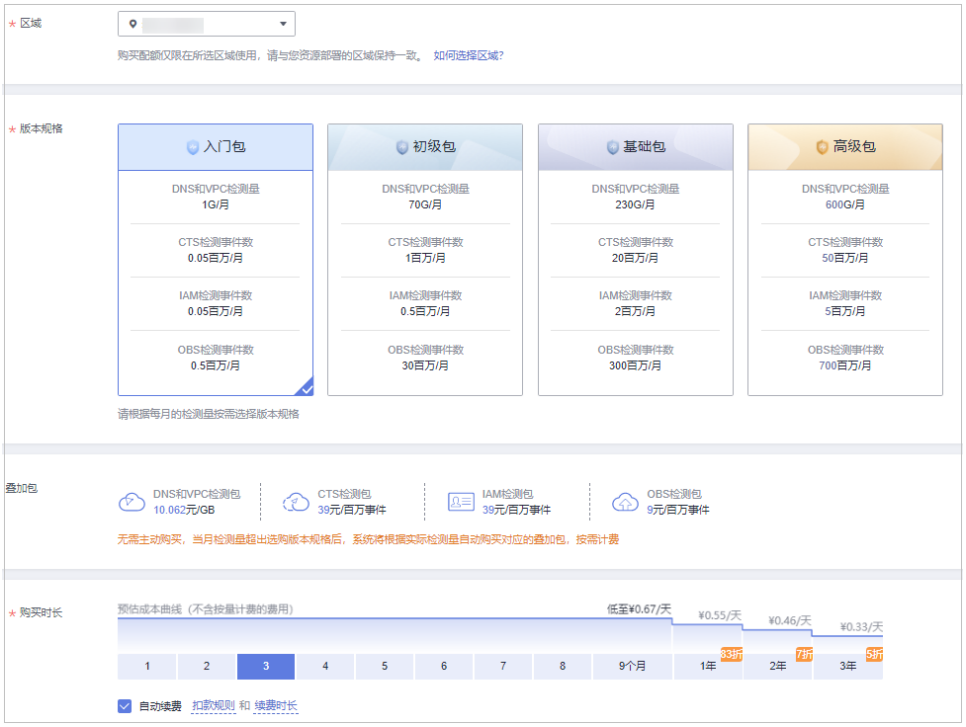
步骤3 在左侧导航树中，单击，选择“安全与合规 > 威胁检测服务”，进入威胁检测服务界面，如图1-1所示。

图 1-1 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1-2所示。

图 1-2 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1-3**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 1-3 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1-4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 1-4 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1-5所示。

图 1-5 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1-6所示。

图 1-6 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。

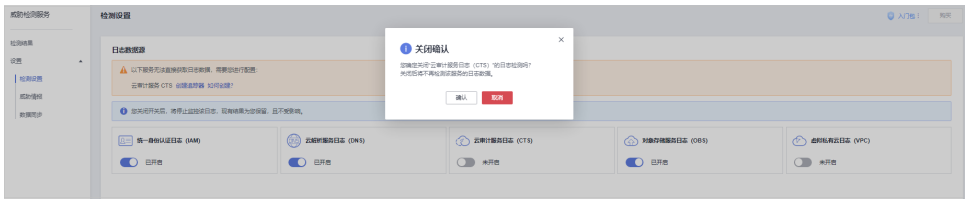
图 1-7 配置转储

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。

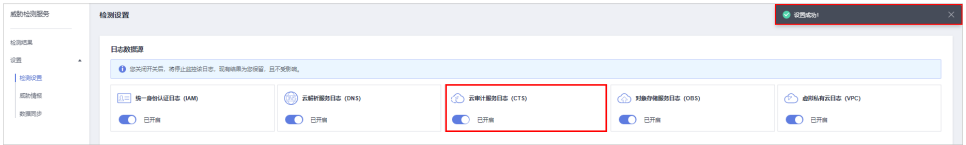
步骤7 在页面左上角选择“设置>检测设置”,进入检测设置界面，单击“云审计服务日志（CTS）”后的 ，在弹出的关闭确认窗口中单击“确认”关闭CTS日志检测，如图 关闭云审计服务日志所示。结束操作后，页面右上角提示“设置成功！”。

