# 威胁检测服务

最佳实践

文档版本03发布日期2022-02-15





# 版权所有 © 华为云计算技术有限公司 2024。保留一切权利。

非经本公司书面许可,任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部,并不得以任何形式传播。

## 商标声明

# 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 快速掌控 MTD 潜在威胁	1
2 "MTD+OBS" 数据同步	5
3 名单库策略提升检测效率	9
A 修订记录	16



MTD服务是检测您在目标区域所使用的华为云全局服务的IAM日志、DNS日志、CTS 日志、OBS日志、VPC日志,如<mark>图</mark>1-1所示。MTD实时检测日志中访问者的IP或域名是 否存在潜在的恶意活动和未经授权行为并进行告警,您可通过本实践操作步骤快速掌 控MTD检测潜在威胁,对已发现的告警信息按照告警等级由高至低的优先级对告警信 息进行核查、处理,保障您所使用服务的安全和运行能力。

# 图 1-1 MTD 检测原理



# 检测结果总览

- 步骤1 登录管理控制台。
- **步骤2** 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<mark>图1-2</mark>所示。

## 图 1-2 进入威胁检测服务



## 步骤3 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1-3所示。

# 图 1-3 未发现风险

© Dimonosin-singerone, electrone, electrone, rationa,					
2 <b>1</b> 272574					14.04
金田田間	51 51	- Beverser	21	() パカパラルは形日世	11
E#192505	11	() 24+6305	6		2
含蓄失使	描述		1887	5में,	
IAM / Exploit	[⊕#t] Vulnerability access through IP		100 M	89	
IAM / Bruteforder	[#9]] IP brute-force cracking access		sint	馬約獲役	
IAM / Attacker	[분위]] IP maloicos attack access		stat	82	
IAM / BlackList	(E-th) Stucker P access		#893	89	
WM/CrC	(규래) CNC server IP access		#103	ta	
IAM / Compromised	[(89]] IP penetration(compromised) access		5327	et.	
IAM / Crawler	【例例】 Crawler access		1527	82	
IAM / DDoS	(元句1) COss IP access		<b>成計畫</b> 目		
IAM / Malicious Ste	[#80] Maloices site IP access		sint	#4	
IAM / Malware	【田府】 Malware site IP access		8007	#2	

• 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1-1**所示。

ᆂ	1 1	上敬に	旨白
衣	1-1	「言に	この

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	支持多种告警,更多详细内容请参见 <mark>查看告警类型详情</mark> 。
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			
	· · · · · · · · · · · · · · · · · · ·			
	告警信息目前需要人工核查处理,建议您参照 <mark>查看告警类型详</mark> <mark>情</mark> 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,可单击与切换排序。			
首次发生	该告警首次发生的具体时间,可单击↓三切换排序。			
最近发生	该告警最近一次发生的具体时间,可单击↓三切换排序。			

- b. 单击"标题"列的值可查看"结果详情",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。
- 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"。
- 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"。

----结束

# 告警类型详情

威胁检测服务目前支持3种检测方式,分别是威胁情报、规则基线、AI引擎,详情如 表1-2所示。涵盖71种告警类型。

### 🛄 说明

单条告警根据计算方式和风险系数结果存在单个告警等级或多个告警等级。

# 表 1-2 检测方式详情

检测方式	检测描述	检测数据源及数量
AI引擎	利用机器学习挖掘陌生访问行为来发现 陌生行为是否存在潜在威胁。	IAM日志:8种
规则基线	遵循已有标准的、固定的规则对日志进 行检测。	OBS日志: 11种。
威胁情报	基于三方收集的历史有效情报对日志信 息进行关联性分析检测,三方情报每天 更新一次。	<ul> <li>IAM日志: 22种</li> <li>CTS日志: 5种</li> <li>VPC日志: 12种</li> <li>DNS日志: 11种</li> </ul>

# 2 "MTD+OBS" 数据同步

# 场景说明

MTD默认存储最近30天数据,如需长期存储数据,您需要将MTD告警数据转存至OBS 桶。

# 操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 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,选择 "设置>数据同步",如<mark>图</mark>2-1所示。

图 2-1 进入数据同步页面

螩 华为云				
			€	安全与合规 威胁检测服务
威胁检测服务	数排	居同步		*
检测结果 设置		存储至OBS桶 为满足合规要求。您的她果敢振需要存储180天,"威胁检则服务	默认存储最近30天数据,4	7储更长时间请存储至OBS
或称信报 数据同步				

**步骤3** 单击"存储至OBS桶"后的 如图2-2所示,可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2-1所示。

# 图 2-2 存储至 OBS 桶

存储至OBS桶		
为满足合规要求,	您的结果数据需要存储180天,	"威胁检测服务"默认存储最近30天数据,存储更长时间请存储至OBS桶。
结果更新频率	请选择更新频率	▼
桶名称	请输入桶名称	查看/创建桶
对象名称	请输入对象名称	
存储路径	obs:///	
	确定取消	

