Managed Threat Detection

User Guide

Issue	10
Date	2022-12-02

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Usage.......... 1

1.1 Step 1: Purchase MTD and Create a Detector.......... 1

1.2 Step 2: Create a Tracker.......... 4

2 MTD Overview.......... 7

3 Viewing Detection Results.......... 10

4 Viewing Alarm Types.......... 13

4.1 IAM Alarms.......... 13

4.2 CTS Alarms.......... 20

4.3 DNS Alarms.......... 22

4.4 OBS Alarms.......... 25

4.5 VPC Alarms.......... 28

5 Log Detection Management.......... 32

5.1 Enabling Log Detection.......... 32

5.2 Disabling Log Detection.......... 33

5.3 Viewing Log Detection Information.......... 34

6 Threat Intelligence Management.......... 36

6.1 Importing a Threat Intelligence File.......... 36

6.2 Deleting Threat Intelligence.......... 38

6.3 Viewing Intelligence Details 39

7 Whitelist Management.......... 41

7.1 Importing a Whitelist.......... 41

7.2 Deleting a Whitelist.......... 43

7.3 Viewing Whitelist Details.......... 44

8 Synchronizing Detection Results.......... 46

9 Configuring Alarm Notifications.......... 48

10 Permissions Management.......... 50

10.1 Creating a User Group and Granting Permissions.......... 50

A Change History.......... 52

1 Usage

1.1 Step 1: Purchase MTD and Create a Detector

MTD uses a detector to scan service logs in the target region in real time.

Prerequisites

MTD permissions have been granted to a user of the IAM account. For details, see **How Do I Use My IAM Account to Grant MTD Permissions to a User?**

NOTICE

To create a detector and then perform other operations, you need to obtain permissions from the IAM account first.

Otherwise, you cannot perform operations on MTD.

If you are an administrator, perform the following operations to grant required permissions to the user:

1. Create a custom policy.

Create a custom policy on the IAM console. For details, see **Creating a Custom Policy**.

2. Create a user group and grant permissions to the user group.

Grant policy permissions to the group where the user belongs. For details, see **Creating a User Group and Assigning Permissions**.

Constraints

- Currently, MTD is supported in **AP-Bangkok**, **AP-Singapore**, **LA-MexicoCity1**, **LA-Sao Paulo1**, **CN-Hong Kong**, **AF-Johannesburg**, and **LA-Santiago** regions only.
- You can create a detector only in the region where your cloud services locate.

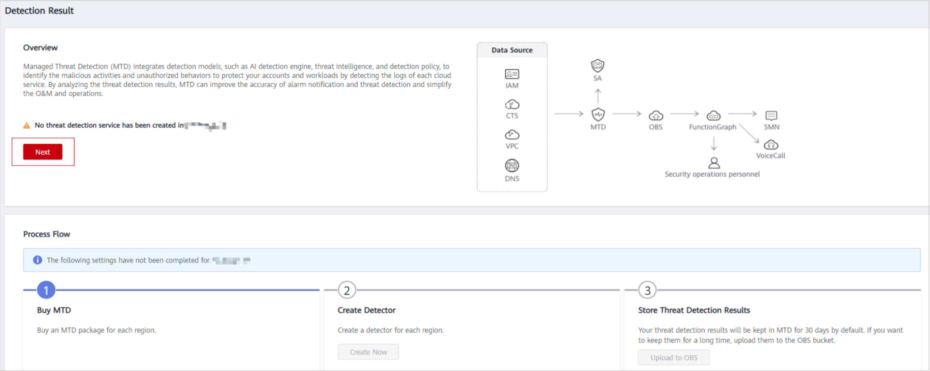
Procedure

Step 1 **Log in to the management console.**

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the navigation pane on the left and choose **Security & Compliance** > **Managed Threat Detection**.

Figure 1-1 Home page of MTD



Detection Result

Overview

Managed Threat Detection (MTD) integrates detection models, such as AI detection engine, threat intelligence, and detection policy, to identify the malicious activities and unauthorized behaviors to protect your accounts and workloads by detecting the logs of each cloud service. By analyzing the threat detection results, MTD can improve the accuracy of alarm notification and threat detection and simplify the O&M and operations.

No threat detection service has been created in[redacted]

Next

Process Flow

The following settings have not been completed for [redacted]

1 Buy MTD

Buy an MTD package for each region.

2 Create Detector

Create a detector for each region.

Create Now

3 Store Threat Detection Results

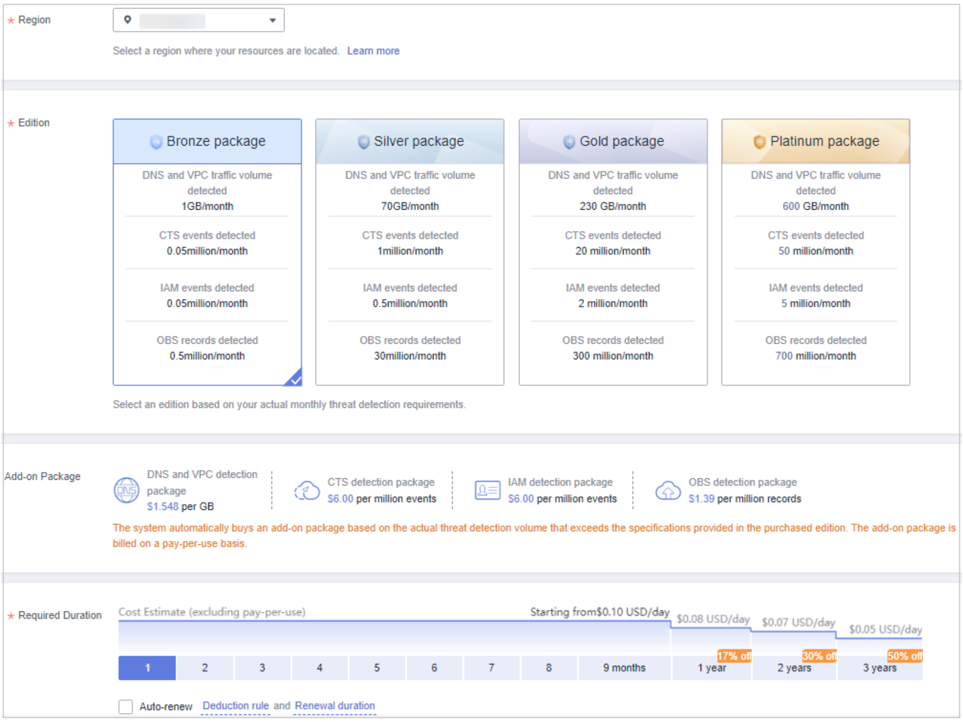
Your threat detection results will be kept in MTD for 30 days by default. If you want to keep them for a long time, upload them to the OBS bucket.

Upload to OBS

Step 4 Click **Create Now**. The purchase details page is displayed.

Step 5 On the displayed page, set the **Region**, **Edition**, and **Required Duration** as needed.

Figure 1-2 Purchasing MTD



* Region [redacted]

Select a region where your resources are located. Learn more

* Edition

Bronze package	Silver package	Gold package	Platinum package
DNS and VPC traffic volume detected 1GB/month	DNS and VPC traffic volume detected 70GB/month	DNS and VPC traffic volume detected 230 GB/month	DNS and VPC traffic volume detected 600 GB/month
CTS events detected 0.05million/month	CTS events detected 1million/month	CTS events detected 20 million/month	CTS events detected 50 million/month
IAM events detected 0.05million/month	IAM events detected 0.5million/month	IAM events detected 2 million/month	IAM events detected 5 million/month
OBS records detected 0.5million/month	OBS records detected 30million/month	OBS records detected 300 million/month	OBS records detected 700 million/month

Select an edition based on your actual monthly threat detection requirements.

Add-on Package

DNS and VPC detection package $1.548 per GB | CTS detection package $6.00 per million events | IAM detection package $6.00 per million events | OBS detection package $1.39 per million records

The system automatically buys an add-on package based on the actual threat detection volume that exceeds the specifications provided in the purchased edition. The add-on package is billed on a pay-per-use basis.

* Required Duration

Cost Estimate (excluding pay-per-use) Starting from$0.10 USD/day $0.08 USD/day $0.07 USD/day $0.05 USD/day

1 2 3 4 5 6 7 8 9 months 1 year (17% off) 2 years (30% off) 3 years (50% off)

□ Auto-renew Deduction rule and Renewal duration

1. Specify the **Region**.

   Select the desired region. MTD cannot be used across regions.

2. Select the **Edition**.

   There are four detection packages you can choose from. Each package allows you to scan different volumes of cloud service logs. For details, see **Specifications**. DNS and VPC service logs are counted by data volume, and CTS, IAM, and OBS service logs are counted by event (one log is an event).

Table 1-1 Specifications

Edition	DNS and VPC Logs	CTS Logs	IAM Logs	OBS Logs
Bronze package	1 GB/month	50 thousand/ month	50 thousand/ month	500 thousand/ month
Silver package	70 GB/ month	1 million/ month	500 thousand/ month	30 million/ month
Gold package	230 GB/ month	20 million/ month	2 million/ month	300 million/ month
Platinum package	600 GB/ month	50 million/ month	5 million/ month	700 million/ month

3. Choose an **Add-on Package**.

   The system automatically purchases an add-on package based on the volume of scanned data that exceeds the purchased package. The add-on package is billed on a pay-per-use basis.

4. Specify the **Required Duration**.

   The required duration can be from one month to three years.

NOTICE

- For archiving purposes, you are advised to buy at least three months of the service.
- You can enable **Auto-renew** after specifying the required duration.

  Deduction rule: The renewal charges are automatically deducted from your account balance. For details, see **Auto-Renewal Rules**.

  Renewal duration: For a monthly subscription, the system renews the package on a monthly basis. For a yearly subscription, the system renews the package on a yearly basis.

Step 6 Read and select *Managed Threat Detection Service Disclaimer* and *Add-on Pack Usage Rules*.

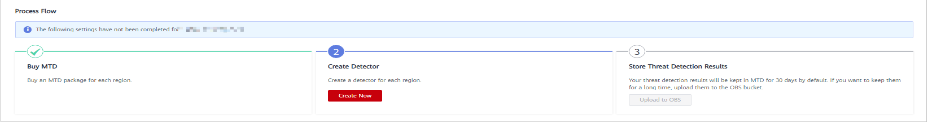
Step 7 Click **Create Now** in the lower right corner to continue on the confirmation page.

Step 8 Confirm the purchase information and click **Pay Now** in the lower right corner. The **Pay** page is displayed.

Step 9 Select a payment method and complete the payment. **Payment processed successfully.** is displayed.

Step 10 Click **Back to Console** to switch to the MTD management console. On the **Detection Result** page, view the **Process Flow**. If **Buy MTD** is checked as shown in **Figure 1-3**, the purchase is successful. You then need to create a detector in the current region.

Figure 1-3 MTD successfully purchased



The following settings have not been completed for [redacted]

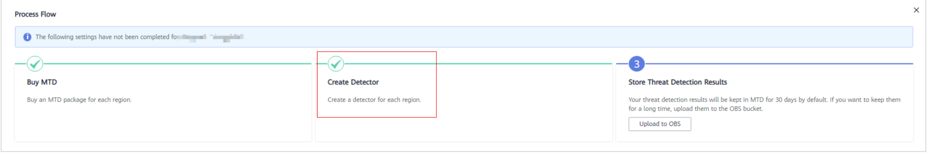
Buy an MTD package for each region.

Create a detector for each region.

Your threat detection results will be kept in MTD for 30 days by default. If you want to keep them for a long time, upload them to the OBS bucket.

Step 11 Click **Create Now** in the **Create Detector** pane. After the creation is complete, **Detector created.** is displayed. The page is automatically refreshed. Click in the upper left corner of the page to show the **Process Flow**. If **Create Detector** is checked as shown in **Figure 1-4**, the detector is successfully created. The purchased package is displayed in the upper right corner of the page.

Figure 1-4 Detector created successfully



The following settings have not been completed for [redacted]

Buy an MTD package for each region.

Create a detector for each region.

Your threat detection results will be kept in MTD for 30 days by default. If you want to keep them for a long time, upload them to the OBS bucket.

NOTE

The detection function is enabled for logs of all supported services by default after you create the detector for the first time.

----End

1.2 Step 2: Create a Tracker

After you create the detector, CTS threat detection is enabled by default. However, MTD cannot obtain log data from the CTS service without a tracker.