图 1-8 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 1-9 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 1-10 配置追踪器成功

----结束

2 威胁检测服务总览

该任务指导您通过“检测结果”界面查看威胁检测服务的概况，包括服务简介、流程引导和告警信息。

前提条件

已成功购买威胁检测服务。

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2-1所示。

图 2-1 威胁检测服务首页

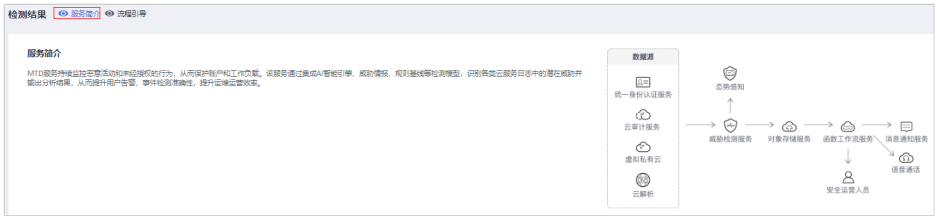
步骤4 查看服务简介。服务简介包含威胁检测服务的服务简介，包含服务介绍和架构。

- 当您所在的Region未够买威胁检测服务时，服务简介下方会出现未购买服务的提示，如图2-2所示，您可以单击“立即购买”进入服务购买界面，够买该服务。

图 2-2 未购买服务

- 当您所在的Region已够买威胁检测服务，服务简介会自动隐藏，单击 展开服务简介，如图2-3所示。

图 2-3 服务简介展开



单击右上角“关闭”后，“服务简介”模块将不再默认显示。

说明

当您未在当前Region够买威胁检测服务时，服务简介模块会默认开启且无法关闭。

步骤5 查看流程引导。

威胁检测服务分为“购买威胁检测服务”、“创建检测引擎”和“数据存储与同步”三个流程。

1. 购买威胁检测服务

   每一个Region需单独购买套餐包，当您所在区域已购买威胁检测服务，当前流程的编号 会显示为 。

2. 创建检测引擎

   每个Region单独配置一个检测器，当您所在区域已创建检测引擎，当前流程的编号 会显示为 。

3. 数据存储。

   存储至OBS桶。

   威胁检测服务默认为您存储近30天的检测结果数据，您需要存储更长的时间（为满足合规要求，您的数据需要存储180天），可单击“存储至OBS桶”，跳转至“数据同步”界面，将检测结果存储至OBS桶，更多详细操作请参见同步检测结果。

4. 单击右上角“关闭”后，“流程引导”模块将不再默认显示。

   说明

   - 当您未在当前Region创建检测引擎并开启全部的日志检测时，流程引导模块会默认开启且无法关闭。
   - 关闭后，可单击界面上方的“流程引导”，再次显示流程引导模块的内容。