# 表 2-1 存储检测结果

参数 名称	参数说明	取值样例
结果 更新 频率	威胁检测服务采用实时检测的方式,您可自定义将 检测结果数据存储到OBS桶的频率,自定义频率之 后每次转存将只转存上一频率周期未转存的数据。 • 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进行创建,更多详细操作请 参见 <mark>创建桶</mark> 。	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

# 步骤4 确认信息无误,单击"确认",页面弹出"操作成功",数据转存开启。

----结束

# 数据同步示例

数据同步开启后,可在对象存储服务(OBS)查看同步的告警数据。

🗀 说明

- MTD数据同步开启后,OBS会产生一定的存储费用,默认计费模式为按需计费,计费详情请参见计费说明,无存储空间限制。
- 如果您是购买的包年包月的固定存储空间,您可以对更历史的数据进行清理,但前提是存储 的数据需满足至少存储180天,所需容量可查看OBS已存储的MTD告警数据文件大小作为参 考。
- **步骤1** 登录华为云控制台,在左侧导航树中,单击 ,选择"存储 > 对象存储服务",进入对象存储服务界面。在桶列表找到"桶名称"为"obs-mtd-beijing4"的目标存储桶,单击桶名称"obs-mtd-beijing4"进入桶内。在左侧单击"对象",在"对象"页 签下的列表可找到自定义创建的"mtd-warning-data"对象,如图2-3所示。

对象存储服务		对象存储 / obs-mtd-beijing4 口	
概览		对象 已删除对象 碎片	1
对象		对象是数据存储的基本单位,在OBS中	文件和文件夹都是对象。您可以
访问权限控制	•	上传对象 新建文件夹	恢复 更多 ▼
基础配置	•	□ 名称 」三	存储类别」三
域名管理		The mtd-warning-data	

图 2-3 数据转存对象

**步骤2** 单击对象文件夹名称"mtd-warning-data"可查看存储对象文件,MTD检测的所有服务的告警数据在对象文件夹"mtd-warning-data"进行统一存储,告警数据对象文件按照存储频率进行逐条存储,如图2-4所示。

## 图 2-4 告警对象文件

対象 已删除对象	碎片					
対象是数据存储的基本单位。在0 上传对象 新建文件#	DBS中文件和文件共都是对象。您可以上 表 恢复 更多	(侍任何黃重 (文本、鄧片、視频等) 的	文件,并在稿中对这些文件进行管理 <b>。了解要</b>	13		输入对象名前缀搜
□ 名称 1目	存储类别↓Ξ	大小 4回	加密状态 1三	恢复状态 4三	最后修改时间 1F	操作
← 返回上一级						
1610751600005	标准存储	4.65 KB	未加樹	**	20 07:00:04 GMT+08:00	下载 分享 更多 ▼
1610749800007	标准存储	4.65 KB	未加密		20 + + 06:30:03 GMT+08:00	下载 分享 更多★
1610748000006	标准存储	4.65 KB	未加密		20 + + 06:00:03 GMT+08:00	下载 分享 更多 ▼
1610746200007	标准存储	4.65 KB	来加密		20 05:30:03 SMT+08:00	下载 分享 更多 •
1610744400007	标准存储	4.65 KB	束加密	175	20 + + 05:00:03 3MT+08:00	下载 分享 更多 🗸
1610742600008	标准存储	4.65 KB	束加密		20 + + 04:30:03 SMT+08:00	下载 分享 更多 +
1610740800009	标准存储	4.65 KB	未加密	-	20 + - 04:00:04 SMT+08:00	下载 分享 更多 ▼

#### ----结束

数据同步开启后,如果您需要对"结果更新频率"或"存储路径"进行更改,可通过 操作步骤进入"数据同步"页面,单击"编辑"可对"结果更新频率"和"存储路 径"进行更改,如<mark>图2-5</mark>所示。

## 图 2-5 数据已开启同步

数携	<b>洞</b> 步	
	存储至OBS桶	i 💽
	为满足合规要求	t,您的结果数据需要存储180天,"威胁检测服务"默认存储最近30天数据,存储更长时间请存储至OBS桶。
	结果更新频率	每1小时更新一次(默认)
	存储路径	obs://obs-mtd-beijing4/mtd-warning-data 编辑

# 3 名单库策略提升检测效率

# 场景说明

MTD服务支持添加所有服务发现的情报/白名单IP或域名至名单库,添加后MTD将优先 关联检测名单库中的IP或域名,及时发现(情报)/忽略(白名单)名单库中IP/域名地 址的活动,降低检测响应时间,提升检测效率,减轻MTD运行负载。