This section describes how to configure the tracker.

Limitations and Constraints

CTS threat detection is not supported for the **CN-Hong Kong** region.

Procedure

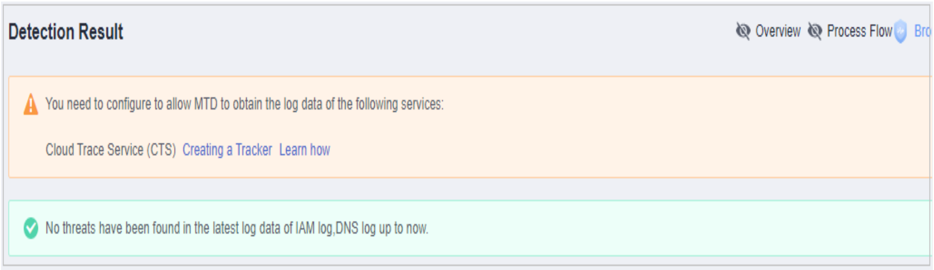
Step 1 **Log in to the management console.**

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the left navigation pane and choose **Security & Compliance** > **Managed Threat Detection**.

View the notice on the **Detection Result** page.

Figure 1-5 Notice on the detection result page



Detection Result

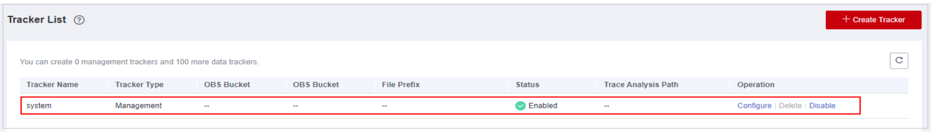
You need to configure to allow MTD to obtain the log data of the following services:

Cloud Trace Service (CTS) Creating a Tracker Learn how

No threats have been found in the latest log data of IAM log,DNS log up to now.

Step 4 Click **Creating a Tracker** to switch to the CTS **Tracker List** page. In the tracker list, locate the only default tracker which is of the **Management** type.

Figure 1-6 Management tracker



Tracker List

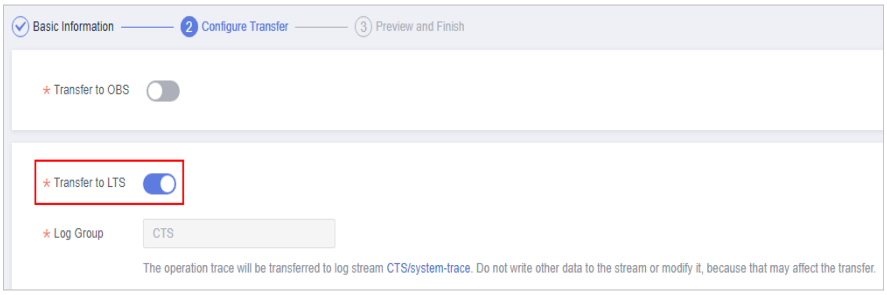
You can create 0 management trackers and 100 more data trackers.

Tracker Name	Tracker Type	OBS Bucket	OBS Bucket	File Prefix	Status	Trace Analysis Path	Operation
system	Management	--	--	--	✓ Enabled	--	Configure | Delete | Disable

Step 5 In the row that contains the target tracker, click **Configure** in the **Operation** column.

1. On the **Basic Information** page, the tracker name is generated by default.
2. Click **Next** to go to the **Configure Transfer** page.
3. On the **Configure Transfer** page, toggle on **Transfer to LTS**.

Figure 1-7 Configure Transfer



Basic Information — 2 Configure Transfer — 3 Preview and Finish

* Transfer to OBS: off

* Transfer to LTS: on

* Log Group: CTS

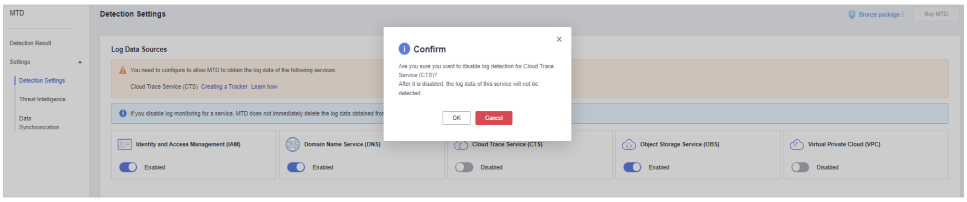
The operation trace will be transferred to log stream CTS/system-trace. Do not write other data to the stream or modify it, because that may affect the transfer.

4. Click **Next** to go to the **Preview and Finish** page
5. Confirm settings and click **Configure**.

Step 6 Go back to the MTD console.

Step 7 In the left navigation pane, choose **Settings > Detection Settings**. On the **Detection Settings** page, click next to **Cloud Trace Service (CTS)** to turn the toggle off. In the displayed dialog box, click **OK** to temporarily disable CTS threat detection. **Operation successfully!** is displayed in the upper right corner.

Figure 1-8 Disabling CTS



You need to configure to allow MTD to obtain the log data of the following services:

Cloud Trace Service (CTS) Creating a Tracker Learn how

If you disable log monitoring for a service, MTD does not immediately delete the log data obtained fro

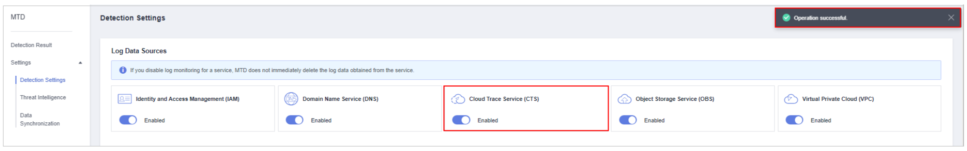
Confirm

Are you sure you want to disable log detection for Cloud Trace Service (CTS)?
After it is disabled, the log data of this service will not be detected.

OK Cancel

Step 8 Click next to **Cloud Trace Service Log (CTS)** to enable CTS threat detection. **Operation successfully!** is displayed in the upper right corner.

Figure 1-9 Enabling CTS

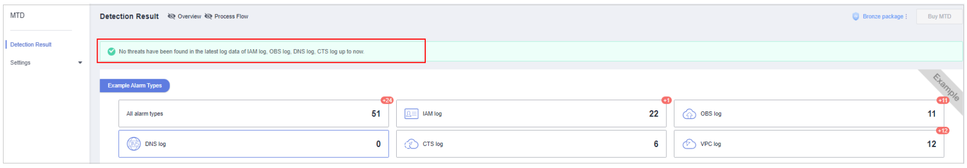


Operation successful.

If you disable log monitoring for a service, MTD does not immediately delete the log data obtained from the service.

Step 9 In the navigation pane on the left, choose **Detection Result**. On the displayed page, "No threats have been found in the latest log data of IAM log, OBS log, DNS log, CTS log up to now" disappears. If CTS threat detection is enabled, the tracker is configured successfully.

Figure 1-10 Tracker configured



No threats have been found in the latest log data of IAM log, OBS log, DNS log, CTS log up to now.

All alarm types	51	IAM log	22	OBS log	11
DNS log	0	CTS log	6	VPC log	12

----End

2 MTD Overview

This section describes how to view the MTD service overview, process flow, and alarms on the **Detection Result** page.

Prerequisites

You have purchased the MTD service in the current region.

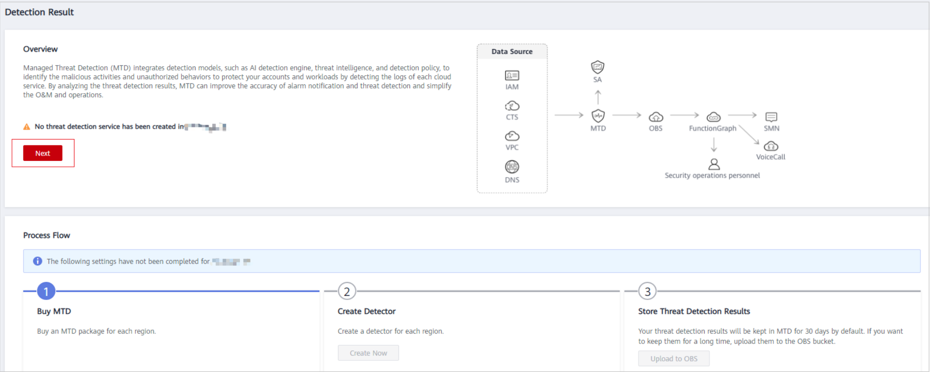
Procedure

Step 1 Log in to the management console.

Step 2 Click ⚲ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the navigation pane on the left and choose **Security & Compliance** > **Managed Threat Detection**.

Figure 2-1 Home page of MTD



Detection Result

Overview

Managed Threat Detection (MTD) integrates detection models, such as AI detection engine, threat intelligence, and detection policy, to identify the malicious activities and unauthorized behaviors to protect your accounts and workloads by detecting the logs of each cloud service. By analyzing the threat detection results, MTD can improve the accuracy of alarm notification and threat detection and simplify the O&M and operations.

⚠ No threat detection service has been created in [redacted]

Process Flow

ⓘ The following settings have not been completed for [redacted]

1 Buy MTD

Buy an MTD package for each region.

2 Create Detector

Create a detector for each region.

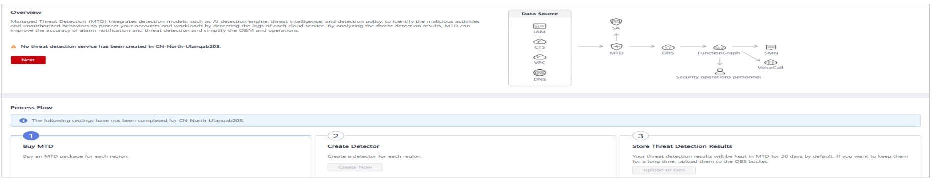
3 Store Threat Detection Results

Your threat detection results will be kept in MTD for 30 days by default. If you want to keep them for a long time, upload them to the OBS bucket.

Step 4 Check the service overview. It introduces main functions of MTD and the service architecture.

- **No threat detection service has been created** is displayed, if you did not create the detection service in your region. You can click **Buy MTD** in the upper right corner to go to the service purchase page.

Figure 2-2 Detection service not purchased



Overview

Managed Threat Detection (MTD) integrates detection models, such as AI detection engine, threat intelligence, and detection policy, to identify the malicious activities and unauthorized behaviors to protect your accounts and workloads by detecting the logs of each cloud service. By analyzing the threat detection results, MTD can improve the accuracy of alarm notification and threat detection and simplify the O&M and operations.

⚠ No threat detection service has been created in CN-North-Ulanqab203.

Process Flow

The following settings have not been completed for CN-North-Ulanqab203.

1 Buy MTD

Buy an MTD package for each region.

2 Create Detector

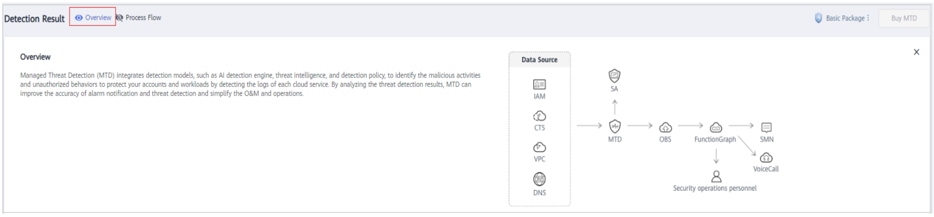
Create a detector for each region.

3 Store Threat Detection Results

Your threat detection results will be kept in MTD for 30 days by default. If you want to keep them for a long time, upload them to the OBS bucket.

- If you have purchased MTD package in your region, the service overview is automatically hidden. To show it, click ⊘ .

Figure 2-3 Service overview



Overview

Managed Threat Detection (MTD) integrates detection models, such as AI detection engine, threat intelligence, and detection policy, to identify the malicious activities and unauthorized behaviors to protect your accounts and workloads by detecting the logs of each cloud service. By analyzing the threat detection results, MTD can improve the accuracy of alarm notification and threat detection and simplify the O&M and operations.

If you click the close button in the upper right corner, the overview pane will not be displayed next time.

NOTE

If you did not purchase the MTD package in the current region, the service overview module is displayed by default and cannot be closed.

Step 5 View the process flow.

To use MTD, you need to buy MTD, create a detector, and store threat detection results.