步骤6 查看规格包详情。页面右上角会显示购买的规格包名称，鼠标移动至规格包，弹出规格包详情如图2-4所示。

图 2-4 查看规格包信息

步骤7 查看告警示例类型或告警信息，详情请参见查看检测结果。

----结束

3 查看检测结果

该章节指导您通过威胁检测服务查看被检测日志的告警详细信息。

前提条件

已购买威胁检测服务且已开启服务日志威胁检测。

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。

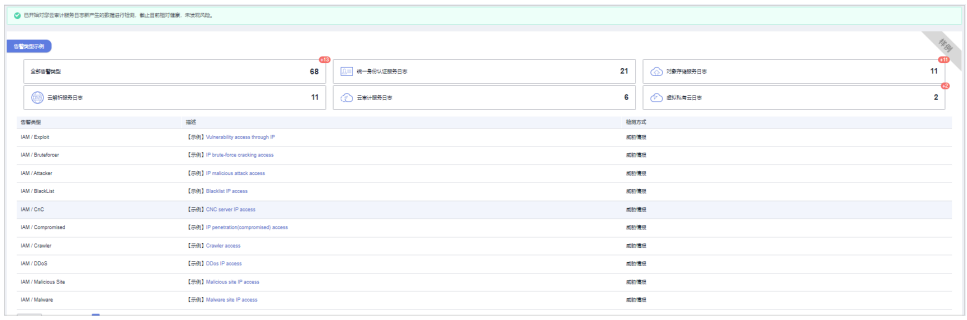
步骤3 在左侧导航树中，单击，选择“安全与合规 > 威胁检测服务”，进入威胁检测服务界面，如图3-1所示。

图 3-1 威胁检测服务首页

步骤4 查看威胁检测结果总览。

- 当未检测出威胁告警时。页面提示“已开始对您全部XX服务日志新产生的数据进行检测，截止目前相对健康，未发现风险。”，并展示告警类型示例，如图3-2所示。

图 3-2 未发现风险



- 当已检测出威胁告警信息时。页面展示告警详情。

  说明

  - 单击“当前已支持XX种告警类型”，页面弹出“告警类型示例”窗口，可查看所有告警类型示例和各服务日志分别的告警类型示例，详情请参见**查看告警类型详情**。
  - 由于AI检测模型的普遍特性，一般上线后需要基于您的真实数据学习训练大致3个月，学习阶段检测结果可能存在误差，您可以在告警列表的“操作”列单击“反馈可信度”反馈出现的问题。

  a. 告警详细信息按照最新发生时间靠前的排序方式进行排序，相关参数说明如**表3-1**所示。

  表 3-1 告警信息

参数名称	参数说明
日志类型	产生该告警的服务日志。 ■ 统一身份认证服务（IAM） ■ 虚拟私有云（VPC） ■ 云解析服务（DNS） ■ 云审计服务（CTS） ■ 对象存储服务（OBS）
告警类型	支持68种告警，更多详细内容请参见**查看告警类型详情**。
标题	告警类型的具体描述。

参数名称	参数说明
严重等级	告警的风险等级，分为： ■ 致命 ■ 高危 ■ 中危 ■ 低危 ■ 提示 告警信息目前需要人工核查处理，建议您参照**查看告警类型详情**对应描述，按照告警等级由高到低的优先级进行处理。
受影响资源	受到威胁攻击的资源个数。
发生次数	该告警产生的次数，可单击切换排序。
首次发生	该告警首次发生的具体时间，可单击切换排序。
最近发生	该告警最近一次发生的具体时间，可单击切换排序。

b. 单击“标题”列的值可查看“结果详情”，如图**图3-3**所示，您可根据告警结果详情的资源名称、ID、类型、区域以及攻击这些主要信息，为处理潜在威胁提供方向。

图 3-3 结果详情

c. 反馈可信度。

说明

反馈可信度：指反馈告警结果是否准确。

- 单条告警反馈。单击“操作”列“反馈可信度”，在弹出窗口中确认反馈的告警信息的准确性，告警结果可信单击“准确”，告警结果与实际情况存在偏差单击“不准确”，如图3-4所示。

图 3-4 告警可信度单条反馈

- 批量告警反馈。选中多条告警信息最左侧的复选框，单击复选框上方“反馈可信度”，在弹出窗口中确认反馈的告警信息的准确性，告警结果可信单击“准确”，告警结果与实际情况存在偏差单击“不准确”，如图3-5所示。

图 3-5 告警可信度批量反馈

----结束

4 查看告警类型详情

4.1 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。

4.2 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。

4.3 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。

4.4 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。

4.5 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。

5 日志检测管理

5.1 开启日志检测

前提条件

已购买威胁检测服务且已创建检测引擎。

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。

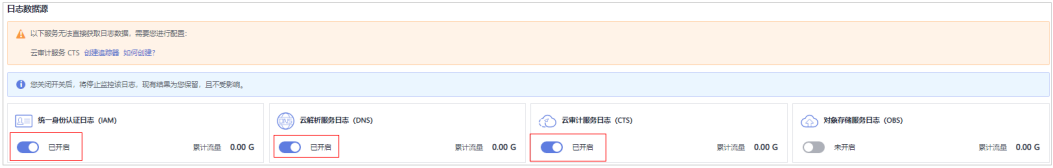
步骤3 在左侧导航树中，单击，选择“安全与合规 > 威胁检测服务”，进入威胁检测服务界面，如图5-1所示。