## 须知

如果目标IP或域名同时出现在情报和白名单中,因白名单优先级更高,因此目标IP或域 名检测时将会直接被忽略。

# 前提条件

- 因MTD服务添加的情报/白名单是从OBS桶添加至MTD服务,因此在MTD服务添加情报/白名单时,需要添加的情报/白名单对象文件需已上传至OBS桶中,OBS桶上传对象操作详情请参见上传文件。
- 由于MTD添加的情报/白名单仅支持Plaintext格式,因此OBS桶上传的对象需按照 Plaintext格式编写。Plaintext格式编写详情请参见如何编辑Plaintext格式的对 象?。

# 🛄 说明

情报:也称作黑名单,指受访问时被禁止的IP或域名。

# 操作步骤

# 步骤1 登录管理控制台。

**步骤2** 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,选择"设置>威胁情报",按照<mark>图</mark>1所示。 **图 3-1** 进入威胁情报页面

<b>Ma</b>		
		安全与合规
威胁检测服务	威胁情报	- <u>+</u>
	6 为"7億千方安日計画新 法扣据控/内公前前语失在"对争互接联系。上传(	网络文件。 上使对象 查看操作详悟
	<ul> <li>         ・         ・         ・</li></ul>	
2 2 2 2 2 2 2 2 2 2 2 2 2 2		英型

- 步骤3添加情报/白名单。
  - 1. 添加情报。
    - a. 选择"情报 > 添加情报",弹出"添加情报"对话框,如<mark>图</mark>2所示,相关参数如<mark>表</mark>1所示。

# **图 3-2** 添加情报

添加情期	辰	×
文件名称	请输入文件名称	
对象类型	IP 域名	
情报路径	1) 服务将基于您情报内的IP地址进行威胁检测。	
<b>1</b> 输入 式)	、路径之前,请先确认您已经在OBS上传了情报文件(仅支持Plaintext格 。  上传情报	
桶名称	请输入桶名称 查看/创建桶	
对象名称	请输入对象名称	
存储路径	obs:///	
	确定取消	

## 表 3-1 情报参数说明

参数名称	参数说明	取值样例
文件名称	添加的情报文件名称,建议自定义。	BlackList
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
	■ IP: 服务将基于您情报内的IP地址进行 威胁检测。	
	<ul> <li>域名:服务将基于您情报内的域名进行 威胁检测。</li> </ul>	
	添加至MTD情报后,威胁检测服务将优先 关联检测情报内的IP或域名,对日志中存 在相似的情报信息快速生成告警。	
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 <mark>创建桶</mark> 。	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- blacklist- ip.txt
存储路径	情报在OBS桶的存储路径。	obs://obs- mtd- beijing4/ mtd- blacklist- ip.txt

- b. 确认信息无误,单击"确定",导入的文件显示在情报列表,表示情报导入 成功。
- 2. 添加白名单。
  - a. 选择"白名单 > 添加白名单",弹出"添加白名单"对话框,如<mark>图</mark>3所示, 相关参数如<mark>表</mark>2所示。

# **图 3-3** 添加白名单

添加白谷	3单	×
文件名称	请输入文件名称	
对象类型	IP 域名	
白名单路往	服务将基于您白名单内的IP地址进行威胁检测。 至	
<b>1</b> 输入 式)	路径之前,请先确认您已经在OBS上传了白名单文件(仅支持Plaintext格 。 上传白名单	
桶名称	请输入桶名称 查看/创建桶	
对象名称	请输入对象名称	
存储路径	obs:///	
	确定取消	

# 表 3-2 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
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
	■ IP: 服务将基于您白名单内的IP地址进 行威胁检测。	
	<ul> <li>■ 域名:服务将基于您白名单内的域名 进行威胁检测。</li> </ul>	
	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。	
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 <mark>创建桶</mark> 。	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

参数名称	参数说明	取值样例
存储路径	情报在OBS桶的存储路径。	obs://obs-mtd- beijing4/mtd- securitylist- ip.txt

- b. 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。
- **步骤4** 在"威胁情报"页面,选择"情报"或"白名单"页签,可查看已添加的情报/白名单 详情列表,如<mark>图</mark>4/<mark>图</mark>5所示。

**图 3-4** 情报列表

情报 白名单				
批量調除				
文件名称	类型	格式	上传时间	操作
· · · · · · · · · · · · · · · · · · ·		TXT	: + + + + + + +0	ÐR

### **图 3-5** 白名单列表

情报 白名单				
批量删除 添加白名单				
文件名称	类型	格式	上传时间	操
	IP	TXT	2011/01/0111011110111101010	<b>批</b> 网