1. Buy MTD.

   You need to purchase a package for each region. If you have purchased one in the current region, ① in the process flow changes to ✓.

2. Create a detector.

   Create a detector for each region. If a detector has been created for the current region, ② changes to ✓.

3. Configure data storage.

   You can upload data to OBS.

   By default, MTD stores the detection results of the last 30 days. To store the data of a longer period (180 days to meet compliance requirements), click **Upload to OBS** to go to the **Data Synchronization** page and enable the function. For details, see **Synchronizing Detection Results**.

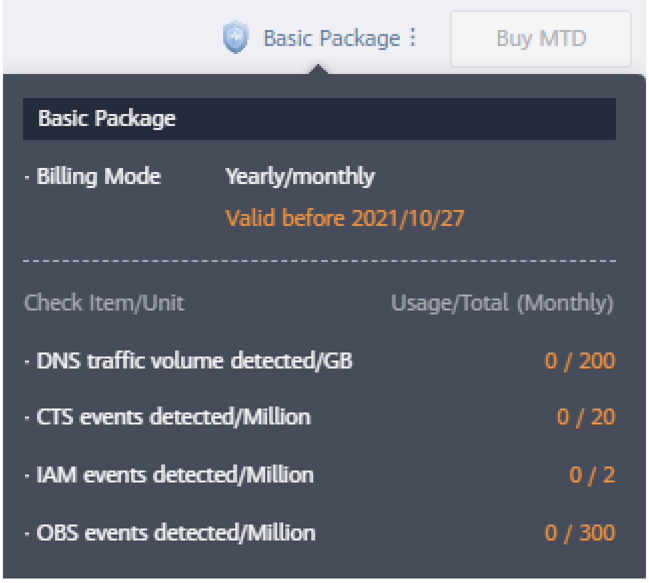
4. Click the close button in the upper right corner of the pane. The overview pane will not be displayed next time.

NOTE

- If you have not created a detector or enabled the all log detection items for your services in the current region, the **Process Flow** pane is displayed by default and cannot be closed.
- After **Process Flow** is closed, you can click **Process Flow** in the upper part of the page to show the **Process Flow**.

Step 6 View package details. The name of the purchased package is displayed in the upper right corner of the page. Move the cursor to the package. The package details are displayed, as shown in **Figure 2-4**.

Figure 2-4 Viewing package details



Basic Package

· Billing Mode Yearly/monthly
Valid before 2021/10/27

Check Item/Unit	Usage/Total (Monthly)
· DNS traffic volume detected/GB	0 / 200
· CTS events detected/Million	0 / 20
· IAM events detected/Million	0 / 2
· OBS events detected/Million	0 / 300

Step 7 View alarm types and alarm details. For details, see **Viewing Detection Results**.

----End

3 Viewing Detection Results

This section describes how to view alarm details about the detected logs.

Prerequisites

You have purchased the MTD package and enabled log detection.

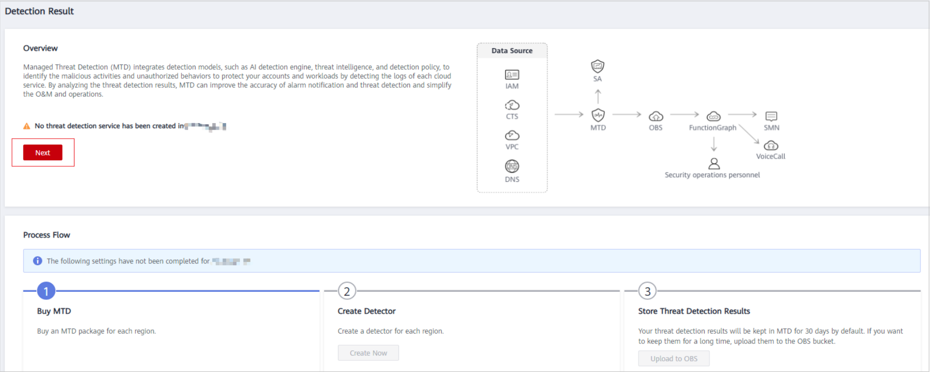
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the navigation pane on the left and choose **Security & Compliance** > **Managed Threat Detection**.

Figure 3-1 Home page of MTD



Detection Result

Overview

Managed Threat Detection (MTD) integrates detection models, such as AI detection engine, threat intelligence, and detection policy, to identify the malicious activities and unauthorized behaviors to protect your accounts and workloads by detecting the logs of each cloud service. By analyzing the threat detection results, MTD can improve the accuracy of alarm notification and threat detection and simplify the O&M and operations.

⚠ No threat detection service has been created in [redacted]

Process Flow

ⓘ The following settings have not been completed for [redacted]

1 Buy MTD

Buy an MTD package for each region.

2 Create Detector

Create a detector for each region.

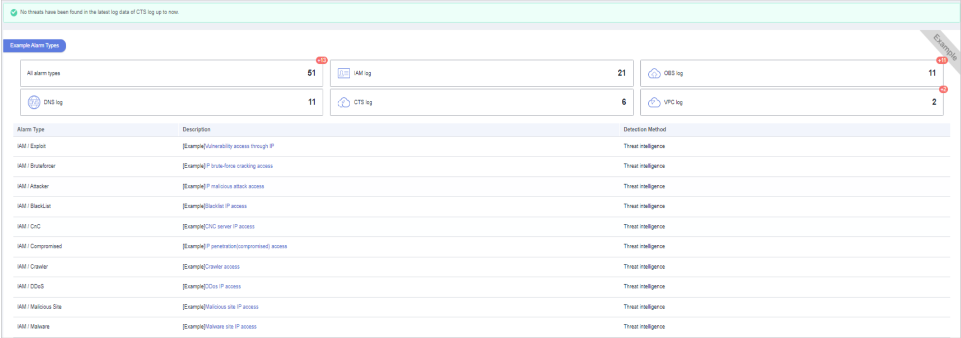
3 Store Threat Detection Results

Your threat detection results will be kept in MTD for 30 days by default. If you want to keep them for a long time, upload them to the OBS bucket.

Step 4 Choose **Detection Result** in the navigation pane on the left.

- If there is no alarm, a message is displayed, indicating that no threats are found in the latest log data of your service. The alarm types are displayed.

Figure 3-2 No threats found



No threats have been found in the latest log data of CTS log up to now.

Example Alarm Types

All alarm types	51 (+13)	IAM log	21	OBS log	11 (+11)
DNS log	11	CTS log	6	VPC log	2 (+2)

Alarm Type	Description	Detection Method
IAM / Exploit	[Example]Vulnerability access through IP	Threat intelligence
IAM / Bruteforcer	[Example]IP brute-force cracking access	Threat intelligence
IAM / Attacker	[Example]IP malicious attack access	Threat intelligence
IAM / BlackList	[Example]Blacklist IP access	Threat intelligence
IAM / CnC	[Example]CNC server IP access	Threat intelligence
IAM / Compromised	[Example]IP penetration(compromised) access	Threat intelligence
IAM / Crawler	[Example]Crawler access	Threat intelligence
IAM / DDoS	[Example]DDos IP access	Threat intelligence
IAM / Malicious Site	[Example]Malicious site IP access	Threat intelligence
IAM / Malware	[Example]Malware site IP access	Threat intelligence

- If there are alarms, they are displayed.

  NOTE

  – Click **Currently, xx alarm types are supported**. In the displayed pane, you can view examples of all alarm types for logs of different services. For details, see **Example Alarms and Statistics**.

  – It takes about three months to train the AI detection model based on your actual data after the model is brought online. The detection result in the training phase may be inaccurate. To help MTD improve the accuracy, click **Report Alarm Accuracy** in the **Operation** column of the alarm list.

  a. Alarms are sorted in descending order of the latest occurrence time. **Table 3-1** describes information about the alarm list.

Table 3-1 Alarm information

Parameter	Description
Log Type	Service logs for which the alarm is generated ■ IAM ■ VPC ■ DNS ■ CTS ■ OBS
Alarm Type	Multiple types of alarms are supported. For details, see **Viewing Alarm Types**.
Alarm Title	Description of an alarm

Parameter	Description
Severity	Severity of an alarm ▪ Critical ▪ High ▪ Medium ▪ Low ▪ Informational Currently, alarm must be manually checked and handled. You are advised to **view alarm types** and handle the alarms in descending order of the alarm severity.
Affected Resources	Number of resources that may be under threats
Alarms Triggered	Number of times that an alarm is generated. You can click ↓≡ to switch the sorting order.
First Occurrence	Time when the alarm is generated for the first time. You can click ↓≡ to switch the sorting order.
Last Occurrence	Time when the alarm was generated last time. You can click ↓≡ to switch the sorting order.

b. Click an alarm title to view details. You can come up with a handling method of the potential threats based on attack information such as the resource name, ID, type, and region.

c. Report alarm accuracy.

NOTE

You can report the detection accuracy to help MTD improve.

- Report accuracy for a single alarm. Click **Report Alarm Accuracy** in the **Operation** column. In the dialog box that is displayed, click **Accurate** or **Inaccurate**.

- Report accuracy for alarms in batches. Select multiple alarms and click **Report Alarm Accuracy** above the check boxes. In the dialog box that is displayed, click **Accurate** or **Inaccurate**.

----End

4 Viewing Alarm Types

4.1 IAM Alarms

Attacker

Access from an attacker's IP address similar to historical intelligence is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

BlackList

Access from a blacklisted IP address similar to historical intelligence is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

CnC

A CnC IP address similar to historical intelligence is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Compromised

A compromised IP address similar to historical intelligence is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Crawler

A crawler's IP address similar to historical intelligence is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

DDoS

A DDoS IP address similar to historical intelligence is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Exploit

An IP address used for vulnerability exploitation is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

MaliciousSite

Access through the destination IP addresses of a malicious site is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Malware

Access from a malware's IP address is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Miner

Access from a miner's IP address is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

MiningPool

Access through the destination IP addresses of a mining pool is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Payment

Access through the destination IP addresses of a fraudulent payment website is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Phishing

Access from a phishing website's IP address is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Proxy

Access from a malicious agency's IP address is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Scanner

Access from a malicious scanner's IP address is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

SinkHole

Access from a sinkhole IP address is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Spammer

Access from a spammer IP address is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Suspicious

Access to a suspicious IP address that is similar to historical intelligence is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Tor

A Tor node IP address similar to historical intelligence is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Zombie

Access from a malicious website/zombie network is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Bruteforce

Brute-force password cracking attempts are detected.

Severity: medium

Data source: IAM logs

This IAM account may have been cracked. Check whether this account has weak passwords or password leak risks.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

BruteforceSuccess

The password may have been successfully cracked through brute-force attacks.

Severity: high

Data source: IAM logs

The IAM account may have been cracked and the password may have been disclosed.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

AkSkLeakage

There is a risk of AK/SK credential leak.

Severity: medium

Data source: IAM logs

The AK of this IAM account may be exploited. Check whether the AK and SK of this account is leaked.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

AkSkLeakageSuccess

The AK/SK credential may have been disclosed.

Severity: high

Data source: IAM logs

The AK and SK of this IAM account may have been disclosed.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

BlindIpLogin

An unauthorized IP address is detected trying to log in to this IAM account.

Severity: medium

Data source: IAM logs

The IAM account is being used for multiple login attempts through an unauthorized IP address. Check whether this account has a weak password or whether the password has been disclosed.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

BlindIpLoginSuccess

An unauthorized IP address has been used to log in to this IAM account.

Severity: high

Data source: IAM logs

The IAM account has been logged in through an unauthorized IP address. The password may have been disclosed.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

IllegalAssume

The IAM account is detected trying to create a malicious agency.

Severity: medium

Data source: IAM logs

The IAM account may be involved in activities related to malicious agencies.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

IllegalAssumeSuccess

The IAM account has been used to successfully create a malicious agency.

Severity: high

Data source: IAM logs

The IAM account may have established a malicious agency.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

TokenLeakage

There is a risk that the token is used maliciously.

Severity: medium

Data source: IAM logs

The IAM account is at risk of token exploitation. Check whether the token is disclosed.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

TokenLeakageSuccess

The token has been used maliciously.

Severity: high

Data source: IAM logs

The token of this IAM account has been used maliciously. The token may have been disclosed.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

4.2 CTS Alarms

NetworkPermissions

A malicious IP address similar to historical intelligence is found calling an API that is typically used to change permission of network access to security groups, routes, and ACLs in your account.

Severity: This alarm can be of any severity levels within **High**, **Medium**, and **Low**. MTD determines the potential risk the finding could have to your network.