图 5-1 威胁检测服务首页

步骤4 在左侧选择“设置 > 检测设置”，进入“检测设置”界面。

步骤5 选择需要开启检测的服务日志，单击，服务日志下的图标变为，表示目标服务的日志实时检测已开启，如图5-2所示。

图 5-2 已开启服务日志检测



说明

- 首次开启CTS的服务日志会出现需配置追踪器的提示框，需要您手动配置追踪器，威胁检测服务才能正常对接日志进行威胁检测。
- 单击提示框中的“创建追踪器”，可跳转至追踪器页面配置追踪器，操作详情请参见**配置追踪器**。
- 单击提示框中的“如何创建？”，可跳转至CTS用户指南，查看如何**创建追踪器**。

----结束

5.2 关闭日志检测

该章节指导您关闭Region下的服务日志检测，关闭后停止对服务新产生的日志数据的检测，不影响历史已检测的数据及结果。

前提条件

已购买威胁检测服务且已创建检测引擎。

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5-3**所示。

图 5-3 威胁检测服务首页

步骤4 在左侧选择“设置 > 检测设置”，进入“检测设置”界面。

步骤5 选择需要停止检测的服务日志数据源，单击  ，服务日志下的图标变为  ，表示目标服务的日志实时检测已关闭，如图5-4所示。

图 5-4 已关闭服务日志数据源

说明

关闭开关后，状态显示为“未开启”，MTD将停止对该服务新产生的日志进行检测，但现有的检测结果将会为您保留，且不受影响。

----结束

5.3 查看日志检测信息

您可以查看当前正在检测中的服务日志。

前提条件

已购买威胁检测服务且已创建检测引擎。

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5-5所示。

图 5-5 威胁检测服务首页

步骤4 在左侧选择“设置 > 检测设置”，进入“检测设置”界面。

步骤5 在页签“日志数据源”，可查看开启/未开启日志数据源的检测服务，如图5-6所示，单击对应服务的开关可关闭/开启对应服务的日志数据源检测，相关参数说明如表5-1所示。

图 5-6 日志数据源

表 5-1 日志检测

参数	说明
开关状态	是否开启该服务的日志检测。 •  ：开启状态 •  ：关闭状态
累计流量	从开启服务日志检测到当前，累计的日志检测总量。

----结束

6 威胁情报管理

6.1 导入威胁情报

该章节指导您导入Plaintext格式的第三方威胁情报数据源及可信IP列表，导入后服务将优先关联检测您导入的情报内的IP地址或域名进行威胁检测。

前提条件

Plaintext格式的威胁情报已上传至对象存储服务，上传威胁情报至对象存储服务的具体方法请参见**上传文件**。

说明

- 情报：也称作黑名单，指受访问时被禁止的IP或域名，目前只能新增1个情报文件，文件内可容纳10000条IP或域名记录。
- Plaintext格式：您的可信IP列表和情报列表中，IP地址范围必须每行显示一个，详情请参见**如何编辑Plaintext格式的对象？**。

6.2 删除威胁情报

该章节指导您删除导入的威胁情报文件。

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。

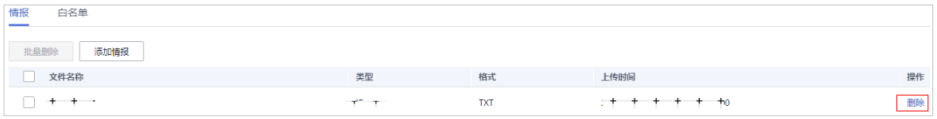
步骤3 在左侧导航树中，单击，选择“安全与合规 > 威胁检测服务”，进入威胁检测服务界面，如**图6-1**所示。