----结束

# 添加情报示例

假设:创建需上传至OBS桶的情报对象文件名称为"mtd-blacklist-ip",OBS桶名称为"obs-mtd-bejing4",MTD添加情报文件名称为"BlackList,"需要对历史发现的 情报IP121.3X.XX.XXX进行拦截,则将此IP添加到MTD情报,便可实现直接拦截。

- 1. 创建Plaintext格式的情报对象文件。按照Plaintext格式将IP地址121.3X.XX.XXX写 入需上传至OBS的对象文件,Plaintext格式编辑详情请参见如何编辑Plaintext格 式的对象?。
- 上传对象文件。登录控制台,在左侧导航树中,单击 —,选择"存储 > 对象存储服务",进入对象存储服务界面,按照上传文件操作步骤将对象文件上传至目标OBS桶,如图7所示。

## 图 3-6 上传情报对象

时象存储 / obs-mtd-beijing4 口	
对象 已删除对象 碎片	
对象是数据存储的基本单位,在OBS中文( 上传对象 新建文件夹	中和文件夹都是对象。您可以 恢复 更多 ▼
□ 名称 ↓三	存储类别 1三
📄 🖻 mtd-warning-data	
mtd-blacklist-ip.txt	标准存储

 在MTD服务选择"设置>威胁情报",进入"威胁情报"界面,选择"情报"页 签,单击添加情报,在添加情报弹窗填写相关信息,如图8所示;确认信息无误, 单击"确认",页面右上角提示添加成功,在情报列表可查看已添加的情报,如 图9所示。

图 3-7 添加 IP 情报

添加情期	艮
文件名称	BlackList
对象类型	IP 域名
情报路径	服务将基于恐情报内的IP地址进行威胁检测。
<b>1</b> 输入 式)	、路径之前,请先确认您已经在OBS上传了情报文件(仅支持Plaintext格 。  上传情报
桶名称	obs-mtd-beijing4 查看/创建桶
对象名称	mtd-blacklist-ip.txt
存储路径	obs://obs-mtd-beijing4/mtd-blacklist-ip.txt
	<b>确定</b> 取消

## 图 3-8 情报添加成功

威	协情报				☑ 添加成功!	
	为了便于内容自动更新, 添加情报/白名单龄请先在"对象存储服务"上传想的文件。	上传对象 查看操作详情				
Г	情报 白名单					
	批是删除 添加情报					
	文件名称	类型	格式	上传时间	操作	
	BlackList	IP	тхт	201-171-171-171-1MT+08:00	删除	

4. 情报添加后,MTD会对目标区域接入的所有服务日志进行检测,检测时会优先关 联名单库中的IP或域名。如图10所示。

# **图 3-9** 情报告警

检測結果 🥺 服务商介 🥺 調経引导		结果详情
⑦ 威胁检测服务将于2021/06/30 00:00:00 GMT+08:00正式	成转商,转商后将自动转化为按需计费,如需继续使用,请确保您的账户	<sup>影中余额并</sup> 基本信息
▲ 以下服务无法直接获取日本数据,需要您进行配置: 云帝计服务 CTS 创建自动器 站内创建?		古智学型 Backlist 戸田寺県 ●中告 日さ学型 統一身份以互振労 単次21生 20
由于AI检测模型的普遍特性,一般上线后需要基于用户I	真实数据学习训练大致3个月,预计于2021/04/20 00:00:00 GMT+08:00	00上电正 描述
MART WEREARS FILLING ON WENT		Suspicious IP Address
近30天, 检测日志思量0.00G, 同比少100.00%; 检测音量	2回数179个,回出2→0。	资源信息
反馈可信度		资源名称 资源D 资源关型 资源区域
日志类型 告營类型 林	示题 严重等级 受影响资源	理 英: 2****** b6972
(统一身份认证服务 BlackList S	Suspicious IP Address  ● 中告 1	1
统一身份认证服务 IAM_AI_Bruteforce 2	≠IAM账号疑似受到暴破攻击 ● 中危 1	相户信息 1 ITCIID 0720 TTIC 02560 项目保守
	≠IAM账号疑似受到暴破攻击●中抱 1	1 区域 cn-north-4 项目D 6a8936
	中IAM账号疑似受到暴破攻击 • 中抱 1	1
统一身份认证服务 IAM_AI_Bruteforce 2	本IAM账号疑似受到暴破攻击 • 中危 1	攻击信息 1 101-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-
第一身份认证服务 IAM_AI_Bruteforce 2	和AM账号题织受到要被攻击 • 中危 1	Analastari         Analastari           1         攻击勝端口



发布日期	修改说明
2022-02-15	第三次正式发布。
2021-07-10	第二次正式发布。
2021-05-27	第一次正式发布。