Data source: CTS logs

A malicious IP address similar to historical intelligence is detected. The IP address tried to call an API that is typically used to change permission of network access to security groups, routes, and ACLs in your account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

ResourcePermissions

A malicious IP address similar to historical intelligence is found calling an API that is typically used to change secure access policies for various resources in your account.

Severity: This alarm can be of any severity levels within **High**, **Medium**, and **Low**. MTD determines the potential risk the finding could have to your network.

Data source: CTS logs

A malicious IP address similar to historical intelligence is detected. The IP address tried to call an API that is typically used to change secure access policies for various resources in your account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

UserPermissions

A malicious IP address similar to historical intelligence is found calling an API that is typically used to add, modify, or delete IAM users, groups, or policies in your account.

Severity: This alarm can be of any severity levels within **High**, **Medium**, and **Low**. MTD determines the potential risk the finding could have to your network.

Data source: CTS logs

A malicious IP address similar to historical intelligence is detected. The IP address tried to call an API that is typically used to add, modify, or delete IAM users, groups, or policies in your account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

ComputeResources

A malicious IP address similar to historical intelligence is found calling an API that is typically used to start compute resources, such as ECS instances.

Severity: This alarm can be of any severity levels within **High**, **Medium**, and **Low**. MTD determines the potential risk the finding could have to your network.

Data source: CTS logs

A malicious IP address similar to historical intelligence is detected. The IP address tried to call an API that is usually used to start computing resources, such as ECS instances.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

PasswordPolicyChange

A malicious IP address similar historical intelligence is found trying to change the account password policy.

Severity: This alarm can be of any severity levels within **High**, **Medium**, and **Low**. MTD determines the potential risk the finding could have to your network.

Data source: CTS logs

A malicious IP address similar to historical intelligence is detected. The IP address tried to change the account password policy.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

4.3 DNS Alarms

Adware

Access to adware is detected.

Severity: medium

Data source: DNS logs

Your ECS accessed a malicious adware similar to historical intelligence.

Suggestions

If this is an expected activity, add the IP address of the ECS to the whitelist.

CnC

Access to a CnC server is detected.

Severity: medium

Data source: DNS logs

Your ECS accessed a CnC server similar to historical intelligence.

Suggestions

If this is an expected activity, add the IP address of the ECS to the whitelist.

Exploit

Access to a domain name that exploits system vulnerabilities is detected.

Severity: medium

Data source: DNS logs

Your ECS accessed a domain name similar to historical intelligence, which may exploit system vulnerabilities.

Suggestions

If this is an expected activity, add the IP address of the ECS to the whitelist.

MaliciousSite

Access to a malicious website is detected.

Severity: medium

Data source: DNS logs

Your ECS accessed a malicious website that is similar to historical intelligence.

Suggestions

If this is an expected activity, add the IP address of the ECS to the whitelist.

Malware

Access to malware is detected.

Severity: medium

Data source: DNS logs

Your ECS accessed malware that is similar to historical intelligence.

Suggestions

If this is an expected activity, add the IP address of the ECS to the whitelist.

Miner

Access to a miner is detected.

Severity: medium

Data source: DNS logs

Your ECS accessed a miner that is similar to historical intelligence.

Suggestions

If this is an expected activity, add the IP address of the ECS to the whitelist.

MiningPool

Access to a mining pool is detected.

Severity: medium

Data source: DNS logs

Your ECS accessed a mining pool that is similar to historical intelligence.

Suggestions

If this is an expected activity, add the IP address of the ECS to the whitelist.

Payment

Access to a payment domain name is detected.

Severity: medium

Data source: DNS logs

Your ECS accessed a payment domain name that is similar to historical intelligence.

Suggestions

If this is an expected activity, add the IP address of the ECS to the whitelist.

Phishing

Access to a phishing website is detected.

Severity: medium

Data source: DNS logs

Your ECS accessed a phishing website that is similar to historical intelligence.

Suggestions

If this is an expected activity, add the IP address of the ECS to the whitelist.

Spammer

Access to a spammer is detected.

Severity: medium

Data source: DNS logs

Your ECS accessed a spammer that is similar to historical intelligence.

Suggestions

If this is an expected activity, add the IP address of the ECS to the whitelist.

Suspicious

Suspicious access is detected.

Severity: medium

Data source: DNS logs

The ECS access is similar to historical intelligence.

Suggestions

If this is an expected activity, add the IP address of the ECS to the whitelist.

4.4 OBS Alarms

UserFirstAccess

A specific user accessed an OBS bucket for the first time.

Severity: low

Data source: OBS logs

A user who has never accessed the bucket before accessed it.

Suggestions

If the user is not authorized, credentials may have been disclosed or OBS permissions are not restrictive enough. In this case, remediate the access policy of the compromised OBS bucket.

IPFirstAccess

A specific IP address was used for the first time to access an OBS bucket.

Severity: low

Data source: OBS logs

An IP address that has never accessed the bucket before accessed it.

Suggestions

If the IP address is not authorized, credentials may have been disclosed or OBS permission is not restrictive enough. In this case, remediate the access policy of the compromised OBS bucket, or enable OBS URL validation with the Referer added to the blacklist.

ClientFirstAccess

A new client was used to access an OBS bucket.

Severity: low

Data source: OBS logs

A client that has never accessed the bucket before accessed it.

Suggestions

If the login client is not commonly used, remediate the access policy of the compromised OBS bucket or enable OBS URL validation with the Referer added to the blacklist.

UserFirstCrossDomainAccess

An OBS instance is being accessed for the first time by a user who does not belong to your account.

Severity: low

Data source: OBS logs

A user who does not belong to your account accessed the bucket. The user client has never accessed the bucket before.

Suggestions

If the user is not authorized, credentials may have been disclosed or OBS permissions are not restrictive enough. In this case, remediate the access policy of the compromised OBS bucket.

UserAccessFrequencyAbnormal

A user accessed a specific OBS bucket frequently.

Severity: low

Data source: OBS logs

Access frequency of a user that belongs to your account to the bucket is abnormal.

Suggestions

If this activity is unexpected, your OBS permissions are not restrictive enough. In this case, remediate the access policy of the compromised OBS bucket.

IPAccessFrequencyAbnormal

An IP address was used to access a specific OBS bucket frequently.

Severity: low

Data source: OBS logs

The access frequency of this IP address to the bucket is abnormal.

Suggestions

If this activity is unexpected, your OBS permissions are not restrictive enough. In this case, remediate the access policy of the compromised OBS bucket.

UserDownloadAbnormal

Abnormal download behavior is detected.

Severity: low

Data source: OBS logs

The download volume from the bucket is abnormal.

Suggestions

If this activity is unexpected, the user credential may have been disclosed or the OBS permissions are not restrictive enough. In this case, remediate the access policy of the compromised OBS bucket.

UserIPDownloadAbnormal

An IP address is detected in a user's abnormal download behavior.

Severity: low

Data source: OBS logs

The download volume from the bucket through the specific IP address is abnormal.

Suggestions

If this activity is unexpected, user credentials may have been disclosed or OBS permissions are not restrictive enough. In this case, remediate the access policy of the compromised OBS bucket.

UnauthorizedAccess

Unauthorized access is detected.

Severity: low

Data source: OBS logs

Multiple unauthorized API calls on the bucket occurred during a specific period.

Suggestions

If the activity is authorized, add the permission to the access policy for the user. If the activity is unauthorized, enable OBS URL validation with the Referer added to the blacklist.

UserHourLevelAccessAbnormal

Abnormal hourly access is detected.

Severity: low

Data source: OBS logs

API calling frequency of the bucket is abnormal in the same period of every day.

Suggestions

If this activity is unexpected, remediate the access policy of the compromised OBS bucket.

IPSwitchAbnormal

Abnormal IP address switch is detected.

Severity: low

Data source: OBS logs

The bucket is accessed by multiple IP addresses during a specific period. The number of IP addresses used is inconsistent with the number in your historical behavior.

Suggestions

If this activity is unexpected, your OBS permissions are not restrictive enough. In this case, remediate the access policy of the compromised OBS bucket, or enable OBS URL validation with the Referer added to the blacklist.

4.5 VPC Alarms

DDoSTcpDns

Your ECSs may have been used to perform Denial of Service (DoS) attacks using the DNS protocol. The port number is 53.

Severity: high

Data source: VPC flow logs

Some ECSs may be performing DoS attacks using the DNS protocol. The port number is 53.

Suggestions: If this activity is unexpected, your ECS may have been compromised. Check whether the processes on port 53 are abnormal and clear any detected malware. If necessary, stop the ECS and start a new ECS to take over the workloads.

DDoSTcp

Your ECSs may have been used to perform Denial of Service (DoS) attacks using the TCP protocol. As a result, a large volume of inbound/outbound TCP traffic is generated.

Severity: high

Data source: VPC flow logs

Some ECSs may have been used to perform Denial of Service (DoS) attacks using the TCP protocol. As a result, a large volume of inbound/outbound TCP traffic is generated.

Suggestions: If this activity is unexpected, your ECS may have been compromised. Check whether suspicious processes exist and clear any detected malware. If necessary, stop the ECS and start a new ECS to take over the workloads.

DDoSUdp

Your ECSs may have been used to perform Denial of Service (DoS) attacks using the UDP protocol. As a result, a large volume of inbound/outbound UDP traffic is generated.

Severity: high

Data source: VPC flow logs

Some ECSs may have been used to perform Denial of Service (DoS) attacks using the UDP protocol. As a result, a large volume of inbound/outbound UDP traffic is generated.

Suggestions: If this activity is unexpected, your ECS may have been compromised. Check whether suspicious processes exist and clear any detected malware. If necessary, stop the ECS and start a new ECS to take over the workloads.

DDoSTcp2Udp

Your ECSs may have been used to perform Denial of Service (DoS) attacks using the UDP protocol on a TCP port. For example, port 80 usually used for TCP communications is found used for UDP communications at a specific time point. As a result, a large volume of inbound/outbound UDP traffic is generated.

Severity: high

Data source: VPC flow logs

Some ECSs may be performing a DoS attack using the UDP protocol on a TCP port. For example, port 80 usually used for TCP communications is found used for UDP communications at a specific time point. As a result, a large volume of inbound/outbound UDP traffic is generated.

Suggestions: If this activity is unexpected, your ECS may have been compromised. Check whether suspicious processes exist and clear any detected malware. If necessary, stop the ECS and start a new ECS to take over the workloads.

DDoSUnusualProtocol

Your ECSs may have been used to perform Denial of Service (DoS) attacks using an unusual protocol. Unusual protocols are those except TCP, UDP, ICMP, IPv4, IPv6 and STP protocols.

Severity: high

Data source: VPC flow logs

Some ECSs may be performing a DoS attack using an unusual protocol. Unusual protocols are those except TCP, UDP, ICMP, IPv4, IPv6 and STP protocols.

Suggestions: If this activity is unexpected, your ECS may have been compromised. Check whether suspicious processes exist and clear any detected malware. If necessary, stop the ECS and start a new ECS to take over the workloads.

JunkMail

Your ECSs are communicating with remote hosts through port 25 and sending junk mails.

Severity: medium

Data source: VPC flow logs

Some ECSs are communicating with remote hosts through port 25 and sending junk mails.

Suggestions: If this activity is unexpected, your ECS may be compromised. Check whether port 25 is enabled. If necessary, disable port 25 in the security group and clear any detected malware.

UnusualNetworkPort

Your ECSs are using abnormal ports to communicate with remote hosts and may be engaged in malicious activities. The abnormal port may be any custom open port.

Severity: medium

Data source: VPC flow logs

Some ECSs are using abnormal ports to communicate with remote hosts and may be engaged in malicious activities. The abnormal port may be any custom open port.

Suggestions: If this activity is unexpected, your ECS may have been compromised. Check whether suspicious processes exist and clear any detected malware. If necessary, stop the ECS and start a new ECS to take over the workloads.

UnusualTrafficFlow

Your ECSs are generating a large volume of outbound traffic that deviates from the normal baseline and is all directed to the remote host.

Severity: medium

Data source: VPC flow logs

Some ECSs are generating a large volume of outbound traffic that deviates from the normal baseline and is all directed to the remote host.

Suggestions: If this activity is unexpected, your ECS may have been compromised. Check whether suspicious processes exist and clear any detected malware. If necessary, stop the ECS and start a new ECS to take over the workloads.