图 6-1 威胁检测服务首页

步骤4 在左侧选择“设置 > 威胁情报”，进入“威胁情报”界面。

步骤5 在待删除的威胁情报文件的“操作”列，单击“删除”，如图6-2所示。

图 6-2 删除情报



步骤6 在弹出的“删除情报”对话框中，单击“是”，完成删除情报文件。

----结束

6.3 查看威胁情报信息

您可以查看威胁情报的具体信息，包括文件名称、文件类型、文件格式和文件上传时间。

前提条件

已导入威胁情报，导入威胁情报详细操作请参见**导入威胁情报**。

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6-3所示。

图 6-3 威胁检测服务首页

步骤4 在左侧选择“设置 > 威胁情报”，进入“威胁情报”界面。

步骤5 查看威胁情报的详细信息，如表6-1所示。

表 6-1 威胁情报

参数	说明
文件名称	威胁情报文件的名称。
类型	威胁情报文件的类型，包括“IP”和“域名”。
格式	威胁情报文件的格式，目前仅支持Plaintext格式的文件，详情请参见**如何编辑Plaintext格式的对象？**。
上传时间	威胁情报文件的上传时间。

----结束

7 白名单管理

7.1 导入白名单

该章节指导您导入Plaintext格式的可信IP列表，导入后服务将基于您情报内的IP地址或域名进行威胁检测。

前提条件

Plaintext格式的白名单已上传至对象存储服务，上传白名单至对象存储服务的具体方法请参见**上传文件**。

说明

- 目前只能新增1个白名单文件，文件内可容纳10000条IP或域名记录。
- Plaintext格式：您的可信IP列表和情报列表中，IP地址范围必须每行显示一个，详情请参见**如何编辑Plaintext格式的对象？**。

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7-1**所示。

图 7-1 威胁检测服务首页

步骤4 在左侧选择“设置 > 威胁情报”，进入“威胁情报”界面。

步骤5 选择“白名单 > 添加白名单”，弹出“添加白名单”对话框，如图1所示，相关参数如表1所示。

图 7-2 添加白名单

表 7-1 白名单参数说明

参数名称	参数说明	取值样例
文件名称	添加的白名单文件名称，建议自定义。	SecurityList

参数名称	参数说明	取值样例
对象类型	选择需要从OBS桶添加至MTD服务的对象文件类型。 ● IP：服务将基于您白名单内的IP地址进行威胁检测。 ● 域名：服务将基于您白名单内的域名进行威胁检测。 添加至MTD白名单后，威胁检测服务将优先关联检测白名单内的IP或域名，对日志中存在关联的白名单信息进行忽略。	IP
桶名称	对象文件所在的OBS桶名称。 **说明** 如果没有可选择的OBS桶，可单击“查看/创建桶”，进入对象存储服务管理控制台，查看/创建OBS桶，更多详细操作请参见**创建桶**。	obs-mtd-bejing4
对象名称	桶内存储情报信息的对象名称。 **须知** 填写对象名称时文件扩展名也需要填写。	mtd-securitylist-ip.txt
存储路径	情报在OBS桶的存储路径。	obs://obsmtd-beijing4/mtd-securitylistip.txt

步骤6 确认信息无误，单击“确定”，导入的文件显示在白名单列表，表示白名单导入成功。

----结束

7.2 删除白名单

该章节指导您删除上传的白名单文件。

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。

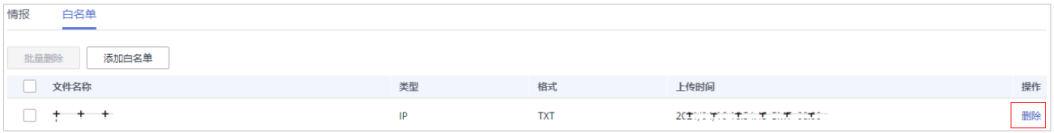
步骤3 在左侧导航树中，单击，选择“安全与合规 > 威胁检测服务”，进入威胁检测服务界面，如**图7-3**所示。

图 7-3 威胁检测服务首页

步骤4 在左侧选择“设置 > 威胁情报”，进入“威胁情报”界面。

步骤5 选择“白名单”页签，在待删除的白名单文件的“操作”列，单击“删除”，如图7-4所示。

图 7-4 删除白名单



步骤6 在弹出的“删除白名单”对话框中，单击“是”，完成删除白名单文件。

----结束

7.3 查看白名单信息

您可以查看白名单的具体信息，包括文件名称、文件类型、文件格式和文件上传时间。

前提条件

已导入白名单，导入白名单详细操作请参见导入白名单。

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7-5所示。

图 7-5 威胁检测服务首页

步骤4 在左侧选择“设置 > 威胁情报”，进入“威胁情报”界面。

步骤5 选择“白名单”页签，查看白名单的详细信息，如表7-2所示。

表 7-2 白名单

参数	说明
文件名称	白名单文件的名称。
类型	白名单文件的类型，包括“IP”和“域名”。
格式	白名单文件的格式，目前仅支持Plaintext格式的文件，详情请参见**如何编辑Plaintext格式的对象？**。
上传时间	白名单文件的上传时间。

----结束

8 同步检测结果

威胁检测服务告警结果默认保存30天，按照等保合规要求数据至少需要存储180天，为了满足等保合规要求对于MTD数据的存储要求，需将MTD数据转存至OBS桶满足等保合规要求。

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8-1所示。

图 8-1 威胁检测服务首页

步骤4 在左侧选择“设置 > 数据同步”，进入“数据同步”界面。

步骤5 存储检测结果。

- 单击“存储至OBS桶”后的开启转存，如图8-2所示，将检测结果按照指定的频率存储至OBS桶，相关参数说明如表8-1所示。

图 8-2 存储至 OBS 桶

表 8-1 存储检测结果

参数名称	参数说明	取值样例
结果更新频率	威胁检测服务是实时检测的方式，你可自定义将检测结果数据存储到OBS桶的频率。 – 每30分钟更新一次 – 每1小时更新一次（默认） – 每3小时更新一次	每30分钟更新一次
桶名称	输入存储告警数据的OBS桶名称。 **说明** 如果没有可选择的OBS桶，可单击“查看/创建桶”，进入对象存储服务管理控制台，查看/创建OBS桶，更多详细操作请参见**创建桶**。	obs-mtd-beijing4
对象名称	存储告警信息的对象名称。可填写桶内已有对象名称，也可自行定义，自定义对象名称若不存在，OBS桶将自行创建，建议您自定义对象名称。	mtd-warning-data
存储路径	检测结果在OBS桶的存储路径。	obs://obs-mtd-beijing4/mtd-warning-data

- 单击“存储至OBS桶”后的  ，在弹出的“关闭确认”对话框中单击“确认”，可不再将新的检测结果数据存储至OBS桶。

----结束

9 设置告警通知

MTD可以将检测出的异常行为（潜在的恶意活动、未经授权行为等）通过短信或邮件的方式发送给用户。

设置告警通知需要联动态势感知服务（SA）对接消息通知服务（SMN）来实现，具体操作方法见本章节进行处理。

前提条件

- 已购买MTD并创建威胁检测引擎，具体操作请参见**购买和创建威胁检测引擎**。
- 已购买态势感知**“标准版”**或**“专业版”**。
- 已开通消息通知服务。

说明

消息通知服务为付费服务，价格详情请参见**SMN价格详情**。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知页面。

步骤3 在左侧导航栏选择“设置 > 通知设置”，并在设置页面，选择“告警设置 > 通知告警”