Cryptomining

Your ECSs are accessing IP addresses that are associated with crypto-mining-related activity and may be engaged in illegal activities.

Severity: high

Data source: VPC flow logs

Some ECSs are accessing IP addresses that are associated with crypto-mining-related activity and may be engaged in illegal activities.

Suggestions: If this activity is unexpected, your ECS may have been compromised. Check whether suspicious processes exist and clear any detected malware. If necessary, stop the ECS and start a new ECS to take over the workloads.

CommandControlActivity

Your ECS is used to send messages to a high-risk network.

Severity: high

Data source: VPC flow logs

The IP address of the ECS is querying an IP address that is associated with a known command and control server.

Suggestions: If this activity is unexpected, your ECS may have been compromised. Check whether suspicious processes exist and clear any detected malware. If necessary, stop the ECS and start a new ECS to take over the workloads.

PortDetection

Your ECS is probing a port on a large number of IP addresses.

Severity: high

Data source: VPC flow logs

Some ECSs are scanning ports that are active on a large number of IP addresses. The ECSs may have been compromised for slow remote port scan attacks.

Suggestions: If this activity is unexpected, your ECS may have been compromised. Check whether suspicious processes exist and clear any detected malware. If necessary, stop the ECS and start a new ECS to take over the workloads.

PortScan

Your ECS is scanning a port on a large number of IP addresses.

Severity: medium

Data source: VPC flow logs

Some ECSs are scanning the outbound ports of remote resources and may be engaged in malicious activities.

Suggestions: If this activity is unexpected, your ECS may have been compromised. Check whether suspicious processes exist and clear any detected malware. If necessary, stop the ECS and start a new ECS to take over the workloads.

5 Log Detection Management

5.1 Enabling Log Detection

Prerequisites

You have purchased MTD and created a detector in the current region.

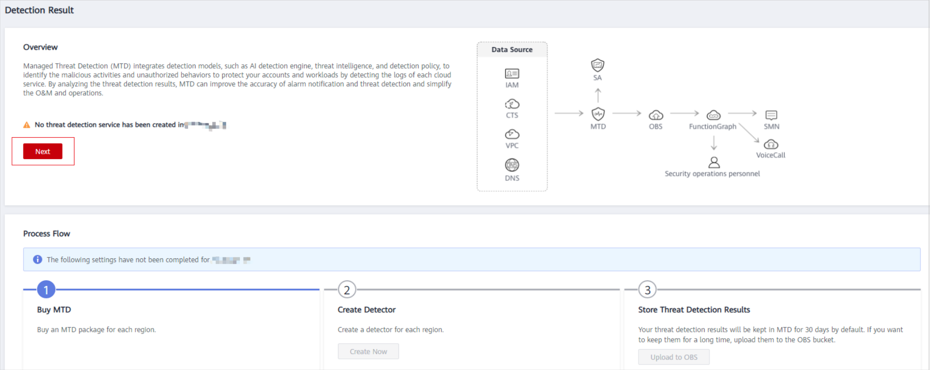
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the navigation pane on the left and choose **Security & Compliance** > **Managed Threat Detection**.

Figure 5-1 Home page of MTD



Detection Result

Overview

Managed Threat Detection (MTD) integrates detection models, such as AI detection engine, threat intelligence, and detection policy, to identify the malicious activities and unauthorized behaviors to protect your accounts and workloads by detecting the logs of each cloud service. By analyzing the threat detection results, MTD can improve the accuracy of alarm notification and threat detection and simplify the O&M and operations.

No threat detection service has been created in [redacted]

Next

Process Flow

The following settings have not been completed for [redacted]

1 Buy MTD

Buy an MTD package for each region.

2 Create Detector

Create a detector for each region.

Create Now

3 Store Threat Detection Results

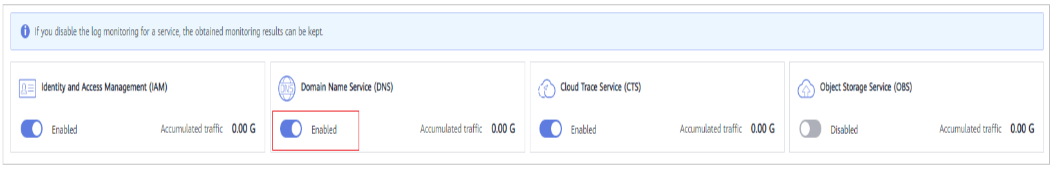
Your threat detection results will be kept in MTD for 30 days by default. If you want to keep them for a long time, upload them to the OBS bucket.

Upload to OBS

Step 4 Choose **Settings** > **Detection Settings** in the left navigation pane.

Step 5 Select the target service and click to enable log detection for the service. If the icon under the service name changes to , the real-time log detection is successfully enabled.

Figure 5-2 Log detection enabled



If you disable the log monitoring for a service, the obtained monitoring results can be kept.

Identity and Access Management (IAM) Enabled Accumulated traffic 0.00 G

Domain Name Service (DNS) Enabled Accumulated traffic 0.00 G

Cloud Trace Service (CTS) Enabled Accumulated traffic 0.00 G

Object Storage Service (OBS) Disabled Accumulated traffic 0.00 G

NOTE

- When you enable service log detection for the first time, a dialog box is displayed, asking you to configure a tracker accessing the service logs.
- You can click **Create a Tracker** to switch to the **Tracker List** page. For details, see **Step 2: Create a Tracker**.
- You can click **Learn how** to view how to **create a tracker** in the CTS user guide.

----End

5.2 Disabling Log Detection

This section describes how to disable log detection. After the function is disabled, MTD will not detect new log data generated by your services, which does not affect the historical detection and results. You can also unsubscribe from the detector of the current region.

Prerequisites

You have purchased MTD and created a detector in the current region.

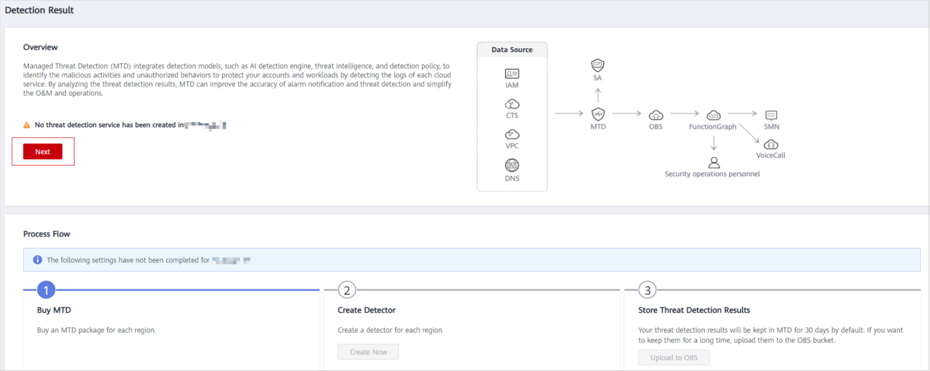
Procedure

Step 1 **Log in to the management console.**

Step 2 Click ⦿ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the navigation pane on the left and choose **Security & Compliance** > **Managed Threat Detection**.

Figure 5-3 Home page of MTD



Detection Result

Overview

Managed Threat Detection (MTD) integrates detection models, such as AI detection engine, threat intelligence, and detection policy, to identify the malicious activities and unauthorized behaviors to protect your accounts and workloads by detecting the logs of each cloud service. By analyzing the threat detection results, MTD can improve the accuracy of alarm notification and threat detection and simplify the O&M and operations.

No threat detection service has been created in [redacted]

Process Flow

The following settings have not been completed for [redacted]

1 Buy MTD

Buy an MTD package for each region.

2 Create Detector

Create a detector for each region.

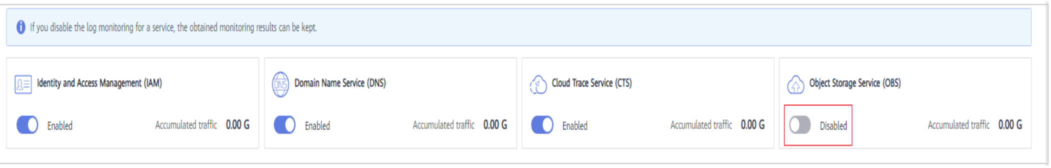
3 Store Threat Detection Results

Your threat detection results will be kept in MTD for 30 days by default. If you want to keep them for a long time, upload them to the OBS bucket.

Step 4 In the navigation pane on the left, choose **Settings** > **Detection Settings**.

Step 5 Select the target service and click to disable log detection for the service. If the icon under the service name changes to , the real-time log detection is successfully disabled.

Figure 5-4 Log detection disabled



If you disable the log monitoring for a service, the obtained monitoring results can be kept.

Service	Status	Accumulated traffic
Identity and Access Management (IAM)	Enabled	0.00 G
Domain Name Service (DNS)	Enabled	0.00 G
Cloud Trace Service (CTS)	Enabled	0.00 G
Object Storage Service (OBS)	Disabled	0.00 G

NOTE

After you disable the log detection for a service, MTD will stop detection newly generated logs, but the historical detection results are kept.

----End

5.3 Viewing Log Detection Information

This section describes how to view the log detection information.

Prerequisites

You have purchased MTD and created a detector in the current region.

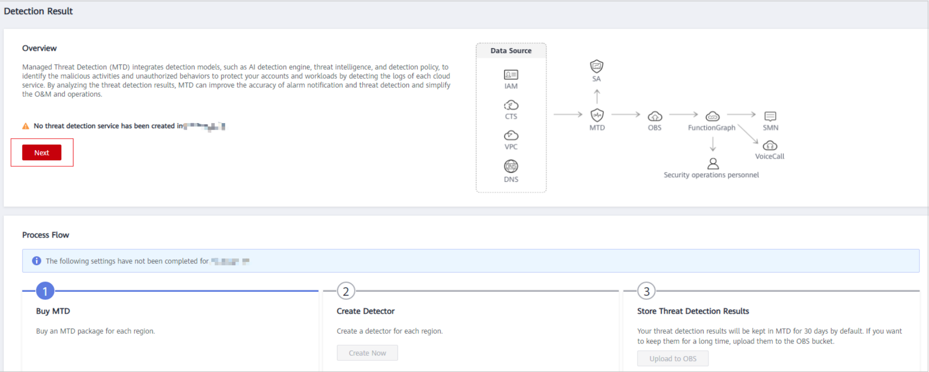
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the navigation pane on the left and choose **Security & Compliance** > **Managed Threat Detection**.

Figure 5-5 Home page of MTD



Detection Result

Overview

Managed Threat Detection (MTD) integrates detection models, such as AI detection engine, threat intelligence, and detection policy, to identify the malicious activities and unauthorized behaviors to protect your accounts and workloads by detecting the logs of each cloud service. By analyzing the threat detection results, MTD can improve the accuracy of alarm notification and threat detection and simplify the O&M and operations.

No threat detection service has been created in [redacted]

Next

Process Flow

The following settings have not been completed for [redacted]

1 Buy MTD

Buy an MTD package for each region.

2 Create Detector

Create a detector for each region.

Create Now

3 Store Threat Detection Results

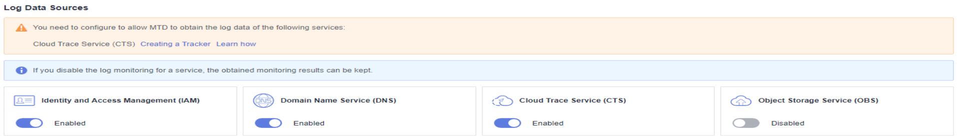
Your threat detection results will be kept in MTD for 30 days by default. If you want to keep them for a long time, upload them to the OBS bucket.

Upload to OBS

Step 4 Choose **Settings** > **Detection Settings** in the left navigation pane.

Step 5 In the **Log Data Sources** pane, you can view the services for which the log data source detection function is enabled or disabled.

Figure 5-6 Log data sources



Log Data Sources

You need to configure to allow MTD to obtain the log data of the following services:
Cloud Trace Service (CTS) Creating a Tracker Learn how

If you disable the log monitoring for a service, the obtained monitoring results can be kept.

Identity and Access Management (IAM) Enabled

Domain Name Service (DNS) Enabled

Cloud Trace Service (CTS) Enabled

Object Storage Service (OBS) Disabled

Table 5-1 Log detection options

Options	Description
Switch status	Whether to enable log detection for the service ● : Enabled ● : Disabled
Accumulated traffic	Size of detected logs since the log detection is enabled

----End

6 Threat Intelligence Management

6.1 Importing a Threat Intelligence File

This section describes how to import a third-party threat intelligence file and trusted IP list in the Plaintext format. MTD will detect threats based on the IP addresses or domain names contained in the imported file.

Prerequisites

You have uploaded the threat intelligence file to an OBS bucket. For details, see **Uploading a File**.

NOTE

- Intelligence: A blacklist of IP addresses or domain names. Access requests from them are rejected. Currently, only one intelligence file with a maximum of 10,000 IP address or domain names can be uploaded.
- Plaintext format: In your trusted IP list and intelligence file, ensure that each line contains only one IP address. For details, see **How Do I Edit and Upload a Plaintext File to OBS?**

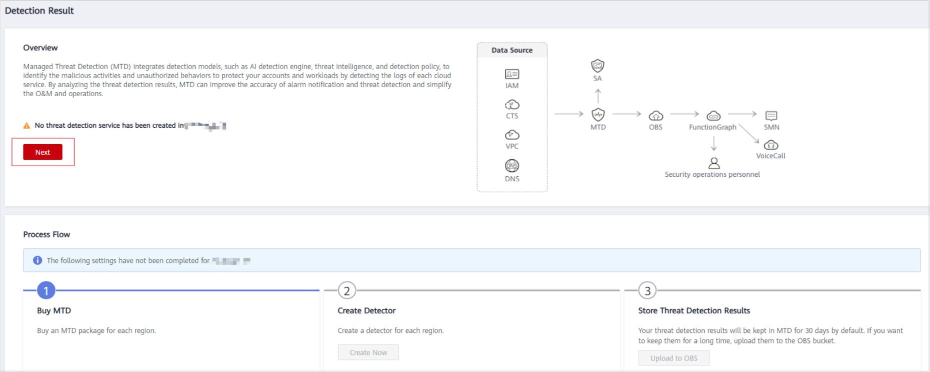
Procedure

Step 1 **Log in to the management console.**

Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the navigation pane on the left and choose **Security & Compliance** > **Managed Threat Detection**.

Figure 6-1 Home page of MTD



Detection Result

Overview

Managed Threat Detection (MTD) integrates detection models, such as AI detection engine, threat intelligence, and detection policy, to identify the malicious activities and unauthorized behaviors to protect your accounts and workloads by detecting the logs of each cloud service. By analyzing the threat detection results, MTD can improve the accuracy of alarm notification and threat detection and simplify the O&M and operations.

⚠ No threat detection service has been created in [redacted]

Process Flow

ⓘ The following settings have not been completed for [redacted]

1 Buy MTD

Buy an MTD package for each region.

2 Create Detector

Create a detector for each region.

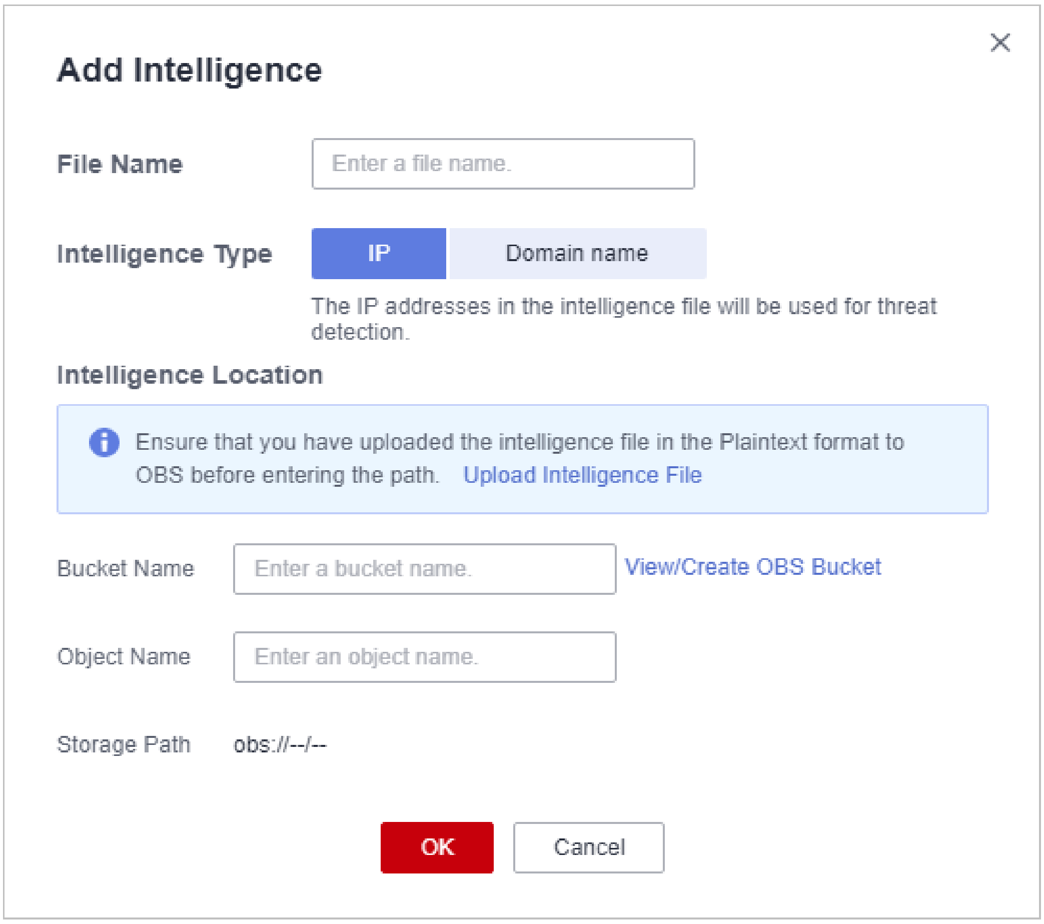
3 Store Threat Detection Results

Your threat detection results will be kept in MTD for 30 days by default. If you want to keep them for a long time, upload them to the OBS bucket.

Step 4 Choose **Settings** > **Threat Intelligence** in the left navigation pane.

Step 5 On the **Intelligence** tab page, click **Add Intelligence**. The **Add Intelligence** dialog box is displayed.

Figure 6-2 Adding intelligence



Add Intelligence

File Name: Enter a file name.

Intelligence Type: IP | Domain name

The IP addresses in the intelligence file will be used for threat detection.

Intelligence Location

ⓘ Ensure that you have uploaded the intelligence file in the Plaintext format to OBS before entering the path. Upload Intelligence File

Bucket Name: Enter a bucket name. View/Create OBS Bucket

Object Name: Enter an object name.

Storage Path: obs://--/--

Table 6-1 Intelligence file parameters

Parameter	Description	Example Value
File Name	Name of the intelligence file to add	BlackList
Intelligence Type	Content type of the file to be uploaded from the OBS bucket to MTD ● **IP**: MTD will detect threats based on the IP addresses in the intelligence file. ● **Domain name**: MTD will detect threats based on the domain names in the intelligence file. MTD preferentially generates alarms that are associated with the IP addresses or domain names in the intelligence file.	IP
Bucket Name	Name of the OBS bucket where the file is located **NOTE** If no OBS bucket is available, click **View/ Create OBS Bucket**. For details, see **Creating a Bucket**.	obs-mtd-bejing4
Object Name	Name of the object in the bucket that stores the intelligence **NOTICE** The object name must contain the file name extension.	mtd-blacklist-ip.txt
Storage Path	Path of the OBS bucket storing the intelligence file	obs://obsmtd-beijing4/mtd-blacklistip.txt

Step 6 Confirm the information and click **OK**. If the added file is displayed in the intelligence list, the operation is successful.

----End

6.2 Deleting Threat Intelligence

This section describes how to delete an imported threat intelligence file.

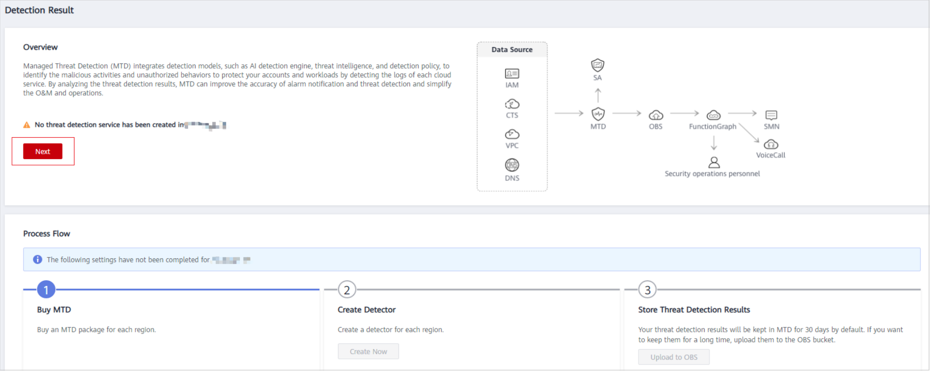
Procedure

Step 1 **Log in to the management console.**

Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the navigation pane on the left and choose **Security & Compliance** > **Managed Threat Detection**.

Figure 6-3 Home page of MTD



Detection Result

Overview

Managed Threat Detection (MTD) integrates detection models, such as AI detection engine, threat intelligence, and detection policy, to identify the malicious activities and unauthorized behaviors to protect your accounts and workloads by detecting the logs of each cloud service. By analyzing the threat detection results, MTD can improve the accuracy of alarm notification and threat detection and simplify the O&M and operations.

No threat detection service has been created in [redacted]

Process Flow

The following settings have not been completed for [redacted]

1 Buy MTD

Buy an MTD package for each region.

2 Create Detector

Create a detector for each region.

3 Store Threat Detection Results

Your threat detection results will be kept in MTD for 30 days by default. If you want to keep them for a long time, upload them to the OBS bucket.

Step 4 Choose **Settings** > **Threat Intelligence** in the left navigation pane.

Step 5 In the **Operation** column of the intelligence file to be deleted, click **Delete**.

Step 6 In the displayed **Delete Intelligence** dialog box, click **Yes**.

----End

6.3 Viewing Intelligence Details

This section describes how to view the details about an imported intelligence file, including the file name, intelligence type, file format, and upload time.

Prerequisites

You have imported a threat intelligence file. For details about how to import threat intelligence, see **Importing a Threat Intelligence File**.

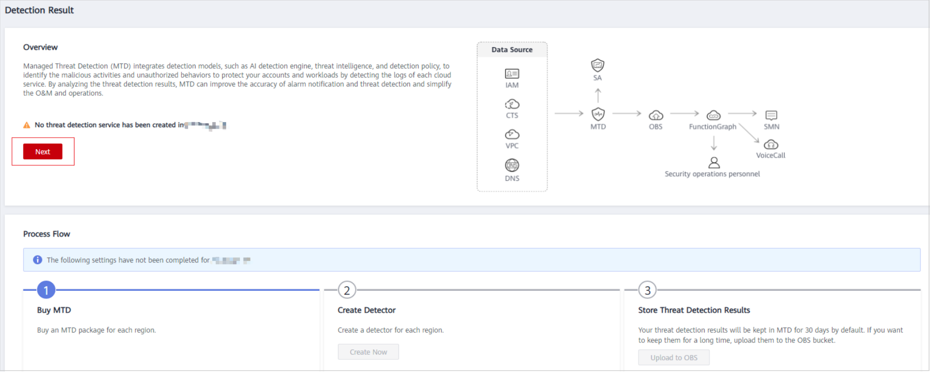
Procedure

Step 1 **Log in to the management console.**

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the navigation pane on the left and choose **Security & Compliance** > **Managed Threat Detection**.

Figure 6-4 Home page of MTD



Detection Result

Overview

Managed Threat Detection (MTD) integrates detection models, such as AI detection engine, threat intelligence, and detection policy, to identify the malicious activities and unauthorized behaviors to protect your accounts and workloads by detecting the logs of each cloud service. By analyzing the threat detection results, MTD can improve the accuracy of alarm notification and threat detection and simplify the O&M and operations.

No threat detection service has been created in [redacted]

Process Flow

The following settings have not been completed for [redacted]

1 Buy MTD

Buy an MTD package for each region.

2 Create Detector

Create a detector for each region.

3 Store Threat Detection Results

Your threat detection results will be kept in MTD for 30 days by default. If you want to keep them for a long time, upload them to the OBS bucket.

Step 4 Choose **Settings** > **Threat Intelligence** in the left navigation pane.

Step 5 View details about an imported intelligence file. **Table 6-2** describes the detailed information about an intelligence file.