步骤4 通知项目选择“异常行为”，并选择重点关注的告警等级。

图 9-1 告警通知设置页面

- 每日告警通知

  每日告警通知会在每天10:00向您发送告警通知消息。

  只有当“通知项目”选中“异常行为”且“告警等级”有选项被选中时，每日告警通知才能够生效。

- 实时告警通知

  实时告警通知会在威胁告警发生后的整点时刻向您发送告警提示消息。

  只有当“通知项目”选中“异常行为”且“告警等级”有选项被选中时，实时告警通知才能够生效。

  为了避免过多信息打扰您的日常工作，除了全天通知，您还可以选择仅在特定时段发送实时告警通知。在通知时间栏选择“24小时”或指定时间段。

步骤5 选择消息通知主题。

- 通过下拉框选择已有的主题，或者单击“查看消息通知主题”创建新的主题，具体操作请参见**创建主题**。
- 每个消息通知主题可添加多个订阅，并可选择多种订阅终端（例如短信、邮件等），详细订阅说明请参见**添加订阅**。

  说明

  在选择主题前，请确保您主题中订阅状态为“已确认”，即当前订阅终端可用，否则可能不能收到告警通知。

更多关于主题和订阅的信息，请参见《消息通知服务用户指南》。

步骤6 单击“应用”，生效告警通知。

----结束

10 权限管理

10.1 创建用户组并授权使用 MTD

如果您需要对您所拥有的MTD进行精细的权限管理，您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用MTD资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将MTD资源委托给更专业、高效的其他账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用MTD服务的其它功能。

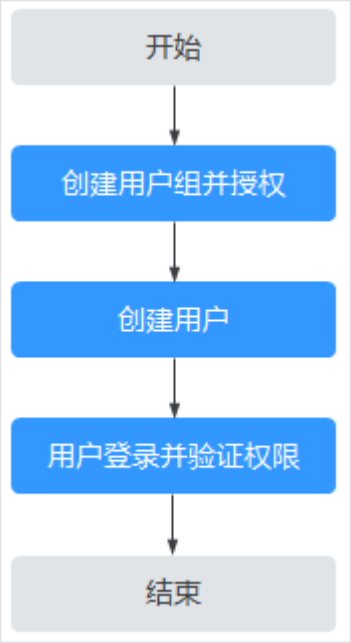
本章节为您介绍对用户授权的方法，操作流程如**图10-1**所示。

前提条件

给用户组授权之前，请您了解用户组可以添加的MTD权限，并结合实际需求进行选择。若您需要对除MTD之外的其它服务授权，IAM支持服务的所有权限请参见**系统权限**。

示例流程

图 10-1 给用户授权服务权限流程



1. **创建用户组并授权**
   在统一身份认证控制台创建用户组，并授予MTD权限。
2. **创建用户并加入用户组**
   在统一身份认证控制台创建用户，并将其加入**1**中创建的用户组。
3. **创建自定义策略**
   创建自定义策略。
4. **用户登录**并验证权限
   新创建的用户登录控制台，切换至授权区域，验证权限：
   在“服务列表”中选择除MTD外（假设当前策略仅包含MTD）的任一服务，若提示权限不足，表示MTD已生效。

A 修订记录

发布日期	修改记录
2022-10-26	第十次正式发布。 优化**步骤一：购买和创建威胁检测引擎**章节内容。
2022-05-06	第九次正式发布。 增加**设置告警通知**章节，说明告警通知设置方式。
2022-01-14	第八次正式发布。 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**威胁检测服务使用**。 修改**查看告警类型详情**。
2021-12-13	第七次正式发布。 修改**查看告警类型详情**。
2021-11-17	第六次正式发布。 • 新增细粒度授权，增加**创建用户组并授权使用MTD**。 • 修改**步骤二：配置追踪器** • 修改告警类型为大驼峰命名。
2021-10-30	第五次正式发布。 购买时新增入门包和初级包的选择说明。
2021-09-29	第四次正式发布。 补充OBS告警类型描述：**查看告警类型详情**。
2021-08-25	第三次正式发布。 修改统计图显示相关的内容描述。
2021-07-10	第二次正式发布。
2021-01-20	第一次正式发布。