Table 6-2 Intelligence file information

Parameter	Description
File Name	Name of an intelligence file
Intelligence Type	Content type of the intelligence file, which can be **IP** and **domain name**.
Format	Format of an intelligence file. Currently, only plaintext files are supported. For details, see **How Do I Edit and Upload a Plaintext File to OBS?**
Uploaded	Time when an information file is uploaded

----End

7 Whitelist Management

7.1 Importing a Whitelist

This section describes how to import an IP address whitelist. MTD will ignore threats related to the IP addresses or domain names contained in the whitelist.

Prerequisites

You have uploaded a plaintext whitelist to an OBS bucket. For details, see **Uploading a File**.

NOTE

- Currently, only one whitelist file with a can be maximum of 10,000 IP address or domain names can be uploaded.
- Plaintext format: In your trusted IP list and intelligence file, ensure that each line contains only one IP address. For details, see **How Do I Edit and Upload a Plaintext File to OBS?**

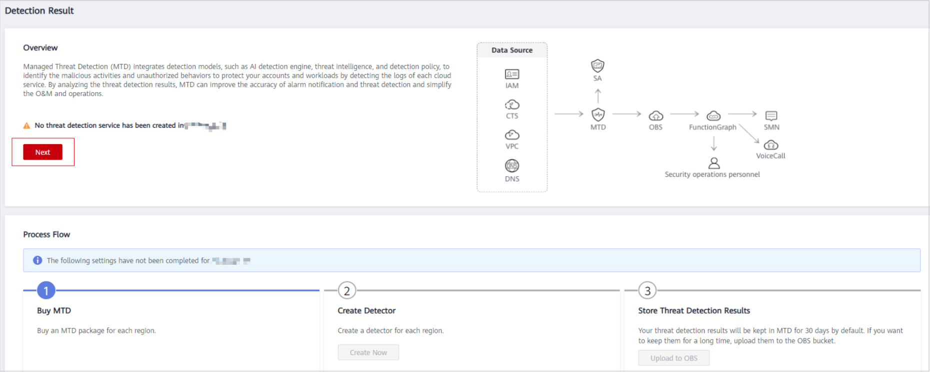
Procedure

Step 1 **Log in to the management console.**

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click ≡ in the navigation pane on the left and choose **Security & Compliance** > **Managed Threat Detection**.

Figure 7-1 Home page of MTD



Detection Result

Overview

Managed Threat Detection (MTD) integrates detection models, such as AI detection engine, threat intelligence, and detection policy, to identify the malicious activities and unauthorized behaviors to protect your accounts and workloads by detecting the logs of each cloud service. By analyzing the threat detection results, MTD can improve the accuracy of alarm notification and threat detection and simplify the O&M and operations.

No threat detection service has been created in [redacted]

Process Flow

The following settings have not been completed for [redacted]

1 Buy MTD

Buy an MTD package for each region.

2 Create Detector

Create a detector for each region.

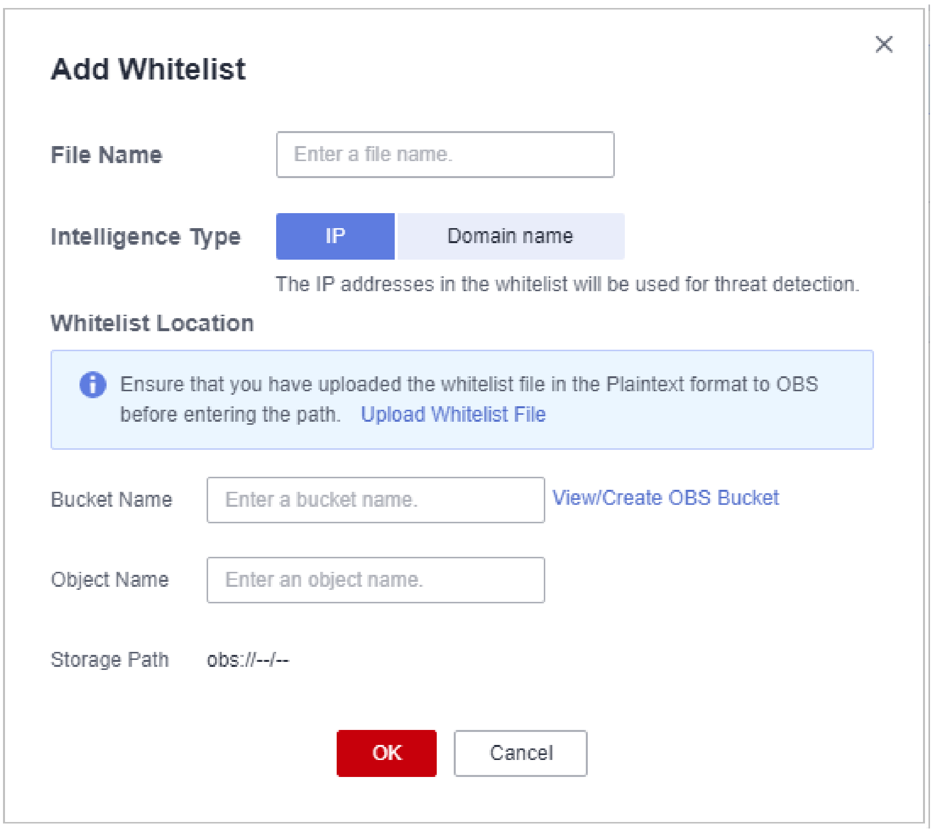
3 Store Threat Detection Results

Your threat detection results will be kept in MTD for 30 days by default. If you want to keep them for a long time, upload them to the OBS bucket.

Step 4 Choose **Settings** > **Threat Intelligence** in the left navigation pane.

Step 5 On the **Whitelist** tab, click **Add Whitelist**. The **Add Whitelist** dialog box is displayed.

Figure 7-2 Add a whitelist



Add Whitelist

File Name: Enter a file name.

Intelligence Type: IP | Domain name

The IP addresses in the whitelist will be used for threat detection.

Whitelist Location

Ensure that you have uploaded the whitelist file in the Plaintext format to OBS before entering the path. Upload Whitelist File

Bucket Name: Enter a bucket name. View/Create OBS Bucket

Object Name: Enter an object name.

Storage Path: obs://--/--

Table 7-1 Whitelist file parameters

Parameter	Description	Example Value
File Name	Name of the intelligence file to add	SecurityList

Parameter	Description	Example Value
Intelligence Type	Content type of the file to be uploaded from the OBS bucket to MTD ● **IP**: MTD will detect threats based on the IP addresses in the whitelist file. ● **Domain name**: MTD will detect threats based on the domain names in the whitelist file. MTD ignores log information that is associated with the IP addresses or domain names in the whitelist file.	IP
Bucket Name	Name of the OBS bucket where the file is located **NOTE** If no OBS bucket is available, click **View/ Create OBS Bucket**. For details, see **Creating a Bucket**.	obs-mtd-bejing4
Object Name	Name of the object in the bucket that stores the intelligence **NOTICE** The object name must contain the file name extension.	mtd-securitylist-ip.txt
Storage Path	Path of the OBS bucket storing the intelligence file	obs://obsmtd-beijing4/ mtd-securitylistip.txt

Step 6 Confirm the information and click **OK**. If the added file is displayed in the whitelist pane, the operation is successful.

----End

7.2 Deleting a Whitelist

This section describes how to delete an imported whitelist.

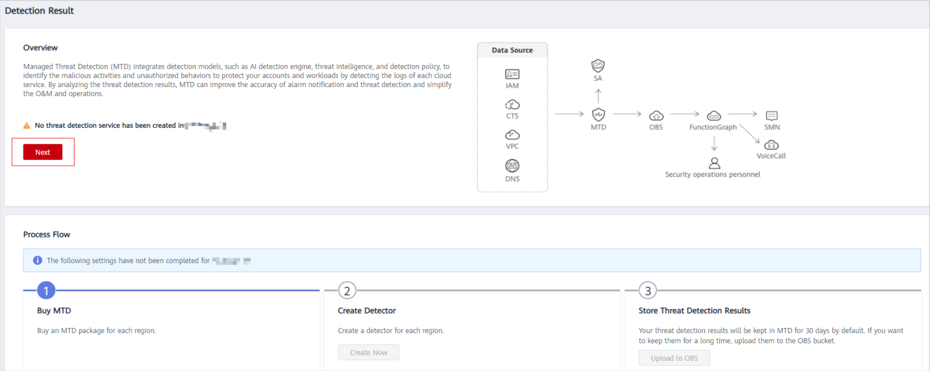
Procedure

Step 1 **Log in to the management console.**

Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the navigation pane on the left and choose **Security & Compliance** > **Managed Threat Detection**.

Figure 7-3 Home page of MTD



Detection Result

Overview

Managed Threat Detection (MTD) integrates detection models, such as AI detection engine, threat intelligence, and detection policy, to identify the malicious activities and unauthorized behaviors to protect your accounts and workloads by detecting the logs of each cloud service. By analyzing the threat detection results, MTD can improve the accuracy of alarm notification and threat detection and simplify the O&M and operations.

No threat detection service has been created in [redacted]

Process Flow

The following settings have not been completed for [redacted]

1 Buy MTD

Buy an MTD package for each region.

2 Create Detector

Create a detector for each region.

3 Store Threat Detection Results

Your threat detection results will be kept in MTD for 30 days by default. If you want to keep them for a long time, upload them to the OBS bucket.

Step 4 Choose **Settings** > **Threat Intelligence** in the left navigation pane.

Step 5 Click the **Whitelist** tab. In the **Operation** column of the whitelist file to be deleted, click **Delete**.

Step 6 In the displayed **Delete Whitelist** dialog box, click **Yes**.

----End

7.3 Viewing Whitelist Details

This section describes how to view the details about an imported whitelist, including the file name, object type, file format, and upload time.

Prerequisites

You have imported a whitelist. For details about how to import a whitelist, see **Importing a Whitelist**.

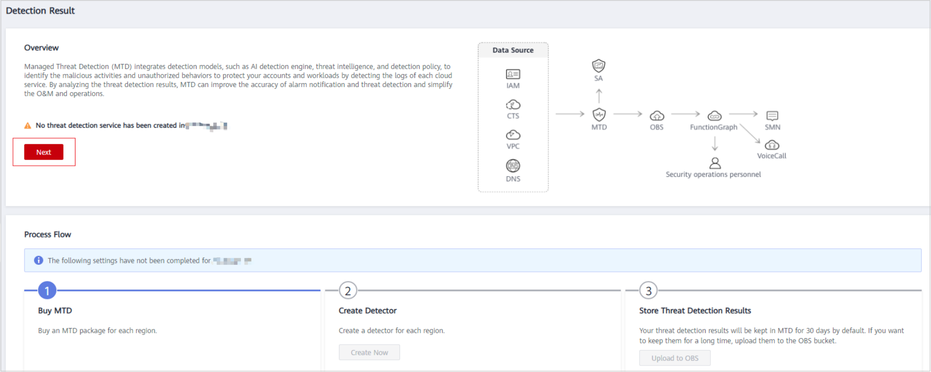
Procedure

Step 1 **Log in to the management console.**

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the navigation pane on the left and choose **Security & Compliance** > **Managed Threat Detection**.

Figure 7-4 Home page of MTD



Detection Result

Overview

Managed Threat Detection (MTD) integrates detection models, such as AI detection engine, threat intelligence, and detection policy, to identify the malicious activities and unauthorized behaviors to protect your accounts and workloads by detecting the logs of each cloud service. By analyzing the threat detection results, MTD can improve the accuracy of alarm notification and threat detection and simplify the O&M and operations.

No threat detection service has been created in [redacted]

Process Flow

The following settings have not been completed for [redacted]

1 Buy MTD

Buy an MTD package for each region.

2 Create Detector

Create a detector for each region.

3 Store Threat Detection Results

Your threat detection results will be kept in MTD for 30 days by default. If you want to keep them for a long time, upload them to the OBS bucket.

Step 4 Choose **Settings** > **Threat Intelligence** in the left navigation pane.

Step 5 Click the **Whitelist** tab and view details about the whitelist file.

Table 7-2 Whitelist file

Parameter	Description
File Name	Name of a whitelist file
Intelligence Type	Content type of the whitelist file, which can be **IP** or **domain name**.
Format	Format of the whitelist file. Currently, only plaintext files are supported. For details, see **How Do I Edit and Upload a Plaintext File to OBS?**
Uploaded	Time when a whitelist file is uploaded

----End

8 Synchronizing Detection Results

By default, MTD stores the detection results of the last 30 days. You can upload the data to an OBS bucket for long-term storage.

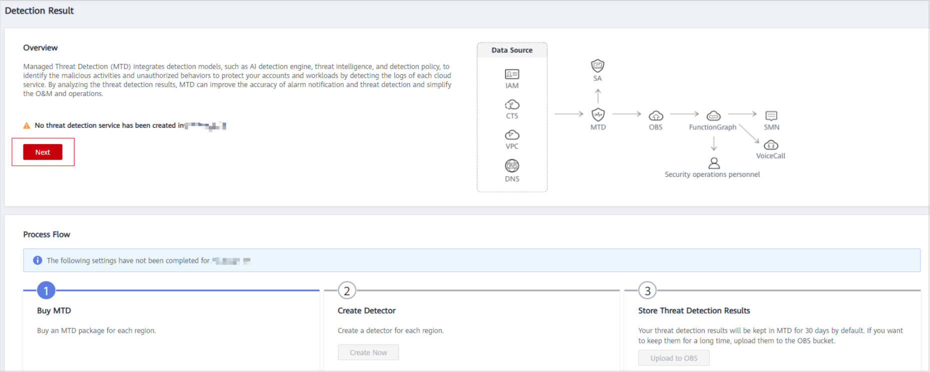
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the navigation pane on the left and choose **Security & Compliance** > **Managed Threat Detection**.

Figure 8-1 Home page of MTD



Detection Result

Overview

Managed Threat Detection (MTD) integrates detection models, such as AI detection engine, threat intelligence, and detection policy, to identify the malicious activities and unauthorized behaviors to protect your accounts and workloads by detecting the logs of each cloud service. By analyzing the threat detection results, MTD can improve the accuracy of alarm notification and threat detection and simplify the O&M and operations.

No threat detection service has been created in [redacted]

Next

Process Flow

The following settings have not been completed for [redacted]

1 Buy MTD

Buy an MTD package for each region.

2 Create Detector

Create a detector for each region.

Create Now

3 Store Threat Detection Results

Your threat detection results will be kept in MTD for 30 days by default. If you want to keep them for a long time, upload them to the OBS bucket.

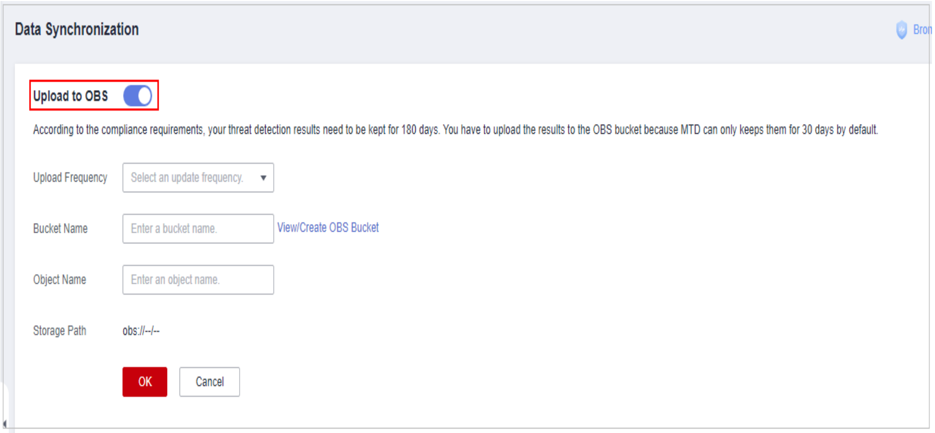
Upload to OBS

Step 4 Choose **Settings** > **Data Synchronization** in the left navigation pane.

Step 5 Store detection results.

- Click next to **Upload to OBS** and set required parameters. Figure 8-2 describes the parameters. The detection results will be uploaded to the configured OBS bucket according to the specified frequency.

Figure 8-2 Uploading detection results to the OBS bucket



Data Synchronization

Upload to OBS

According to the compliance requirements, your threat detection results need to be kept for 180 days. You have to upload the results to the OBS bucket because MTD can only keeps them for 30 days by default.

Upload Frequency: Select an update frequency.

Bucket Name: Enter a bucket name. View/Create OBS Bucket

Object Name: Enter an object name.

Storage Path: obs://--/--

Table 8-1 Parameter description

Parameter	Description	Example Value
Upload Frequency	Frequency of uploading real-time detection results to the OBS bucket – Every 30 minutes – Every hour (default) – Every 3 hours	Every 30 minutes
Bucket Name	Name of the OBS bucket that stores the detection results **NOTE** If no OBS bucket is available, click **View/Create OBS Bucket**. For details, see **Creating a Bucket**.	obs-mtd-beijing4
Object Name	Name of the object storing the detection results. You can enter the name of an existing object in the bucket or customize an object name. If the custom object name does not exist, an OBS bucket will be automatically created. You are advised to customize a name.	mtd-warning-data
Storage Path	Path of the OBS bucket storing the detection results	obs://obs-mtd-beijing4/mtd-warning-data

- Click ● next to **Upload to OBS** to disable the data synchronization. In the dialog box that is displayed, click **OK**. Detection results generated after the data synchronization is disabled will not be uploaded to the OBS bucket.

----End

9 Configuring Alarm Notifications

MTD can send you detected abnormal behaviors (such as potential malicious activities and unauthorized behaviors) via SMS messages or emails.

To enable alarm notifications, configure Simple Message Notification (SMN) interconnection on SA.

Prerequisites

- You have purchased MTD and created a threat detector by referring to **Step 1: Purchase MTD and Create a Detector**.
- You have purchased SA of the standard or professional edition.
- SMN has been enabled.

  NOTE

  SMN is a paid service. For pricing details, see **MTD Pricing Details**.

Procedure

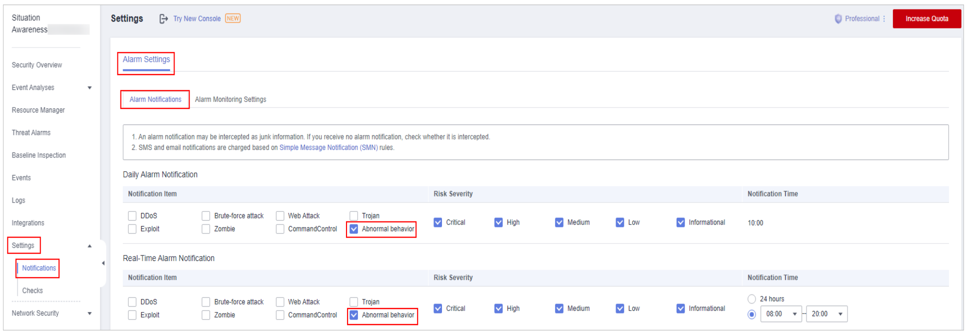
Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Situation Awareness**.

Step 3 In the left navigation pane, choose **Settings** > **Notifications**.

Step 4 On the **Alarm Notifications** tab page displayed, select **Abnormal behavior** under **Notification Item** in both the **Daily Alarm Notification** and **Real-Time Alarm Notification** areas, and select the risk severities that you are concerned about.

Figure 9-1 Alarm Notifications



1. An alarm notification may be intercepted as junk information. If you receive no alarm notification, check whether it is intercepted.
2. SMS and email notifications are charged based on Simple Message Notification (SMN) rules.

Daily Alarm Notification

Notification Item	Risk Severity	Notification Time
□ DDoS □ Brute-force attack □ Web Attack □ Trojan □ Exploit □ Zombie □ CommandControl ☑ Abnormal behavior	☑ Critical ☑ High ☑ Medium ☑ Low ☑ Informational	10:00

Real-Time Alarm Notification

Notification Item	Risk Severity	Notification Time
□ DDoS □ Brute-force attack □ Web Attack □ Trojan □ Exploit □ Zombie □ CommandControl ☑ Abnormal behavior	☑ Critical ☑ High ☑ Medium ☑ Low ☑ Informational	○ 24 hours ● 08:00 - 20:00

- **Daily Alarm Notification**

  Alarm notifications are sent to you at 10:00 every day.

  Daily Alarm Notification takes effect only when **Abnormal behavior** is selected for **Notification Item** and at least one risk severity is selected for **Risk Severity**.

- **Real-Time Alarm Notification**

  Real-time alarm notifications are sent on the hour after a threat alarm occurs.

  Real-Time Alarm Notification takes effect only when **Abnormal behavior** is selected for **Notification Item** and at least one risk severity is selected for **Risk Severity**.

  To avoid disturbing, you can select **24 hours** or a specified time period in the **Notification Time** column. Then you will receive notifications only in the specified period.

Step 5 Select an SMN notification topic.

- Select an existing topic from the drop-down list or click **View** to create a topic. For details about how to create an SMN topic, see **Creating a Topic**.
- You can add multiple subscriptions to a topic and select multiple subscription endpoints (such as SMS messages and emails). For details about how to add a subscription, see **Adding a Subscription**.

  NOTE

  Before selecting a topic, ensure that the subscription status of the topic is **Confirmed**. Otherwise, alarm notifications may not be received.

For details about topics and subscriptions, see *Simple Message Notification User Guide*.

Step 6 Click **Apply**.

----End

10 Permissions Management

10.1 Creating a User Group and Granting Permissions

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing MTD resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust an account or cloud service to perform efficient O&M on your MTD resources.

If your account does not need individual IAM users, you may skip over this section.

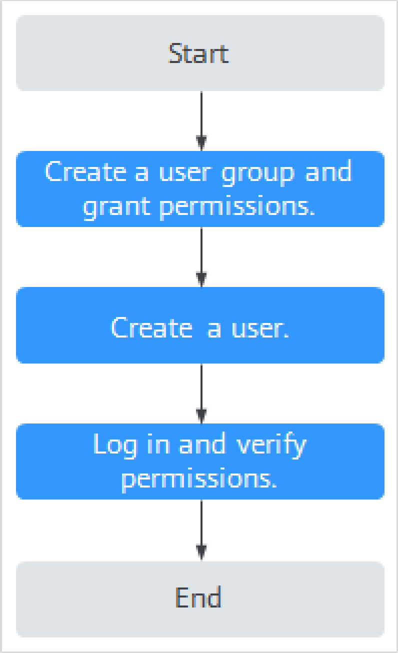
The following walks you through how to grant permissions. **Figure 10-1** shows the process.

Prerequisites

Learn about the permissions supported by MTD and choose policies or roles according to your requirements.

Authorization Process

Figure 10-1 Process for granting permissions


Start
Create a user group and grant permissions.
Create a user.
Log in and verify permissions.
End

1. **Create a user group and assign permissions**.

   Create a user group on the IAM console, and assign MTD permissions to the group.

2. **Create an IAM user and add it to the user group**.

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Create a custom policy**.

   Create a custom policy.

4. **Log in** and verify permissions.

   Log in to the MTD console by using the created user, and verify that the user only has permissions for MTD.

   Choose any other service in **Service List**. Assuming that the current permissions contain only **MTD Administrator**, you should get a message indicating that you have insufficient permissions.

A Change History

Date	Description
2022-12-02	This issue is the tenth official release. Updated **Step 1: Purchase MTD and Create a Detector**: MTD is supported in the **LA-Santiago** region.
2022-10-26	This issue is the ninth official release. Optimized **Step 1: Purchase MTD and Create a Detector**.
2022-09-08	This issue is the eighth official release. Added the **AF-Johannesburg** region.
2022-08-10	This issue is the seventh official release. Added the **LA-Sao Paulo** region.
2022-04-26	This issue is the sixth official release. Added the **CN-Hong Kong** region.
2022-03-28	This issue is the fifth official release. Added the **AP-Singapore** region.
2022-01-14	This issue is the fourth official release. Bronze and silver packages became available for AP-Bangkok and LA-MexicoCity regions. Added VPC threat detection and optimized the description. Added **Step 1: Purchase MTD and Create a Detector** and **Step 2: Create a Tracker** to **Usage**. Modified **Viewing Alarm Types**.
2021-12-13	This issue is the third official release. Modified **Viewing Alarm Types**.

Date	Description
2021-11-17	This issue is the second official release. ● Added the fine-grained authorization. For details, see **Creating a User Group and Granting Permissions**. ● Modified **Step 2: Create a Tracker**. ● Changed alarm type names to upper camel case.
2021-10-12	This issue is the first official release.